DCS | DEPARTMENT OF COMPUTER SCIENCE

UNIVERSITY OF LUXEMBOURG

FACULTY OF SCIENCE, TECHNOLOGY AND MEDICINE

Department of Computer Science

Activity Report 2021

DCS | DEPARTMENT OF COMPUTER SCIENCE

Department of Computer Science

Activity Report 2021

Keywords:
Activity Report, University of Luxembourg, Department of Computer Science, UL, DCS

Department of Computer Science
Activity Report 2021

Address:

Department of Computer Science (DCS)
University of Luxembourg
Faculty of Science, Technology and Communication
6, avenue de la Fonte
L-4364 Esch-sur-Alzette
Luxembourg

Administrative Contact:

Isabelle Glemot-Schroeder, Andrea Puech and Fabienne Schmitz
Email: dcs@uni.lu

Editor:	Christian Glodt
Release date:	7.2.2023
Note:	This report was created using LaTeX with a template based on previous work by Sebastien Varrette.

[

Preface]Preface

Dear reader,

This annual report synthesizes the progress and activities of the Department of Computer Science in 2021, including our research projects, teaching programs, organized events, awarded papers, visiting researchers and publications. We hope that you will find this report stimulating and inspiring. On behalf of the Department of Computer Science, we invite you to contact any one of us if you have any questions regarding the research we conduct in the DCS.

Best regards,

Sjouke Mauw
Nicolas Navet

Contents

Chapter 1

Mission

Our vision and mission phrase our long-term view on the relation between ICT and society and our role in shaping it.

DCS vision: A society in which technology and information are seamlessly integrated and in which advanced communicative, intelligent, and secure software systems provide functionality for the benefit of people and society.

DCS mission: To perform groundbreaking fundamental and applied research in computer science, commonly inspired by industrial and societal challenges.

In practice, a clear-cut distinction between fundamental and applied research is unfeasible or artificial. Very often fundamental and applied research interact within the same research project. DCS supports academic freedom and sees the pursuit of long-term scientific goals as an important task.

Computer science is a fast moving area. Agility is therefore crucial and consequently we have set up a structure that can deal with a dynamic environment. The multiple research areas and interests of DCS professors and researchers offer a broad expertise which is readily available. This allows to cope with the high expectations and challenging demands of the local societal and industrial players, but also to participate in new international research programs. This diversity and agility continue to provide a very solid base for visible and relevant research in a changing world.

Chapter 2

Executive Summary

The Department of Computer Science, also known as DCS (https://dcs.uni.lu), includes a staff of roughly 175 full-time equivalent members involved in both teaching and research activities.

Strategic development was one of the priorities of the department in 2021, leading to the definition of a number of positions to strengthen the department's research and teaching activities. We selected three professor profiles for submission to the rectorate, covering the fields of Machine Learning, Algorithmics, and Software Engineering. The recruitment process for two of these positions has already started.

Our research activities have led to many publications in top journals and conferences and have also led to significant outreach in the academic and social context. Our productivity has benefited strongly from the large number of externally funded projects executed in our department.

Following the sanitary developments in the country, the department introduced a hybrid mode for teaching and research in order to prepare for a gradual transition towards a more stable mode of operation.

The results of the university-wide teaching evaluation became available in 2021. The final report clearly shows that the Computer Science teaching cluster provides high quality teaching. We are very happy with this result, but quality management is of course a dynamic process. Therefore, the outcome of the evaluation will serve as a solid basis to further improve the teaching quality and optimise resource allocation through synergies between programmes.

In addition to the positive overall teaching evaluation, three of our educational programmes have been officially accredited by the German Accreditation, Certification and Quality Assurance Institute (ACQUIN). The three concerned programmes are: the Bachelor in Applied Information Technology (BINFO), the Bachelor in Applied Information Technology - Continuing Education Programme (BINFO-CEP), and the Master in Information and Computer Science (MICS).

In the near future we will aim at starting an accreditation procedure for our relatively new Bachelor in Computer Science (BICS). The management team of the BICS has been renewed recently. After the foundational work of the previous course director Nicolas Guelfi, it's now up to the new directors Martin Theobald and Alfredo Capozucca to model the BICS programme towards accreditation.

A consortium of European partners led by the University of Luxembourg has

been selected by the EuroHPC Joint Undertaking to design and implement the first pan-European High Performance Computing (HPC) pilot Master's programme. Our department was heavily involved in this initiative, which shows that our decade long investments in HPC facilities and research, led by Pascal Bouvry, has made us a major player in this field.

The scope of the lectures in the study programs includes topics covering fundamental aspects of computer science as well as practical ones. DCS is responsible for two bachelor programs, three master programs, a doctoral program, and a certificate Smart ICT for business innovation.

DCS is divided into 4 themes:

- Communicative Systems (https://comsys.uni.lu),
- Intelligent and Adaptive Systems (https://ilias.uni.lu),
- Algorithmics, Cryptography and Security (https://lacs.uni.lu).
- Advanced Software Systems (https://lassy.uni.lu).

Many of DCS faculty staff members, as well as their research groups, are involved in the three interdisciplinary research centers of the university, called SnT, C^2DH and LCSB, thus forging a tighter connection between the computer science department and these research centers.

DCS is cooperating in a large set of international as well as regional projects.

Head

- Sjouke Mauw, professor, Head of DCS

Vice head

- Nicolas Navet, professor, Vice Head of DCS and Departmental Head of Teaching

Academic Staff

- Alex Biryukov, professor
- Pascal Bouvry, professor
- Jean-Sébastien Coron, professor
- Thomas Engel, professor, head of COMSYS
- Dov Gabbay, guest professor
- Nicolas Guelfi, professor
- Pierre Kelsen, professor, head of LASSY
- Franck Leprévost, professor, head of LACS
- Sjouke Mauw, professor, head of DCS
- Yves Le Traon, professor
- Volker Müller, associate professor
- David Naccache, honorary professor
- Nicolas Navet, professor, vice head of DCS
- Henderik Proper, affiliated professor
- Peter Y. A. Ryan, professor
- Steffen Rothkugel, associate professor
- Jürgen Sachau, professor
- Christoph Schommer, associate professor
- Ulrich Sorger, professor

- Bernard Steenis, associate professor
- Martin Theobald, professor, head of ILIAS
- Leon van der Torre, professor
- Denis Zampunieris, professor

More information: https://dcs.uni.lu

Since DCS counts among its major achievements the continued support of the SnT, please look at the SnT 2021 annual report to get a complementary overview of DCS activities in the area of Security, Reliability and Trust.

Chapter 3

Research Areas

History

The University of Luxembourg (UL) was created in 2003 by merging several higher-education institutions, notably the Centre Universitaire (CU) (undergraduate level) and the Institut Supérieur de Technologie (IST) (industrial engineering). Accordingly, computer science was initially split between two faculties, resulting within the FDEF faculty in the Laboratory of Algorithmics, Cryptography and Systems (LACS) and the Applied Mathematics Service, and resulting within the FSTC faculty in the Applied Informatics department (DIA).

In 2003, DIA evolved into the Computer Science and Communications Department (CSC) including the Communicative Systems Lab (COMSYS), the Interdisciplinary Lab for Intelligent and Adaptive Systems (ILIAS), and the Lab of Advanced Software Systems (LASSY). In 2006, LACS and the Decision Support chair also joined CSC.

The creation of the academic master in 2005 offered a strategic opportunity to recruit new professors and strengthened the existing laboratories, as reflected by the increasing quantity and quality of publications, modulo variable funding opportunities. Since 2012, the doctoral program offers a systematic framework for doctoral education and research.

ICT being a key technology and national priority, local needs and collaboration with industry have played a major role in the development of CSC and of the associated professional bachelor and academic master. Many PhD/research projects have industrial partners. In 2009, CSC spun-off the Interdisciplinary Centre for Security, Reliability and Trust (SnT), whose purpose was to promote and efficiently handle industrial contracts and administrative challenges. Its theme followed the former UL-priority P1 on 'Security and Reliability of Information Technology'. CSC also collaborates with the LCSB and the C^2DH, and supports the computational science initiative.

Until 2020, the three faculties of the University of Luxembourg were formally subdivided into Research Units, one of which was CSC. From January 1st, 2020, a new substructuring of the faculties came into force, which formally led to the transformation of CSC into the Department of Computer Science (DCS). This provided a more independent role of the department in relation to teaching, which led to the creation of the position of Departmental Head of Teaching.

Research Program

The research program describes, given the relevant side conditions, on which research priorities we work to contribute to our mission. First of all, our research program identifies the four major research fields that we consider essential for achieving our more generic vision and mission (communication, artificial intelligence, software and security).

- Communication: computer systems become more connected,
- Artificial Intelligence: computer systems are used for more complex tasks,
- Security: we increasingly depend on evasive computer systems operating in a hostile environment,
- Software: computer systems become more complex.

Given side conditions like available expertise, interest, funding opportunities, national interests, expected impact, etc, the department has identified within each of the research fields a number of research priorities. This set of research priorities is intended as an evolving program.

At the moment of writing, an important line is 'Security, Trust, Reliability' that is going across labs, but which also forms the key initial target for the first interdisciplinary center, SnT. Moreover, new interdisciplinary research lines are also bundling and fostering together key forces of DCS, such as systems biomedicine (second interdisciplinary center), and FinTech (national priority). In the upcoming years we will further diversify and improve collaborations with other units, notably LCSB, the third interdisciplinary center on digital humanities called C^2DH, and the faculty priority on computational sciences. Moreover, we will invest in upcoming research areas of interest to such domains, such as machine learning.

The top-down cohesion is visible when DCS defines the research profiles for new positions, that strengthen or complete the topics covered by DCS according to this priority. Instead of a top-down overarching cohesion, we have underlying synergies/cohesion within and between labs/themes coming from shared research interests. Another dimension that should not be neglected is cohesion through the elaboration of consistent teaching programs.

Detailed Research Program

Communicative Systems

The Communicative Systems Laboratory (ComSys) performs state of the art research in digital communications. The rapidly growing demand for information exchange in people's daily lives requires technologies like ubiquitous and pervasive computing to meet the expectations of the information society and novel adaptive concepts tackling the continuing data challenges. Embracing the end-to-end arguments in system design, ComSys focuses on integrated research in the areas of Information Transfer and Communicative Systems. Information Transfer is concerned with information transmission over potentially complex channels and networks. Communicative Systems in turn are the com-

position of multiple distributed entities employing communication networks to collaboratively achieve a common goal. ComSys has strong technical and personal facilities to improve existing and develop new solutions in the following research topics:

- Secure communication protocols
- Network and systems security, 5G and beyond, IoT
- Collaborative socio-technical systems
- Virtual and augmented reality
- Vehicular communication (V2X, in car, C-ITS)
- Reliable distributed energy-systems
- Buffered PV Integration in Utility Grids
- Distributed anonymity and privacy
- Machine learning and adaptive networking
- Network science

ComSys consists of the following collaborating groups and labs performing research in complementary fields: the Collaborative and Socio-Technical Systems (COaST) group, the Digital Power Systems and Control Engineering (DPSCE) group, and the Security and Networking (SECAN) lab.

COaST focuses on distributed collaborative systems, complex networks and self-organisation, socio-technical modelling, educational technologies and mediated reality. The group operates the VR/AR Lab at the Department of Computer Science.

DPSCE is devoted to systems and control technology development and demonstration for reliable large-scale grid integration of solar-power systems, including conversion and storage and open for solar-fed structures for transport and thermal energy use.

SECAN-Lab conducts fundamental and applied research in computer networking, privacy, and security, namely in the areas of privacy by distribution, network and system security, SCADA and cyber security, IoT, vehicular communication and multimodal traffic management, and wireless networks and mobile security.

Intelligent and Adaptive Systems

The *Intelligent and Adaptive Systems Research Group* (ILIAS; see ilias.uni.lu) is home to 5 research groups and the associated scientific staff.

ILIAS investigates the theoretical foundations and algorithmic realisations of Intelligent Systems for complex problem solving and decision making in uncertain and dynamic environments. Our activities include interdisciplinary research that fits to the rapidly growing role of Artificial Intelligence and Data Science.

Collaboration with the interdisciplinary centres **C^{2}DH, LCSB** and **SnT** and the **Faculty of Law, Economics and Finance**, as well as with the **Faculty of Humanities, Education and Social Sciences**, participation in the **High Performance Computing** (HPC) facility and collaboration with the **Computational Sciences**

Initiative reflect the importance of ILIAS to Luxembourg's strategic priorities and future. In recent years, ILIAS has contributed to **Esch2022** with the AI&Art Pavilion and created a centre for knowledge exchange with the **Computational Creativity Hub**.

The research areas are orthogonal and adhere to the following disciplines:

- **Big Data** (Prof. Theobald): we investigate scalable architectures for the distributed indexing, querying and analysis of large volumes of data. Specific focus areas include information extraction, probabilistic and temporal database models as well as distributed graph and streaming engines.
- **Computational Interaction** (Prof. Leiva): The Computational Interaction group conducts research at the intersection of Human-Computer Interaction and Machine Learning, grounded on both foundational and practical principles via computational methods and data-driven models that can enable, support, explain, and improve any kind of user interaction.
- **Knowledge Discovery and Mining** (Prof. Schommer): the research areas include fundaments and applications of Machine Learning including Deep Learning, Sentiment Analysis, the use of Natural Language Processing for a ChatBot design, and Data/Text Mining.
- **Knowledge Representation and Reasoning** (Prof. van der Torre): we concern ourselves with normative reasoning in Multi-Agent Systems, particularly, Logics for Security and Compliance as well as Machine Ethics, Legal Knowledge Representation, Inference under Uncertainty and Inconsistency, Logic-based models for intelligent Agents and Robots, and Computational Choice.
- **Parallel Computing and Optimization** (Prof. Bouvry): the research on Parallel Computing and Optimisation Techniques, in particular how different species may co-evolve taking local decisions while ensuring global objectives, tackle large and difficult problems. The main application domains are Security, Trust and Reliability, Reliable Scheduling and Routing on new generations of networks, and Sustainable Development and Systems Biomedicine.

Our outreach activities are manifold, diverse, and interdisciplinary, and span collaborations with other departments. We regularly do presentations at schools and student fairs and cooperate with industry, if our expertise for the society is requested. We motivate young students to work with robots, for example within the AIRoboLab, and prepare them for new upcoming disciplines in Artificial Intelligence, Machine Learning, and beyond.

Algorithmics, Cryptology and Security

The proliferation of digital communication and the transition of social interactions into cyberspace have raised new concerns in terms of security and privacy. These issues are interdisciplinary in their essence, drawing on several fields: algorithmic number theory, cryptography, network security, signal processing, software engineering, legal issues, and many more. Our work on Information Security (LACS) focuses on:

- Cryptography:
  - Theoretical foundations: study of cryptographic primitives, cryptanalysis, sidechannel analysis, computational number theory.

  - Applications: digital currencies, public key encryption and signatures.
- System and network security: frameworks and tools to analyse security primitives, protocols and systems, the design of novel security protocols and other security controls, human aspects in security, privacy, e.g., in social networks, voting systems.
- Information security management: the development of a methodology and tools to assess system security and to select appropriate security controls.

Advanced Software and Systems

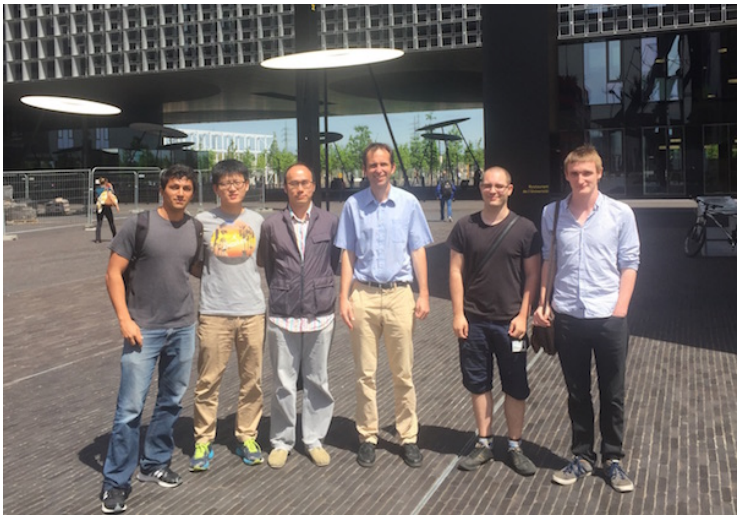
Our research on Advanced Software and Systems (LASSY) can be structured into five partly overlapping dimensions: modelling, methodology, computing paradigms, dependability (including security) and main application domains.

- Modelling: we investigate the foundations of model-driven engineering (MDE) as well as applications of MDE in fields as diverse as mobile computing, the Internet of things and the automotive sector, to name just a few.
- Methodology: a new integrated approach has been developed supported by an open-source tool that integrates theories, methods and tools from several software engineering subdisciplines such as requirements, testing and maintenance.
- Computing paradigms: the topic of pro-active computing, which is based on anticipating the user's needs, is investigated.
- Dependability: several research topics deal with dependability. In particular, innovative software testing and debugging techniques are studied. Another research topic within this dimension is the study of software intensive real-time systems, trying to improve their safety and lower their development costs. This line of investigation is supported by analytic and simulation models as well as by software engineering concepts such as domain-specific languages and system synthesis. Building trustable AI systems is a major challenge today, in particular concerning their correctness, security and ethics. This research aims at providing means to assess that the machine learning system works reliably and as expected, without deviating over time from its initial performances and being robust to adversarial attacks.
- Application domains: examples are automotive and aerospace embedded systems, enterprise architectures, cyberphysical systems, e-learning and pervasive healthcare systems.

Chapter 4

Research Groups

4.1 Applied Crypto Group (ACG)



Head of research group: Jean-Sebastien Coron

The Applied Crypto Group (ACG) is doing research in cryptography, within the Department of Computer Science (DCS) of the University of Luxembourg. ERC Advanced Grant CLOUDMAP (2018-2023).

Summary of the group's achievements in 2021

- 1 publication at top-tier conference in cryptography (Crypto 2021)

Three most interesting publications (or other achievements) in 2019.

- Jean-Sébastien Coron, Lorenzo Spignoli. Secure Wire Shuffling in the Probing Model. CRYPTO (3) 2021: 215-244

  We describe an efficient algorithm for side-channel countermeasure, with complexity quasi-linear in the number of probes, as opposed to quadratic.

- Jean-Sebastien Coron, Agnese Gini. Provably Solving the Hidden Subset Sum Problem via Statistical Learning. To appear at Journal of Mathematical Cryptology. Available at https://eprint.iacr.org/2021/1007.

  We describe an efficient algorithm for solving the hidden subset sum problem.

4.2 Applied Security and Information Assurance (APSIA)

Head of research group: Prof. Dr. Peter Y A Ryan

The APSIA group is part of the SnT and has strong connections to DCS and the LACS laboratory. The group specialises in the design and analysis of security and privacy primitives and protocols. Of particular interest: secure, verifiable voting protocols, authenticated key establishment protocols, both classical and quantum, including password-based and out of band-based. APSIA also has expertise in the socio-technical aspects of security and trust. The group recently established the APSIA Quantum Lab that specialises in the design and analysis of both quantum crypto and "post-quantum" (aka quantum resistant) and hybrid crypto.

Summary of the group's achievements in 2021

Despite the Covid situation the group still has a successful year. Notably APSIA hosted, virtually the ETAPS conference, with Ryan as Chair and Peter Roenne as Organisation Chair. This was deemed to have been highly successful by all despite the remote format. In particular the Steering Committee were so impressed that they have invited us to bid for the 2024 edition, which we all hope will be back to in person format (or maybe still hybrid).

1. Research projects:

   The group was highly successful in the CORE call and was awarded three new projects:

   (a) The FNR CORE Junior: Transition Of Low-entropy Authentication Ciphersuites Into A Post-quantum World (FuturePass)

   (b) The FNR/DFG Inter: Real-world Implementation And Human-centered Design Of Pake Technologies (ImPAKT)

   (c) New FNR CORE joint with the FinTrax group: Privacy-preserving Tokenisation Of Artworks (PABLO)

   (d) LuxQCI

2. Ryan gave lectures at the 20^{th} edition of the FOSAD school, at the LeADS

project training program in Pisa and a keynote to the ACM CYSARM conference.

3. Petra Sala defended her doctoral thesis and was nominated for the Excellent Doctoral Thesis Award.

4. Ehsan Estaji's PhD Colloquium presentation was awarded best PhD presentation at E-Vote-ID 2020.

5. Software: High-throughput and low-latency AVX-512 implementations of CSIDH at https://gitlab.uni.lu/APSIA/AVX-CSIDH. Unlinkable Updatable Hiding Databases and Privacy-Preserving Loyalty Programs: https://gitlab.uni.lu/APSIA/uuhd-ppls. A prototype of the secure voting scheme with transparent verification Selene (and by extension Hyperion) under development.

Courses taught: Information Security Basics, Security Modelling and Principles of Security Engineering. Dr Mestel proposed, and had accepted, a new MICS course on "Advanced Computing" to start summer semester 2021. Dr Zollinger taught a Java course and the group also contributed to the supervision and evaluation of several BSP projects in the BICS. The group continues to run the internal "breakfast" talks as well as organizing the bulk of the SRMs, the joint SATOSS/APSIA seminars.

Three most interesting publications in 2021

1. Xavier Boyen, Thomas Haines, Johannes Müller: Epoque: Practical End-to-End Verifiable Post-Quantum-Secure E-Voting. EuroS&P 2021: 272-291

2. Cheng, H., Fotiadis, G., Großschädl, J., Ryan, P. Y. A., & Rønne, P. B. (2021). Batching CSIDH Group Actions using AVX-512. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2021(4), 618–649. DOI: https://doi.org/10.46586/tches.v2021.i4.618-649

3. Tore Vincent Carstens, Ehsan Ebrahimi, Gelo Noel Tabia, Dominique Unruh: Relationships Between Quantum IND-CPA Notions. TCC (1) 2021: 240-272

4.3 BigData, Data Science & Databases (BigData)

Head of research group: Prof. Dr. Martin Theobald

The ”Big Data” group at the University of Luxembourg has been established in February 2017. The group is headed by Prof. Dr. Martin Theobald, who previously held positions at the Max-Planck-Institute in Saarbrücken, at the University of Antwerp, and at Ulm University. The group currently consists of three PhD students, Alessandro Temperoni, Mauro Dalle Lucca Tosi and Jingjing Xu, as well as four post-doctoral researchers, Dr. Maria Birykuv, Dr. Jeremie Dauphin, Dr. Maciej Skorski and Dr. Vinu Venugopal, and has thereby reached an unprecedented size of eight researchers in 2021. Two further PhD students, Valentina Leone and Aiste Gerybaite have jointly been supervised in the context of the “Joint International Doctoral (Ph.D.) Degree in Law, Science and Technology” in collaboration with the Universities of Bologna and Turin, of which Valentina Leone graduated in Summer 2021. Three of the above post-doctoral positions have been funded via an FNR-CORE project “BigText: A Distributed Graph Database for Large-Scale Text Analytics” as well as by a grant from the Luxembourgish Government (SMC & SCRIPT) to organize a new online course called “Elements of AI” which provided an online introduction about the broad area of Artificial Intelligence to more than 300 participants in Luxembourg. While the COVID19 crisis certainly also affected our group in the past year, our research activities continued to focus on the following main areas:

(1) Information Extraction & Knowledge-Base Construction

In collaboration with the Max-Planck-Institute in Saarbrücken, we investigate the full NLP pipeline for information extraction from natural-language sources, including probabilistic-graphical models for named-entity recognition and disambiguation, relation extraction, and knowledge-base construction. We intensified our collaboration in the context of an FNR-CORE project, which has been accepted for funding at the University of Luxembourg in 2017, and for which the Max-Planck-Institute kindly serves as external collaborator. The project has been concluded in November 2021.

(2) AIR – Distributed Dataflow Engine based on Asynchronous Iterative Routing

We continued to work on the development of our AIR asynchronous stream-processing engine over the past year, which applies a number of concepts from our previous works to the real-time processing of continuous data streams. Initial experiments demonstrate performance gains of a factor of up to 15 over the default platforms for processing these kinds of data streams, such as Apache Spark and Flink. Current research activities also include the investigation of Deep Learning techniques directly into this stream-processing platform. Several publications have meanwhile been achieved based on this architecture. Dr. Vinu Venugopal, the lead engineer of this project, has left our group in 2021 and accepted an offer as Assistant Professor at IIT Bangalore.

Our teaching activities focus on Databases, Data Science and Big Data Analytics:

We intensively employed current Big Data platforms, such as the Apache Hadoop/Pig/HIVE/HBase software stack, Spark, Giraph, GraphX, as well as

MongoDB, for teaching and application development. In particular Spark offers a wealth of constantly updated Machine Learning libraries (MLlib), which we applied to a variety of data collections in the context of different student projects. The group also actively contributes to the curricula for three study programs at the Departments of Computer Science (Bachelor & Master in Computer Science) as well as the Department of Mathematics (Master in Data Science) with four lectures per year. Two lectures in the areas of "Cloud Computing & NoSQL Databases" and "Big Data Analytics" are shared among the two Master programs.

Summary of the group's achievements in 2021

1. Organization of the "Elements of Artificial Intelligence" online course funded by SMC & SCRIPT with more than 300 participants from Luxembourg
2. Research publication: Maciej Skorski, Alessandro Temperoni, Martin Theobald: Revisiting Weight Initialization of Deep Neural Networks. ACML 2021: 1192-1207
3. Research collaborations: Max Planck Institute for Informatics (Saarbrücken), NVIDIA AI Technology Center (Mainz)
4. Completion of our FNR-CORE project "BigText: A Distributed Graph Database for Large-Scale Text Analytics"

4.4 Collaborative and Socio-Technical Systems (COaST)

Head of research group: Assoc.-Prof. Dr. Steffen Rothkugel

The COaST group focuses on distributed collaborative systems, complex networks and self-organization, socio-technical modelling, educational technologies, and mediated reality. The group operates the VR/AR Lab at the Department of Computer Science.

Summary of the group's achievements in 2021

At the end of 2021, the COaST group counted 5 members (1 professor, 1 senior researcher, 3 PhD candidates), and 9 publications.The group's research, particularly in the context of the ongoing projects ChronoPilot and DELICIOS, appeared in renowned academic publications and was presented at various international conferences and scientific events. After successfully deploying the Légionnaires Rallye, a digital treasure hunt accompanying the exhibition at the Musée Dräi Echelen, a follow-up collaboration between the VR/AR Lab and the C^{2}DH to promote the Esch2022 exhibition "Remixing Industrial Pasts – Constructing the Identity of the Minett" was launched. Members of the group were involved in the organisation of various international scientific events and conferences such as IEEE ACSOS, LIFELIKE, and ACM MMSys/MMVE. The COaST group's teaching activities comprised numerous lectures and seminars in the different bachelor and master programs (BINFO, BICS, MICS, BINFO-FC) offered by the University of Luxembourg.

Three most important publications in 2021

1. **Jean Botev, Knut Drewing, Heiko Hamann, Yara Khaluf, Pieter Simoens, Argiro Vatakis.** ChronoPilot – Modulating Time Perception. In Proc. 4th IEEE International Conference on Artificial Intelligence and Virtual Reality (AIVR 2021), pp.215-218, 2021.
   This paper introduces the fundamental concepts of the ChronoPilot project. Although time can be measured objectively, human time perception is remarkably subjective and influenced by cognitive states, individual motivations, and social factors. Mediated-reality approaches, such as virtual and augmented reality, have enormous potential for presenting the users with visual, auditory, and haptic stimulation patterns that directly or indirectly influence their subjective time also beyond individual scenarios, e.g., collaborative environments involving humans alone or humans and robots, where one group member's actions may affect other members' perception.

2. **Ningyuan Sun, Jean Botev.** Intelligent Autonomous Agents and Trust in Virtual Reality. In Computers in Human Behavior Reports (CHBR), Vol-

ume 4, October 2021.
From chatbots, over personal virtual assistants and medical decision-aiding systems, to self-driving or self-piloting systems, whether unbeknownst to the users or not, Intelligent Autonomous Agents (IAA) are increasingly integrated into many aspects of daily life. This article provides an overview of the numerous factors involved in establishing trust between users and IAA, spanning scientific disciplines as diverse as psychology, philosophy, sociology, computer science, and economics. Focusing on Virtual Reality (VR), different types of trust are discussed, and foundational factors are classified into three interrelated dimensions, offering a taxonomy that facilitates the study of trustful interaction and collaboration between users and IAA in VR settings.

3. **Jean Botev, Christian Grévisse, Steffen Rothkugel**. Student Response Systems in Remote Teaching. In Proc. 23rd International Conference on Human-Computer Interaction (HCI International 2021) / 8th International Conference on Learning and Collaboration Technologies (LCT 2021), pp.387-400, 2021.
Student response systems (SRS) are a popular and effective tool to promote active learning, improving student engagement and attention, motivation, and learning performance. Traditionally, SRS are designed for on-site settings. However, the safety measures regarding the recent COVID-19 pandemic resulted in remote teaching at an unprecedented scale, with online courses becoming the rule. This paper discusses the utilisation of interactive SRS in such remote settings for which they initially were not designed. Several empirical studies across different student groups indicate that, while common interactive features of videoconferencing tools, such as chat or polls, are well appreciated, there is still a need for dedicated SRS with game-based elements and feature sets beyond standard multiple-choice questions.

4.5 Computational Interaction (COIN)

Head of research group: Prof. Dr. Luis Leiva

Members: Dr. Mateusz Dubiel (September 2021), Mr. Kayhan Latifzadeh (January 2022) and Dr. Bereket Yilma (February 2022)

The COIN group was established in February 2021 and is part of the Interdisciplinary Lab for Intelligent and Adaptive Systems (ILIAS) of the Department of Computer Science. We use computational methods and data-driven models in user interaction research. In particular, our work addresses both fundamental and applied research activities in the following areas:

- Human-Computer Interaction, with a strong focus on computational user interface design and interactive input techniques.
- Machine Learning, in particular research with Deep Learning models.
- Information Retrieval, especially related to human factors and interfaces.
- Natural Language Processing, including text generation, phrase sampling, and text entry.

In addition, teaching and supervision of both Master of Science and Doctorate students rank high in the group's activities. We pursue a strong educational policy and actively combine state-of-the-art research with the training of next generation of high-class researchers. The group also engages in strong cooperative research activities by direct and peer-to-peer interactions with relevant industrial actors resulting in jointly funded PhD students and significant technology transfer.

Summary of achievements

In 2021 the group started with two members (1 professor and 1 postdoctoral researcher) and published 5 conference papers and 6 journal articles in top scientific venues in their respective fields. The group taught two new courses in the BiCS (both also shared with BINFO) and started preparing a new course for the recently created Master's in Data Science (MADS) and another new course for the MiCS. The group has attracted funding from the Horizon 2020 FET program of the European Union as well as internal funding from UniLu through the RISE program. The group has initiated collaborations with the Centre for Contemporary and Digital History (C2DH), NVIDIA AI Luxembourg, LuxProvide/MeluXina and Whonix. The group has participated in the organization of 10 scientific conferences and has reviewed articles for 5 journals. Prof. Luis Leiva participated as panel evaluator for the Spanish Ministry of Science and Education ("Juan de la Cierva" and "Ramón y Cajal" Fellowships) and was invited as guest lecturer at Aalto University (Finland) in the "CS-C3240: Machine Learning" and "ELEC-E7890: User Research" courses.

Research Projects

- BANANA: Brainsourcing for Affective Attention Estimation. Supported by EC Horizon 2020 FET, ERA-NET Cofund.
- Mouse Movements Anonymization. In collaboration with Whonix (formerly TorBOX).

Public Outreach

- Luis Leiva: Keynote talk at Elements of AI Luxembourg: "It's not what you do, but how you do it: Information retrieval with implicit interaction". https://www.elementsofai.lu/
- Luis Leiva: Keynote talk at Marie Skłodowska-Curie's multiToUCH Innovative Training Network: "Synthesizing Human-like Stroke Gestures with the Kinematic Theory". https://multitouch-itn.eu/events
- Luis Leiva: Contribution to Finland's AI Day 2021: "Mid-Air Gesture Recognition from Point Clouds". https://fcai.fi/ai-day-2021

Software

- MouseFaker: A web browser extension that anonymizes your mouse movements to prevent user profiling. https://github.com/luileito/mousefaker
- Design Maps: Interactive Exploration of Large-scale UI Datasets. https://gitlab.com/luileito/ui-clustering

Datasets

- Conversations with GUIs: Data-related queries posed by users from three different groups (end-users, designers, developers). https://osf.io/g25wh/
- How We Swipe: A Large-scale Shape-writing Dataset for Text Entry. https://osf.io/sj67f/

Three most interesting publications in 2021

1. Leiva, Luis A.; Arapakis, Ioannis; Iordanou, Costas. *My Mouse, My Rules: Privacy Issues of Behavioral User Profiling via Mouse Tracking.* Proceedings of ACM SIGIR Conference on Human Information Interaction and Retrieval (CHIIR), 2021.

   We show how straightforward is to capture behavioral data about the users at scale, by unobtrusively tracking their mouse cursor movements, and predict user's demographics information. Based on our results, we propose an adversarial method to mitigate user profiling techniques that make use of mouse cursor tracking.

2. Kumar T., Lokesh; Leiva, Luis A. *Attentive Sequence-to-Sequence Modeling of Stroke Gestures Articulation Performance.* IEEE Transactions on Human-Machine Systems 51(6), 2021.

   We introduce a deep learning model that estimates the velocity profile of any stroke gesture using only spatial information, providing thus a fine-grained estimation of the moment-by-moment behavior of the user's articulation performance.

3. Todi, Kashyap; Bailly, Gilles; Leiva, Luis A.; Oulasvirta, Antti. *Adapting User Interfaces with Model-based Reinforcement Learning.* Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI), 2021.

   We present a computational approach for adaptive user interfaces that can improve usability while avoiding unexpected changes that surprise the user or require relearning. Our approach simulates several possible sequences of adaptations and evaluates them using predictive models in HCI.

4.6 Critical Real-Time Embedded Systems (CRTES)

Head of research group: Prof. Nicolas Navet

The CRTES group, part of the LASSY laboratory, studies how to build provably safe mission-critical embedded systems in a time and cost-efficient manner. The focus of this group is on software-intensive real-time systems having strong dependability constraints and a significant societal impact such as transportation systems (road vehicles, aircrafts, etc).

Summary of the group's achievements in 2021

In 2021 the CRTES group comprised 5 members (1 professor, 1 research scientist, 3 PhD students) and had 6 peer-reviewed publications published or accepted. The group's members have taught 4 courses, both at the Bachelor (professional and academic) and Master levels, and supervised 6 Bachelor semester projects (BSP). Prof. Navet serves since July 2020 as deputy head of the department in charge of teaching. Group members were in the defense board of 3 PhD and Master thesis, 3 PhD supervisory committees and TPC member of 5 conferences.

Most of our work in 2021 was in the field of E/E architecture design and real-time communication networks, be it in the automotive or aerospace domains. Our work aims to further automate the design activities based on constraints and goals. We have been investigating for several years an approach rooted in computational thinking where system designers break down the general multi-dimensional design problem into smaller problems that algorithmic tools can solve in a near optimal way. In the continuity of the work performed in 2020, progresses were made this year in the development of deep-learning models, based on Graph Neural Networks (GNN), that speed-up by several orders of magnitude the performance evaluation of Ethernet networks with respect to simulation or mathematical analysis.

Three most interesting publications in 2021

1. **T.L. Mai, N. Navet, "Deep Learning to Predict the Feasibility of Priority-Based Ethernet Network Configurations", ACM Trans. on Cyber-Physical Systems (TCPS), Special Issue on Artificial Intelligence and Cyber-Physical Systems, Volume 5, Issue 4, October 2021.** This work presents what is, to the best of our knowledge, the first deep learning model for determining whether a real-time Ethernet network meets a set of timing constraints. The Graph Neural Network model developed possesses the ability to exploit relations among flows, links, and queues in the networks. Over 13 testing sets built from real E/E architectures, the GNN model has proven an ability to generalize beyond the training data that is significantly superior to existing algorithms. When using ensembles of 32 GNN models, the speedup factor over schedulability analysis still ranges from 77 to 1715 in our testing sets, which facilitates the implementation of DSE algorithms in the design of E/E architectures.

A follow-up paper improving the model with recent deep-learning techniques was presented at RTNS'2021 conference in April 2021.

2. **C. Mauclair (Airbus Helicopters), M. Gutiérrez, J. Migge, N. Navet, "Do we really need TSN in Next-Generation Helicopters? Insights from a Case-Study", Proc. 40th Digital Avionics Systems Conference (DASC 2021), San Antonio, Texas, October 3-7, 2021.** As Ethernet rapidly replaces legacy networks as the core high-speed network in helicopter's avionics and mission systems, we ask in this paper the question of the technical benefits of migrating to Ethernet Time-Sensitive-Networking (TSN). This work explores the use of TSN timing QoS mechanisms for helicopter's avionics and mission systems on a case-study representative of the communication requirements of next-generation systems. This study provides quantified insights into what can be expected from TSN in terms of timing, memory usage and extensibility.

3. **G. Bloom, J. Sherrill, Tingting Hu, Ivan Cibrario Berlotti, "Real-Time Systems Development with RTEMS and Multicore Processors", CRC Press, 534 pages, ISBN 9781351255790, Nov. 2020.** Multicore/manycore processors are increasing adopted in transportation systems, in particular in the centralized E/E architecture envisioned for automated and autonomous driving. RTOSes able to take full advantage of the hardware power become an essential component of such systems. This book summarizes our in-depth study of real-time system development for multicore systems, illustrated with the RTEMS operating system.

4.7 Critical and Extreme Security and Dependability (CritiX)

Head of research group: Prof. Dr. Marcus Völp

The CritiX lab (https://wwwen.uni.lu/snt/research/critix) investigates and develops paradigms and techniques for defeating extreme adversary power and sustaining perpetual and unattended operation. CritiX focusses on four scientific priorities: Resilience of cyber-physical system infrastructures and control; Internet and cloud infrastructures resilience; Security and dependability of embedded components; Data privacy and integrity in highly sensitive sectors. Our midterm development plan relies on investigating and publishing state-of-the-art advances along the following strategic objectives, which we deploy as research lines:

- Ultra-resilient minimal roots-of-trust and enclaves;
- Hybridisation aware distributed algorithms, models, and architectures;
- High-confidence vertical verification of mid-sized software;
- Privacy- and integrity-preserving decentralised data processing, namely in biomedical and in blockchain fields.

Summary of the group's achievements in 2021

In 2021, CritiX contributed to teaching in the Master of Information and Computer Science (MICS) through the course *Fault and Intrusion Tolerant Systems* as well as to the Doctoral School in Science and Engineering (DSCE) in the doctoral programme Computer Science and Computer Engineering (CSCE) through the courses *Distributed Real-Time and Embedded Systems* and *Resilient Computing*. CritiX has successfully kicked off the FNR Core project HERA on hypervisor-enforced radiation tolerance and ramped up its activities in the H2020 project ADMORPH and the FNR Core Inter Projects ByzRT and ThreatAdapt. In the context of the latter, we published the first Threat Adaptive BFT SMR algorithm at the 40th International Symposium on Reliable Distributed Systems (SRDS), as well as a result on Randomization as Mitigation of Directed Timing Inference Based Attacks on Time-Triggered Real-Time Systems with Task Replication in the LITES Transactions on Embedded Systems and in the context of ByzRT. This is complemented with seven further applications on genomic privacy, the role of formal verification in replicated systems, authentication in cellular-connected IoT devices, and a consensus-based defense mechanism against cyber-antisatellite weapons. The publication *Characterizing the Impact of Network Delay on Bitcoin Mining* at SRDS'21 marked the final piece of Dr. Tong Cao's thesis *ANALYZING THE PRIVACY AND SECURITY OF PROOF-OF-WORK CRYPTOCURRENCIES*, which he successfully defended in February, 2022. With the newly signed Partnership with Huawei on the Cyber Intrusion Resilience for Control Systems of Intelligent Vehicles, CritiX started the year with many interesting insights, including on the impact of injecting crash faults in autonomous driving stacks, such as Apollo, causing a several second stop of the car until perception could be re-established. Prof. Völp was appointed IEEE senior member and had the pleasure to serve as general chair and executive board member of the 33rd Euromicro Conference on Real-Time Systems.

4.8 CryptoLux

Head of research group: Professor Dr. Alex Biryukov

The CryptoLux group is part of LACS/DCS/FSTM as well as SnT and works on all aspects of symmetric cryptography, ranging from the design and analysis of primitives over efficient and secure implementation to the deployment in real-world systems and networks. CryptoLux is also pursuing research on digital currencies, smart contracts, and other emerging areas in information security, privacy, and anonymity. In 2021, the CryptoLux group consisted of 7 members: a full professor, a research and development specialist (shared), three postdoctoral researchers, and two Ph.D. students. Further information about the group is available at https://www.cryptolux.org.

In July 2021, the CryptoLux group successfully completed the FNR CORE project FinCrypt, which ran over a period of three years and brought many new insights into the security and scalability of blockchains and smart contracts, respectively. Furthermore, the FNR INTER project APLICA, whose goal is to research

both the theoretical and practical security of authenticated encryption algorithms, was started in January 2021. APLICA is a joint research project with the Workgroup for Symmetric Cryptography (Prof. Gregor Leander) of the Ruhr-University Bochum. Members of the CryptoLux group published a total of 12 formal papers in 2021 and served on the technical program committee of 11 major international journals and conferences in the area of cryptology and information security. The group taught various courses in the bachelor and master programs and supervised student projects.

Most interesting achievements in 2021

1. In 2021, the CryptoLux group made important new discoveries in White-Box Cryptography (WBC), a relatively young area of security research that combines methods of encryption and obfuscation with the goal of providing secure cryptographic implementations, even under the assumption that an attacker has full access to (and control over) the source code. More concretely, WBC uses mathematical techniques and transformations to blend together a cryptographic algorithm and a secret key in such a way that the latter can not be extracted from an implementation. WBC has many potential applications, ranging from mobile payments systems to digital rights management, but until now all (academic) approaches to build a secure white-box system have failed; in fact, most of them can be easily broken by standard side-channel techniques. The CryptoLux group proposed to apply shuffling, which is a well-known side-channel countermeasure, against linear and higher-degree algebraic attacks in the white-box setting and demonstrated its effectiveness using three white-box AES implementations as case study.

2. The authenticated encryption algorithm Schwaemm and the hash function Esch (both based on the SPARKLE permutation) made it into the final round of the LightWeight Cryptography (LWC) project of the U.S. National Institute of Standards and Technology (NIST), whose goal is to standardize new symmetric algorithms that are suitable for the Internet of Things. Initially, the LWC project received 57 candidate algorithms from cryptography research groups all over the world, of which 32 advanced to the second round after a careful evaluation. The second-round candidates were further scrutinized over a period of more than 1.5 years, taking into account both security and efficiency aspects. In March 2021, the NIST announced 10 candidates for the third and final round of evaluation, which is expected to take until the end of 2022. The CryptoLux group is actively developing highly-optimized implementations of the SPARKLE suite in hardware and software to give it a competitive edge in the final round and increase its chances of becoming a NIST standard.

3. Members of the CryptoLux group also contributed to another standardization effort of the NIST, namely the Post-Quantum Cryptography (PQC) project. It is widely believed that a large-scale quantum computer would

be able to break essentially any public-key cryptosystem used today, including RSA and ECC, which form the foundation of the Internet's public-key infrastructure. Research in PQC is concerned with the design, analysis and implementation of cryptographic algorithms that remain secure in the dawning era of quantum computing. SIKE (and abbreviation of Supersingular Isogeny Key Encapsulation) is a promising PQC cryptosystem that distinguishes itself from other candidates by relatively short key lengths. It was developed by a team of researchers and engineers from academia and industry (including companies like Amazon, IBM, and Microsoft). In order to motivate security analysis of SIKE, Microsoft published two challenges with reduced-size instances of SIKE and offered bounties for the first to provide a solution. The CryptoLux group solved the smaller instance of the SIKE challenge and, in this way, contributed to a better understanding of the real-world security of the SIKE cryptosystem.

Top-3 academic publications in 2021

1. Alex Biryukov and Aleksei Udovenko. Dummy Shuffling Against Algebraic Attacks in White-Box Implementations. Advances in Cryptology – EUROCRYPT 2021, vol. 12697 of Lecture Notes in Computer Science, pp. 219-248, Springer Verlag, 2021.

2. Kai Hu, Siwei Sun, Yosuke Todo, Meiqin Wang, and Qingju Wang. Massive Superpoly Recovery with Nested Monomial Predictions. Advances in Cryptology – ASIACRYPT 2021, vol. 13090 of Lecture Notes in Computer Science, pp. 392-421, Springer Verlag, 2021.

3. Si Gao, Johann Groszschaedl, Ben Marshall, Dan Page, Thinh Hung Pham, and Francesco Regazzoni. An Instruction Set Extension to Support Software-Based Masking. IACR Transactions on Cryptographic Hardware and Embedded Systems, vol. 2021, no. 4, pp. 283-325, Sept. 2021

4.9 Foundations of Model-Driven Engineering (FMDE)

Head of research group: Prof. Dr. Pierre Kelsen

FMDE is a small research group: besides the head (Pierre Kelsen) it comprised 2 members in 2021: Qin Ma (research scientist, half-time) and Christian Glodt (research and development specialist). The research group explores fundamental questions in the area of model-driven engineering but also interests itself in concrete applications (e.g., enterprise architecture and smart grids).

Summary of the group's achievements in 2021

In 2021 Pierre Kelsen elaborated and submitted a proposal for a Master in Secondary Education - Computer Science. The aim of this proposal was to complement the existing tracks in humanities and mathematics with a computer science track providing training for teachers in computer science for Luxembourgish secondary schools. Pierre Kelsen continued his teaching activities in the following courses: Algorithms 1 (Binfo), Programming Fundamentals 1 and Algorithms&Complexity (Bics), Formal Methods and Model-Driven Software Development (Mics).

In 2021, Qin Ma participated in the proposal writing for a joint List-UL PhD position with Prof. Kelsen and Prof. Erik, and the recruiting activities for this position. The proposed work was also published in a workshop affiliated to the 40th International Conference on Conceptual Modeling (publication number 1 below). In parallel, she continued her collaboration with colleagues from TU Eindhoven, the University of Duisburg-Essen, and the Mexico Autonomous Institute of Technology in the field of smart grids initiative valuation and validation and verification of domain specific modeling languages/methods. Qin Ma participated in the teaching of lab sessions for the "Programming Fundamentals 1" course in the BICS program, delivered the lectures on the FUDOMO framework and supervised FUDOMO projects in the model-driven software development course of the MICS program. Qin Ma was also a PC member of the 8th International Conference on Future Internet of Things and Cloud (FiCloud 2021).

Christian Glodt continued working on improving the web-based Fudomo tool. He also maintained and improved "Accord", the research information database of the DCS, as well as "MiCSM", the information management system of the Master in Computer Science programme. In addition, he participated in the organisation of lab sessions for the "Programming Fundamentals 1" course and supervised several BSP projects in the "Bachelor in Computer Science (BICS)".

Three most interesting publications in 2021

1. Feltus, C., Ma, Q., Proper, H. A., & Kelsen, P. (2021, October). Towards AI Assisted Domain Modeling. In International Conference on Conceptual Modeling (pp. 75-89). Springer, Cham.

2. Sybren de Kinderen, Monika Kaczmarek-Heß, Qin Ma, Iván S. Razo-Zapata: A Modeling Method in Support of Strategic Analysis in the Realm of Enterprise Modeling On the Example of Blockchain-Based Initiatives for the Electricity Sector. International Journal of Conceptual Modeling on Enterprise Modelling and Information Systems Architectures, 16: 2:1-2:36 (2021).

3. Qin Ma, Monika Kaczmarek-Heß, Sybren de Kinderen: Validation and Verification in Domain-Specific Modeling Method Engineering. In Proceedings of the 14th IFIP WG 8.1 Working Conference on Practice of Enterprise Modeling, PoEM 2021: 119-133.

4.10 Individual and Collective Reasoning Group (ICR)

Head of the research group: Prof. Dr. Leon van der Torre

ICR is a major research group of the Interdisciplinary Lab for Intelligent and Adaptive Systems. It locally collaborates among others with the Department of Philosophy, the Department of Law, the Center for Contemporary and Digital History, the SnT, and LIST. There are strong connections with leading research institutes worldwide, e.g. the Institute for Logic and Cognition at Zhejiang University (Hangzhou, China). ICR investigates the theoretical and computational modeling of high-level cognition for AIs. Specifically: Normative reasoning in multi-agent contexts, Logics for AI, Defeasible inference, including Formal and Computational Argumentation, Legal and Ethical AI, and Explainable AI. ICR has also been a driving force behind the AI Robolab of DCS.

Summary of the group's achievements in 2021

ICR hosted in 2021 18 researchers: 1 full professor, 2 research scientists, 5 postdocs, 1 R&D specialist, 7 UL and 2 LAST-JD PhD students.

In the context of the collaborative framework between the prestigious Zhejiang University and UL, the inauguration ceremony of the "Zhejiang University - University of Luxembourg Joint Lab on Advanced Intelligent Systems and Reasoning" (ZLAIRE), initiated by ICR and co-directed by Leon van der Torre, was held online on Dec. 6, honoured by the presence of the president of UL and the vice-president of ZJU. First results were the "First International Workshop on Logics for New-Generation Artificial Intelligence" (LNGAI 2021) and the creation of the "Journal of Logic and Computation" corner on "Logic for AI".

An important ICR/AIRobolab activity cluster, preparing our multi-faceted contribution to Esch2022, was centered on AI&Art. On the education side, Sana Nouzri co-offered a course on AI for artists and also organized an AI&Art seminar with talks by leading experts. On the outreach side, the AIRobolab collaborated with the Scienteens Lab and the Luxembourg Science Center to implement its Smart Photo Booth project, which aims at raising the public interest in and understanding of specific AI-areas. On the scientific side, ICR organized the AIFA workshop "AI and the Future of Art", which took place at the Computational Creativity Hub of UL in Belval, with more than 100 participants. AI&Art was also a focal point of the BENELUX reference conference for AI&ML, which ICR co-organized with LIST in Nov.

Amro Najjar was co-chair of the EXTRAAMAS@AAMAS workshop devoted to explainable AI (XAI). 2021 also saw the start of the INTER project EXPECTATION, concerned with Personalized XAI in the context of decentralized knowledge, and of the Industrial Partnership Block Grant COLLABORATION 21, together with CISCO and SCRIPT, where ICR is represented by Amro Najjar. Alexander Steen was co-proposer of the winning COST action "EuroProofNet". He is now assistant professor in Greifswald. Two new exciting research projects initiated by Reka Markovich were started in legal reasoning: "Deontic Logic for Epistemic Rights" (DELIGHT - FNR OPEN), and "Analytics for Decisions of Legal

Cases" (ADELE - H2020 Justice Program). She became also one of 4 members of the international steering committee of the "Foundation for Legal Knowledge Based Systems" conference (JURIX). Together with Leon van der Torre, a course "Introduction to Deontic Logic and Its Application" was offered at ESSLLI 2020/2021. In addition ICR continued its interdisciplinary educational engagement with the MSCA ITN program LAST-JD-RIoE (Joint Int. Doctoral Degree in Law, Science, and Technology - Rights of the Internet of Everything).

Most important publications in 2021

1. **L. Yu, D. Chen, L. Qiao, Y. Shen, L. van der Torre.** *A Principle-based Analysis of Abstract Agent Argumentation Semantics.* Proc. of KR 2021, pp. 629-639. ("The first systematic study of this kind")
2. **R. Markovich and O. Roy.** *A Logical Analysis of Freedom of Thought.* Deontic Logic and Normative Systems, Proc. of DEON 2020/21, F. Liu et al. (eds.), College Publications, 2021, pp. 245-260.
3. **A. Najjar et al.** *Real-time multi-agent systems: rationality, formal model, and empirical results.* Autonomous Agents and Multi-Agent Systems, 35(1), pp. 1-37.

4.11 Knowledge Discovery and Mining (MINE)

Head of research group: Prof. Christoph Schommer

Description: We take an interdisciplinary approach to research and act as a bridge and research facilitator for the field of Artificial Intelligence and in particular in the application of Machine Learning and Natural Language Processing. We collaborate with colleagues from all faculties as well as with colleagues from C2DH, Scienteens Lab, and our industry partners such as Zortify, LuxAI, Magrid, RTL, IEE, and Post.

Activities: Highlights of the past year were the preparation and various activities in connection with the AI&Art Pavilion for Esch 2022, the establishment of the CCH Centre and the collaboration on the AI RoboLab, numerous public outreach activities for the EU, newspapers and radio, the organisation of the AI4Health Lecture Series, Prof. Schommer's invited teaching at the FU Berlin and the Singapore University of Technology and Design, public speeches in Luxembourg and Brussels, as well as our support in the establishment of the newly founded Centre of Ethics in Digitalization. 10 academic courses were held; 7 supervised master's students and 2 supervised doctoral students defended their dissertation projects. In addition, Prof Schommer was involved in the defence of other dissertation projects (also in London and Bologna) and in various project submissions, of which the following were accepted: Remedis (FNR Jump; Prof Schommer, MSc Daniel Karpati), SmartPhotoBooth (FNR PSP; Prof Schommer; Msc Daniel Karpati), BeCoS (FNR PSP; Dr Elisabeth John, Scienteens Lab), Collaboration21 (FNR IGBP; Prof Koenig), D4H (PRIDE; Prof Andreas Fickers). Unfortunately, the projects DETECT (FNR Bridges; Prof. Schom-

mer, with EastNets S.A.) and DPLERN (FNR CORE; Prof. Schommer, Dr. Vanhove, Massachusetts General Hospital) were not accepted, but a resubmission is planned for 2022. The research group also participated in the organisation of the BNAIC/Benelux conference; the STRIPS research project (with the Prof. Gilles and Prof. Purschke, both Department of Linguistics) was successfully completed.

Publications:

- Fagherazzi, G., Fischer, A., Muhannad, I., Despotovic, V.: Voice for Health: The Use of Vocal Biomarkers from Research to Clinical Practice. In: Digital Biomarkers (2021), 5(1), 78-88
- Leiva, L. A., Pruski, C., Markovich, R., Najjar, A., & Schommer, C. (Eds.). (2021). Proceedings of BNAIC/BeneLearn 2021. Luxembourg: BnL.
- Peric, Z., Denic, B., Despotovic, V. Algorithm based on 2bit adaptive delta modulation and fractional linear prediction for Gaussian source coding. In: IET Signal Processing (2021), 15(6), 410-423.
- Peric, Zoran; Savic, Milan; Simic, Nikola, Despotovic, V. Design of a 2-Bit Neural Network Quantizer for Laplacian Source. In: Entropy (2021), 23(8), 933.
- Schommer, C. About AI and Arts. Paper presented at AI and Arts Workshop, Belval-Université, Luxembourg.
- Schommer, C.. Future living with AI and IA. Paper presented at 33rd Benelux Conference on Artificial Intelligence (BNAIC), Belval-Université, Luxembourg.
- Schommer, C.. The Future of Living with AI. Paper presented at International Symposium "The Future of Living"; https://www.bozar.be/en/calendar/symposium-future-living, Brussels, Belgium.
- Schommer, C. Getting Creative - AI and Arts. Paper presented at AIFA - Artificial Intelligence and the Future of Arts 2021, CCH, UL, Luxembourg.
- Schommer, C. Ist die Künstliche Intelligenz für oder gegen die Menschheit? Paper presented at Les cylcles de l'UNESCO, Bibliothèque Nationale du Luxembourg, Kirchberg, Luxembourg.
- Schommer, C., Sauter, T., Pang, J., Satagopam, V., Despotovic, V., & Goncalves, J. Proceedings of the AI4Health Lecture Series (2021). Paper presented at AI4Health Lectures Series (2021), Campus Belval, University of Luxembourg, Luxembourg.

4.12 Methods and Tools for Software Engineering, DevOps and Artificial Intelligence (MESSIR)

Head of research group: Prof. Dr. Nicolas Guelfi

General information

The MESSIR group is part of the LASSY laboratory. Our group focuses on methods and tools for Software Engineering, DevOps and Artificial Intelligence in order to improve the quality of IT systems. Our methods and tools are developed using sound scientific basis. We develop open source tools to support our languages and to allow for research collaboration or technology transfer with industrial
partners. Our aim is to offer novel and efficient approaches for the engineers to ensure system development and deployment. Specific fields are currently under important development:

- software engineering methods and tools for neural networks engineering
- software engineering methods and tools for ecological cyber physical systems
- DevOps and Agile methods

Highlights in 2021

The group has played a key role in the management of, and teaching support for the first and second-year students of the recently opened Bachelor in Computer Science (BiCS) at the University of Luxembourg. In this context, the BiCS Management Tool (BMT) has been improved by the team to ease the management of the projects students perform every semester along with either staff of the university or external collaborators.

Another highlight was the successful completion of the second BiCS Promotion The development of a new bachelor has been led by the Messir group since 2015. After six years of successful development the BiCS represents 110 highly skilled students that will contribute to the future of computer science.

Last but not least, the BicsLab, a R&D student laboratory has been setup with the supervision of a number of student semester projects around software, greenware, and senseware; industrial partnership agreements have been signed resulting in projects companies (Pall Center, Ahrs, Goodyear, ...).

Three most interesting publications (or other achievements) in 2020

1. Ries Benoit, Guelfi Nicolas, Jahic Benjamin. "An MDE Method for Improving Deep Learning Dataset Requirements Engineering using Alloy and UML". February 2021. This paper introduces a novel model-driven software engineering approach focused on the requirements engineering of datasets for deep-learning based-systems. Thanks to this approach the software analysts are able to specify the requirements for datasets, then

requirements properties may be validated or invalidated thanks to the formalization in Alloy.

2. Management of the COVID crisis in the BiCS program and transition of the BiCS management and data to the new academic team. Including, among others, the development of a new lightweight software for the management of the BiCS Semester Projects (BSP) with student jobs.

3. Submission and acceptance of the research project for the sabbatical of Prof. N.Guelfi. The aim and motivation of this sabbatical is to extend his research domain to the learning domain and the artificial intelligence mainly related to deep learning with neurons in order to set the basis for a novel methodological approach for the engineering of intelligent systems.

4.13 Parallel Computing and Optimisation Group (PCOG)

Head of research group: Prof. Dr. Pascal Bouvry

Deputy Head of research group: Dr. Grégoire Danoy

Solving today's scientific and real-world problems not only requires high performance computing (HPC), but also new generations of Artificial Intelligence algorithms. PCOG conducts research in parallel computing, search and optimisation techniques, to provide efficient, scalable and robust solutions to state-of-the-art, large-scale discrete/combinatorial problems. The main application domains are security, trust and reliability; reliable scheduling and routing on new generations of networks; sustainable development and systems biomedicine; unmanned autonomous vehicles (UAV), smart cities. In addition, PCOG is at the heart of the digital strategy of the university by managing the High Performance Computing (HPC) developments and the associated facility since 2007. Detailed information about the group is available at http://pcog.uni.lu/.

Summary of the group's achievements in 2021

At the end of 2021, PCOG counted 22 members (1 professor, 4 research scientists, 1 partnership development officer, 8 postdocs, 7 PhD students, 1 R&D Specialist) and produced a total of 14 peer-reviewed publications (5 journal articles, and 9 conference articles) and 3 technical reports. In 2021, two PhD students defended their thesis entitled « Social Network Analysis for Digital Humanities » and « A Distributed Unmanned Aerial Vehicles Traffic Management System » respectively.

PCOG has run five research projects in 2021.The second ILNAS/ANEC Research Programme (2021-2024) which focuses on three new pillars (Aerospace, ICT and Construction), the HUNTED (Heterogeneous multi-swarms of UNmanned autonomous systEms for mission Deployment) project co-funded by the Office of Naval Research Global (ONRG – US Navy) and US Air Force, the FNR CORE

ADARS (Automating the Design of Autonomous Robot Swarms), the STARE-BEI STAIRS (A Sustainable and Trustworthy AI Recommitment System) project (2021) funded by the European Investment Bank (EIB) and the H2020 PRACE-6IP, the 6th implementation phase of the « Partnership for Advanced Computing » which is a permanent pan-European High Performance Computing service. PCOG was also leading one technology transfer project funded by the FNR Proof-of-Concept program, SIMMS (Swarms of Intelligent Missions systeMS).

PCOG acquired two new research projects in 2021: (1) FNR CORE COMOC (A Concurrent Model of Computation for Trustworthy GPU Programming, 2021-2024) ; (2) FNR CORE CBD (Cloud-based Computational Decision By Leveraging Artificial Ultra Intelligence, 2021-2024). PCOG also initiated a new research partnership between SnT and Luxprovide, the national high-performance computing center of Luxembourg. In addition, it was selected by the EuroHPC Joint Undertaking to design and implement the first pan-European Master's programme in HPC, leading a consortium of European universities, research/supercomputing centres and industrial partners.

PCOG also manages the new Master in Technopreneurship (MTECH), in partnership with ILNAS (Luxembourg's standards body), the Luxembourg Lifelong Learning Center (LLLC) and the Chambre des Salariés Luxembourg (CSL), which first promotion started in February 2021.

PCOG team members taught in several Bachelor, Master and PhD programs (BICS, BINFO, MICS, MTECH, Doctoral School in Computer Science), and organized the HPC workshop.

PCOG is in charge of the management of the High-Performance Computing (HPC) facility of the University, those developments as well as the associated expert IT team managing and supporting it, are led by Pascal Bouvry who is acting as "Chargé de Mission auprès du Recteur", and Sébastien Varrette who is managing the HPC system administration team. Since June 2020, Pascal Bouvry has been appointed as co-CEO of the National HPC centre, LuxProvide. The University of Luxembourg, Luxprovide and Luxinnovation also joined forces to become the national HPC competence centre as part of the EURO-HPC network.

Three high impact publications in 2021

1. **Nader S. Labib, Matthias R. Brust, Grégoire Danoy and Pascal Bouvry:** The Rise of Drones in Internet of Things: A Survey on the Evolution, Prospects and Challenges of Unmanned Aerial Vehicles. IEEE Access 9: 115466-115487 (2021).

2. **E. Kieffer, F. Pinel, T. Meyer, G. Gloukoviezoff, H. Lucius and P. Bouvry,** "Evolutionary Learning of Private Equity Recommitment Strategies," 2021 IEEE Symposium Series on Computational Intelligence (SSCI), 2021, pp. 1-8, doi: 10.1109/SSCI50451.2021.9660088.

3. **M.R. Brust, G. Danoy, D.H. Stolfi and P. Bouvry.** Swarm-based counter UAV defense system.Discov Internet Things 1, 2 (2021). https://doi.org/10.1007/s43926-021-00002-x

4.14 Proactive Computing

Head of research group: Prof. Dr. Denis Zampuniéris

This small group, counting 3 members (1 professor, 1 PhD student, 1 technical assistant) is part of the LASSY research laboratory. It focuses on formalizing and implementing proactive computing principles into the development of innovative and autonomic software systems for multiple real-world application fields. The proactive computing paradigm provides us with a new way to make the multitude of computing systems, devices and sensors spread through our modern environment, work for/pro the human beings and be active on our behalf.

Summary of the group's achievements in 2021

Apart from their regular research work and their participation in IT teaching programmes offered by our Faculty, the group welcomed and supervised several students (local or from universities abroad) in internship for their Bachelor or Master thesis.

4.15 Security and Networking Lab (SECAN-Lab)

Head of research group: Prof. Dr. Thomas Engel

SECAN-Lab addresses both fundamental and applied research activities in computer networking and security. The group's main research activities cover the following areas:

- Privacy-enhancing technologies (PETs), privacy by distribution, privacy-preserving cryptographic protocols, protection against network traffic analysis
- V2X and C-V2X communications
- Network and systems security including machine learning for big data analysis, malware detection and IT forensics
- SCADA and cyber security
- Wireless networks and mobile security
- Vehicular and multimodal traffic management based on V2X communications
- Automotive Ethernet
- Internet of Things, Quality of Service, IPv6 integration
- 5G key technologies (Software Defined Networks, Network Function Virtualization, Multi-Access Edge Computing)

Headed by Prof. Dr. Thomas Engel, SECAN-Lab is composed of a balanced team of established high-level research associates, doctoral candidates and research management professionals spanning across a variety of fields, and with many contributing with a significant industry expertise gained at both national and international levels.

Summary of the group's achievements in 2021

In 2021, SECAN-Lab conducted research in the scope of 8 publicly and industry-funded projects. In particular, we were able to win two new projects during this year, 5G-INSIGHT and SETICA, allowing us to consolidate our research on communication security in automotive networks. The INTER project 5G-INSIGHT, funded by ANR and FNR, focusses on network slicing as the key technology of an agile V2X use-case deployment to ensure network flow isolation, resource assignment, and network scalability. Building on key 5G technologies (SDN, NFV) and machine learning algorithms (federated and deep learning), 5G-INSIGHT aims at (a) proposing new techniques for road and network traffic prediction, thus allowing the early detection of intrusions and anomalies within 5G vehicular slices, (b) enforcing security-by design and privacy-preserving slicing policies for attack mitigation and personal data anonymization respectively, and (c) developing resource orchestration and management across multiple potential providers using federated slicing. All this is done while considering the specific but very sensitive case of cross-border areas (i.e., the France-Luxembourg border-crossing case). The FNR BRIDGES project SETICA, with our collaboration partner Honda, considers next-generation in-vehicle communication systems facilitating future functionalities and services, such as autonomous driving, connected cars, and ADAS functions, which will require all of high bandwidth, precise timing, and security. The goal of SETICA is to develop an automotive Time Sensitive Networking (TSN) profile which includes answering challenging research questions and a thorough evaluation. For the latter a realistic security-enabled TSN testbed will be constructed.

We successfully completed the EU projects HiedTec, 5G-MOBIX, 5G-DRIVE, and CITIES2030. HiedTec developed concepts for adapting the educational systems to the digital generation and created centers for innovative education technology. 5G-MOBIX focussed on the worldwide 5G Fora and verticals in the V2X ecosystem to generate some genuine exchange among the leaders of these ecosystems. The project has been very successful at creating, initiating, and attracting worldwide 5G Fora executives to work together since 2018. 5G-DRIVE aimed at testing and validating the interoperability between EU & China 5G networks for enhanced Mobile Broadband (eMBB) and vehicle-to-everything communications (V2X) scenarios. The project has delivered exceptional results with significant immediate or potential impact including an SDN-based location privacy protection framework for 5G vehicular networks. With more than 40 involved partners from around Europe, CITIES2030 goal was to improve the resilience and sustainability of the urban food supply chain. SECAN-Lab worked on advancing the current state-of-the-art research in causal machine learning and conformal learning and studied the relationship between nonconformity metrics and the efficiency of conformal classifiers.

In terms of academic contributions, SECAN-Lab has also been very successful in 2021 with 20 publications in international workshops, conferences, journals, and books. Team members were involved as (Co-)Chairs or program committee members in 19 international conferences and workshops, including the Privacy Enhancing Technologies Symposium (PETS), the IFIP Summer School on Privacy and Identity Management, the IEEE Global Communications Conference

(GLOBECOM), and the IEEE Vehicular Networking Conference (VNC).

Regarding our educational mission, team members have taught extensively within the University of Luxembourg's BSc and MSc programs and supervised numerous bachelor and master student projects and theses.

Three most interesting publications in 2021

1. Alessio Buscemi, Ion Turcanu, German Castignani, Romain Crunelle, Thomas Engel: CANMatch: A Fully Automated Tool for CAN Bus Reverse Engineering Based on Frame Matching. IEEE Trans. Veh. Technol. 70(12): 12358-12373 (2021).

   Controller Area Network (CAN) is the most frequently used in-vehicle communication system in the automotive industry today. The communication inside the CAN bus is typically encoded using proprietary formats in order to prevent easy access to the information exchanged on the

   bus. However, it is still possible to decode this information through reverse engineering, performed either manually or via automated tools. Existing automated CAN bus reverse engineering methods are still time-consuming and require some manual effort, i.e., to inject diagnostic messages in order to trigger specific responses. In this paper, we propose CANMatch – a fully automated CAN bus reverse engineering framework that does not require any manual effort and significantly decreases the execution time by exploiting the reuse of CAN frames across different vehicle models. We evaluate the proposed solution on a dataset of CAN logs, or traces, related to 479 vehicles from 29 different automotive manufacturers, demonstrating its improved performance with respect to the state of the art.

2. Abdelwahab Boualouache, Hichem Sedjelmaci, Thomas Engel:

   Consortium Blockchain for Cooperative Location Privacy Preservation in 5G-Enabled Vehicular Fog Computing. IEEE Trans. Veh. Technol. 70(7): 7087-7102 (2021).

   Privacy is a key requirement for connected vehicles. Cooperation between vehicles is mandatory for achieving location privacy preservation. However, non-cooperative vehicles can be a big issue to achieve this objective. To this end, we propose a novel monetary incentive scheme for cooperative location privacy preservation in 5G-enabled Vehicular Fog Computing. This scheme leverages a consortium blockchain-enabled fog layer and smart contracts to ensure a trusted and secure cooperative Pseudonym Changing Processes (PCPs). We also propose optimized smart contracts to reduce the monetary costs of vehicles while providing more location privacy preservation. Moreover, a resilient and lightweight Utility-based Delegated Byzantine Fault Tolerance (U-DBFT) consensus protocol is proposed to ensure fast and reliable block mining and validation. The performance analysis shows that our scheme has effective incentive techniques to stimulate non-cooperative vehicles and provides

optimal monetary cost management and secure, private, fast validation of blocks.

3. Christiane Kuhn, Dennis Hofheinz, Andy Rupp, Thorsten Strufe:

   Onion Routing with Replies. ASIACRYPT (2) 2021: 573-604.

   Onion routing (OR) protocols are a crucial tool for providing anonymous internet communication. An OR protocol enables a user to anonymously send requests to a server. A fundamental problem of OR protocols is how to deal with replies: ideally, we would want the server to be able to send a reply back to the anonymous user without knowing or disclosing the user's identity. Existing OR protocols do allow for such replies, but do not provably protect the payload (i.e., message) of replies against manipulation. Kuhn et al. (IEEE S&P 2020) show that such manipulations can in fact be leveraged to break anonymity of the whole protocol. In this work, we close this gap and provide the first framework and protocols for OR with protected replies. We define security in the sense of an ideal functionality in the universal composability model, and provide corresponding (less complex) game-based security notions for the individual properties. We also provide two secure instantiations of our framework: one based on updatable encryption, and one based on succinct non-interactive arguments (SNARGs) to authenticate payloads both in requests and replies. In both cases, our central technical handle is an implicit authentication of the transmitted payload data, as opposed to an explicit, but insufficient authentication (with MACs) in previous solutions. Our results exhibit a new and surprising application of updatable encryption outside of long-term data storage.

4.16 Security and Trust of Software Systems (SaToSS)

Head of research group: Prof. Sjouke Mauw

Since its establishment in 2007, the SaToSS group has been focusing on formalizing and applying formal reasoning to real-world security problems. The group carries out research on a variety of topics such as:

- security protocols (e.g., e-voting, distance-bounding, blockchain),
- attack trees and security analysis,
- privacy (e.g., location privacy, privacy in social networks and machine learning),
- modelling and analysis of biological systems,
- process algebra and model checking,
- deep learning,
- malware detection and mobile systems security,
- security of cyber-physical socio-technical systems,
- trust management,
- software security (e.g., vulnerability detection),
- security in space.

SaToSS is part of the LACS and ComSys laboratories and has a strong connection to SnT. For more information, please visit our webpage at http://satoss.uni.lu.

Summary of the group's achievement in 2021

In 2021, the SaToSS group counted 20 researchers (1 professor, 1 senior researcher, 10 postdocs, 8 PhD students). Currently the group runs 9 externally funded projects: 2 FNR INTER projects (SURCVS on secure voting systems, and SLANT on NLP security), 2 FNR PRIDE projects (SPsquared on deep learning, and DRIVEN on social analysis) , 2 AFR projects (PriML on privacy in machine learning, and ATTEST on secure attestation and erasure of remote memory), 1 project funded by ESA (ATMonSAT on CubeSat security) and 2 COST Action projects (EuroProofNet on automated theorem provers, and DKG on knowledge representation). The group has also secured fundings of an FNR CORE project HETERS and an IAS project GENERIC both of which will start in 2022. In 2021, the group has successfully completed the Junior CORE project PrivDA on privacy in social graph release and the FNR INTER project AlgoReCell on bioinformatics. The group has contributed to the organization of a number of scientific events (e.g., FM2021, VTSA 2021). In 2021, SaToSS continued its active involvement in teaching and student supervision for bachelor and master programs in Computer Science (BINFO, BICS, MICS, MSSI).

Three most interesting publications in 2021

1. **Election verifiability revisited: Automated security proofs and attacks on Helios and Belenios. Sevdenur Baloglu, Sergiu Bursuc, Sjouke Mauw and Jun Pang,** in Proceedings of the 34th IEEE Computer Security Foundations Symposium (CSF) 2021: 1-15. Election verifiability aims to ensure

that the outcome produced by electronic voting systems correctly reflects the intentions of eligible voters, even in the presence of an adversary that may corrupt various parts of the voting infrastructure. Protecting such systems from manipulation is challenging because of their distributed nature involving voters, election authorities, voting servers and voting platforms. An adversary corrupting any of these can make changes that, individually, would go unnoticed, yet in the end will affect the outcome of the election. It is, therefore, important to rigorously evaluate whether the measures prescribed by election verifiability achieve their goals. We propose a formal framework that allows such an evaluation in a systematic and automated way. We demonstrate its application to the verification of various scenarios in Helios and Belenios, two prominent internet voting systems, for which we capture features and corruption models previously outside the scope of formal verification. Relying on the Tamarin protocol prover for automation, we derive new security proofs and attacks on deployed versions of these protocols, illustrating trade-offs between usability and security.

2. **Stealing Machine Learning Models: Attacks and Countermeasures for Generative Adversarial Networks. Hailong Hu and Jun Pang,** in Proceedings of the 37th Annual Computer Security Applications Conference (ASSAC) 2021: 1-16. Model extraction attacks aim to duplicate a machine learning model through query access to a target model. Early studies mainly focus on discriminative models. Despite the success, model extraction attacks against generative models are less well explored. In this paper, we systematically study the feasibility of model extraction attacks against generative adversarial networks (GANs). Specifically, we first define fidelity and accuracy on model extraction attacks against GANs. Then we study model extraction attacks against GANs from the perspective of fidelity extraction and accuracy extraction, according to the adversary's goals and background knowledge. We further conduct a case study where the adversary can transfer knowledge of the extracted model which steals a state of-the-art GAN trained with more than 3 million images to new domains to broaden the scope of applications of model extraction attacks. Finally, we propose effective defense techniques to safeguard GANs, considering a trade-off between the utility and security of GAN models.

3. **Compositional Analysis of Protocol Equivalence in the Applied pi-Calculus Using Quasi-open Bisimilarity. Ross Horne, Sjouke Mauw and Semen Yurkov,** in Proceedings of the 18th International Colloquium on Theoretical Aspects of Computing (ICTAC) 2021: 235-255. This paper shows that quasi-open bisimilarity is the coarsest bisimilarity congruence for the applied π-calculus. Furthermore, we show that this equivalence is suited to security and privacy problems expressed as an equivalence problem in the following senses: (1) being a bisimilarity is a safe choice since it does not miss attacks based on rich strategies; (2) being a congruence it enables a compositional approach to proving certain equivalence problems such as unlinkability; and (3) being the coarsest such bisimilarity congruence it can establish proofs of some privacy properties where finer equivalences fail to do so.

4.17 Security, Reasoning and Validation (SerVal)

Head of research group: Prof. Dr. Yves Le Traon

The SerVal – SEcurity, Reasoning and VALidation Research Group is headed by Professor Yves Le Traon and mixes researchers from SnT and DCS. SerVal conducts research on Software Engineering and Software Security, with a focus on data intensive, mobile and complex systems.

Researchers in the team leverage various techniques around three main pillars including:

- Software Testing (Mutation Testing, Search-Based Testing, ...)
- Data Analytics, predictive and prescriptive techniques (Decision Support Services)
- Machine Learning System Engineering and Security

SerVal strives to be ahead of the challenges of tomorrow's world. The research group builds innovative research solutions for trending and exciting domains such as the Android ecosystem and mobile security, next generations of information systems for banking and public administration, IoT, Fintech, Industry 4.0, and Smart Grid infrastructures.

Summary of the group's achievements in 2021

SerVal has been successful in several dimensions in 2021.

The number of researchers has increased to around 40 researchers.

The scientific group published 15 papers in top venues such as ICSE, TSE, MSR, ASE, ICCV. While this number is in line with 2020, the COVID crisis and the shift to remote work impacted 2021 publications.

The team also received a best paper award for their paper "Confuzzion: A Java Virtual Machine Fuzzer for Type Confusion Vulnerabilities" at QRS'21.

In terms of project acquisition, SERVAL managed to consolidate existing partnerships (CREOS, Cebi), as well as secure new ones (Statec), but also got several FNR projects (2 junior CORE, 1 Bridge, 1 CORE).

Finally, the team successfully organized the International Conference on Software Maintenance and Evolution 2021 (ICSME 21), with Pr. Yves Le Traon and Dr. Mike Papadakis acting as Co general Chair.

Main publications and achievements in 2021

1. CONFUZZION: A Java Virtual Machine Fuzzer for Type Confusion Vulnerabilities : QRS'21 Best Paper Award, William Bonnaventure, Ahmed Khanfir, Alexandre Bartel, Mike Papadakis, Yves Le Traon .

   Current Java Virtual Machine (JVM) fuzzers aim at generating syntactically valid Java programs, without targeting any particular use of the stan-

dard Java library. While effective, such fuzzers fail to discover specific kinds of bugs or vulnerabilities, such as type confusion, that are related to the standard API usage. To deal with this issue, we introduce a mutation-based feedback-guided black-box JVM fuzzer, called Confuzzion. Confuzzion, as the name suggests, targets security-relevant object-oriented flaws with a particular focus on type confusion vulnerabilities. We show that in less than 4 hours, on commodity hardware and without any predefined initialization seed, Confuzzion automatically generates Java programs that reveal JVM vulnerabilities, i.e., the Common Vulnerabilities and Exposures CVE-2017-3272. We also show that state-of-the-art fuzzers or even traditional automatic testing techniques are not capable of detecting such faults, even after 48 hours of execution in the same environment. To the best of our knowledge, Confuzzion is the first fuzzer able to detect JVM type confusion vulnerabilities.

2. Test Selection for Deep Learning Systems. ACM Trans. Softw. Eng. Methodology: Wei Ma, Mike Papadakis, Anestis Tsakmalis, Maxime Cordy, Yves Le Traon

   Testing of deep learning models is challenging due to the excessive number and complexity of the computations involved. As a result, test data selection is performed manually and in an ad hoc way. This raises the question of how we can automatically select candidate data to test deep learning models. Recent research has focused on defining metrics to measure the thoroughness of a test suite and to rely on such metrics to guide the generation of new tests. However, the problem of selecting/prioritising test inputs (e.g., to be labelled manually by humans) remains open. In this article, we perform an in-depth empirical comparison of a set of test selection metrics based on the notion of model uncertainty (model confidence on specific inputs). Intuitively, the more uncertain we are about a candidate sample, the more likely it is that this sample triggers a misclassification. Similarly, we hypothesise that the samples for which we are the most uncertain are the most informative and should be used in priority to improve the model by retraining. We evaluate these metrics on five models and three widely used image classification problems involving real and artificial (adversarial) data produced by five generation algorithms. We show that uncertainty-based metrics have a strong ability to identify misclassified inputs, being three times stronger than surprise adequacy and outperforming coverage-related metrics. We also show that these metrics lead to faster improvement in classification accuracy during retraining: up to two times faster than random selection and other state-of-the-art metrics on all models we considered.

3. MuDelta: Delta-Oriented Mutation Testing at Commit Time: ICSE'21, Wei Ma, Thierry Titcheu Chekam, Mike Papadakis, Mark Harman

   To effectively test program changes using mutation testing, one needs to use mutants that are relevant to the altered program behaviours. In view of this, we introduce MuDelta, an approach that identifies commit-relevant mutants; mutants that affect and are affected by the changed program behaviours. Our approach uses machine learning applied on

a combined scheme of graph and vector-based representations of static code features. Our results, from 50 commits in 21 Coreutils programs, demonstrate a strong prediction ability of our approach; yielding 0.80 (ROC) and 0.50 (PR Curve) AUC values with 0.63 and 0.32 precision and recall values. These predictions are significantly higher than random guesses, 0.20 (PR-Curve) AUC, 0.21 and 0.21 precision and recall, and subsequently lead to strong relevant tests that kill 45%more relevant mutants than randomly sampled mutants (either sampled from those residing on the changed component(s) or from the changed lines). Our results also show that MuDelta selects mutants with 27% higher fault revealing ability in fault introducing commits. Taken together, our results corroborate the conclusion that commit-based mutation testing is suitable and promising for evolving software.

4.18 Systems and Control Engineering (SCE)

Head of research group: Prof. Dr. Jürgen Sachau

The Systems and Control Engineering group is affiliated to the department of computer science sharing common labs with Electrical Engineering. The group's works have been focused on developing systems and control technology for reliable large-scale grid integration of solar power systems, including storage and sector-coupling for transport and thermal energy use.

Summary of the group's achievements in 2021

In 2021, the PhD works towards enhanced hosting capacity for large-scale photovoltaic generation distributed in grids were completed for guaranteeing control stability, failsafe protection and curtailment. For the complete subsets of radial and meshed MV-grid configurations, both overcurrent and overvoltage constraints need to be respected. Complete subset analysis guarantees supply security within the tolerances required, while securing reconfiguration freedom of the grid operator. By forecasting bottlenecks at substation transformers and overloading of lines for large-scale integration of PV plants, cost-intensive network reinforcement can be avoided resp. deferred by allocation of distributed storage with reactive current feed-in and grid code enhancement. Feasibility and dynamics of a novel control strategy have been examined by hardware-oriented simulations, in view of large-scale integration of PV in the national grid, as planned in the National Energy and Climate Plan, laying the ground for cooperative distributed control including droops and decentral curtailment.

Cooperation with Eurosolar and the Swiss Solar Agency have been continued with Prof. Sachau as member of the Norman Foster PEB committee and the European Solarprize committee. In delegation to the Joint Research Center(JRC), Ispra, Prof. Sachau has further elaborated the foundations for supply-security under integration of large-scale distributed feed-in into power grids within EU electrical energy security and Luxembourg's National Energy and Climate Plan.In continuation of his previous works as scientific officer of

DG Research, Brussels and of the EC-JRC Energy Institute, the EC Guideline EUR 30723-EN on Monitoring of Storage in Subgrids with Photovoltaic Power Generation, Document A could be established, complementing the European PV Monitoring Guidelines. Consultations with Luxembourg'sgrid operator, it's Haute Commissariat Protection Nationale and the MarketRegulator have been continued. Following alignment of spatial and temporal aggregation of key data on progress towards climate-neutrality in consultation with Eurostat, Luxembourg, initial exchange could be established with the Benelux Office, Brussels and the European Investment Bank, Luxembourg.

4.19 Team Leprévost

LACS : Prof. Dr. Franck Leprévost & Raluca Chitic (PhD Student) & Ali Osman Topal (Post-Doc)

Summary of the group's achievements in 2021

A series of organizational events occurred during the year 2021, including in particular the arrival in March of Ali Osman Topal as post-doc. Like everyone, we continued to cope with the situation created by the COVID. Still, we managed to obtain useful results, and to pursue our on-going work on evolutionary algorithms and their usage to fool neural networks for image recognition. A series of results led to the publication in particular of a conference paper (Best Paper Award) and a journal paper. Additional articles were published as well as two books (one tutorial in English, and one book published in French as well as in English).

CSC cluster activities in the context of the teaching evaluation, coordinated by F. Leprévost and that started in 2020, came to an end in 2021. This task was successful since the evaluation of the cluster by the international panel was highly positive (Feb. 2021).

Talks:

- Raluca Chitic: Presentation of 'Robustness of Adversarial Images against Filters' (article 2), OLA, 22nd June 2021.

List of published articles:

1. Raluca Chitic, Ali Osman Topal and Franck Leprévost. Evolutionary Algorithm-based images, humanly indistinguishable and adversarial against Convolutional Neural Networks: efficiency and robustness. IEEE Access 9, pp. 160758 - 160778 (2021).
2. Raluca Chitic, Nathan Deridder, Franck Leprévost, Nicolas Bernard. Robustness of Adversarial Images against Filters. Proceedings of the conference OLA 2021. Springer, CCIS, Vol. 1443, pp. 1-14. (2021).
3. Franck Leprévost. Le role civilisationnel des universités. La Revue des Deux Mondes, pp. 165-172 (April 2021).

4. Gent Imeraj, Erilda Muka, Ali Osman Topal, Mevlida Zenuni, Kristjan Marcinaj. Cognitive Health Reflection to Keto Diet Attitude with Machine Learning Clustering. Proceedings of the international conference on Computing, Networking, Telecommunications & Engineering Sciences Applications (CoNTESA) – IEEE, pp. 61-68 (December 2021)

5. Arban Uka, Albana Ndreu Halili, Xhoena Polisi, Ali Osman Topal, Gent Imeraj, Nihal E Vrana. Basis of image analysis for evaluating cell biomaterial interaction using brightfield microscopy. Vol.210, No. 2, pp.77-104, Cells Tissues Organs (2021)

List of publications - Books:

- Franck Leprévost : « Order Matters! A Hands-On Tutorial on Linear Algebra ». Ed. Amazon. ISBN : 139798595860642 (2021).
- Franck Leprévost: "Universities and Civilizations". Ed. ISTE and Wiley. Knowledge Management Series. ISBN : 9781786306685 (2021).
- Franck Leprévost : "Universités et civilisations". Ed. ISTE. ISBN : 9781784057510 (2021)

4.20 Team Müller

Head of research group: Prof. Dr. Volker Müller

Volker Müller and his small research team are interested in algorithmic aspects of common number-theoretic problems – especially about a simultaneous version of the classical Chinese Remainder Theorem (CRT). As side-effect of that research activity, the group member Jim Barthel could develop a new attack on the (M)inTRU assumption in the integer case which was published in ProvSec 2021. In addition, he could find a flaw in a common definition used for functional encryption. The description of this observation was submitted to EuroCrypt 2022, but finally not accepted, and is currently pending for resubmission. In another research, Jim worked on Carmichael's conjecture and Pomerance's conjecture, leading to a new conjecture related with primes in arithmetic conjectures. He was able to partially prove the new conjecture with a large-scale computation. A paper describing the results is accepted for publication in the American Mathematical Monthly later this year. Research on the Simultaneous Chinese Remaindering (S-CRT), a generalization of the well-known Chinese Remainder Theorem popular in number theory, has been continued and several new small (mostly theoretical) improvements could be proven. A thorough statistical analysis of simulated data was done which led to new insights. These findings finally lead to the observation that S-CRT is in its general form NP-hard – the proof is currently finalized and will appear in the Jim Barthel's dissertation due later in 2022.

As programme director of the "Bachelor in Applied Information Technology" and its life-long learning variant "Bachelor in Applied Information Technology – Continuing Education Programme", Volker Müller was strongly involved in smooth organization of the two programmes, especially in the dynamically changing special situation in 2021 due to the Corona virus. Albeit the difficult situation, 18 BINFO students could be graduated in 2021 after having finished their final Bachelor project linking applied scientific training with professional needs. The successful accreditation of both programmes by ACQUIN without objections in 2021 was one of the highlights from an academic point of view.

CHAPTER 5

Organizational Structure

The Department of Computer Science is organized according to the following structure.

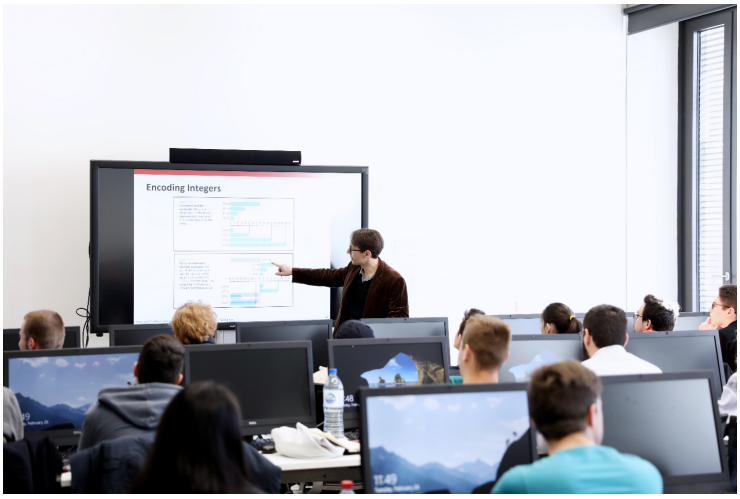
- The department is meant to be responsible for research and education performed by its members. The head of the department is therefore responsible for both.
- The head is seconded by a vice-head, who is able to take over all the head's responsibilities whenever needed, e.g. due to temporary absence or unavailability of the head. The head is also seconded by a Departmental Head of Teaching, to whom tasks in relation to teaching management are delegated. The roles of vice-head and Departmental Head of Teaching can be assumed by one person. Together, they perform the daily management of the department.
- DCS forms two sub-committees: an education management committee (EMC) and a research management committee (RMC). The purpose of the EMC is to coordinate all teaching-related activities of DCS. The purpose of the RMC is to represent DCS in discussions and decisions with regards to research coordination and its general and financial management.
- The head of DCS is the head of the RMC and the Departmental Head of Teaching is head of the EMC. The head of DCS is a regular member of the EMC and the vice-head is a regular member of the RMC. Further, these committees are formed by the heads of the educational programs (EMC) and by the lab heads (RMC).
- Besides these committees, the general DCS professors meeting is the final decision body of DCS.
- The head and vice-head/Departmental Head of Teaching are supported by the secretary team of the department and whenever needed by a research facilitator of the faculty.
- The head and vice-head/Departmental Head of Teaching of DCS represent DCS at the various UL levels. The internal communication within DCS is based on an effective communication infrastructure. Short summaries of the DCS professors meeting and the meetings of the EMC and RMC are made available. DCS labs organize DCS resources and competencies with a long-term view, and are governed by the following guidelines.
- There are three hierarchical levels within DCS: DCS (all members of DCS) + LAB (a substructure of DCS) + GRP (a research group consisting of a DCS professor and his team members). The duties, responsibilities and organization of a department and the tasks and duties of individual professors (and the employees that are hierarchically subordinate to the professor) are (partly)

defined in the law and internal UL rules. DCS can delegate responsibilities to other entities (such as the management team, heads of studies, labs, heads of labs, ad-hoc groups, individuals). Research groups are named after their main topic(s) of study.

- The purpose of a LAB is at least to coordinate and distribute tasks, and to distribute money and share resources (like rooms). Moreover, labs can be used for PR and visibility, to represent its members within DCS, to stimulate research cooperation, to organize joint seminars, or to coordinate education in a given domain, etc.
- Labs can determine their own organisational structure. Every lab has a lab head. The lab professors can delegate responsibilities of the lab to the lab head. The lab professors can define other responsibilities (e.g. vice lab head). The lab head is (s)elected by and from the lab professors. Every lab decides on a set of rules defining the (s)election of the lab head and the internal functioning.
- One can be a member of one primary and one or more secondary LABS. A lab should have at least two professors as primary members. Professors, members from their research groups and support staff can be member of a lab. The proposing professors are automatically members of a newly created lab. If a professor wants to join a lab or proposes one of his assistants as a lab member, he may request this to the professors that are currently member of the lab. The lab professors will take a motivated decision on this request. A professor can decide to not become a member of any lab. DCS can allocate resources to professors that are not member of any lab.
- The set of LABS remains stable for long term (e.g. at least 4 years). DCS decides on the discontinuation of existing labs and the creation of new labs. A group of professors can propose to DCS to create a new lab.
- A certain percentage of the DCS budget and of the other resources (secretaries, technical assistants, etc.) is assigned to the LABs. Each lab decides on how to internally distribute (the use of) the assigned resources. The structural positions for assistants are not assigned to labs, but to professors.

Chapter 6

Education



The DCS educational offer in computer science aims at meeting the quickly growing societal needs for academic and professional education in computer science. DCS offers a spectrum of study programs suited to the needs of different groups of students:

- Academically-oriented programs, at the bachelor (BICS, see section 6.6) and master level (MICS, see section 6.2), suited for students with a strong academic background willing primarily to continue their studies towards a master program (when in a bachelor program) or a PhD (when in a master program).
- Professionally-oriented programs at the bachelor level (BINFO, see section 6.7) and Master level (ISM, see section 6.4), designed mainly for students intending to enter the job market with a training well suited to meet the needs of local companies and institutions.
- Lifelong learning programs, both at the bachelor (BINFO-CEP, see section 6.8) and at the master level (MISSM, see section 6.3 and MTECH, see section 6.5), that are organised with a partner: the Chambre des Salariés (CSL), the Luxembourg Institute of Science and Technology (LIST) or the Luxembourg Institute of Standardisation, Accreditation, Safety and Quality of Products and Services (ILNAS). These programs target students with a substantial professional experience validated through the procedure of recognition of prior education and professional experience.
- A Doctoral program in Computer Science and Computer Engineering (see sec-

tion 6.1) to train Doctoral Candidates from DCS and SnT on a wide range of advanced and interdisciplinary subjects including the fundamentals of teaching. In addition to its own study programs, DCS is also contributing to the teaching in programs managed by other departments such as the engineering and mathematics departments.

For the purpose of quality assurance and to further improve the quality of teaching in all its facets, DCS has initiated the certification of its study programs by international agencies. The MICS, BINFO and BINFO-CEP were the first programs to undergo the accreditation process of the Accreditation, Certification and Quality Assurance Institute (ACQUIN), which they obtain without reservation in 2021.

6.1 Doctoral Programme in Computer Science and Computer Engineering

The Doctoral programme in Computer Science and Computer Engineering (DP-CSCE) is part of the Doctoral School in Science and Engineering (DSSE). The DP-CSCE is the joint doctoral programme of the Department of Computer Science (DCS) and the Interdisciplinary Centre for Security, Reliability and Trust (SnT), which provides an excellent environment for pursuing doctoral studies in computer science and computer engineering at an internationally competitive level and in broad interdisciplinary application.

Candidates successfully terminating doctoral education at the DP-CSCE will be awarded a Doctoral Degree in “Informatique”. The main research areas concern: Communicative Systems, Intelligent & Adaptive Systems, Security & Cryptology, Software Engineering, High Performance Computing and Big Data.

The DP-CSCE now hosts over 210 doctoral candidates of 46 different nationalities, which makes it the biggest doctoral programme of the University of Luxembourg.

6.2 Master in Information and Computer Sciences (MiCS)

The Master in Information and Computer Sciences (MICS) is a continuation of the Bachelor studies as a first step towards the PhD. The programme started in 2004 and was partly redesigned in 2010 in terms of profiles to provide more flexible specialisation options. The structure is as follows.

The first semester is mandatory for all. It is dedicated to the fundamentals of computer science. By the end of the first semester, the student selects courses based on one or more profiles that she/he would like to pursue. Profiles are similar to specialisations with the added benefit that multiple profiles can be realised. There are currently four profiles offered:

- Artificial Intelligence

- Communication Systems
- Information Security
- Reliable Software Systems

The second and third semester offer specialised courses in the selected field, preparing the candidate for the Master Thesis in the fourth semester. The MICS adheres to the Bologna agreement.

In 2021 there were around 80 students from more than 20 countries in the MICS.

6.3 Master in Information System Security Management

The MISSM (Master in Information System Security Management) allows professionals to increase their knowledge and develop their skills to analyse, interpret and provide adequate solutions in the field of information security.

It is a lifelong learning Master degree programme with a well-established reputation in Luxembourg and the Greater Region. Created in 2007, together with market stakeholders, the MISSM graduates every year between 12 and 18 professionals in the field of security management. The ISSM master is specifically aimed at training CISOs, which is why the program covers all interdisciplinary aspects related to this role. The focus is on the implementation of best practices and standards for security management, complemented by the acquisition of knowledge in the technical, legal, and social fields.

Thanks to our teaching team, composed of academics and professionals, we provide the interdisciplinary, applied and academic
background (technical, managerial, legal...) required for security officers to face the challenges of nowadays security threats.

6.4 Interdisciplinary Space Master

The growing research and innovation in space exploration and exploitation will require university graduates who are prepared to contribute to this growing and dynamic industry. In Luxembourg, the space industry includes telecommunications and broadcast services as well as manufacturers and systems operators, but also many “New Space” SMEs and Start-Ups that were attracted in recent years. This industry offers career opportunities across multiple disciplines. In addition to these industrial sectors, two public research organizations, the Luxembourg Institute of Science and Technology and the University of Luxembourg, are also developing space research activities. The domains covered by industry and the public research institutes include:

- The space segment comprising the development and manufacturing of micro- and nanosatellites, structures, electronic equipment, space robotics and systems for space resource utilization and in-space manufacturing.
- The ground segment, consisting of ground station development, mechanical and electrical ground support equipment, and communication networks.

- The service segment, embracing teleport, satellite broadband, risk management and automatic identification system (AIS) services, remote sensing and space-based data analytics.

To respond to a growing need for people educated to contribute to these fields in Luxembourg and Europe, the Interdisciplinary Space Master (ISM) has been created in 2019 at UL in close collaboration with the Luxembourg Space Agency (LSA). Through a project-based learning approach, graduates will obtain a fundamental understanding of the science that motivates space sector industry and what is technically required to establish and manage space missions. Students will also learn computer skills required to interpret observations from space (big data; machine learning, artificial intelligence). In addition, the graduates will be educated in the business, entrepreneurial, finance, and legal aspects required to develop start-ups that will contribute to the value chain for space exploration and exploitation in Luxembourg.

The space value chain is a commercial space venture that includes commercial or research operations on the Moon and near-Earth asteroids. More specifically, courses will touch upon space systems engineering, space operations, space data mining and intelligent systems, satellite communications, and robotics. Theoretical and practical concepts in business, entrepreneurship, finance and project management are also components of the study programme. The lectures will be delivered by UL professors, with guest lectures from renowned partner universities and industrial experts having significant experience working in the space sector. During the Master, students will make use of cutting-edge Labs, such as the LunaLab, CubeSat Lab, Concurrent Design Facility, SatComLab and Zero-G Lab. In the fourth semester of the master, the students will work on their Master's thesis, which can also be done in collaboration with an external partner such as a company or an agency. To gain additional work experience, students are also encouraged to do a voluntary internship in a space company.

The ISM is already running for four cohorts and has attracted a distinctive mix of international students with interdisciplinary background.

6.5 Master in Technopreneurship (MTECH)

The Master in Technopreneurship (MTECH) at the University of Luxembourg is developed in partnership with the Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services (ILNAS) and the Luxembourg Lifelong Learning Center (LLLC) of the Chambre des Salariés (CSL). The Master MTECH is extremely innovative. On one hand, it provides students with a base of knowledge on topics reflecting current issues and those at the cutting edge of Smart ICT, and on the other hand, it serves as a catalyst for growth in the ICT Industry by offering practical examples and case studies illustrating the use of technical standardisation as a tool to give common technical language, build trust, and foster effectiveness in Smart ICT. The Master degree is also supported by the European standardisation organisations, namely the European Committee for Standardization (CEN) and the European Commit-

tee for Electrotechnical Standardization (CENELEC), as well as the European Telecommunications Standards Institute (ETSI).

The second promotion of the MTECH will start in February 2023.

6.6 Bachelor in Computer Science (BiCS)

The Department of Computer Science (DCS) offers a bachelor programme in computer science (BiCS) meant for students interested in learning the foundational theoretical aspects of computer science and develop skills to make use of such theories in practical contexts. In the end, students who have successfully completed the programme will be ready to pursue studies in a master programme on computer science either at the University of Luxembourg or any other world-class university.

The main strengths of the BiCS are:

- programme designed from the international standard ACM / IEEE CS 2013,
- scientific quality to enhance interest and strengths in science and technology for the future,
- project-based learning as a signature pedagogy, in line with the university's drive for "research-based teaching",
- applied multilingualism for effective integration into the Luxembourgish or international labour market.

The complete programme dedicated to computer science brings:

- greater focus on key skills needed for computer scientists,
- more systematic consideration and implementation of the internationally recognised standards in computer science education,
- better offer to industry and societal requirements
- more thoughtful selection of specific types of pedagogies necessary to train highly effective students.

A R&D laboratory for BiCS students has been set up (the BiCSLab). Its objectives are to:

- provide a common space for BiCS students where they can develop their own ideas and initiatives,
- develop industrial collaborations,
- host selected Bachelor Semester Projects (BSPs) to be done in partnership with industrial partners,
- provide an initial R&D support structure for selected BiCS students

The BiCSLab is financed internally using the BiCS programme budget line and externally using industrial partners registration fees. More about the BicsLab can be found at https://bicslab.uni.lu.

Last, but not least it is worth recalling that BiCS was launched in the academic year 2017-2018. Up to now, the BiCS counts with a total of 107 students attending courses and 23 graduated.

The figures for academic year 2020/2021 are:

- 77 total applicants: 17% female, 83% male,
- admission rate: 65%,
- high school degrees: 86% classic, 14% vocational & others,
- high school country: 48% Luxembourg, 19% Greater region, 33% others

More information and news about BiCS can be found at https://bics.uni.lu .

6.7 Bachelor in Applied Information Technology (BINFO)

The "Bachelor in Applied Information Technology" (BINFO) offers a practice-oriented study programme that provides students with highly-demanded professional skills to enter the job market after graduation, be it in the public or the private sector. The BINFO trains students with a combination of theoretical lectures and many practical projects such that the students master basic professional skills and applied IT know-how needed for continuous training and professional development during their career. Beyond technical training in practically relevant IT-related technologies, BINFO is humanly rich and offers a bilingual study programme (English, French) with classmates and instructors from diverse cultural backgrounds and a mobility semester abroad. The main learning objectives of the BINFO are the following:

- Be competent in software programming and, more widely, in methods required to develop computer systems;
- Acquire a specialization in one application domain of computer science such as big data, mobile and web applications, banking information technology or distributed applications, especially deepening applied knowledge on the latest trends in the IT industry;
- Be able to efficiently communicate orally and in writing, in English and French, in cross cultural professional environments;
- Understand how companies operate and be well prepared for a professional career, through a final 3 months Bachelor project done in professional partner institutions and teaching delivered by experienced practitioners;
- Be able to work autonomously, analyze and anticipate issues, propose solutions in various professional situations.

In the Winter semester 2021-2022, a total of 153 students are registered within the BINFO program (59 in the first year, 41 in the second, and 53 students in the third year). The number of BINFO graduates in 2021 is 18. More information on the programme can be found at https://binfo.uni.lu. During the years 2020 and 2021, an in-depth analysis of internal processes and a self-reflection about the strengths and weaknesses of the programme was done in the context of a Programme Accreditation done by the German accreditation agency ACQUIN. On 24 October 2021, an accreditation with only minor remarks on potential quality improvements was granted to the programme until September 2028 by ACQUIN.

6.8 Bachelor in Applied Information Technology – Continuous Education Programme (BINFO-CEP)

The "Bachelor in Applied Information Technology – Continuous Education Programme" (BINFO-CEP) offers a practice-oriented part-time study programme that corresponds to the needs of the Luxembourgish labor market for continued professional development. The programme is organized in cooperation with the Lifelong Learning Center of the Chambre des Salaires (CSL). Students require a minimum of 6 years of professional experience in the IT domain, which is honored in the programme with the acknowledgment of a certain number of ECTS credits. The BINFO-CEP trains its students with a combination of theoretical lectures and many practical projects, especially focusing on certain practically important areas like programming, web applications, or software engineering. A special objective of the programme is the empowerment of its students for continuous training and further professional development during their future professional career. Beyond technical training in practically relevant IT-related technologies, BINFO-CEP is humanly rich and offers a bilingual study programme (English, French) with classmates and instructors from diverse cultural and professional background.

The main learning objectives of the BINFO-CEP are the following:

- Be competent in software programming and, more widely, in methods required to develop computer systems;
- Acquire a broad basis knowledge in several application domains of computer science such as programming, web applications, algorithms and data structures, blockchains, distributed applications, data-centered applications, software engineering, and others, especially deepening already existing practical expertise on latest trends in the IT industry;
- Be able to efficiently communicate orally and in writing, in English and
- French, in cross cultural professional environments;
- Be able to work autonomously, analyze and anticipate issues, propose solutions in various professional situations.

In the Winter semester 2021-2022, a total of 26 students are registered within the BINFO-CEP program (11 in the first, 15 students in the second/third year). The number of BINFO-CEP graduates in 2021 is 11. More information on the programme can be found at https://binfo-cep.uni.lu. During the years 2020 and 2021, an in-depth analysis of internal processes and a self-reflection about the strengths and weaknesses of the programme was done in the context of a Programme Accreditation done by the German accreditation agency ACQUIN. On 24 October 2021, an accreditation with only minor remarks on potential quality improvements was granted to the programme until September 2028 by ACQUIN.

Appendix A

Publication List

The publications listed in this chapter have been obtained from ORBilu, the official publication record repository of the university. Please note that the list of books includes those where a DCS member contributed as an editor.

Publication Category	Quantity	Section
Books	2	A.1 (p.58)
Book Chapters	6	A.2 (p.58)
Journal Articles	78	A.3 (p.58)
Conference Papers	135	A.4 (p.66)
Theses	18	A.5 (p.80)
Miscellaneous Writings	1	A.6 (p.82)
Total	*240*	

Table A.1: Overview of publications per category

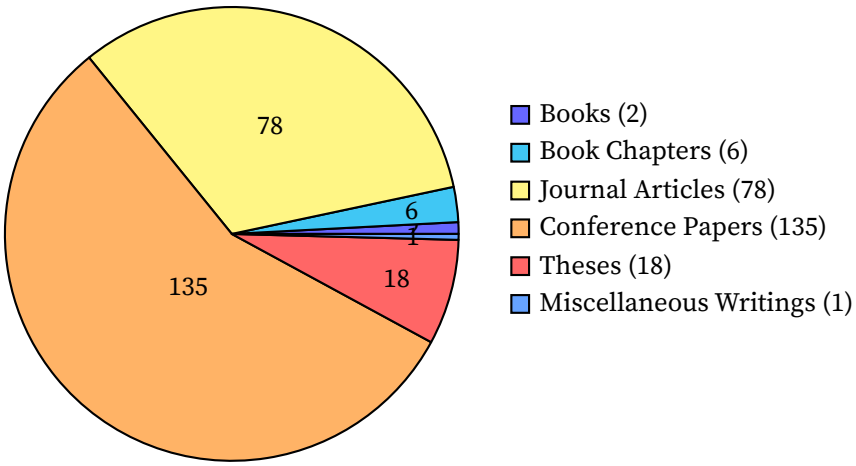


Figure A.1: Distribution of Types of Publications

A.1 Books

[1] Luis A. Leiva, Cedric Pruski, Réka Markovich, Amro Najjar, and Christoph Schommer, eds. *Proceedings of BNAIC/BeneLearn 2021*. BnL, 2021. ISBN: 0-2799-2527-X. URL: http://hdl.handle.net/10993/48924.

[2] Franck Leprevost. *Universities and Civilizations*. ISTE and Wiley, 2021. URL: http://hdl.handle.net/10993/46589.

A.2 Book Chapters

[3] Wilhelmina Maria Botes and Arianna Rossi. "Back to the Future with Icons and Images: "Low-Tech" to Communicate and Protect Privacy and Data". In: *Legal Design Perspectives. Theoretical and Practical Insights from the Field*. Ed. by Rossana Ducato and Alain Strowel. Ledi Publishing, 2021, pp. 209–226. ISBN: 9788855265669. URL: http://hdl.handle.net/10993/50100.

[4] Jean Botev, Tarek El-Ghazawi, and Christopher Stewart. "Message from the General Chairs". In: *Proceedings of the 2nd IEEE International Conference on Autonomic Computing and Self-Organizing Systems (ACSOS)*. IEEE, 2021. URL: http://hdl.handle.net/10993/48592.

[5] Jean Botev, Peter R. Lewis, Anthony Stein, and Sven Tomforde. "Lifelike Computing Systems Workshops (LIFELIKE 2020 & 2021)". In: *Proceedings of the 1st and 2nd International Workshop on Lifelike Computing Systems (LIFELIKE)*. CEUR WS, 2021. URL: http://hdl.handle.net/10993/48591.

[6] Wojciech Jamroga, Peter Y A Ryan, Steve Schneider, Carsten Schürmann, and Philip B. Stark. "A Declaration of Software Independence". In: *Protocols, Strands, and Logic - Essays Dedicated to Joshua Guttman on the Occasion of his 66.66th Birthday*. Springer, 2021, pp. 198–217. DOI: 10.1007/978-3-030-91631-2_11. URL: http://hdl.handle.net/10993/48859.

[7] Arianna Rossi and Helena Haapio. "Proactive Legal Design for Health Data Sharing based on Smart Contracts". In: *Smart Contracts. Technological, Business and Legal Perspectives*. Ed. by Marcelo Corrales Compagnucci, Mark Fenwick, and Stefan Wrbka. Hart Publishing, 2021, pp. 101–121. URL: http://hdl.handle.net/10993/49595.

[8] Sandra Schmitz and Stefan Schiffner. "Ein Schritt vor, zwei Schritte zurück? - Folgen einer verpflichtenden Zugriffsmöglichkeit auf verschlüsselte Daten". In: *Im Fokus der Rechtsentwicklung – Die Digitalisierung der Welt*. Ed. by Jürgen Taeger. OlWIR, 2021, pp. 289–304. ISBN: 978-3-955990-74-9. URL: http://hdl.handle.net/10993/48116.

A.3 Journal Articles

[9] Ki Yung Ahn, Ross James Horne, and Alwen Tiu. "A Characterisation of Open Bisimilarity using an Intuitionistic Modal Logic". In: *Logical*

Methods in Computer Science 17 (2021), 2:1–2:40. DOI: 10.46298/lmcs-17(3:2)2021. URL: http://hdl.handle.net/10993/50043.

[10] Marharyta Aleksandrova and Oleg Chertov. "SCR-Apriori for Mining 'Sets of Contrasting Rules'". In: *Studies in Fuzziness and Soft Computing* 393 (2021), pp. 77–89. DOI: 10.1007/978-3-030-47124-8_7. URL: http://hdl.handle.net/10993/49345.

[11] Nuwan T. Attygalle, Luis A. Leiva, Matjaž Kljun, Christian Sandor, Alexander Plopski, Hirokazu Kato, et al. "No Interface, No Problem: Gesture Recognition on Physical Objects Using Radar Sensing". In: *Sensors* 21 (2021). DOI: 10.3390/s21175771. URL: http://hdl.handle.net/10993/48693.

[12] Francesco Belardinelli, Rodica Condurache, Catalin Dima, Wojciech Jamroga, and Michał Knapik. "Bisimulations for Verifying Strategic Abilities with an Application to the ThreeBallot Voting Protocol". In: *Information and Computation* 276 (2021), Article 104552. DOI: 10.1016/j.ic.2020.104552. URL: http://hdl.handle.net/10993/45850.

[13] Jean Botev and Francisco J. Rodríguez Lera. "Immersive Robotic Telepresence for Remote Educational Scenarios". In: *Sustainability* (2021). DOI: 10.3390/su13094717. URL: http://hdl.handle.net/10993/47058.

[14] Abdelwahab Boualouache and Thomas Engel. "Federated Learning-based Scheme for Detecting Passive Mobile Attackers in 5G Vehicular Edge Computing". In: *Annals of Telecommunications* (2021). URL: http://hdl.handle.net/10993/48006.

[15] Abdelwahab Boualouache, Hichem Sedjelmaci, and Thomas Engel. "Consortium Blockchain for Cooperative Location Privacy Preservation in 5G-enabled Vehicular Fog Computing". In: *IEEE Transactions on Vehicular Technology* (2021). URL: http://hdl.handle.net/10993/47570.

[16] Matthias R. Brust, Grégoire Danoy, Daniel Stolfi Rosso, and Pascal Bouvry. "Swarm-based counter UAV defense system". In: *Discover Internet of Things* 1 (2021). DOI: 10.1007/s43926-021-00002-x. URL: http://hdl.handle.net/10993/49678.

[17] Alessio Buscemi, Ion Turcanu, German Castignani, Romain Crunelle, and Thomas Engel. "CANMatch: A Fully Automated Tool for CAN Bus Reverse Engineering based on Frame Matching". In: *IEEE Transactions on Vehicular Technology* (2021). DOI: 10.1109/TVT.2021.3124550. URL: http://hdl.handle.net/10993/48502.

[18] Rachele Carli and Amro Najjar. "Rethinking Trust in Social Robotics". In: *arXiv* (2021). URL: http://hdl.handle.net/10993/49807.

[19] Walter Carnielli, Marcelo Coniglio, and David Fuenmayor Pelaez. "Logics of Formal Inconsistency enriched with replacement: an algebraic and modal account". In: *Review of Symbolic Logic* online first (2021). DOI: 10.1017/S1755020321000277. URL: http://hdl.handle.net/10993/49074.

[20] Thiago Castro, Leopoldo Teixeira, Vander Alves, Sven Apel, Maxime Cordy, and Rohit Gheyi. "A Formal Framework of Software Product Line Analyses". In: *ACM Transactions on Software Engineering and Methodology* 30 (2021), pp. 1–37. URL: http://hdl.handle.net/10993/45577.

[21] Ninghan Chen, Zhiqiang Zhong, and Jun Pang. “An Exploratory Study of COVID-19 Information on Twitter in the Greater Region”. In: *Big Data and Cognitive Computing* 5 (2021), article 5. DOI: 10.3390/bdcc5010005. URL: http://hdl.handle.net/10993/46927.

[22] Ioana Raluca Chitic, Nathan Deridder, Franck Leprevost, and Nicolas Bernard. “Robustness of Adversarial Images against Filters”. In: *Optimization and Learning* 1443 (2021), pp. 101–114. URL: http://hdl.handle.net/10993/49669.

[23] Ioana Raluca Chitic, Ali Osman Topal, and Franck Leprevost. “Evolutionary Algorithm-based images, humanly indistinguishable and adversarial against Convolutional Neural Networks: efficiency and filter robustness”. In: *IEEE Access* (2021). URL: http://hdl.handle.net/10993/49149.

[24] Maxime Cordy, Sami Lazreg, Mike Papadakis, and Axel Legay. “Statistical model checking for variability-intensive systems: applications to bug detection and minimization”. In: *Formal Aspects of Computing* 33 (2021), pp. 1147–1172. DOI: 10.1007/s00165-021-00563-2. URL: http://hdl.handle.net/10993/49668.

[25] Mauro Dalle Lucca Tosi and Julio Cesar Dos Reis. “Keyphrase extraction from single textual documents based on semantically defined background knowledge and co-occurrence graphs”. In: *International Journal of Metadata, Semantics and Ontologies* 15 (2021), pp. 121–132. URL: http://hdl.handle.net/10993/52022.

[26] Mauro Dalle Lucca Tosi and Julio Cesar dos Reis. “SciKGraph: A knowledge graph approach to structure a scientific field”. In: *Journal of Informetrics* 15 (2021), p. 101109. URL: http://hdl.handle.net/10993/52021.

[27] Nadia Daoudi, Kevin Allix, Tegawendé François D Assise Bissyande, and Jacques Klein. “Lessons Learnt on Reproducibility in Machine Learning Based Android Malware Detection”. In: *Empirical Software Engineering* 26 (2021). DOI: 10.1007/s10664-021-09955-7. URL: http://hdl.handle.net/10993/47296.

[28] Huimin Dong, Jun Pang, and Yi Wang. “Preface of the special issue ‘Logic, argumentation and AI’ in JLC”. In: *Journal of Logic and Computation* 31 (2021), pp. 1901–1902. URL: http://hdl.handle.net/10993/49138.

[29] Alireza Esfahani, Jérémie Decouchant, Marcus Volp, Shahid Mumtaz, and Kostromitin Konstantin Igorevich. “SIAKAV: Secure integrated authentication and key agreement for cellularconnected IoT devices in vehicular social networks”. In: *Transactions on Emerging Telecommunications Technologies* (2021). DOI: 10.1002/ett.4279. URL: http://hdl.handle.net/10993/48866.

[30] Guy Fagherazzi, Aurelie Fischer, Muhannad Ismael, and Vladimir Despotovic. “Voice for Health: The Use of Vocal Biomarkers from Research to Clinical Practice”. In: *Digital Biomarkers* 5 (2021), pp. 78–88. DOI: 10.1159/000515346. URL: http://hdl.handle.net/10993/46861.

[31] Antonio Maria Fiscarelli, Matthias R. Brust, Roland Bouffanais, Grégoire Danoy, Apivadee Piyatumrong, and Pascal Bouvry. “Interplay between success and patterns of human collaboration: case study of a Thai Research Institute”. In: *Scientific Reports* (2021). DOI: 10.1038/s41598-020-79447-z. URL: http://hdl.handle.net/10993/45674.

[32] Raphaël Frank and Faisal Hawlader. “Poster: Commercial 5G Performance: A V2X Experiment”. In: *Proceedings of the 13th Vehicular Networking Conference 2021* (2021). URL: http://hdl.handle.net/10993/48766.

[33] Dov M. Gabbay. “What is Negation in a System 2020?” In: *IfCoLog Journal of Logics and Their Applications* 8 (2021), pp. 1977–2034. URL: http://hdl.handle.net/10993/49963.

[34] Dov M. Gabbay, Massimiliano Giacomin, Guillermo Ricardo Simari, and Matthias Thimm. “Preface - Journal of Applied Logics”. In: *IfCoLog Journal of Logics and Their Applications* 8 (2021), pp. 1335–1338. URL: http://hdl.handle.net/10993/50372.

[35] Salah Ghamizi, Maxime Cordy, Mike Papadakis, and Yves Le Traon. “Evasion Attack STeganography: Turning Vulnerability Of Machine Learning ToAdversarial Attacks Into A Real-world Application”. In: *Proceedings of International Conference on Computer Vision 2021* (2021). URL: http://hdl.handle.net/10993/47832.

[36] Yonglin Hao, Gregor Leander, Willi Meier, Yosuke Todo, and Qingju Wang. “Modeling for Three-Subset Division Property without Unknown Subset”. In: *Journal of Cryptology* 34 (2021), p. 22. DOI: 10.1007/s00145-021-09383-2. URL: http://hdl.handle.net/10993/49481.

[37] Faisal Hawlader and Raphaël Frank. “Towards a Framework to Evaluate Cooperative Perception for Connected Vehicles”. In: *Proceedings of the 13th IEEE Vehicular Networking Conference 2021* (2021). URL: http://hdl.handle.net/10993/48765.

[38] Ross James Horne and Sjouke Mauw. “Discovering ePassport Vulnerabilities using Bisimilarity”. In: *Logical Methods in Computer Science* 17 (2021), 24:1–24:52. DOI: 10.23638/LMCS-17(2:24)2021. URL: http://hdl.handle.net/10993/50044.

[39] Lilo Humpreys, Guido Boella, Leon van der Torre, Livio Robaldo, Luigi Di Caro, Sepideh Ghanavati, et al. “Populating legal ontologies using semantic role labeling”. In: *Artificial Intelligence and Law* 29 (2021), pp. 171–211. DOI: 10.1007/s10506-020-09271-3. URL: http://hdl.handle.net/10993/49905.

[40] Wojciech Jamroga, David Mestel, Peter Roenne, Peter Y A Ryan, and Marjan Skrobot. “A Survey of Requirements for COVID-19 Mitigation Strategies”. In: *Bulletin of The Polish Academy of Sciences: Technical Science* 69 (2021), e137724. DOI: 10.24425/bpasts.2021.137724. URL: http://hdl.handle.net/10993/49347.

[41] Patrick Keller, Abdoul Kader Kabore, Laura Plein, Jacques Klein, Yves Le Traon, and Tegawendé François D Assise Bissyande. "What You See is What it Means! Semantic Representation Learning of Code based on Visualization". In: *ACM Transactions on Software Engineering and Methodology* (2021). URL: http://hdl.handle.net/10993/48899.

[42] Sybren de Kinderen, Monika Kaczmarek-Heß, Qin Ma, and Ivan Razo-Zapata. "A Modeling Method in Support of Strategic Analysis in the Realm of Enterprise Modeling - On the Example of Blockchain-Based Initiatives for the Electricity Sector". In: *Enterprise Modelling and Information Systems Architectures* 16 (2021), 2:1–2:36. DOI: 10.18417/emisa.16.2. URL: http://hdl.handle.net/10993/46368.

[43] Aleks Knoks. "Conciliatory reasoning, self-defeat, and abstract argumentation". In: *Review of Symbolic Logic* First View (2021), pp. 1–48. DOI: 10.1017/S1755020321000502. URL: http://hdl.handle.net/10993/49577.

[44] Aleks Knoks. "Misleading Higher-Order Evidence, Conflicting Ideals, and Defeasible Logic". In: *Ergo, An Open Access Journal of Philosophy* 8 (2021), pp. 141–174. DOI: 10.3998/ERGO.1143. URL: http://hdl.handle.net/10993/48986.

[45] Pingfan Kong, Li Li, Jun Gao, Timothée Riom, Yanjie Zhao, Tegawendé François D Assise Bissyande, et al. "ANCHOR: locating android framework-specific crashing faults". In: *Automated Software Engineering* (2021). URL: http://hdl.handle.net/10993/49670.

[46] Diego Kozlowski, Jennifer Dusdal, Jun Pang, and Andreas Zilian. "Semantic and Relational Spaces in Science of Science: Deep Learning Models for Article Vectorisation". In: *Scientometrics* (2021). DOI: 10.1007/s11192-021-03984-1. URL: http://hdl.handle.net/10993/45095.

[47] Liu Kui, Li Li, Anil Koyuncu, Kim Dongsun, Zhe Liu, Jacques Klein, et al. "A critical review on the evaluation of automated program repair systems". In: *Journal of Systems and Software* (2021). URL: http://hdl.handle.net/10993/46079.

[48] Lokesh Kumar T. and Luis A. Leiva. "Attentive Sequence-to-Sequence Modeling of Stroke Gestures Articulation Performance". In: *IEEE Transactions on Human-Machine Systems* 51 (2021). DOI: 10.1109/THMS.2021.3112961. URL: http://hdl.handle.net/10993/48694.

[49] Luis A. Leiva, Asutosh Hota, and Antti Oulasvirta. "Interactive Exploration of Large-scale UI Datasets with Design Maps". In: *Interacting with Computers* (2021). DOI: 10.1093/IWCOMP/IWAB006. URL: http://hdl.handle.net/10993/46880.

[50] Tomer Libal and Dale Miller. "Functions-as-constructors Higher-order Unification: Extended Pattern Unification". In: *Annals of Mathematics and Artificial Intelligence* (2021). URL: http://hdl.handle.net/10993/53278.

[51] Wei Ma, Mike Papadakis, Anestis Tsakmalis, Maxime Cordy, and Yves Le Traon. "Test Selection for Deep Learning Systems". In: *ACM Transactions on Software Engineering and Methodology* 30 (2021), 13:1–13:22. DOI: 10.1145/3417330. URL: http://hdl.handle.net/10993/44550.

[52] Tieu Long Mai and Nicolas Navet. “Deep Learning to Predict the Feasibility of Priority-Based Ethernet Network Configurations”. In: *ACM Transactions on Cyber-Physical Systems* 5 (2021), pp. 1–26. DOI: 10.1145/3468890. URL: http://hdl.handle.net/10993/44092.

[53] Karola Marky, Marie-Laure Zollinger, Peter Roenne, Peter Y A Ryan, Tim Grube, and Kai Kunze. “Investigating Usability and User Experience of Individually Verifiable Internet Voting Schemes”. In: *ACM Transactions on Computer-Human Interaction* 28 (2021), pp. 1–36. URL: http://hdl.handle.net/10993/49089.

[54] Nesryne Mejri, Konstantinos Papadopoulos, and Djamila Aouada. “Leveraging High-Frequency Components for Deepfake Detection”. In: *IEEE Workshop on Multimedia Signal Processing* (2021). DOI: 10.1109/MMSP53017.2021.9733606. URL: http://hdl.handle.net/10993/48389.

[55] Xian Mo, Jun Pang, and Zhiming Liu. “Effective Link Prediction with Topological and Temporal Information using Wavelet Neural Network Embedding”. In: *Computer Journal* 64 (2021), pp. 325–336. DOI: 10.1093/comjnl/bxaa085. URL: http://hdl.handle.net/10993/46921.

[56] Dimiter Ostrev. “QKD parameter estimation by two-universal hashing leads to faster convergence to the asymptotic rate”. In: *Quantum* (2021). DOI: 10.22331/q-2023-01-13-894. URL: http://hdl.handle.net/10993/48038.

[57] Sameera Palipana, Dariush Salami, Luis A. Leiva, and Stephan Sigg. “Pantomime: Mid-Air Gesture Recognition with Sparse Millimeter-Wave Radar Point Clouds”. In: *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 5 (2021). DOI: 10.1145/3448110. URL: http://hdl.handle.net/10993/46834.

[58] Túlio Pascoal, Jérémie Decouchant, Antoine Boutet, and Paulo Esteves-Verissimo. “DyPS: Dynamic, Private and Secure GWAS”. In: *Proceedings on Privacy Enhancing Technologies* (2021). DOI: 10.2478/popets-2021-0025. URL: http://hdl.handle.net/10993/44966.

[59] Zoran Peric, Bojan Denic, and Vladimir Despotovic. “Algorithm based on 2bit adaptive delta modulation and fractional linear prediction for Gaussian source coding”. In: *IET Signal Processing* 15 (2021), pp. 410–423. DOI: 10.1049/sil2.12040. URL: http://hdl.handle.net/10993/47858.

[60] Zoran Peric, Milan Savic, Nikola Simic, Bojan Denic, and Vladimir Despotovic. “Design of a 2-Bit Neural Network Quantizer for Laplacian Source”. In: *Entropy* 23 (2021), p. 933. DOI: 10.3390/e23080933. URL: http://hdl.handle.net/10993/47940.

[61] Julien Polge, Sankalp Ghatpande, Sylvain Kubler, Jérémy Robert, and Yves Le Traon. “BlockPerf: A Hybrid Blockchain Emulator/Simulator Framework”. In: *IEEE Access* 9 (2021), pp. 107858–107872. DOI: 10.1109/ACCESS.2021.3101044. URL: http://hdl.handle.net/10993/47953.

[62] Timothée Riom, Delwende Donald Arthur Sawadogo, Kevin Allix, Tegawendé François D Assise Bissyande, Naouel Moha, and Jacques Klein. "Revisiting the VCCFinder approach for the identification of vulnerability-contributing commits". In: *Empirical Software Engineering* 26 (2021). DOI: 10.1007/s10664-021-09944-w. URL: http://hdl.handle.net/10993/47035.

[63] Jordan Samhi, Kevin Allix, Tegawendé François D Assise Bissyande, and Jacques Klein. "A First Look at Android Applications in Google Play related to Covid-19". In: *Empirical Software Engineering* (2021). DOI: 10.1007/s10664-021-09943-x. URL: http://hdl.handle.net/10993/46245.

[64] Jordan Samhi and Alexandre Bartel. "On The (In)Effectiveness of Static Logic Bomb Detector for Android Apps". In: *IEEE Transactions on Dependable and Secure Computing* (2021). DOI: 10.1109/TDSC.2021.3108057. URL: http://hdl.handle.net/10993/48098.

[65] Sandra Schmitz and Stefan Schiffner. "Don't Tell Them now (or at all) – Responsible Disclosure of Security Incidents under NIS Directive and GDPR". In: *International Review of Law, Computers and Technology* 35 (2021). DOI: 10.1080/13600869.2021.1885103. URL: http://hdl.handle.net/10993/46908.

[66] Sandra Schmitz and Stefan Schiffner. "Responsible Vulnerability Disclosure under the NIS 2.0 Proposal". In: *Journal of Intellectual Property, Information Technology and E-Commerce Law* 12 (2021). URL: http://hdl.handle.net/10993/50281.

[67] Hichem Sedjelmaci, Sidi Mohammed Senouci, Nirwan Ansari, and Abdelwahab Boualouache. "A Trusted Hybrid Learning Approach to Secure Edge Computing". In: *IEEE Consumer Electronics Magazine* (2021). DOI: 10.1109/MCE.2021.3099634. URL: http://hdl.handle.net/10993/50279.

[68] Joshgun Sirajzade. "Review of: Romain Hilgert (ed.): Michel Rodange, Renert: De Fuuss am Frack an a Maansgréisst. Komplett Editioun mat historeschen a politeschen Explicatioune, Lëtzebuerg: Éditions Guy Binsfeld, 2020". In: *Hemecht: Zeitschrift für Luxemburger Geschichte* 73 (2021), pp. 377–378. URL: http://hdl.handle.net/10993/52783.

[69] Alexander Steen and Christoph Benzmüller. "Extensional Higher-Order Paramodulation in Leo-III". In: *Journal of Automated Reasoning* 65 (2021), pp. 775–807. DOI: 10.1007/s10817-021-09588-x. URL: http://hdl.handle.net/10993/46727.

[70] Borce Stojkovski, Ruba Abu-Salma, Karen Triquet, and Gabriele Lenzini. ""Unless One Does the Research, It May Seem as Just a Useless Battery-Consuming App" - Field Notes on COVID-19 Contact Tracing Applications". In: *Digital Threats: Research and Practice* (2021). DOI: 10.1145/3480466. URL: http://hdl.handle.net/10993/49489.

[71] Daniel Stolfi Rosso, Matthias R. Brust, Grégoire Danoy, and Pascal Bouvry. "UAV-UGV-UMV Multi-Swarms for Cooperative Surveillance". In: *Frontiers in Robotics and AI* 8 (2021), p. 5. DOI: 10.3389/frobt.2021.616950. URL: http://hdl.handle.net/10993/49680.

[72] Daniel H. Stolfi, Matthias R. Brust, Grégoire Danoy, and Pascal Bouvry. "A competitive Predator–Prey approach to enhance surveillance by UAV swarms". In: *Applied Soft Computing* 111 (2021), p. 107701. DOI: 10.1016/j.asoc.2021.107701. URL: http://hdl.handle.net/10993/49053.

[73] Daniel H. Stolfi, Matthias R. Brust, Grégoire Danoy, and Pascal Bouvry. "CONSOLE: intruder detection using a UAV swarm and security rings". In: *Swarm Intelligence* 15 (2021), pp. 205–235. DOI: 10.1007/s11721-021-00193-7. URL: http://hdl.handle.net/10993/49054.

[74] Cui Su and Jun Pang. "CABEAN: a software for the control of asynchronous Boolean networks". In: *Bioinformatics* 36 (2021), pp. 879–881. DOI: 10.1093/bioinformatics/btaa752. URL: http://hdl.handle.net/10993/47170.

[75] Cui Su, Jun Pang, and Soumya Paul. "Towards optimal decomposition of Boolean networks". In: *IEEE/ACM Transactions on Computational Biology and Bioinformatics* 18 (2021), pp. 2167–2176. DOI: 10.1109/TCBB.2019.2914051. URL: http://hdl.handle.net/10993/48940.

[76] Ningyuan Sun and Jean Botev. "Intelligent Autonomous Agents and Trust in Virtual Reality". In: *Computers in Human Behavior Reports* (2021). DOI: 10.1016/j.chbr.2021.100146. URL: http://hdl.handle.net/10993/48544.

[77] Xiaoyu Sun, Li Li, Tegawendé François D Assise Bissyande, Jacques Klein, Damien Octeau, and John C. Grundy. "Taming Reflection: An Essential Step Toward Whole-program Analysis of Android Apps". In: *ACM Transactions on Software Engineering and Methodology* 30 (2021), pp. 1–36. DOI: 10.1145/3440033. URL: http://hdl.handle.net/10993/49407.

[78] Thierry Titcheu Chekam, Mike Papadakis, Maxime Cordy, and Yves Le Traon. "Killing Stubborn Mutants with Symbolic Execution". In: *ACM Transactions on Software Engineering and Methodology* 30 (2021), 19:1–19:23. DOI: 10.1145/3425497. URL: http://hdl.handle.net/10993/44339.

[79] V. Javier Traver, Luis A. Leiva, Vicente Martí-Centelles, and Rubio-Magnieto Jenifer. "Educational Videogame to Learn the Periodic Table: Design Rationale and Lessons Learned". In: *Journal of Chemical Education* (2021). DOI: 10.1021/acs.jchemed.1c00109. URL: http://hdl.handle.net/10993/47545.

[80] V. Javier Traver, Judith Zorío, and Luis A. Leiva. "Glimpse: A Gaze-Based Measure of Temporal Salience". In: *Sensors* 21 (2021). DOI: 10.3390/s21093099. URL: http://hdl.handle.net/10993/46987.

[81] Ion Turcanu, Thomas Engel, and Christoph Sommer. "Adaptive Content Seeding for Information-Centric Networking under High Topology Dynamics: Where You Seed Matters". In: *IEEE Vehicular Technology Magazine* 16 (2021). DOI: 10.1109/MVT.2021.3050728. URL: http://hdl.handle.net/10993/45417.

[82] A. Uka, A. Ndreu Halili, X. Polisi, Ali Osman Topal, G. Imeraj, and N. E. Vrana. "Basis of Image Analysis for Evaluating Cell Biomaterial Interaction Using Brightfield Microscopy". In: *Cells Tissues Organs* 210 (2021), pp. 77–104. DOI: 10.1159/000512969. URL: http://hdl.handle.net/10993/49656.

[83] Piergiorgio Vitello, Andrea Capponi, Claudio Fiandrino, Guido Cantelmo, and Dzmitry Kliazovich. “Mobility-Driven and Energy-Efficient Deployment of Edge Data Centers in Urban Environments”. In: *IEEE Transactions on Sustainable Computing* (2021). DOI: 10.1109/TSUSC.2021.3056621. URL: http://hdl.handle.net/10993/46403.

[84] Piergiorgio Vitello, Richard Connors, and Francesco Viti. “The Impact of SARS-COVID-19 Outbreak on European Cities Urban Mobility”. In: *Frontiers in Future Transportation* (2021). URL: http://hdl.handle.net/10993/49566.

[85] Deheng Yang, Kui Liu, Dongsun Kim, Anil Koyuncu, Kisub Kim, Haoye Tian, et al. “Where were the repair ingredients for Defects4j bugs?” In: *Empirical Software Engineering* 26 (2021), pp. 1–33. URL: http://hdl.handle.net/10993/49399.

[86] Yanjie Zhao, Li Li, Haoyu Wang, Haipeng Cai, Tegawendé François D Assise Bissyande, Jacques Klein, et al. “On the Impact of Sample Duplication in Machine Learning based Android Malware Detection”. In: *ACM Transactions on Software Engineering and Methodology* 30 (2021), pp. 1–38. URL: http://hdl.handle.net/10993/49372.

A.4 Conference Papers

[87] Mathieu Acher, Gilles Perrouin, and Maxime Cordy. “BURST: a benchmarking platform for uniform random sampling techniques”. In: *SPLC ’21: 25th ACM International Systems and Software Product Line Conference, Leicester, United Kindom, September 6-11, 2021, Volume B*. ACM, 2021, pp. 36–40. DOI: 10.1145/3461002.3473070. URL: http://hdl.handle.net/10993/49465.

[88] Marharyta Aleksandrova and Oleg Chertov. “Impact of model-agnostic nonconformity functions on efficiency of conformal classifiers: an extensive study”. In: *Proceedings of Machine Learning Research*. Vol. 152. Microtome Publishing, 2021. URL: http://hdl.handle.net/10993/49344.

[89] Yusuf Arslan, Kevin Allix, Lisa Veiber, Cedric Lothritz, Tegawendé François D Assise Bissyande, Jacques Klein, et al. “A Comparison of Pre-Trained Language Models for Multi-Class Text Classification in the Financial Domain”. In: *Companion Proceedings of the Web Conference 2021 (WWW ’21 Companion), April 19–23, 2021, Ljubljana, Slovenia*. Association for Computing Machinery, 2021, pp. 260–268. ISBN: 9781450383134. DOI: 10.1145/3442442.3451375. URL: http://hdl.handle.net/10993/47288.

[90] Niloofar Asadi, Farzaneh Gholami-Boroujeni, Bishwajit Gogoi, Sofie Iommi, Michele Jamrozik, Panagiotis Karakatsanis, et al. “Global land dampness characterization using reflectometry by students (GOLDCREST): mission and CubeSat design”. In: *Proceedings of the 12th European CubeSat symposium*. 2021. URL: http://hdl.handle.net/10993/49677.

[91] Andrea Baiocchi, Ion Turcanu, Nikita Lyamin, Katrin Sjöberg, and Alexey Vinel. “Age of Information in IEEE 802.11p”. In: *17th IFIP/IEEE International Symposium on Integrated Network Management (IM): ITAVT Workshop*. 2021. URL: http://hdl.handle.net/10993/46583.

[92] Andrea Baiocchi, Ion Turcanu, and Alexey Vinel. “To Buffer or Not To Buffer: IEEE 802.11p/bd Performance Under Different Buffering Strategies”. In: *33 Edition of International Teletraffic Congress (ITC), Avignon, France, August 31st - September 3rd 2021*. 2021. URL: http://hdl.handle.net/10993/47774.

[93] Sevdenur Baloglu, Sergiu Bursuc, Sjouke Mauw, and Jun Pang. “Election Verifiability Revisited: Automated Security Proofs and Attacks on Helios and Belenios”. In: *IEEE 34th Computer Security Foundations Symposium, Dubrovnik 21-25 June 2021*. IEEE Computer Society, 2021. ISBN: 978-1-7281-7607-9. DOI: 10.1109/CSF51468.2021.00019. URL: http://hdl.handle.net/10993/45565.

[94] Sevdenur Baloglu, Sergiu Bursuc, Sjouke Mauw, and Jun Pang. “Provably Improving Election Verifiability in Belenios”. In: *Electronic Voting 6th International Joint Conference, E-Vote-ID 2021 Virtual Event, October 5–8, 2021, Proceedings*. Springer, 2021, pp. 1–16. ISBN: 978-3-030-86941-0. URL: http://hdl.handle.net/10993/48238.

[95] Sevdenur Baloglu, Sergiu Bursuc, Sjouke Mauw, and Jun Pang. “Provably Improving Election Verifiability in Belenios”. In: *Electronic Voting 6th International Joint Conference, E-Vote-ID 2021 Virtual Event, October 5–8, 2021, Proceedings*. Springer, 2021, pp. 1–16. ISBN: 978-3-030-86941-0. URL: http://hdl.handle.net/10993/48245.

[96] Jim Jean-Pierre Barthel, Marc Beunardeau, Razvan Rosie, Rajeev Anand Sahu, Huang Qiong, and Yu Yu. “Partitioned Searchable Encryption”. In: *Provable and Practical Security, 15th International Conference, ProvSec 2021, Guangzhou, November 5 – November 8, 2021, Proceedings*. Springer, 2021, pp. 63–79. ISBN: 978-3-030-90401-2. DOI: 10.1007/978-3-030-90402-9_4. URL: http://hdl.handle.net/10993/47997.

[97] Jim Jean-Pierre Barthel, Volker Müller, Razvan Rosie, Huang Qiong, and Yu Yu. “On the (M)iNTRU assumption in the integer case”. In: *Provable and Practical Security, 15th International Conference, ProvSec 2021, Guangzhou, November 5 – November 8, 2021, Proceedings*. Springer, 2021, pp. 190–211. ISBN: 978-3-030-90401-2. DOI: 10.1007/978-3-030-90402-9_11. URL: http://hdl.handle.net/10993/47990.

[98] Jim Jean-Pierre Barthel, Razvan Rosie, Huang Qiong, and Yu Yu. “NIKE from Affine Determinant Programs”. In: *Provable and Practical Security, 15th International Conference, ProvSec 2021, Guangzhou, November 5 – November 8, 2021, Proceedings*. Springer, 2021, pp. 98–115. ISBN: 978-3-030-90401-2. DOI: 10.1007/978-3-030-90402-9_6. URL: http://hdl.handle.net/10993/47992.

[99] Christoph Benzmüller and David Fuenmayor Pelaez. “Value-oriented Legal Argumentation in Isabelle/HOL”. In: *International Conference on Interactive Theorem Proving (ITP-2021) - Proceedings*. 2021. DOI: 10.4230/LIPIcs.ITP.2021.0. URL: http://hdl.handle.net/10993/49075.

[100] Alexei Biryukov and Aleksei Udovenko. “Dummy Shuffling Against Algebraic Attacks in White-Box Implementations”. In: *Advances in Cryptology – EUROCRYPT 2021*. Ed. by Anne Canteaut and Francois-Xavier Standaert. Springer International Publishing, 2021, pp. 219–248. ISBN: 978-3-030-77886-6. DOI: 10.1007/978-3-030-77886-6_8. URL: http://hdl.handle.net/10993/49462.

[101] Alexei Biryukov, Aleksei Udovenko, and Giuseppe Vitto. “Cryptanalysis of a Dynamic Universal Accumulator over Bilinear Groups”. In: *Topics in Cryptology – CT-RSA 2021*. 2021. DOI: 10.1007/978-3-030-75539-3_12. URL: http://hdl.handle.net/10993/49496.

[102] Kerstin Bongard-Blanchy, Arianna Rossi, Salvador Rivas, Sophie Doublet, Vincent Koenig, and Gabriele Lenzini. “”I am definitely manipulated, even when I am aware of it. It’s ridiculous!” - Dark Patterns from the End-User Perspective”. In: *Proceedings of ACM DIS Conference on Designing Interactive Systems*. ACM, 2021. DOI: 10.1145/3461778.3462086. URL: http://hdl.handle.net/10993/47008.

[103] William Bonnaventure, Ahmed Khanfir, Alexandre Bartel, Mike Papadakis, and Yves Le Traon. “CONFUZZION: A Java Virtual Machine Fuzzer for Type Confusion Vulnerabilities”. In: *IEEE International Conference on Software Quality, Reliability, and Security (QRS), 2021*. 2021. URL: http://hdl.handle.net/10993/48983.

[104] Wilhelmina Maria Botes and Arianna Rossi. “Visualisation Techniques for Consent: Finding Common Ground in Comic Art with Indigenous Populations”. In: *2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. 2021, pp. 292–297. ISBN: 978-1-6654-1491-3. URL: http://hdl.handle.net/10993/48262.

[105] Jean Botev, Knut Drewing, Heiko Hamann, Yara Khaluf, Pieter Simoens, and Argiro Vatakis. “ChronoPilot – Modulating Time Perception”. In: *Proceedings of the 4th IEEE International Conference on Artificial Intelligence and Virtual Reality (AIVR)*. 2021. DOI: 10.1109/AIVR52153.2021.00049. URL: http://hdl.handle.net/10993/48563.

[106] Jean Botev, Christian Grevisse, and Steffen Rothkugel. “Student Response Systems in Remote Teaching”. In: *Proceedings of the 23rd International Conference on Human-Computer Interaction (HCI International)*. 2021. URL: http://hdl.handle.net/10993/46307.

[107] Abdelwahab Boualouache, Ridha Soua, Tang Qiang, and Thomas Engel. “Software-Defined Location Privacy Protection for Vehicular Networks”. In: *Machine Intelligence and Data Analytics for Sustainable Future Smart Cities*. Springer, 2021. ISBN: 978-3-030-72064-3. URL: http://hdl.handle.net/10993/46666.

[108] Xavier Boyen, Thomas Haines, and Johannes Mueller. “Epoque: Practical End-to-End Verifiable Post-Quantum-Secure E-Voting”. In: *IEEE European Symposium on Security and Privacy, EuroS&P 2021, Vienna, Austria, September 6-10, 2021*. 2021. URL: http://hdl.handle.net/10993/49302.

[109] Lukas Brückner, Ioannis Arapakis, and Luis A. Leiva. "When Choice Happens: A Systematic Examination of Mouse Movement Length for Decision Making in Web Search". In: *Proceedings of the International ACM SIGIR Conference on Research and Development in Information Retrieval (SIGIR)*. 2021. DOI: 10.1145/3404835.3463055. URL: http://hdl.handle.net/10993/46986.

[110] Davide Calvaresi, Giovanni Ciatto, Amro Najjar, Reyhan Aydogan, Leon van der Torre, Andrea Omicini, et al. "Expectation: Personalized Explainable Artificial Intelligence for Decentralized Agents with Heterogeneous Knowledge". In: *Explainable and Transparent AI and Multi-Agent Systems - Third International Workshop, EXTRAAMAS 2021, Virtual Event, May 3-7, 2021, Revised Selected Papers*. Springer, 2021, pp. 331–343. DOI: 10.1007/978-3-030-82017-6_20. URL: http://hdl.handle.net/10993/49904.

[111] Jan Camenisch, Maria Dubovitskaya, and Alfredo Rial. "Concise UC Zero-Knowledge Proofs for Oblivious Updatable Databases". In: *2021 34th IEEE Computer Security Foundations Symposium*. 2021. URL: http://hdl.handle.net/10993/39423.

[112] Luan Cardoso Dos Santos and Johann Groszschädl. "An Evaluation of the Multi-Platform Efficiency of Lightweight Cryptographic Permutations". In: *Innovative Security Solutions for Information Technology and Communications 14th International Conference, SECITC 2021, Virtual Event, November 25-26, 2021, Revised Selected Papers*. Ed. by Peter Y A Ryan and Cristian Toma. Springer Verlag, 2021, pp. 70–85. ISBN: 978-3-031-17509-1. DOI: 10.1007/978-3-031-17510-7_6. URL: http://hdl.handle.net/10993/52367.

[113] Jinsheng Chen, Beishui Liao, Leon van der Torre, Pietro Baroni, Christoph Benzmüller, and Yì N. Wáng. "Base Argumentation as an Abstraction of Deductive Argumentation". In: *Logic and Argumentation - 4th International Conference, CLAR 2021, Hangzhou, China, October 20-22, 2021, Proceedings*. Springer, 2021, pp. 468–476. ISBN: 978-3-030-89390-3. DOI: 10.1007/978-3-030-89391-0_26. URL: http://hdl.handle.net/10993/49909.

[114] Hao Cheng, Georgios Fotiadis, Johann Groszschädl, Peter Y A Ryan, and Peter Roenne. "Batching CSIDH Group Actions using AVX-512". In: *IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES)*. Vol. 2021. Ruhr-Universität Bochum, 2021, pp. 618–649. DOI: 10.46586/tches.v2021.i4.618-649. URL: http://hdl.handle.net/10993/49349.

[115] Hao Cheng, Johann Groszschädl, Peter Roenne, and Peter Y A Ryan. "AVRNTRU: Lightweight NTRU-based Post-Quantum Cryptography for 8-bit AVR Microcontrollers". In: *2021 Design, Automation and Test in Europe Conference and Exhibition, DATE 2021, Grenoble, France, February 1-5, 2021, Proceedings*. IEEE, 2021, pp. 1272–1277. ISBN: 978-3-9819263-5-4. DOI: 10.23919/DATE51398.2021.9474033. URL: http://hdl.handle.net/10993/49346.

[116] Thibaud Comelli, Frederic Pinel, and Pascal Bouvry. “Comparing elementary cellular automata classifications with a convolutional neural network”. In: *Proceedings of International Conference on Agents and Artificial Intelligence (ICAART)*. 2021. URL: http://hdl.handle.net/10993/46102.

[117] Jean-Sébastien Coron and Lorenzo Spignoli. “Secure Wire Shuffling in the Probing Model”. In: *Crypto 2021*. 2021. URL: http://hdl.handle.net/10993/48507.

[118] Aditya Shyam Shankar Damodaran and Alfredo Rial. “Unlinkable Updatable Hiding Databases and Privacy-Preserving Loyalty Programs”. In: *Proceedings on Privacy Enhancing Technologies*. Vol. 2021. Sciendo, 2021, pp. 95–121. DOI: 10.2478/popets-2021-0039. URL: http://hdl.handle.net/10993/49090.

[119] Nadia Daoudi, Jordan Samhi, Abdoul Kader Kabore, Kevin Allix, Tegawendé François D Assise Bissyande, and Jacques Klein. “DexRay: A Simple, yet Effective Deep Learning Approach to Android Malware Detection Based on Image Representation of Bytecode”. In: *Communications in Computer and Information Science*. Springer, 2021. DOI: 10.1007/978-3-030-87839-9_4. URL: http://hdl.handle.net/10993/48789.

[120] Jérémie Dauphin, Tjitze Rienstra, and Leon van der Torre. “New Weak Admissibility Semantics for Abstract Argumentation”. In: *International Conference on Logic and Argumentation*. 2021, pp. 112–126. URL: http://hdl.handle.net/10993/48743.

[121] Gabriel Duflo, Grégoire Danoy, El-Ghazali Talbi, and Pascal Bouvry. “A Q-Learning Based Hyper-Heuristic for Generating Efficient UAV Swarming Behaviours”. In: *Intelligent Information and Database Systems - 13th Asian Conference ACIIDS 2021, Phuket, Thailand, April 7-10, 2021, Proceedings*. Springer, 2021, pp. 768–781. DOI: 10.1007/978-3-030-73280-6_61. URL: http://hdl.handle.net/10993/49055.

[122] Christophe Feltus, Qin Ma, Henderik A. Proper, and Pierre Kelsen. “Towards AI Assisted Domain Modeling”. In: *Advances in Conceptual Modeling - ER 2021 Workshops CoMoNoS, EmpER CMLS, St. John’s, NL, Canada, October 18-21, 2021, Proceedings*. Springer, 2021, pp. 75–89. DOI: 10.1007/978-3-030-88358-4_7. URL: http://hdl.handle.net/10993/49725.

[123] Christof Ferreira Torres, Ramiro Camino, and Radu State. “Frontrunner Jones and the Raiders of the Dark Forest: An Empirical Study of Frontrunning on the Ethereum Blockchain”. In: *USENIX Security Symposium, Virtual 11-13 August 2021*. 2021. URL: http://hdl.handle.net/10993/47450.

[124] Christof Ferreira Torres, Antonio Ken Iannillo, Arthur Gervais, and Radu State. “ConFuzzius: A Data Dependency-Aware Hybrid Fuzzer for Smart Contracts”. In: *European Symposium on Security and Privacy, Vienna 7-11 September 2021*. 2021. URL: http://hdl.handle.net/10993/46746.

[125] Christof Ferreira Torres, Antonio Ken Iannillo, Arthur Gervais, and Radu State. “The Eye of Horus: Spotting and Analyzing Attacks on Ethereum Smart Contracts”. In: *International Conference on Financial Cryptography and Data Security, Grenada 1-5 March 2021*. 2021. URL: http://hdl.handle.net/10993/46244.

[126] Christian Franck and Johann Groszschädl. “Optimized Implementation of SHA-512 for 16-bit MSP430 Microcontrollers”. In: *Innovative Security Solutions for Information Technology and Communications 14th International Conference, SECITC 2021, Virtual Event, November 25-26, 2021, Revised Selected Papers*. Ed. by Peter Y A Ryan and Cristian Toma. Springer Verlag, 2021, pp. 86–97. ISBN: 978-3-031-17509-1. DOI: 10.1007/978-3-031-17510-7_7. URL: http://hdl.handle.net/10993/49799.

[127] David Fuenmayor Pelaez and Alexander Steen. “A Flexible Approach to Argumentation Framework Analysis using Theorem Proving”. In: *First International Workshop on Logics for New-Generation Artificial Intelligence*. College Publications, 2021, pp. 18–32. URL: http://hdl.handle.net/10993/47770.

[128] Dov M. Gabbay, Timotheus Kampik, Beishui Liao, Luo Jieting, and Leon van der Torre. “A Brief Introduction to the Shkop Approach to Conflict Resolution in Formal Argumentation”. In: *Logics for New-Generation AI 2021*. College Publications, 2021, pp. 46–62. ISBN: 978-1-84890-373-9. URL: http://hdl.handle.net/10993/49962.

[129] Robert J. van Glabeek, Peter Höfner, and Ross James Horne. “Assuming Just Enough Fairness to make Session Types Complete for Lockfreedom”. In: *36th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS ’21)*. IEEE, 2021, pp. 1–16. DOI: 10.1109/LICS52264.2021.9470531. URL: http://hdl.handle.net/10993/50042.

[130] Ricardo Gonzalez de Oliveira, Indrasen Raghupatruni, Arne Hamman, and Achim Henkel. “Virtual Verification of Cause-Effect Chains in Automotive Cyber-Physical Systems”. In: *21. Internationales Stuttgarter Symposium*. Springer, 2021, p. 12. URL: http://hdl.handle.net/10993/46251.

[131] Johann Groszschädl, Christian Franck, and Zhe Liu. “Lightweight EdDSA Signature Verification for the Ultra-Low-Power Internet of Things”. In: *Information Security Practice and Experience, 16th International Conference, ISPEC 2021, Nanjing, China, December 17–19, 2021, Proceedings*. Ed. by Robert Deng, Feng Bao, Guilin Wang, Jian Shen, Mark Ryan, Weizhi Meng, et al. Springer Verlag, 2021, pp. 263–282. ISBN: 978-3-030-93205-3. DOI: 10.1007/978-3-030-93206-0_16. URL: http://hdl.handle.net/10993/49970.

[132] Guillaume Haben, Sarra Habchi, Mike Papadakis, Maxime Cordy, and Yves Le Traon. “A Replication Study on the Usability of Code Vocabulary in Predicting Flaky Tests”. In: *18th International Conference on Mining Software Repositories*. 2021. URL: http://hdl.handle.net/10993/46924.

[133] Thomas Haines and Johannes Mueller. “A Novel Proof of Shuffle: Exponentially Secure Cut-and-Choose”. In: *Information Security and Privacy - 26th Australasian Conference, ACISP 2021, Virtual Event, December 1-3, 2021, Proceedings*. 2021. URL: http://hdl.handle.net/10993/48814.

[134] Thomas Haines and Johannes Mueller. “Optimal Randomized Partial Checking for Decryption Mix Nets”. In: *Information Security and Privacy - 26th Australasian Conference, ACISP 2021, Virtual Event, December 1-3, 2021, Proceedings*. 2021. URL: http://hdl.handle.net/10993/48813.

[135] Weili Han, Dingjie Chen, Jun Pang, Kai Wang, Chen Chen, Dapeng Huang, et al. "Temporal Networks Based Industry Identification for Bitcoin Users". In: *Proceedings of 16th International Conference on Wireless Algorithms, Systems, and Applications (WASA'21)*. Springer, 2021, pp. 108–120. DOI: 10.1007/978-3-030-85928-2_9. URL: http://hdl.handle.net/10993/48111.

[136] Faisal Hawlader, Abdelwahab Boualouache, Sébastien Faye, and Thomas Engel. "Intelligent Misbehavior Detection System for Detecting False Position Attacks in Vehicular Networks". In: *The 2021 IEEE International Conference on Communications (the 4th Workshop on 5G and Beyond Wireless Security)*. 2021. URL: http://hdl.handle.net/10993/46911.

[137] Sviatlana Hoehn and Niko Faradouris. "What does it cost to deploy an XAI system: A case study in legacy systems". In: *Proceedings of EXTRAAMAS 2021*. 2021. DOI: 10.1007/978-3-030-82017-6_11. URL: http://hdl.handle.net/10993/49708.

[138] Sviatlana Hoehn, Sjouke Mauw, and Nicholas Asher. "Examining Linguisic Biases with a Game Teoretic Analysis". In: *Proceedings of the 3rd Multidisciplinary International Symposium on Disinformation in Open Online Media*. Springer, 2021. URL: http://hdl.handle.net/10993/47885.

[139] Ross James Horne, Sjouke Mauw, Semen Yurkov, Antonio Cerone, and Peter Csaba Ölveczky. "Compositional Analysis of Protocol Equivalence in the Applied pi-Calculus Using Quasi-open Bisimilarity". In: *Theoretical Aspects of Computing – ICTAC 2021*. Springer International Publishing, 2021, pp. 235–255. ISBN: 978-3-030-85315-0. DOI: 10.1007/978-3-030-85315-0_14. URL: http://hdl.handle.net/10993/50045.

[140] Nina Hosseini Kivanani, Roberto Gretter, Marco Matassoni, and Giuseppe Daniele Falavigna. "Experiments of ASR-based mispronunciation detection for children and adult English learners". In: *BNAIC/BeneLearn 2021*. BnL, 2021, pp. 203–216. ISBN: 0-2799-2527-X. URL: http://hdl.handle.net/10993/51660.

[141] Hailong Hu and Jun Pang. "Membership Inference Attacks against GANs by Leveraging Over-representation Regions". In: *Proceedings of the 27th ACM SIGSAC Conference on Computer and Communications Security (CCS'21)*. ACM, 2021, pp. 2387–2389. DOI: 10.1145/3460120.3485338. URL: http://hdl.handle.net/10993/48640.

[142] Hailong Hu and Jun Pang. "Stealing Machine Learning Models: Attacks and Countermeasures for Generative Adversarial Networks". In: *Proceedings of the 37th Annual Computer Security Applications Conference (ACSAC'21)*. ACM, 2021, pp. 1–16. DOI: 10.1145/3485832.3485838. URL: http://hdl.handle.net/10993/48864.

[143] Kai Hu, Siwei Sun, Yosuke Todo, Meiqin Wang, and Qingju Wang. "Massive Superpoly Recovery with Nested Monomial Predictions". In: *Advances in Cryptology - ASIACRYPT 2021 - 27th International Conference on the Theory and Application of Cryptology and Information Security Singapore, December 6-10, 2021, Proceedings, Part I*. Springer, 2021, pp. 392–421. DOI: 10.1007/978-3-030-92062-3_14. URL: http://hdl.handle.net/10993/49480.

[144] Qiang Hu, Yuejun Guo, Maxime Cordy, Xie Xiaofei, Wei Ma, Mike Papadakis, et al. "Towards Exploring the Limitations of Active Learning: An Empirical Study". In: *The 36th IEEE/ACM International Conference on Automated Software Engineering*. 2021. URL: http://hdl.handle.net/10993/48351.

[145] Wojciech Jamroga, Wojciech Penczek, and Teofil Sidoruk. "Strategic Abilities of Asynchronous Agents: Semantic Side Effects". In: *Proceedings of AAMAS 2021*. ACM, 2021, pp. 1545–1547. URL: http://hdl.handle.net/10993/48860.

[146] Wojciech Jamroga, Wojciech Penczek, and Teofil Sidoruk. "Strategic Abilities of Asynchronous Agents: Semantic Side Effects and How to Tame Them". In: *Proceedings of KR 2021*. 2021. URL: http://hdl.handle.net/10993/48792.

[147] Timotheus Kampik, Dov M. Gabbay, Davide Calvaresi, Amro Najjar, Michael Winikoff, and Kary Främling. "Explainable Reasoning in Face of Contradictions: From Humans to Machines". In: *Explainable and Transparent AI and Multi-Agent Systems - Third International Workshop, EXTRAAMAS 2021, Virtual Event, May 3-7, 2021, Revised Selected Papers*. Springer, 2021, pp. 280–295. DOI: 10.1007/978-3-030-82017-6_17. URL: http://hdl.handle.net/10993/49966.

[148] Timotheus Kampik, Dov M. Gabbay, Giovanni Sartor, Pietro Baroni, Christoph Benzmüller, and Yiqun Wang. "The Burden of Persuasion in Abstract Argumentation". In: *Logic and Argumentation - 4th International Conference, CLAR 2021 Hangzhou, China, October 20-22, 2021, Proceedings*. Springer, 2021, pp. 224–243. DOI: 10.1007/978-3-030-89391-0_13. URL: http://hdl.handle.net/10993/49965.

[149] Timotheus Kampik, Dov M. Gabbay, Jirina Vejnarová, and Nic Wilson. "The Degrees of Monotony-Dilemma in Abstract Argumentation". In: *Symbolic and Quantitative Approaches to Reasoning with Uncertainty - 16th European Conference, ECSQARU 2021, Prague, Czech Republic September 21-24, 2021, Proceedings*. Springer, 2021, pp. 89–102. DOI: 10.1007/978-3-030-86772-0_7. URL: http://hdl.handle.net/10993/49964.

[150] Emmanuel Kieffer, Frederic Pinel, Thomas Meyer, Georges Gloukoviezoff, Hakan Lucius, and Pascal Bouvry. "Evolutionary Learning of Private Equity Recommitment Strategies". In: *2021 IEEE Symposium Series on Computational Intelligence (SSCI)*. 2021. URL: http://hdl.handle.net/10993/48723.

[151] Emmanuel Kieffer, Frederic Pinel, Thomas Meyer, Georges Gloukoviezoff, Hakan Lucius, and Pascal Bouvry. "Proximal Policy Optimisation for a Private Equity Recommitment System". In: *Springer CCIS series*. 2021. URL: http://hdl.handle.net/10993/48722.

[152] Jacques Klein. "A Journey Through Android App Analysis: Solutions and Open Challenges". In: *International Symposium on Advanced Security on Software and Systems*. ACM, 2021, pp. 1–6. URL: http://hdl.handle.net/10993/49371.

[153] Aleks Knoks. "Moral Principles: Hedged, Contributory, Mixed". In: *Deontic Logic and Normative Systems, 15th International Conference, DEON 2020/2021*. College Publications, 2021, pp. 272–290. ISBN: 978-1-84890-352-4. URL: http://hdl.handle.net/10993/48985.

[154] Christiane Kuhn, Dennis Hofheinz, Andy Rupp, and Thorsten Strufe. "Onion Routing with Replies". In: *Advances in Cryptology - ASIACRYPT 2021 - 27th International Conference on the Theory and Application of Cryptology and Information Security Singapore, December 6-10, 2021, Proceedings, Part II*. Springer, 2021, pp. 573–604. DOI: 10.1007/978-3-030-92075-3_20. URL: http://hdl.handle.net/10993/50222.

[155] Damian Kurpiewski, Witold Pazderski, Wojciech Jamroga, and Yan Kim. "STV+Reductions: Towards Practical Verification of Strategic Ability Using Model Reductions". In: *Proceedings of AAMAS*. ACM, 2021, pp. 1770–1772. URL: http://hdl.handle.net/10993/49342.

[156] Luis A. Leiva, Ioannis Arapakis, and Costas Iordanou. "My Mouse, My Rules: Privacy Issues of Behavioral User Profiling via Mouse Tracking". In: *Proceedings of ACM SIGIR Conference on Human Information Interaction and Retrieval (CHIIR)*. 2021. DOI: 10.1145/3406522.3446011. URL: http://hdl.handle.net/10993/46879.

[157] Luis A. Leiva, Sunjun Kim, Wenzhe Cui, Xiaojun Bi, and Antti Oulasvirta. "How We Swipe: A Large-scale Shape-writing Dataset and Empirical Findings". In: *Proceedings of the ACM International Conference on Human-Computer Interaction with Mobile Devices and Services (MobileHCI)*. 2021. DOI: 10.1145/3447526.3472059. URL: http://hdl.handle.net/10993/47546.

[158] Qian Li, Zhichao Wang, Gang Li, Jun Pang, and Guandong Xu. "Hilbert Sinkhorn Divergence for Optimal Transport". In: *Proceedings of 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition - CVPR'21*. IEEE, 2021, pp. 3835–3844. URL: http://hdl.handle.net/10993/47974.

[159] Tomer Libal and Tereza Novotna. "Towards Transparent Legal Formalization". In: *Explainable and Transparent AI and Multi-Agent Systems*. 2021. URL: http://hdl.handle.net/10993/53271.

[160] Yonhui Liu, Li Li, Pingfan Kong, Xiaoyu Sun, and Tegawendé François D Assise Bissyande. "A First Look at Security Risks of Android TV Apps". In: *A First Look at Security Risks of Android TV Apps*. 2021. URL: http://hdl.handle.net/10993/49671.

[161] Cedric Lothritz, Kevin Allix, Bertrand Lebichot, Lisa Veiber, Tegawendé François D Assise Bissyande, and Jacques Klein. "Comparing MultiLingual and Multiple MonoLingual Models for Intent Classification and Slot Filling". In: *26th International Conference on Applications of Natural Language to Information Systems*. Springer, 2021, pp. 367–375. DOI: 10.1007/978-3-030-80599-9_32. URL: http://hdl.handle.net/10993/47529.

[162] Qin Ma, Monika Kaczmarek-Heß, and Sybren De Kinderen. “Validation and Verification in Domain-Specific Modeling Method Engineering”. In: *The Practice of Enterprise Modeling - 14th IFIP WG 8.1 Working Conference, PoEM 2021, Riga, Latvia, November 24-26, 2021, Proceedings*. Springer, 2021, pp. 119–133. DOI: 10.1007/978-3-030-91279-6_9. URL: http://hdl.handle.net/10993/49727.

[163] Wei Ma, Chekam Thierry Titcheu, Mike Papadakis, and Mark Harman. “MuDelta: Delta-Oriented Mutation Testing at Commit Time”. In: *International Conference on Software Engineering (ICSE)*. 2021. URL: http://hdl.handle.net/10993/46742.

[164] Tieu Long Mai and Nicolas Navet. “Improvements to Deep-Learning-based Feasibility Prediction of Switched Ethernet Network Configurations”. In: *The 29th International Conference on Real-Time Networks and Systems (RTNS2021)*. 2021. URL: http://hdl.handle.net/10993/46241.

[165] Ovidiu-Cristian Marcu, Alexandru Costan, Bogdan Nicolae, and Gabriel Antonin. “Virtual Log-Structured Storage for High-Performance Streaming”. In: *2021 IEEE International Conference on Cluster Computing (CLUSTER)*. 2021, pp. 135–145. DOI: 10.1109/Cluster48925.2021.00046. URL: http://hdl.handle.net/10993/50836.

[166] Réka Markovich, Amro Najjar, and Leon van der Torre. “New-Generation AIs Reasoning about Norms and Values”. In: *Logics for New-Generation AI 2021*. 2021. URL: http://hdl.handle.net/10993/50009.

[167] Réka Markovich and Olivier Roy. “A Logical Analysis of Freedom of Thought”. In: *Deontic Logic and Normative Systems*. College Publications, 2021. ISBN: 978-1-84890-352-4. URL: http://hdl.handle.net/10993/49937.

[168] Réka Markovich and Olivier Roy. “Cause of Action and the Right to Know”. In: *Legal Knowledge and Information Systems*. 2021. ISBN: 978-1-64368-252-5. URL: http://hdl.handle.net/10993/49967.

[169] Réka Markovich and Olivier Roy. “Formalizing the Right to Know – Epistemic Rights as Normative Positions”. In: *Logics for New-Generation AI 2021*. 2021. ISBN: 978-1-84890-373-9. URL: http://hdl.handle.net/10993/49938.

[170] Cédric Mauclair, Marina Gutiérrez, Jörn Migge, and Nicolas Navet. “Do We Really Need TSN in Next-Generation Helicopters? Insights From a Case-Study”. In: *2021 AIAA/IEEE 40th Digital Avionics Systems Conference (DASC)*. IEEE, 2021. URL: http://hdl.handle.net/10993/48093.

[171] Chao Niu, Muzhou Li, Meiqin Wang, Qingju Wang, and Siu-Ming Yiu. “Related-Tweak Impossible Differential Cryptanalysis of Reduced-Round TweAES”. In: *Selected Areas in Cryptography - SAC 2021 - 24th International Conference, Ottawa, ON, Canada, September 29 - October 01, 2021, Revised Selected Papers*. 2021, pp. xxx–xxx. URL: http://hdl.handle.net/10993/49483.

[172] Ludovica Paseri, Sébastien Varrette, and Pascal Bouvry. “Protection of Personal Data in High Performance Computing Platform for Scientific Research Purposes”. In: *Proc. of the EU Annual Privacy Forum (APF) 2021*. Springer International Publishing, 2021, pp. 123–142. ISBN: 978-3-030-76662-7. DOI: 10.1007/978-3-030-76663-4_7. URL: http://hdl.handle.net/10993/47114.

[173] Lisha Qiao, Yiqi Shen, Liuwen Yu, Beishui Liao, Leon van der Torre, and Jieting Luo. “Arguing coalitions in abstract argumentation”. In: *Logics for New-Generation AI 2021*. College Publications, 2021. ISBN: 978-1-84890-373-9. URL: http://hdl.handle.net/10993/49902.

[174] Yihao Qin, Shangwen Wang, Kui Liu, Xiaoguang Mao, and Tegawendé François D Assise Bissyande. “On the Impact of Flaky Tests in Automated Program Repair”. In: *28th IEEE International Conference on Software Analysis, Evolution and Reengineering, Hawaii 9-12 March 2021*. 2021, pp. 295–306. ISBN: 978-1-7281-9630-5. DOI: 10.1109/SANER50967.2021.00035. URL: http://hdl.handle.net/10993/50217.

[175] Ahmad Rida, Ridha Soua, and Thomas Engel. “A Near-Field-based TPMS Solution for Heavy Commercial Vehicle Environement”. In: *2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall) proceedings*. 2021. URL: http://hdl.handle.net/10993/49477.

[176] Ahmad Rida, Ridha Soua, and Thomas Engel. “A Near-Field-based TPMS Solution for Heavy Commercial Vehicle Environement”. In: *2021 IEEE 94th Vehicular Technology Conference - Final Program*. 2021. URL: http://hdl.handle.net/10993/49878.

[177] Ahmad Rida, Ridha Soua, and Thomas Engel. “Evaluation of TPMS Signal Propagation in a Heavy Commercial Vehicle Environement”. In: *2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall) proceedings*. 2021. URL: http://hdl.handle.net/10993/49478.

[178] Benoit Ries, Nicolas Guelfi, and Benjamin Jahic. “An MDE Method for Improving Deep Learning Dataset Requirements Engineering using Alloy and UML”. In: *Proceedings of the 9th International Conference on Model-Driven Engineering and Software Development*. SCITEPRESS, 2021, pp. 41–52. ISBN: 978-989-758-487-9. DOI: 10.5220/0010216600410052. URL: http://hdl.handle.net/10993/45161.

[179] François Robinet and Raphaël Frank. “Refining Weakly-Supervised Free Space Estimation through Data Augmentation and Recursive Training”. In: *Proceedings of BNAIC/BeneLearn 2021*. 2021. URL: http://hdl.handle.net/10993/48622.

[180] Arianna Rossi and Gabriele Lenzini. “Which Properties has an Icon? A Critical Discussion on Evaluation Methods for Standardised Data Protection Iconography”. In: *Proceedings of the 8th Workshop on Socio-Technical Aspects in Security and Trust (STAST)*. Springer, 2021. URL: http://hdl.handle.net/10993/41862.

[181] Jordan Samhi, Alexandre Bartel, Tegawendé François D Assise Bissyande, and Jacques Klein. "RAICC: Revealing Atypical Inter-Component Communication in Android Apps". In: *43rd International Conference on Software Engineering (ICSE)*. 2021. DOI: 10.1109/ICSE43902.2021.00126. URL: http://hdl.handle.net/10993/46080.

[182] Cristiana Santos, Arianna Rossi, Lorena Sanchez Chamorro, Kerstin Bongard, and Ruba Abu-Salma. "Cookie Banners, What's the Purpose? Analyzing Cookie Banner Text Through a Legal Lens". In: *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (CCS '21)*. ACM, 2021. URL: http://hdl.handle.net/10993/48253.

[183] Sandra Schmitz and Stefan Schiffner. "Don't Put the Cart Before the Horse – Effective Incident Handling Under GDPR and NIS Directive". In: *Privacy and Identity Management*. Ed. by Michael Friedewald, Stefan Schiffner, and Stephan Krenn. Springer, 2021, pp. 3–17. ISBN: 978-3-030-72465-8. DOI: 10.1007/978-3-030-72465-8. URL: http://hdl.handle.net/10993/48012.

[184] Wazen Shbair, Eugene Gavrilov, and Radu State. "HSM-based Key Management Solution for Ethereum Blockchain". In: *IEEE International Conference on Blockchain and Cryptocurrency, 3-6 May 2021*. 2021. URL: http://hdl.handle.net/10993/46760.

[185] Maciej Skorski, Alessandro Temperoni, and Martin Theobald. "Revisiting Weight Initialization of Deep Neural Networks". In: *Proceedings of Machine Learning Research*. PMLR, 2021, pp. 1192–1207. URL: http://hdl.handle.net/10993/53910.

[186] Abiodun Solanke, Xihui Chen, and Yunior Ramírez-Cruz. "Pattern Recognition and Reconstruction: Detecting Malicious Deletions in Textual Communications". In: *2021 IEEE International Conference on Big Data (Big Data), Orlando, FL, USA, 15-18 December 2021*. 2021. URL: http://hdl.handle.net/10993/50414.

[187] Alexander Steen. "Goal-Directed Decision Procedures for Input/Output Logics". In: *Deontic Logic and Normative Systems: 15th International Conference (DEON 2020/2021)*. Ed. by Alessandra Marra, Fenrong Liu, Paul Portner, and Frederik Van De Putte. College Publications, 2021. URL: http://hdl.handle.net/10993/43591.

[188] Anthony Stein, Sven Tomforde, Jean Botev, and Peter R. Lewis. "Lifelike Computing Systems". In: *Proceedings of the Lifelike Computing Systems Workshop (LIFELIKE)*. 2021. URL: http://hdl.handle.net/10993/48590.

[189] Borce Stojkovski and Gabriele Lenzini. "A workflow and toolchain proposal for analyzing users' perceptions in cyber threat intelligence sharing platforms". In: *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*. IEEE, 2021, pp. 324–330. ISBN: 978-1-6654-0285-9. DOI: 10.1109/CSR51186.2021.9527903. URL: http://hdl.handle.net/10993/48787.

[190] Borce Stojkovski, Gabriele Lenzini, and Vincent Koenig. “”I Personally Relate It to the Traffic Light”: A User Study on Security & Privacy Indicators in a Secure Email System Committed to Privacy by Default”. In: *Proceedings of the 36th Annual ACM Symposium on Applied Computing*. Association for Computing Machinery, 2021, pp. 1235–1246. ISBN: 9781450381048. DOI: 10.1145/3412841.3441998. URL: http://hdl.handle.net/10993/46937.

[191] Borce Stojkovski, Gabriele Lenzini, Vincent Koenig, and Salvador Rivas. “What’s in a Cyber Threat Intelligence sharing platform?: A mixed-methods user experience investigation of MISP”. In: *Annual Computer Security Applications Conference (ACSAC ’21)*. ACM, 2021, pp. 385–398. ISBN: 978-1-4503-8579-4. DOI: 10.1145/3485832.3488030. URL: http://hdl.handle.net/10993/48192.

[192] Daniel Stolfi Rosso, Mathias Brust, Grégoire Danoy, and Pascal Bouvry. “Improving Pheromone Communication for UAV Swarm Mobility Management”. In: *ICCCI 2021: Computational Collective Intelligence*. 2021, pp. 228–240. DOI: 10.1007/978-3-030-88081-1_17. URL: http://hdl.handle.net/10993/53507.

[193] Daniel H. Stolfi, Matthias R. Brust, Grégoire Danoy, and Pascal Bouvry. “Improving Pheromone Communication for UAV Swarm Mobility Management”. In: *13th International Conference on Computational Collective Intelligence (ICCCI 2021)*. Springer, 2021, pp. 228–240. DOI: 10.1007/978-3-030-88081-1_17. URL: http://hdl.handle.net/10993/49057.

[194] Daniel H. Stolfi, Matthias R. Brust, Grégoire Danoy, and Pascal Bouvry. “Optimising pheromone communication in a UAV swarm”. In: *GECCO ’21: Genetic and Evolutionary Computation Conference, Companion Volume, Lille, France, July 10-14, 2021*. ACM, 2021, pp. 323–324. DOI: 10.1145/3449726.3459526. URL: http://hdl.handle.net/10993/49056.

[195] David D Streit. “Experiments in Causality and STIT”. In: *Proceedings of the First International Workshop on Logics for the New Generation Artificial Intelligence*. 2021. URL: http://hdl.handle.net/10993/49838.

[196] Cui Su and Jun Pang. “CABEAN 2.0: Efficient and Efficacious Control of Asynchronous Boolean Networks”. In: *Proceedings of the 24th International Symposium on Formal Methods (FM 2021)*. Springer, 2021, pp. 581–598. DOI: 10.1007/978-3-030-90870-6_31. URL: http://hdl.handle.net/10993/48570.

[197] Ningyuan Sun and Jean Botev. “Virtual Agent Representation for Critical Transactions”. In: *Proceedings of the 12th ACM Multimedia Systems Conference (MMSys)*. 2021. URL: http://hdl.handle.net/10993/47056.

[198] Ningyuan Sun and Jean Botev. “Why Do We Delegate to Intelligent Virtual Agents? Influencing Factors on Delegation Decisions”. In: *Proceedings of the 9th International Conference on Human-Agent Interaction (HAI)*. 2021. DOI: 10.1145/3472307.3484680. URL: http://hdl.handle.net/10993/48543.

[199] Tiezhu Sun, Nadia Daoudi, Kevin Allix, and Tegawendé François D Assise Bissyande. “Android Malware Detection: Looking beyond Dalvik Bytecode”. In: *2021 36th IEEE/ACM International Conference on Automated Software Engineering Workshops (ASEW)*. 2021. URL: http://hdl.handle.net/10993/48892.

[200] Amal Tawakuli, Daniel Kaiser, and Thomas Engel. “Synchronized Preprocessing of Sensor Data”. In: *2020 IEEE International Conference on Big Data*. IEEE, 2021, pp. 3522–3531. DOI: 10.1109/BigData50022.2020.9377900. URL: http://hdl.handle.net/10993/46665.

[201] Kashyap Todi, Gilles Bailly, Luis A. Leiva, and Antti Oulasvirta. “Adapting User Interfaces with Model-based Reinforcement Learning”. In: *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI)*. 2021. DOI: 10.1145/3411764.3445497. URL: http://hdl.handle.net/10993/46877.

[202] Kashyap Todi, Luis A. Leiva, Daniel Buschek, Pin TIan, and Antti Oulasvirta. “Conversations with GUIs”. In: *Proceedings of the ACM Conference on Designing Interactive Systems (DIS)*. 2021. DOI: 10.1145/3461778.3462124. URL: http://hdl.handle.net/10993/46985.

[203] Ion Turcanu, Andrea Baiocchi, Nikita Lyamin, and Alexey Vinel. “An Age-Of-Information Perspective on Decentralized Congestion Control in Vehicular Networks”. In: *19th Mediterranean Communication and Computer Networking Conference, Online Conference, 15-17 June 2021*. 2021. DOI: 10.1109/MedComNet52149.2021.9501273. URL: http://hdl.handle.net/10993/47266.

[204] Georgios Varisteas, Raphaël Frank, and François Robinet. “RoboBus: A Diverse and Cross-Border Public Transport Dataset”. In: *Proceedings of the 19th International Conference on Pervasive Computing and Communications (PerCom 2021)*. 2021. URL: http://hdl.handle.net/10993/47032.

[205] Sébastien Varrette, Emmanuel Kieffer, Frederic Pinel, Ezhilmathi Krishnasamy, Sarah Peter, Hyacinthe Cartiaux, et al. “RESIF 3.0: Toward a Flexible & Automated Management of User Software Environment on HPC facility”. In: *ACM Practice and Experience in Advanced Research Computing (PEARC’21)*. Association for Computing Machinery (ACM), 2021. DOI: 10.1145/3437359.3465600. URL: http://hdl.handle.net/10993/47115.

[206] Itzel Vazquez Sandoval, Arash Atashpendar, Gabriele Lenzini, and Peter Y A Ryan. “PakeMail: Authentication and Key Management in Decentralized Secure Email and Messaging via PAKE”. In: *E-Business and Telecommunications - 17th International Conference on E-Business and Telecommunications, ICETE 2020, Online Event, July 8-10, 2020, Revised Selected Papers*. Ed. by Mohammad S. Obaidat and Jalel Ben-Othman. Springer, 2021, pp. 102–128. DOI: 10.1007/978-3-030-90428-9_5. URL: http://hdl.handle.net/10993/48788.

[207] Liuwen Yu, Dongheng Chen, Lisha Qiao, Yiqi Shen, Leon van der Torre, Meghyn Bienvenu, et al. “A Principle-based Analysis of Abstract Agent Argumentation Semantics”. In: *Proceedings of the 18th International Conference on Principles of Knowledge Representation and Reasoning, KR 2021, Online event, November 3-12, 2021*. IJCAI Organization, 2021,

pp. 629–639. ISBN: 978-1-956792-99-7. DOI: 10.24963/kr.2021/60. URL: http://hdl.handle.net/10993/49903.

[208] Liuwen Yu, Mirko Zichichi, Amro Najjar, Réka Markovich, Luis A. Leiva, Cedric Pruski, et al. "Argumentation in Trust Services within a Blockchain Environment". In: *Proceedings of the 33rd Benelux Conference on Artificial Intelligence and the 30th Belgian Dutch Conference on Machine Learning (BNAIC/BENELEARN 2021)*. 2021, pp. 1–21. URL: http://hdl.handle.net/10993/50021.

[209] Jingtang Zhang, Kui Liu, Dongsun Kim, Li Li, Zhe Liu, Jacques Klein, et al. "Revisiting Test Cases to Boost Generate-and-Validate Program Repair". In: *IEEE International Conference on Software Maintenance and Evolution (ICSME)*. 2021, pp. 1–12. URL: http://hdl.handle.net/10993/49374.

[210] Liyi Zhou, Kaihua Qin, Christof Ferreira Torres, Duc v Le, and Arthur Gervais. "High-Frequency Trading on Decentralized On-Chain Exchanges". In: *IEEE Symposium on Security and Privacy, 23-27 May 2021*. 2021. URL: http://hdl.handle.net/10993/46939.

[211] Teng Zhou, Kui Liu, Li Li, Zhe Liu, Jacques Klein, and Tegawendé François D Assise Bissyande. "SmartGift: Learning to Generate Practical Inputs for Testing Smart Contracts". In: *IEEE International Conference on Software Maintenance and Evolution (ICSME)*. IEEE, 2021, pp. 1–12. URL: http://hdl.handle.net/10993/49373.

[212] Marie-Laure Zollinger, Ehsan Estaji, Peter Y A Ryan, and Karola Marky. ""Just for the sake of transparency": Exploring Voter Mental Models Of Verifiability". In: *Electronic Voting, Sixth International Joint Conference, E-Vote-ID 2021, Bregenz, Austria, October 5-8*. 2021. URL: http://hdl.handle.net/10993/47769.

A.5 Theses

[213] Nikolaos Antoniadis. "Enhancing Smart Grid Resilience and Reliability by Using and Combining Simulation and Optimization Methods". PhD thesis. University of Luxembourg, Luxembourg, Luxembourg, 2021. URL: http://hdl.handle.net/10993/47433.

[214] Elona Dupont. "Generating 3D Dances From Music Using Deep Neural Networks". MA thesis. University of Luxembourg, Luxembourg, 2021. URL: http://hdl.handle.net/10993/50481.

[215] Federico Galli. "Algorithmic business and EU law on fair trading". PhD thesis. University of Luxembourg, Luxembourg, 2021. URL: http://hdl.handle.net/10993/50697.

[216] Jun Gao. "Mining App Lineages: A Security Perspective". PhD thesis. University of Luxembourg, Luxembourg, 2021. URL: http://hdl.handle.net/10993/45462.

[217] Giulio Giorgione. "Dynamic Pricing Strategies in the Carsharing Business, Profit Maximization and Equity Considerations". PhD thesis. University of Luxembourg, Luxembourg, 2021. URL: http://hdl.handle.net/10993/48080.

[218] Kisub Kim. “Steps Towards Semantic Code Search”. PhD thesis. University of Luxembourg, Luxembourg, Luxembourg, 2021. URL: http://hdl.handle.net/10993/47704.

[219] Pingfan Kong. “Taming Android App Crashes”. PhD thesis. University of Luxembourg, Luxembourg City, Luxembourg, 2021. URL: http://hdl.handle.net/10993/46741.

[220] Augusto Wladimir de La Cadena Ramos. “Multipath Routing on Anonymous Communication Systems: Enhancing Privacy and Performance”. PhD thesis. University of Luxembourg, Luxembourg, 2021. URL: http://hdl.handle.net/10993/45458.

[221] Valentina Leone. “Legal knowledge extraction in the data protection domain based on ontology design patterns”. PhD thesis. University of Luxembourg, Luxembourg, 2021. URL: http://hdl.handle.net/10993/47854.

[222] Nesryne Mejri. “Face-swap Deepfake Detection Using High-frequency Components”. MA thesis. University of Luxembourg, Luxembourg, Luxembourg, 2021. URL: http://hdl.handle.net/10993/48065.

[223] Luca Notarnicola. “Topics in Computational Number Theory and Cryptanalysis - On Euclidean Lattices, Edwards Curves and Cryptographic Multilinear Maps”. PhD thesis. University of Luxembourg, Luxembourg, 2021. URL: http://hdl.handle.net/10993/48503.

[224] Massimo Notarnicola. “Probabilisitic limit theorems and the geometry of random fields”. PhD thesis. University of Luxembourg, Esch sur Alzette, Luxembourg, 2021. URL: http://hdl.handle.net/10993/48639.

[225] Yamila Omar. “Complex Networks in Manufacturing - Suitability and Interpretation”. PhD thesis. University of Luxembourg, Luxembourg, 2021. URL: http://hdl.handle.net/10993/47799.

[226] Sean Rivera. “Securing Robots: An Integrated Approach for Security Challenges adn Monitoring for the Robotic Operating System”. PhD thesis. University of Luxembourg, Luxembourg, 2021. URL: http://hdl.handle.net/10993/46429.

[227] Renaud Rwemalika. “On the Maintenance of System User Interactive Tests”. PhD thesis. University of Luxembourg, Luxembourg, Luxembourg, 2021. URL: http://hdl.handle.net/10993/48254.

[228] Petra Sala. “Attaques et preuves de sécurité des protocoles d’échange de clés authentifiés”. PhD thesis. University of Luxembourg, Esch-sur-Alzette, Luxembourg, 2021. URL: http://hdl.handle.net/10993/48095.

[229] Nader Samir Labib. “A Distributed Unmanned Aerial Vehicles Traffic Management System”. PhD thesis. University of Luxembourg, Luxembourg, 2021. URL: http://hdl.handle.net/10993/48454.

[230] Khachatur Torchyan. “Enhancing Photovoltaic Hosting Capacity in Distribution Grid via Grid Reconfigurations, PV Droops and Battery Inverter Control”. PhD thesis. University of Luxembourg, Luxembourg, Luxembourg, 2021. URL: http://hdl.handle.net/10993/48736.

A.6 Miscellaneous Writings

[231] Sviatlana Hoehn. *BelElect Dataset*. 2021. DOI: 10.5281/zenodo.5844350. URL: http://hdl.handle.net/10993/49661.

Appendix B

Research Projects

This chapter lists research projects that were ongoing during 2021, and whose principal investigator is a DCS member. It is structured to summarize the projects by funding source.

- EC - Erasmus+ - KA2
- EC - H2020
- EC - H2020 - FET Open
- EIB - STAREBEI
- EU - COST Action
- ESA
- NLnet - NGI - NGI0 PET Fund
- FNR
- FNR and UL
- FNR - AFR
- FNR - AFR PhD
- FNR - Bridges
- FNR - CORE
- FNR - CORE - Core Junior
- FNR - Industrial Fellowships
- FNR - INTER
- FNR - INTER MOBILITY
- FNR - OPEN
- FNR - POC
- FNR - PRIDE
- FNR (Luxembourg)/NCBiR (Poland)
- ONRG - NICOP
- UL
- UL and Esch2022
- UL and External Organisation Funding
- External Organisation Funding
- Undefined Funding Source

B.1 EC - Erasmus+ - KA2 Projects

Modernisation of Higher Education in central Asia through new technologies

https://hiedtec.ecs.uni-ruse.bg/?cmd=gsIndex

Acronym:	HiedTec
Reference:	R-AGR-3536-10
PI:	Thomas ENGEL
Funding:	European Commission - Erasmus+ - Key Action 2: Cooperation for innovation and the exchange of good practices
Budget:	988.773,00 €
Duration:	15 Nov 2018 – 14 Nov 2022
Members:	• Thomas ENGEL (Principal Investigator) • Aurel MACHALEK (Researcher) • Stefanie OESTLUND (Project Coordinator) • Latif LADID (Program Coordinator)
Area:	Communicative Systems
Partners:	• Ala-Too Intenational University • Almaty Technological University • Andijan Machine-Building Institute • Innovativa University of Euroasia • International University for the Humanities and Development • Issykkul State University named after K. Tynystanov • Khorog State University • Kyrgyz State Technical University • L.N.Gumilyov Euroasian National University • Ministry of Education and Science of the Kyrgyz Republic • Ministry of Education and Science of the Rep. of Kazakhstan • Ministry of Education and Science of the Rep. of Tajikistan • Ministry of Education of Turkmenistan Turkmenistan • Ministry of Higher and Secondary specialized education • Oguz Han Engineering and Technology University • State Power Engineering Institute of Turkmenistan • Tajik Technical University • Tashkent State University of Economics • Tashkent University of Information Technology • Technological University of Tajikistan • University of Coimbra

- University of Pavia
- University of Russe

Description

In order to respond to:

- the Digital Transformation of Industries (Industry 4.0), which also requires DIGITAL TRANSFORMATION OF EDUCATION with overtaking pace, the consortium will develop Concepts of adapting the educational system to the digital generation, considering the specific conditions of each of the partner countries;
- the requirement of the EU to give the opportunity for EVERYBODY to learn at ANY time and at ANY place with the help of ANY lecturer, using ANY device - computer, laptop, tablet, phablet, smart phone, etc. the consortium will create Centres for innovative education technologies.

Main project outcomes and products:

- Sustainable academic network for sharing experience and exchange of good practices in the field of innovative educational technologies and didactic models;
- 5 Concepts of adapting the education system to the digital generation - 1 per Partner country (PC);
- 15 Centres for innovative educational technologies - 1 at each PC university;
- 45 active learning classrooms - 3 at each PC university;
- Virtual classrooms - one at each PC university;
- Handbook of implementing innovative educational technologies in PC institutions;
- Courses for trainers for the acquisition of digital skills and learning methods;
- Courses for lecturers for the acquisition of digital skills and learning methods;
- 75 e-Learning courses - 5 at each PC university;
- 75 PowerPoint presentations of lectures, suitable for delivering using interactive electronic white board - 5 at each PC university;
- Cloud-based Virtual Library of the digital educational resources.

Impact:

- The project products will be of benefit for all stakeholders in education:
  - National and university policy-makers in the field of education; ”
  - University academics who are trainers / lecturers / learners;
  - Scientific, economic and social partners.
- The project will help to turn partner universities into innovative universities and to improve the quality of the trained specialists, who are necessary to perform the Digital Transformation of Industries (Industry 4.0).

Results

The HiEdTec project did a major progress in the year 2021. The Universities involved in the project, created base of web-based courses. The courses are

developed, designed for your students and developed in courses from each University´s curricula. They are developed in English, in Russian or native language. A course are published on the web site. University of Luxembourg major contribution led to Compendium of Good Practice in the field of innovative educational technologies and creation of sustainable academic network.

B.2 EC - H2020 Projects

5G HarmoniseD Research and TrIals for serVice Evolution between EU and China

http://5g-drive.eu

Acronym:	5G-Drive
Reference:	R-AGR-3451-10
PI:	Thomas ENGEL
Funding:	European Commission - Horizon 2020
Budget:	5.999.130,00 €
Duration:	1 Sep 2018 – 30 Jun 2021
Members:	• Thomas ENGEL (Principal Investigator) • Anne OCHSENBEIN (Project Coordinator) • Stefanie OESTLUND (Project Coordinator) • Mathieu VIAU-COURVILLE (Project Coordinator) • Latif LADID (Program Coordinator) • Ridha SOUA (Post-Doc) • Aurel MACHALEK (Research and Development Specialist)
Area:	Communicative Systems
Partners:	• BMW AG • Dynniq Finland Oy • ERTICO - ITS • EURESCOM • Hellenic Telecommunications Organization S.A. • Joint Research Centre (JRC) • Mandat International • Martel Consulting • ORION INNOVATIONS PRIVATE COMPANY • Orange Polska Spolka Akcyjna • SMARTNET ANONYMI TOURISTIKI KAI KATASKEVASTIKI ETAIREIA PAROCHIS YPIRESION • Spi

- University of Kent
- University of Surrey
- VTT, Finland
- Vediafi Oy

Description

5G-DRIVE will trial and validate the interoperability between EU & China 5G networks operating at 3.5 GHz bands for enhanced Mobile Broadband (eMBB) and 3.5 & 5.9 GHz bands for V2X scenarios. The key objectives are to boost 5G harmonisation & R&I cooperation between EU & China through strong connected trials & research activities, with a committed mutual support from the China "5G Product R&D Large-scale Trial" project led by China Mobile. To achieve these objectives and to deliver the impact for early 5G adoption, 5G-DRIVE structures its main activities into three pillars. The first one will test and demonstrate the latest 5G key technologies in eMBB and V2X scenarios in pre-commercial 5G networks. 5G-DRIVE will run three extensive trials in Finland, Italy and UK. The Chinese project will run large-scale trials in five cities. These twinned trials aim to evaluate synergies and interoperability issues and provide recommendations for technology and spectrum harmonisation. The second one focuses on researching key innovations in network slicing, network virtualisation, 5G transport network, edge computing and New Radio features to fill gaps between standards and real-world deployment. The third one will push EU-China 5G collaboration at all levels thru extensive dissemination and exploitation actions. The project formed a strong team of mobile operators and industry, including a prominent car manufacturer, SMEs, research institutes and universities. This well-balanced consortium has the necessary skills with an established close cooperation with the Chinese consortium will provide first class expertise to achieve full interoperability of the 5G networks and V2X between the EU and China. 5G-DRIVE is ideally set to instill tremendous impact on the validation of standards and trigger the roll-out of real 5G networks and V2X innovative solutions driving new business opportunities and creating thereby new jobs and brand new business models.

Results

5G-DRIVE aimed at trialing and validating the interoperability between EU & China 5G networks operating at 3.5 GHz bands for enhanced Mobile Broadband (eMBB) and 3.5 & 5.9 GHz bands for vehicle-to-everything communications (V2X) scenarios. The project ended in June 2021 and has achieved most of its objectives and milestones. The project has also delivered exceptional results with significant immediate or potential impact.

In 2021, the SECAN-lab team concluded its active contribution to this project by outstanding contributions exploiting 5G key technologies (software-defined networking (SDN) and multi-access edge computing, Blockchain) for the security and privacy of connected vehicles. We have proposed an SDN-based location privacy protection framework for 5G vehicular networks. This solution out-

lines a global picture of the internal architecture of the SDN controller for a context-aware use of pseudonym-changing strategies. We have also proposed a solution that adds a blockchain layer to provide trusted interaction between vehicles in pseudonym-changing processes (PCPs). More specifically, this solution leverages a consortium blockchain-enabled fog layer and smart contracts to incentivize non-cooperative nodes to change their pseudonyms within PCPs. In addition, this solution exploits a lightweight consensus protocol to provide a scalable blockchain system.

5G for cooperative & connected automated MOBIility on X-border corridors

https://www.5g-mobix.com/

Acronym:	5G-MOBIX
Reference:	R-AGR-3457-10
PI:	Thomas ENGEL
Funding:	European Commission - Horizon 2020
Budget:	21.410.205,15 €
Duration:	1 Nov 2018 – 31 Jul 2022
Members:	• Thomas ENGEL (Principal Investigator) • Anne OCHSENBEIN (Project Coordinator) • Stefanie OESTLUND (Project Coordinator) • Mathieu VIAU-COURVILLE (Project Coordinator) • Latif LADID (Program Coordinator) • Abdelwahab BOUALOUACHE (Post-Doc) • Alessio BUSCEMI (Post-Doc) • Ridha SOUA (Post-Doc) • Ion TURCANU (Post-Doc)
Area:	Communicative Systems
Partners:	• AEVAC - Asociación Española del Vehículo Autónomo Conectado • AKKA Informatique et Systemes • ASELSAN Elektronik Sanayi ve Ticaret A.S. • Aalto Korkeakoulusaatio S.R. • Alsa Grupo, S.L.U. • Associação CCG/ZGDV – Centro de Computação Gráfica • Auto-Estradas Norte Litoral • Ayuntamiento de Vigo • Brisa Inovacao e Tecnologia, S.A. • COSMOTE KINITES TILEPIKOINONIES A.E.

- CTAG - Centro Tecnológico de Automoción de Galicia
- DAIMLER AG
- DEKRA Testing and Certification, S.A.U.
- Dalian Roiland Technology Co.,Ltd
- Dalian University of Technology
- Datang Telecom Technology
- ERTICO - ITS
- Eindhoven University of Technology
- Electronics and Telecommunications Research Institute (ETRI)
- Ericsson Arastirma Gelistirme ve Bilisim Hizmetleri A.S.
- Ericsson Hellas
- FONDATION PARTENARIAL MOV'EOTEC (VeDecoM)
- Ford Otomotiv Sanayi A.S.
- Fraunhofer Gesellschaft
- GT-ARC gemeinnützige GmbH
- Gemeente Helmond
- HERE Global B.V.
- ISEL
- Infraestruturas de Portugal S.A.
- Institute of Automation Shandong Academy of Science
- Institute of Communications and Computer Systems (ICCS)
- Instituto da Mobilidade e dos Transportes, I.P. (IMT)
- Instituto de Telecomunicações
- Intelligent and Connected Vehicles Group, China National Heavy Duty Truck
- Intrasoft International S.A.
- JEFATURA CENTRAL DE TRAFICO
- KPN
- Korea Automotive Technology Institute (KATECH)
- Luxembourg Institute of Science & technology (LIST)
- NEDERLANDSE ORGANISATIE VOOR TOEGEPAST NATUUR-WETENSCHAPPELIJK ONDERZOEK (TNO)
- NOKIA SIEMENS NETWORKS PORTUGAL S.A.
- NOKIA SPAIN S.A.
- National Electric Vehicle Sweden (NEVS)
- SNETICT
- Satellite Applications Catapult Limited
- Sensible 4
- Siemens S.A.
- TASS International
- TIS
- TURKCELL Teknoloji ARGE A.S.
- Technical University of Berlin
- Telefonica
- Universidad de Murcia
- VICOMTECH
- VTT, Finland
- Valeo Schalter und Sensoren GmbH
- WINGS ICT

Description

5G-MOBIX aims at executing CCAM trials along x-border and urban corridors using 5G core technological innovations to qualify the 5G infrastructure and evaluate its benefits in the CCAM context as well as defining deployment scenarios and identifying and responding to standardisation and spectrum gaps. 5G-MOBIX will first define the critical scenarios needing advanced connectivity provided by 5G, and the required features to enable those advanced CCAM use cases. The matching between the advanced CCAM use cases and the expected benefit of 5G will be tested during trials on 5G corridors in different EU countries as well as China and Korea. Those trials will allow running evaluation and impact assessments and defining also business impacts and cost/benefit analysis. As a result of these evaluations and also internation consultations with the public and industry stakeholders, 5GMOBIX will propose views for new business opportunity for the 5G enabled CCAM and recommendations and options for the deployment. Also the 5G-MOBIX finding in term of technical requirements and operational conditions will allow to actively contribute to the standardisation and spectrum allocation activities. 5G-MOBIX will evaluate several CCAM use cases, advanced thanks to 5G next generation of Mobile Networks. Among the possible scenarios to be evaluated with the 5G technologies, 5G-MOBIX has raised the potential benefit of 5G with low reliable latency communication, enhanced mobile broadband, massive machine type communication and network slicing. Several automated mobility use cases are potential candidates to benefit and even more be enabled by the advanced features and performance of the 5G technologies, as for instance, but limited to: cooperative overtake, highway lane merging, truck platooning, valet parking, urban environment driving, road user detection, vehicle remote control, see through, HD map update, media & entertainment.

Results

The 5G-MOBIX project has focused on the worldwide 5G Fora and verticals in the V2X ecosystem to generate some genuine exchange among the leaders of these ecosystems. The project has been very successful at creating, initiating and attracting worldwide 5G Fora executives to work together since 2018.

The 5G Fora chairs or executives have been invited to participate the past 4 IEEE 5G World Forum events where they outline their program of 5G in their countries as well as the 5G for CAM experiences and first results. These events have become a yearly forum for them to meet and compare progress and socialise their views in a genuine search of harmonisations and interoperability to lead 5G to an international success story.

The 5G for CAM program initiative by the PO and UNI.LU became the place to meet all European projects researching in the cross-corridors as well as attracting US and Canadian stakeholders in the 2021 IEEE 5G World forum event.

This dual approach has simplified greatly the communication among them and instil synergies in working together under the neutral umbrella of IEEE 5G

Initiative.

ChronoPilot

Acronym:	ChronoPilot
PI:	Jean BOTEV
Funding:	European Commission - Horizon 2020
Budget:	3.000.000,00 €
Duration:	21 Sep 2021 – 20 Sep 2025
Members:	• Jean BOTEV (Principal Investigator) • Stéven PICARD (Doctoral Candidate)
Area:	Computer Science & ICT Security
Partners:	• Ghent University • Justus-Liebig-University Giessen • Panteion University of Social and Political Sciences • University of Lübeck

Description

The ChronoPilot project aims to investigate time perception in individuals and groups of humans, as well as in hybrid systems consisting of humans and machines, such as software agents and robots. ChronoPilot will explore the different dimensions of time perception, and develop a time modulation toolkit capable of improving both the quality and the process of decision-making. By exploring novel methods in the field of cognitive science, and applying mediated-reality technologies such as virtual/augmented reality (VR/AR) and body sensors to different human sensory channels, ChronoPilot's team will develop innovative approaches to control the plasticity of time perception. We aim at a comprehensive understanding, through modeling of key variables and the interplay of different senses in subjective human time perception. On the basis of fundamental knowledge from psychology, we will develop ChronoPilot—a prototype technology for time modulation—and will be able to extend/compress human subjective time adaptively, whenever required.

Co-creating resIlient and susTaInable food systEms towardS FOOD2030

https://cordis.europa.eu/project/id/101000640/de

Acronym:	CITIES2030
Reference:	R-AGR-3906-10
PI:	Thomas ENGEL
Funding:	European Commission - Horizon 2020
Budget:	11.779.827,25 €
Duration:	1 Oct 2020 – 30 Sep 2021
Members:	• Thomas ENGEL (Principal Investigator) • Stefanie OESTLUND (Program Coordinator) • Marharyta ALEKSANDROVA (Post-Doc) • Abdelwahab BOUALOUACHE (Post-Doc) • Latif LADID (Research and Development Specialist) • Aurel MACHALEK (Research and Development Specialist)

Description

Cities can build sustainable food systems to prevent and reduce food waste, provide decent livelihood opportunities and promote sustainable ways of food production. Cities can also ensure food and nutrition security for all. The EU-funded CITIES2030 project will bring together researchers, entrepreneurs, civil society leaders, cities and all agents of urban food systems and ecosystems (UFSE) to create a structure focussed on the transformation of the way systems produce, transport, supply, recycle and reuse food. A digital twin of the entire system will be created using a blockchain-based data-driven UFSE management platform. The project's goal is to create a future-proof and effective UFSE via a connected structure focussed on the citizen and built on trust, with partners encompassing the entire food system.

Results

The CITIES2030 project aims to connect short food supply chains, gathering cities and regions, consumers, start-ups, and enterprises. With more than 40 involved partners from around Europe, this project aims to improve the resilience and sustainability of the urban food supply chain. Within this project, UNI.LU is involved in the development of several crucial components. In particular, we are working on a blockchain-based data-driven management platform, security aspects of the digital platform, and data analytical modules.

During the year 2021, the UNI.LU team contributed to both theoretical and practical deliverables of the project. From the theoretical side, UNI.LU worked on advancing the current state-of-the-art research in causal machine learning and conformal learning. We studied the robustness of causal discovery methods to the impact of noise and generated practical recommendations. Also, we demonstrated the relationship between nonconformity metrics and the efficiency of conformal classifiers. This work resulted in 4 peer-reviewed publications, and the generated knowledge will be used in the data analytical components of

the project. From the practical side, UNI.LU contributed to the development of the sentiment analysis component of the project platform. The purpose of this component is to help local authorities to understand if the citizens support current actions or not. This information will be vital for future action planning.

PRACE Sixth Implementation Phase

Acronym:	PRACE-6IP
PI:	Pascal BOUVRY
Funding:	European Commission - Horizon 2020
Budget:	21.305.000,00 €
Duration:	1 Apr 2019 – 30 Sep 2021
Members:	• Pascal BOUVRY (Principal Investigator) • Sébastien VARRETTE (Researcher) • Ezhilmathi KRISHNASAMY (Research Associate)
Areas:	• Computational Sciences • Security, Reliability and Trust in Information Technology • Sustainable Development
Partner:	Forschungszentrum Jülich

Description

This proposal addresses the continuation of support for the world-class pan-European HPC infrastructure PRACE. This includes its further expansion for both academia and industry, while providing state-of-the-art services that can be accessed by users regardless of their location. A unique catalogue of services is provided by PRACE 2 and complemented by the services provided by the PRACE-6IP project. Pooling, integration and rationalisation of European HPC resources will contribute to the EU strategy, and complement the activities of the Public-Private Partnership (PPP) in order to implement the HPC strategy. The Research Infrastructures Work Programme 2018-2020 lists the following key components that PRACE-6IP aims to address: 1. Provide a seamless and efficient Europe-wide Tier-0 service to users; 2. Support software implementations, helping Tier-0 users and communities in adapting and adopting novel software solutions; 3. Collaborate with Centres of Excellence on HPC and other national and EU funded activities that focus on similar or complementary activities for HPC codes and applications; 4. Identify and support new user needs and ensure openness to new user communities and new applications; reach out to scientific and industrial communities, promoting industrial take-up of HPC services in particular by SMEs; 5. Carry out activities that build on national HPC capabilities (Tier-1) and are necessary to support Tier-0 services and a functional European HPC ecosystem; 6. Run training and skills development programmes

tailored to the research needs of academia and industry and relevant public services and transfer of know-how for the use of HPC; Coordinate at European level such programmes in cooperation with the Centres of Excellence on HPC; 7. Implement inclusive and equitable governance and a flexible business model to ensure long term financial sustainability; 8. Support the development of the strategy for the deployment of a rich HPC environment of world-class systems with different machine architectures; 9. Coordinate activities with the European Technology Platform for HPC (ETP4HPC) and the Centres of Excellence in HPC applications in support of the European HPC strategy towards the next generation of computing systems, technologies and applications. 10. Develop an international cooperation policy and associated activities in the area of HPC.

B.3 EC - H2020 - FET Open Projects

ChronoPilot

Acronym:	ChronoPilot
PI:	Jean BOTEV
Funding:	European Commission - Horizon 2020 - Future and Emerging Technologies
Budget:	3.000.000,00 €
Duration:	1 Sep 2021 – 31 Aug 2025
Member:	Jean BOTEV (Principal Investigator)
Area:	Computer Science & ICT Security
Partners:	• Ghent University • Justus-Liebig-University Giessen • Panteion University of Social and Political Sciences • University of Lübeck

Description

The ChronoPilot project aims to investigate time perception in individuals and groups of humans, as well as in hybrid systems consisting of humans and machines, such as software agents and robots. ChronoPilot will explore the different dimensions of time perception, and develop a time modulation toolkit capable of improving both the quality and the process of decision-making. By exploring novel methods in the field of cognitive science, and applying mediated-reality technologies such as virtual/augmented reality (VR/AR) and body sensors to different human sensory channels, ChronoPilot's team will develop innovative approaches to control the plasticity of time perception. We aim at a comprehensive understanding, through modeling of key variables and the interplay of different senses in subjective human time perception. On the basis of

fundamental knowledge from psychology, we will develop ChronoPilot—a prototype technology for time modulation—and will be able to extend/compress human subjective time adaptively, whenever required.

B.4 EIB - STAREBEI Projects

Toward A.I. Recommitment Strategies for ESG integration in Private Equity

https://pcog.uni.lu/stairs/

Acronym:	STAIRS
PI:	Pascal BOUVRY
Funding:	European Investment Bank - STAges de REcherche BEI-EIB research internships
Duration:	1 Jan 2021 – 31 Aug 2021
Members:	• Pascal BOUVRY (Principal Investigator) • Emmanuel KIEFFER (Researcher)
Area:	Computational Sciences
Partners:	• European Investment bank • Hakan Lucius

Description

The rise of Environmental, Social, and Governance (ESG) factors has been one of the major changes for private equity partners. ESG considerations have redesigned the standards of due diligence and add new objectives on top of financial statements and growth plans. Building private equity portfolios remains a real challenge for limited partners investors with heavy consequences on ESG/Sustainable investments. This lack of guidance is certainly the main barrier to overcome in order to give confidence to investors and encourage investing in innovative and sustainable technologies. Policy makers have tasked institutional investors such as the European Investment Bank (EIB) to invest in a sustainable future for all. Nevertheless, the different objectives, levels of risk aversion, ESG exposure and time-horizons are subject to complex constraints and trade-offs. Under such circumstances, there is a real need to design guidance mechanisms to leverage private equity responsible investments.

Achieving and maintaining high allocation to private equity and keeping allocations at the targeted level through recommitment strategies is a complex task

and needs to be balanced against the risk of becoming a defaulting investor. When looking at recommitments we are quickly faced with a combinatorial explosion of the solution space, rendering explicit enumeration impossible. The multi-objective nature of the recommitment problem creates numerous alternatives that can be difficult to apprehend for investors.

For this reason, investors need guidance and decision aid algorithms producing reliable and robust sustainable and trustworthy recommitment strategies. By trustworthy, we mean intelligible rules for investors and domain experts. Using an optimised AI-assisted system in normal market conditions, strategies are likely to provide more guidance and flexibility while becoming a testbed for extraordinary market conditions. In this project, we propose an innovative approach to generate sustainable and trustworthy recommitment strategies with the aid of AI-based algorithms. Our main attempt is not only to develop an algorithm replacing human strategies but also to design a Sustainable and Trustworthy AI Recommitment System (STAIRS) guiding dynamically the search of recommitment strategies in order to build portfolios of responsible investments. To support all the development and tests, this project will strongly rely on High Performance Computing (HPC) to cope with the computing power requested by such an AI-based system. The use of HPC hardware-accelerated code (e.g. GPU, FPGA, TPU) will be decisive to push back the frontiers of achievable while reducing tremendously the time needed to provide satisfying solutions.

The STAIRS research project will be conducted at the FSTM by Dr. Emmanuel Kieffer, research Scientist in the HPC group, under the supervision of Prof. Dr Pascal Bouvry from the University of Luxembourg and Dr. Hakan Lucius from The European Investment Bank.

Results

The University of Luxembourg and the European Investment Bank (EIB) through the STAREBEI programme have been working together to encourage private equity partners to invest in innovative and sustainable technologies. The research project “Sustainable and Trustworthy Artificial Intelligence Recommitment System (STAIRS)” has been using the capacities of the High Performance Computing (HPC) centre to develop a robust and reliable guidance system.

The project leads to two scientific articles published in peer-reviewed international conferences:

- Proximal Policy Optimisation for a Private Equity Recommitment System [151]
- Evolutionary Learning of Private Equity Recommitment Strategies [150]

B.5 EU - COST Action Projects

Distributed Knowledge Graphs

Acronym:	DKG
PI:	Ross James HORNE
Funding:	European Union - European Cooperation in Science & Technology Action
Duration:	23 Sep 2020 – 22 Sep 2024
Member:	Ross James HORNE (Principal Investigator)

Description

Knowledge Graphs are a flexible way to represent interlinked information about virtually anything. People from a variety of application domains including biomedical research, public and open data, linguistics, journalism, and manufacturing publish, use, and investigate knowledge graphs. As the publication is done in a decentralised fashion across the web, the knowledge graphs form a distributed system.

Due to the ever-increasing uptake of Knowledge Graph technologies in recent years, there are new challenges for research and development including dealing with the scale and the de- gree of distribution of knowledge graphs, while monitoring and maintaining data quality and privacy. Tackling these research challenges will need a stronger collaboration within the research community, and a joint effort to establish a more functional, decentralized Web of Data.

The main aim of the Action is therefore to create a research community for deployable Distributed Knowledge Graph technologies that are standards-based, and open, embrace the FAIR principles, allow for access control and privacy protection, and enable the decentralised publishing of high-quality data. To this end, the Action connects European researchers and practitioners from (1) diverse application domains and (2) the whole life cycle of Distributed Knowledge Graphs, from provisioning to finding, accessing, integrating, programming, deploying, enriching, and analytics. The Action will develop practices for scalable, privacy-respecting, high quality and decentralised Knowledge Graph publication and consumption, reach out to the European industry, and formulate a research agenda.

Results

• Dr. Ross Horne presented on GDPR and the Solid Protocol, MC meeting in Amsterdam, colocated with SEMANTiCS,6-9 September 2021

• Funding approved for Workshops on Privacy Issues in Distributed Social Knowledge Graphs, 13-15 June 2022, at University of Luxembourg, with Ross

Horne as the local organiser

European Network on Future Generation Optical Wireless Communication Technologies

Acronym:	NEWFOCUS
PI:	Thomas ENGEL
Funding:	European Union - European Cooperation in Science & Technology Action
Budget:	4.000.000,00 €
Duration:	1 May 2020 – 30 Apr 2024
Member:	Thomas ENGEL (Principal Investigator)
Area:	Computer Science & ICT Security
Partners:	• (Ben Gurion university of the Negev • (Future Intelligence • (University Ss Cyril and Methodius - Skopje, Republic of Macedonia • Aarhus University • Argotech a.s. • Aristotle University of Thessaloniki • Brno University of Technology • Budapest University of Technology and Economics • Cailabs • Chalmers University of Technology • Czech Technical University in Prague • DAS Photonics, S.L • Delft University of Technology • Ecole Centrale Marseille • Egypt–Japan University of Science and Technology • FUNDACIO PRIVADA I2CAT, INTERNET I INNOVACIO DIGITAL A CATALUNYA • Federal Office of Communications • Ford Otomotiv Sanayi A.S • Fraunhofer - Fraunhofer Heinrich Hertz Institute • German Aerospace Center • Gheorghe Asachi Technical University of Iasi • Harokopio University • Hensoldt Optronics GmbH • Hyperion Technologies • INESC TEC • Innovative Solutions Sławomir Pietrzyk • Institute IRNAS Race • Instituto de Telecomunicações - Instituto de Telecomunicações - Aveiro

- Isocom limited
- KU Leuven
- Kadir Has University
- Lebanese American University
- LightBee S.L
- London South Bank
- Lovefield Wireless GmbH
- MaxLinear Inc - MaxLinear Hispania SL
- McMaster University
- National Institute of Information and Communications Technology
- National Institute of Telecommunications
- Nokia Solutions and Networks GmbH & Co KG
- Northumbria University
- OLEDCOMM
- OMTLAB Research Ltd
- Orange
- Ozyegin University
- Palliser Engineers ltd
- Photonic
- Radio Communications Agency of the Netherlands
- Scuola Superiore Sant'Anna
- Slovak University of Technology
- THE UNIVERSITY OF EDINBURGH
- TU Ilmenau
- Technical University of Sofia
- Technische Universitat Graz
- UNIVERSIDAD CARLOS III DE MADRID
- University of Banja Luka
- University of Cyprus
- University of Luxembourg
- University of Malta
- University of Montenegro
- University of Nis, Faculty of Electronic Engineering
- University of Novi Sad
- University of Tromsø - The Arctic University of Norway
- University of Zagreb
- Università degli Studi Roma Tre
- Vilnius University
- WATGRID
- universidad de Las Palmas de Gran Canaria
- Çankaya University

Description

The design of future wireless communication networks that cope with the ever-growing mobile data traffic as well as support varied and sophisticated services and applications in vertical sectors with a low environmental impact is recognized as a major technical challenge that European engineers face today. The

COST Action NEWFOCUS will propose truly radical solutions with the potential to impact the design of future wireless networks. Particularly, NEWFOCUS aims to establish optical wireless communications (OWC) as an efficient technology that can satisfy the demanding requirements of backhaul and access network levels in beyond 5G networks. This also includes the use of hybrid links that associate OWC with radiofrequency or wired/fiber-based technologies. Towards this vision, NEWFOCUS will carry out a comprehensive research programme under two major pillars. The first pillar is on the development of OWC-based solutions capable of delivering ubiquitous, ultra-high-speed, low-power consumption, highly secure, and low-cost wireless access in diverse application scenarios. The developed solutions will in particular support Internet-of-Things (IoT) for smart environments with applications in vertical sectors. The second pillar concerns the development of flexible and efficient backhaul/fronthaul OWC links with low latency and compatible with access traffic growth. In addition to scientific and technological advances, NEWFOCUS will serve as a global networking platform through capacity building of all relevant stakeholders including universities, research institutions, major industry players, small medium enterprises, governmental bodies and non-governmental organisations. Within this rich consortium, NEWFOCUS will train experts to accompany related European industries for the standardisation and commercialization of the OWC technology.

European Research Network on Formal Proofs

Acronym:	EuroProofNet
PI:	Matteo ACCLAVIO
Funding:	European Union - European Cooperation in Science & Technology Action
Duration:	11 Oct 2021 – 10 Oct 2025
Member:	Matteo ACCLAVIO (Principal Investigator)

Description

If testing can reveal errors in computer programs, only formal verification can guarantee their absence. The highest Evaluation Assurance Levels of the Common Criteria for Information Technology Security Evaluation require automatically checked mathematical proofs of correct- ness. Proofs are also the basis of mathematics and many sciences, and thus are very important in education and research.

In many computer technologies, developers and users rely on standard languages and proto- cols for exchanging data and enabling tool interoperability: TCP/IP for network communication, HTML for web pages, etc. This is however not the case for formal proofs, which is a major bot- tleneck for their adoption by the industry. The main reason is that, currently, proof systems use

14mutually incompatible logical foundations. Fortunately, only small parts of the proofs developed in a system use features that are incompatible with other systems.

Europe is a leading actor in the area of formal proofs: about 65% of the proof systems of the world are developed in Europe, including the two most used proof assistants, Coq and Isabelle. This Action aims at boosting the interoperability and usability of proof systems and making

formal proofs enter a new era. For the first time, it gathers all the developers and users of proof systems in Europe. To make the proofs exchangeable, they will express, in a common logical framework, the logical foundations of their systems and develop tools for inter-translation of the proofs developed in individual systems to and from this common logical framework.

B.6 ESA Projects

Autonomous trustworthy monitoring and diagnosis of CubeSat health

Acronym:	ATMonSAT
PI:	Andrzej MIZERA
Funding:	European Space Agency
Duration:	1 May 2021 – 31 Oct 2022
Member:	Andrzej MIZERA (Principal Investigator)
Area:	Information Security

Description

The objective is to harness state-of-the-art explainable AI and operating system technology to build in an additional layer of dependability, accountability and intelligence between the critical core of a CubeSat and the environment it controls. Our initial evaluation found current operating systems deployed on CubeSats, e.g., FreeRTOS, are not fit for a future in which Launching States increasingly transfer liability for collisions resulting from failures or even cyber attacks to CubeSat Operators. We propose a novel solution that is verified, hence dependable, and which builds auditable real-time anomaly detection and overall health monitoring into the critical core of a CubeSat.

More precisely, this project will result in a framework with the following contributions, which required us to balance the key requirements of verifiability and adaptability:

(A) Trustworthy auditing of system health for post-disaster diagnostics. We will develop a method for automated root-cause analysis for disasters (e.g., tum-

bling and collisions), leveraging the diverse I/O used to maintain a Cubesat. We anticipate insurers will re- quire such an analysis to resolve liability disputes, e.g., to prove that a fault is not due to negligence during CubeSat development and operations.

(B) A hardware-isolated, dependable layer for autonomous disaster recovery. Instead of a set of hard-coded rules for disaster recovery, we will develop suitable AI mechanisms for onboard data analysis that take all I/O into account (not only telemetry). The framework must also adapt to unforeseen scenarios based on new data. Such a mechanism can make swift decisions in response to unexpected failures and perceived risks. Hardware-isolation ensures that monitors cannot be tampered with even when control software is compromised.

Autonomous trustworthy monitoring and diagnosis of CubeSat health

Acronym:	ESA Open Discovery Ideas
PI:	Andrzej MIZERA
Funding:	European Space Agency
Duration:	1 May 2021 – 31 Oct 2022
Member:	Andrzej MIZERA (Principal Investigator)

Description

The objective of this project is to harness state-of-the-art explainable AI and operating system technology to build in an additional layer of dependability, accountability and intelligence between the critical core of a CubeSat and the environment it controls. The initial evaluation found current operating systems deployed on CubeSats, e.g., FreeRTOS, are not fit for a future in which Launching States increasingly transfer liability for collisions resulting from failures or even cyber-attacks to CubeSat Operators. In this project, we propose a novel solution that is verified, hence dependable, and which builds auditable real-time anomaly detection and overall health monitoring into the critical core of a CubeSat.

B.7 NLnet - NGI - NGI0 PET Fund Projects

Dining Cryptographer Networks

https://dcnets.readthedocs.io/

Acronym:	DCnets
Reference:	R-AGR-3956-10
PI:	Christian FRANCK
Funding:	NLnet Foundation - Next Generation Internet - NGI Zero Privacy Enhancing Technologies
Budget:	25.000,00 €
Duration:	10 Apr 2020 – 31 Dec 2021
Members:	• Christian FRANCK (Principal Investigator) • Johann GROSZSCHÄDL (Researcher) • Rubaiya BEGUM (Collaborator)

Description

Software Library for implementing DCnets. Kindly supported by NLnet. Budget mainly used for student jobs.

B.8 FNR Projects

PhotoBooth

Acronym:	PhotoBooth
PI:	Christoph SCHOMMER
Funding:	Fonds National de la Recherche
Budget:	50.000,00 €
Duration:	15 Jan 2021 – 31 Dec 2021
Members:	• Christoph SCHOMMER (Principal Investigator) • Amro NAJJAR (Project Coordinator) • Sana NOUZRI (Project Coordinator)
Partner:	LuxAI

Description

Artificial Intelligence (AI) is no longer only part of science fiction. In recent years, the rapid rise of AI has been simultaneously stunning, promising, sometimes disappointing —and could also be perceived as scary. Views on AI are diverging from experts claiming ”Fear artificial stupidity, not artificial intelligence!” to prominent scientists (e.g. Stephen Hawking) raising their voice to the grave dangers AI could cause to our very existence. What is certain, that AI-driven technologies are part of our everyday life and the more we democratise the knowledge on these technologies the better we are equipped to look for answers both as a society and as individuals.
To start with, AI is symptomatic of the Fourth Industrial Revolution and is the most important of several disruptive technologies. There is a clear need for clarity and understanding of what AI entails today, in order to demystify it and comprehend its impact on our lives, and also, to understand and mitigate its risks.

A group of AI researchers and science communicators have teamed up to develop a playful and interactive intelligent machine - the SMART PHOTO BOOTH - where the users can experiment with AI and learn about how intelligent machines are trained.

The Smart Photo Booth is designed to guide the user to engage with an AI algorithm via manipulating images. Our photo booth will be similar to an interactive Snapchat filter, allowing the user to generate their very own digital portrait in a chosen style of a specific art movement. Hence, the Smart Photo Booth will be very intuitive and appealing to the general public and particularly for teenagers, it is the perfect medium to teach AI, not only for those who are already technology drawn, but also to publics of diverging interests, backgrounds and gender.

The Smart Photo Booth will be adapted and presented in two different venues: a) Space 1 - workshops in the Scienteens Lab at UL for STEM (science, technology, engineering and mathematics) high school students in Luxembourg (April-July 2021); b) Space 2 - permanent exhibition in the Luxembourg Science Center for a wide range of audiences - children, teenagers, and families (August - December 2021). In 2022 we plan to have the Smart Photo Booth exhibited for the whole year in the AI & Art Pavilion.

The Pavilion, supported by the Esch 2022 European Capital of Culture, will be providing various interactive programs and a series of exhibitions for all kinds of visitors for the duration of Esch 2022.

To implement this project, we have an interdisciplinary team of computer scientists and artists, and are partnering with different organizations for the dissemination strategy: the Scienteens Lab (https://wwwen.uni.lu/lcsb/scienteens_lab), the Luxembourg Science Center (https://www.science-center.lu/) and the European Capital of Culture Esch2022 (https://esch2022.lu/en). By partnering with successful and established ‘science in society’ initiatives we ensure proper dissemination of the project. Plus, it will allow for the sustainability of the project beyond this proposal.

Securing Time Critical Traffic in (next gen) Automotive Networks

https://vehicularlab.uni.lu/project/setica/

Acronym:	SETICA
Reference:	R-AGR-3969-10+20
PI:	Thomas ENGEL
Funding:	Fonds National de la Recherche
Budget:	567.481,00 €
Duration:	1 Jun 2021 – 31 May 2024
Members:	• Thomas ENGEL (Principal Investigator) • Stefanie OESTLUND (Project Coordinator) • Daniel KAISER (Post-Doc) • Ion TURCANU (Post-Doc) • Mahdi FOTOUHI (PhD student)
Area:	Communicative Systems
Partner:	Honda r&d Europe GmbH

Description

Today's vehicles incorporate more and more enhanced services such as ADAS systems, smartphone integration, autonomous driving, connectivity, and entertainment for passengers. Efficient communication is the key to facilitate all these services. So far, in-vehicle communication systems have been designed to allow for very stringent end-to-end delays and deterministic communication requirements. However, they are inflexible, will hardly able to provide the bandwidth needs of future cars, and offer little security.

Contrary to conventional in-vehicle communication systems, Ethernet is flexible and offers high bandwidth. While Time Sensitive Networking (TSN) can guarantee tight end-to-end delays, and MACsec can provide security, there is no profile that consolidates these properties. Developing such an automotive TSN profile, which includes answering challenging research questions and thorough evaluation, is of the essence for future cars in terms of safety and security as well as comfort. The importance of this has been acknowledged by the IEEE which started working on such a profile (802.1DG).

The goal of SETICA is solving the research part of this endeavour as well as developing a realistic security-enabled TSN testbed, which, in turn, will allow thorough realistic evaluation. We plan to especially focus on gPTP, the timing protocol of TSN. The impact of successful attacks against gPTP is severe because

many safety-critical applications depend on timing guarantees. We will also research novel approaches that go beyond 802.1DG, among them leveraging SDN for gaining even more flexibility and security.

SETICA will generate significant value, researching and developing important future technology to be used as key communication technology in vehicles to facilitate future functionalities and services, such as autonomous driving, connected cars, and ADAS functions, which will require all of high bandwidth, precise timing, and security.

Results

In June 2021, we started working on SETICA (SEcuring TIme Critical traffic in (next gen) Automotive networks). SETICA is our new FNR BRIDGES project, which leverages results from our Security Analysis Ethernet Testbed we introduced in last year's report. Together with Honda R&D Europe, we will investigate and develop new communication technology in vehicles in order to facilitate future functionalities and services which will require all of high bandwidth, precise timing, and security.

Today's vehicles incorporate more and more enhanced services such as ADAS systems, smartphone integration, autonomous driving, and entertainment for passengers. Efficient communication is the key to facilitate all these services. So far, in-vehicle communication systems have been designed to support deterministic communication. However, they are inflexible, do not provide the bandwidth needs of future cars, and offer little security.

Contrary to in-vehicle communication systems, Ethernet is flexible and offers high bandwidth. While Time Sensitive Networking (TSN) supports deterministic communication, and MACsec can provide security, there is no profile that consolidates these properties. Developing such an automotive TSN profile is of the essence for future cars in terms of safety, security, and comfort. The goal of SETICA is solving the research part of this endeavour, participating in IEEE 802.1DG standardization, as well as developing a realistic security-enabled TSN testbed.

So far, we worked on pen-testing and security with respect to gPTP, which is TSN's time synchronization protocol. We analysed and implemented attacks against unprotected gPTP. Further, we analysed respective security controls for protecting against these attacks. As a part of this, we are also developing a PTP parsing library focusing on efficient pen-testing capabilities.

B.9 FNR and UL Projects

Approaching Indigenous Australian History With Text Mining Methods

https://www.c2dh.uni.lu/people/ekaterina-kamlovskaya

Acronym:	AIAHTMM
PI:	Christoph SCHOMMER
Funding:	Fonds National de la Recherche, University of Luxembourg
Duration:	1 Jan 2017 – 15 May 2021
Members:	• Christoph SCHOMMER (Principal Investigator) • Ekaterina KAMLOVSKAYA (Doctoral Candidate)
Area:	Intelligent and Adaptive Systems

Description

Despite their remarkable value, autobiographies appear to remain one of the most under-utilized historical resources. The proposed research project in digital humanities will apply computational Distant Reading-methods (natural language processing in general and topic modeling in particular) as a complement to traditional ”close reading” of Indigenous Australian autobiographies, aiming to identify meaningful language use patterns in the context of social environment and historical events. Cooperation Partner: C2DH.

See more at: https://acc.uni.lu/index.php?page=projects

B.10 FNR - AFR Projects

Remote memory attestation and erasure through formal verification

Acronym:	ATTEST
PI:	Sjouke MAUW
Funding:	Fonds National de la Recherche - Aide à la Formation Recherche
Duration:	1 Mar 2020 – 31 Jan 2024

Members:
- Sjouke MAUW (Principal Investigator)
- Reynaldo GIL PONS (AFR PhD Applicant)

Description

Resource-constrained computational devices with Internet connectivity are collectively termed Internet of Things (IoT) devices, and are particularly vulnerable to attacks, as they cannot afford the implementation of proactive defences against malicious code. IoT devices not only become easy targets for hackers but also a useful weapon to launch further attacks on major services. Verifying the integrity of a remote device is essential to maintaining a secure computer network, as malicious or erroneous code could be used, for example, to compromise secrets and escalate privileges remotely. The current practice is to rely on forensic techniques such as memory attestation and erasure protocols. The former verifies the integrity of a device's memory and the latter certifies memory has been erased. Both result in devices without unexpected contents in memory. Current attestation and erasure protocols are restricted to highly controlled environments. Either the protocol needs direct access to the device's hardware, or it requires the device to be isolated from the network. Both restrictions are hard to meet in large-scale networks that exhibit a high level of heterogeneity, such as IoT networks. On the one hand, the area of Security Protocol Analysis produces protocols that resist attackers with full control over the network. On the other hand, memory erasure and attestation protocols are limited in terms of their ability to cope with network attackers, i.e. attackers able to intercept and manipulate network messages. This project will use current experience in developing security protocols and adversary models to make novel memory attestation and erasure protocols resilient against network attackers. To this end, we will identify the limits of memory erasure/attestation protocols in terms of the attacker model and security properties they can cope with, and put forward more robust, efficient and versatile protocols.

B.11 FNR - AFR PhD Projects

Privacy Attacks and Protection in Machine Learning as a Service

Acronym: PriML

PI: Jun PANG

Funding: Fonds National de la Recherche - Aide à la Formation Recherche PhD

Duration: 1 Dec 2019 – 30 Nov 2023

Members:
- Jun PANG (Principal Investigator)
- Hailong HU (Doctoral Candidate)

Description

Machine learning (ML) techniques have gained widespread adoption in a large number of real- world applications. Following the trend, machine learning as a service (MLaaS) is provided by leading Internet companies to broaden and simplify ML model deployment. Although MLaaS only provides black-box access to its customers, recent research has identified several attacks to reveal confidential information about model itself and training data. Along this line, this project's goal is to further investigate new attacks in terms of ML models and training data and develop a systematic, practical and general defense mechanism to enhance the security of ML models. The project team including SaToSS and CISPA will also make source codes publicly available and use them in their own courses. This project will provide a deeper understanding of machine learning privacy, thereby increasing the safety of machine learning-based systems such as authentication system and malware detection, helping protect the nation and its citizens from cyber harm. This project PriML combines multiple novel ideas synergistically, organized into three inter-related research thrusts. The first thrust aims to explore potential attacks from the perspective of ML models via black-box explainable machine learning techniques. The second thrust focuses on investigating new attacks from the perspective of training datasets through DeepSets technique which can mitigate the complexity of deep neural networks and facilitate our attacks. Both thrusts include considering different types of neural networks and identifying inherently distinct properties of these types of attacks respectively. The third thrust involves un- derstanding and finding out a set of invariant properties underlying these attacks and developing defense mechanisms that exploit these properties to provide better protection of ML privacy.

Results

Within 2021, the following papers have been published:

• The poster "Membership inference Attacks against GANs by Leveraging Over-representation Regions" has been published in the Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (CCS '21).

• The paper "Stealing Machine Learning Models: Attacks and Countermeasures for Gener- ative Adversarial Networks" has been published in the Annual Computer Security Appli- cations Conference (ACSAC '21).

B.12 FNR - Bridges Projects

SEcuring TIme Critical traffic in (next gen) Automotive networks

Acronym: SETICA

PI:	Thomas ENGEL
Funding:	Fonds National de la Recherche - Bridges
Budget:	609.127,00 €
Duration:	1 Jun 2021 – 31 May 2024
Member:	Thomas ENGEL (Principal Investigator)
Area:	Computer Science & ICT Security
Partner:	Honda R&D Europe (Deutschland) GmbH

Description

In-vehicle communication systems have been designed to allow for very stringent end-to-end delays and deterministic communication requirements. However, they are inflexible, do not provide the bandwidth needs of future cars, and offer no security. Contrary to in-vehicle communication systems, Ethernet is flexible and offers high bandwidth. While Time Sensitive Ethernet (TSN) can guarantee tight end-to-end delays, and MACsec can provide security on the link layer, there is no profile that consolidates these properties. Developing such an automotive Ethernet profile, which includes answering challenging research questions and thorough evaluation, is of the essence for future cars in terms of safety and security as well as comfort. The importance of this has been acknowledged by the IEEE which started working on such a profile (802.1DG). The goal of SETICA is solving the research part of this endeavour as well as developing a realistic security-enabled TSN testbed, which, in turn, will allow thorough realistic evaluation. We plan to especially focus on gPTP, the timing protocol of TSN. Both attacking gPTP and researching counter measures are an integral part of SETICA. The impact of successful attacks against gPTP is severe because many safety-critical applications depend on timing guarantees. SETICA will also research novel approaches that go beyond 802.1DG, among them leveraging SDN for gaining even more flexibility and security.

B.13 FNR - CORE Projects

Automating the Design of Autonomous Robot Swarms

https://adars.uni.lu

Acronym:	ADARS
PI:	Grégoire DANOY
Funding:	Fonds National de la Recherche - CORE

Budget:	953.000,00 €
Duration:	1 May 2021 – 30 Apr 2024
Members:	• Grégoire DANOY (Principal Investigator) • Florian FELTEN (PhD student) • Daniel STOLFI ROSSO (Research Associate) • Pascal BOUVRY (Scientific Advisor) • Pierre-Yves HOUITTE (Research and Development Specialist) • Sébastien VARRETTE (Senior Researcher)

EnCaViBS

https://encavibs.uni.lu/

Acronym:	EnCaViBS
PI:	Thomas ENGEL
Funding:	Fonds National de la Recherche - CORE
Budget:	969.000,00 €
Duration:	1 Sep 2019 – 31 Aug 2022
Members:	• Thomas ENGEL (Principal Investigator) • Stefan SCHIFFNER (Post-Doc) • Sandra SCHMITZ-BERNDT (Post-Doc) • Aurel MACHALEK (Research and Development Specialist)
Area:	Communicative Systems
Partners:	• Mark Cole • University of Luxembourg, Faculty of Law, Economics and Finance

Description

Today's economy and citizens of the EU by proxy, depend on reliable network and information services. Despite a wide selection of technical protection measures being available, attacks on electronic services are on the rise in number and impact. The EU's response under its Cybersecurity Strategy has been the NIS Directive as a legal instrument aiming to ensure that critical information technology systems in central sectors of the economy are secure. The analysis whether and how the legal requirements under the new framework match software requirements and vice versa, calls for a joint effort of legal and technical experts. The abstract notions of the NIS Directive requirements are in need of clarification so that compliant products can to be derived and developers can be

equipped with guidelines how to meet the legal requirements with the currently available technologies. However, technology and the law evolve with different speeds hence these interpretations and guidelines need to be dynamic.

Objective of EnCaViBS is the creation of a living commentary to the NIS Directive that is accompanied with a methodology to select the appropriate technological and organisational measures for NIS Directive compliant IT products.

For more info and current affairs of the project please visit https://encavibs.uni.lu

Results

EnCaViBS hosted the 16th IFIP Summer School on Privacy and Identity Management, which took place during August 16-20, 2021.The summer school had to be held as a fully virtual event, due to the ongoing COVID-19 pandemic and associated uncertainties. It was a joint effort among IFIP Working Groups 9.2, 9.6/11.7, 11.6, and Special Interest Group 9.2.2, in co-operation with the European Union's cybersecurity competence network pilot projects CyberSec4Europe1, SPARTA2 and CONCORDIA3. The summer school was furthermore supported by Forum Privatheit4 and the EnCaViBS. This IFIP Summer School brought together more than 40 junior and senior researchers. As in previous years, one of the goals of the IFIP Summer School was to encourage the publication of thorough research papers by students and emerging scholars. To this end, 20 early stage researchers presented their work at the virtual conference. Insightful keynote talks were held by Kai Kimpaa (”Ethical social engineering penetration testing – can it be done?”), Sebastian Pape (”Serious Games for Security and Privacy Awareness”), François Thill (”Information Security Risk Management”), and Jakub Čegan (”Training Development in KYPO Cyber Range Platform”). Finally, a total of five workshops and tutorials on topics related to privacy and identity management complemented a diverse and educational program, one of them by our Teammeber Sandra Schmitz (”Are we all on the same page? On establishing a common understanding of the state of the art”

Moreover, the EnCaViBS researchers presented their work on several events. e.g. CPDP, BILETA, Ethics Dialogs and contributed to the consultancy during the review process of the NIS Directive, which influenced the NIS 2 draft.

Give control back to users: personalised privacy-preserving data aggregation from heterogeneous social graphs - resubmission

Acronym:	HETERS
PI:	Sjouke MAUW
Funding:	Fonds National de la Recherche - CORE

Budget: 700.621,00 €

Duration: 1 Mar 2021 – 29 Feb 2024

Member: Sjouke MAUW (Principal Investigator)

Area: Computer Science & ICT Security

Description

Heterogeneous social graphs (HSG) have been widely used to analyse social network data to support decision making. Compared to simple social graphs which only model the relations between users, HSGs capture the heterogeneity nature of social networks in terms of data subjects and relations between them. The richer information encoded in HSGs leads to overwhelming better results than those on simple social graphs. In the meantime, it also imposes more risk of a privacy breach. Due to the potential economic and reputation loss, social network operators only publish a limited amount of HSG data for researchers and third-party data analysts. In this project, we address an alternative decentralised solution for data analysts to collect data of HSGs directly from volunteers while guaranteeing volunteers' privacy. Specifically, users privately calculate and share data about their local views of HSGs. Data analysts aggregate these responses into the information of interest. To the best of our knowledge, no works in the literature exist to achieve this goal. Moreover, we will take into account the fact that in real-life scenarios, users may have different privacy requirements, e.g., due to various trust to data collectors. We design methods for users to perturb their local data according to their own personalised privacy requirements. In this manner, we manage to give control back to users over their data by determining the level of privacy protection. In addition to precise privacy preservation, our methods can also ensure better utility for the aggregated data when only a small number of users require high-level protection. To achieve our purpose, we will first extend the notion of local differential privacy to quantify users' personalised privacy requirements over different types of sensitive information, i.e., vertices and edges. Once the privacy properties have been defined, we will design corresponding privacy-preserving methods for two widely studied data aggregation tasks: query answering and graph synthesis. Query answering is used to aggregate statistics of some structural properties of HSGs while graph synthesis allows data analysts to conduct flexible analysis on synthetic HSGs with similar properties to the original graphs. Last but not least, we will develop a comprehensive evaluation framework to evaluate the effectiveness of our methods and define new measures to quantitatively assess the utility of the aggregated data.

Privacy-preserving Publication of Dynamic Social Network Data in the Presence of Active Adversaries

Acronym: PrivDA

PI:	Yunior RAMIREZ CRUZ
Funding:	Fonds National de la Recherche - CORE
Duration:	1 Jun 2018 – 31 May 2021
Members:	• Yunior RAMIREZ CRUZ (Principal Investigator) • Sjouke MAUW (Supervisor / Scientific Advisor) • Xihui CHEN (Research Associate)
Areas:	• Computer Science & ICT Security • Security, Reliability and Trust in Information Technology

Description

Over the last decade, online social networks (OSNs) have become one of the most popular online services. The analysis of social network data allows social scientists, market analysts, economists, among others, to understand societal phenomena, detect consumption patterns, assess the effect of policies, etc. Likewise, companies and public agencies can benefit from these studies to improve their decision-making processes and social outreach. In order to enable such studies, it is necessary that OSN owners release the necessary information about the network structure. However, given the personal and sensitive nature of the information contained in the network, it is necessary to sanitise the released information, to ensure that the privacy of the individual users is protected.

Adversaries seek to re-identify users and learn sensitive private information about them from the sanitised information releases, such as the existence of relations between users, political affiliation, religious beliefs, etc. To that end, the adversary collects pieces of information that identifies each victim in a unique manner, so when the information is released the victims can be re-identified by matching the adversary knowledge to the released information. So-called active adversaries have the capacity of enrolling sybil nodes in the network, which engage in interactions with the targeted victims in order to create unique structural patterns that can later be used as fingerprints to re-identify the victims and infer private information about them.

In this project, we will focus on providing methods for safely releasing structural information about the social network, accounting for, and counteracting, the presence of active adversaries. Given that social networks are inherently dynamic, and numerous analysis tasks require information on the evolution of the social graph over time, we will focus on techniques allowing to release updates on the structural information as the network evolves. We will first study how the dynamic nature of the networks and the release process can be exploited by active adversaries to strengthen their attacks. Then, considering the new vulnerabilities detected, we will define novel ways to quantify privacy in the dynamic scenario. The new privacy properties will be the basis for new models and algorithms allowing OSN owners to safely release information in two manners: (1) periodically publishing anonymised versions of the dynamic social graph, and (2) answering structural queries about the network. The proposed methods will be incremental, in the sense that as the network evolves

and new information is released, each new piece of information will integrate with the previously released ones in such a manner that the privacy properties are globally satisfied.

Quantum Communication with Deniability

Acronym:	Q-CoDe
PI:	Peter Y A RYAN
Funding:	Fonds National de la Recherche - CORE
Duration:	1 Jul 2018 – 30 Jun 2021
Members:	• Peter Y A RYAN (Principal Investigator) • Jeroen VAN WIER (Doctoral Candidate) • Arash ATASHPENDAR (PhD student) • Dimiter OSTREV (Research Associate) • Peter Browne Roenne (Research Associate)

Description

The goal of this project is to conduct a thorough formal analysis of the promising, but poorly understood field of deniable quantum communication. It will entail a systematic analysis and classification of the quantum primitives that are relevant for deniability, and further give precise definitions of deniability and related concepts in quantum protocols. The results will be both in the form of impossibility, as well as feasibility theorems with corresponding protocols. This will be both in the form of modifying existing QKD protocols to restore deniability, as well as devising new quantum protocols that provide deniability for key exchange and beyond, e.g. for e-voting.

Secure, Quantum-Safe, Practical Voting Technologies

Acronym:	EquiVox
PI:	Peter Y A RYAN
Funding:	Fonds National de la Recherche - CORE
Duration:	1 Apr 2020 – 31 Mar 2023
Members:	• Peter Y A RYAN (Principal Investigator) • Peter ROENNE (Researcher) • Georgios FOTIADIS (Research Associate) • Johannes MUELLER (Research Associate)

Description

Digital information and communication technologies, entrenched in the fabric of modern society, enrich and facilitate our lives. Used carefully, the very same tools can also serve to enrich and protect core mechanisms, such as elections, that are fundamental to the functioning of democratic societies. In effect, elections form the foundations of democracy and as such, ensuring their security is of the utmost importance. One of the major security challenges that ought to be dealt with is the threat posed by the emergence of quantum computers. Despite a considerable number of well-designed secure electronic voting schemes proposed over the past few decades, almost all existing schemes depend on cryptography which will be broken by quantum algorithms. Therefore, the goal of this project is to develop and prototype practical e-voting schemes that are secure against attackers capable of performing arbitrary quantum computations.

Security, Scalability, and Privacy in Blockchain Applications and Smart Contracts

https://www.cryptolux.org/index.php/Projects

Acronym:	FinCrypt
PI:	Alexei BIRYUKOV
Funding:	Fonds National de la Recherche - CORE
Duration:	1 Aug 2018 – 31 Jul 2021
Members:	• Alexei BIRYUKOV (Principal Investigator) • Daniel FEHER (Post-Doc) • Sergei TIKHOMIROV (Post-Doc) • Giuseppe VITTO (PhD student)
Area:	Security, Reliability and Trust in Information Technology

Description

Blockchain technology gathered momentum with the popularity of the Bitcoin cryptocurrency. Being an interesting practical proposal which gained a large community of followers in the last 4 years Bitcoin can be seen as a testbed for ideas in the FinTech area. By now it is clear what Bitcoin ideas can be generalized and are valuable but also what are the shortcomings of the concrete Bitcoin instantiation of a distributed ledger and cryptocurrency. For example, the scalability problem has become vital, as the transaction rate growth made the designers think to increase the block size, which in turn might lead

to higher network latency and vulnerability to various network attacks. Also current proof-of-work based blockchains are very energy intensive. Active research is now happening around greener alternatives for consensus protocols, such as fault-tolerant Byzantine agreement or Proof of Stake which tolerate higher transaction rate and were tested on small networks. The security of blockchain applications with an accent on the data confidentiality is an unsolved problem. So far the blockchain ledger is implicitly public, but users demand more confidentiality for their data. On the other hand governments demand access to blockchain information for AML/KYC policies and taxation. The problem of storing and processing encrypted data on the blockchain as well as privacy vs governance tradeoff remain largely unexplored. One of the most interesting blockchain applications are smart contracts. Whereas the Bitcoin ledger consists of transactions only, a smart contract ledger contains programming code of almost arbitrary complexity, so that sophisticated financial instruments, legal contracts, and reputation systems can be encoded and executed automatically. However, the private character of contracts poses a challenge of concealing the exact functionality while, at the same time, still keeping it verifiable to the other protocol participants. Our proposal is to investigate blockchain applications from both the scalability and confidentiality point of view and to suggest new solutions in this area (Work Package 1) as well as to study the privacy and security aspects of smart contracts and to propose new efficient methods to achieve user privacy and contract confidentiality (Work Package 2).

Results

In 2021, the FinCrypt project team developed a tool for automated truncation of differential trails in symmetric cryptographic algorithms. Truncated Differential Cryptanalysis (TDC) is a variant of differential cryptanalysis (DC) and has been applied successfully against a number of symmetric cryptosystems, including cryptosystems that are used in blockchains, most notably hash functions. Similarly to DC, TDC traces the propagation of differences through multiple rounds of a symmetric algorithm. However, TDC does not analyse full but truncated differences, i.e. differences in which only some of the bits are specified, while the rest are truncated (in the sense of not specified). The tool developed by the FinCrypt team works for cryptosystems that are based on the ARX (i.e. modular Addition, bitwise Rotation, and XOR) approach and takes as input a differential trail. It produces as output a set of truncated differential trails that represents all possible truncations of the input trail according to certain predefined rules. In the course of this work a linear-time algorithm for the exact computation of the differential probability of a truncated trail that follows the truncation rules was proposed. Furthermore, the team found a method to merge the set of truncated trails into a compact set of non-overlapping truncated trails with associated probability and demonstrated the application of the tool on the block cipher Speck64. The team also investigated the effect of clustering of differential trails around a fixed input trail. The best cluster found for 15 rounds has probability $2^{-55.03}$ (consisting of 389 unique output differences), which made it possible to build a distinguisher using 128 times less data than the one based on just the single best trail, which has probability 2^{-62}. Thanks to

this tool, it became possible to show examples for Speck64 where a cluster of trails around a suboptimal (in terms of probability) input trail results in higher overall probability compared to a cluster obtained around the best differential trail.

teSTing sELf-LeARning systems

Acronym:	STELLAR
PI:	Yves LE TRAON
Funding:	Fonds National de la Recherche - CORE
Duration:	1 Sep 2019 – 31 Aug 2022
Members:	• Yves LE TRAON (Principal Investigator) • Maxime CORDY (Researcher) • Mike PAPADAKIS (Researcher)

Description

Self-learning software systems (SLS) are integrated into a variety of domains ranging from safety-critical applications (autonomous cars and healthcare) to business-critical applications (finance, smart factories). Engineering such systems, however, is still a new practice, often not well-understood by engineers, and thus errorprone. It is therefore essential to provide engineers with means to assess that the SLS they build work reliably and as expected. In this project, we aim at complementing state-of-the-art machine-learning evaluation processes with testing techniques specifically adapted to the peculiarities of SLS. Indeed, although a plethora of techniques exists for testing traditional software, these are heavily challenged by SLS, their intrinsic probabilistic nature, their vast number of parameters, and their use cases too numerous to be elicited. More precisely, we focus on testing their underlying learning models and target three objectives: (1) measuring the adequacy of existing test cases with criteria that indicate how well the test cases cover the learning model; (2) defining model transformations (mutations) to modify the models, and estimating their sensitivity; (3) designing differential testing methods to discover disagreements between models, thereby obtaining new test cases that reveal errors in the models. Our three objectives are certainly not independent as fulfilling one will help achieve the others. Thus, altogether they will form a triangular chain of techniques to generate a high-quality test suite for learning models.

B.14 FNR - CORE - Core Junior Projects

Automated Reasoning with Legal Entities

Acronym:	AuReLeE
PI:	Alexander STEEN
Funding:	Fonds National de la Recherche - CORE - Core Junior
Budget:	508.697,00 €
Duration:	1 Dec 2020 – 30 Nov 2022
Member:	Alexander STEEN (Principal Investigator)

Description

The process of compliance checking involves the review and assessment of implemented processes and artefacts with respect to conformance towards normative specifications, e.g., addressing aspects of information security or privacy. Compliance checks may be conducted because of self-imposed quality and security policies, but might also be necessary activities required by external (public) regulators. Since compliance checks are time-consuming and expensive processes in general, there are ongoing endeavours to employ computer-assisted methods that reduce the extent and tasks of human actors in this process. A first step usually taken by these projects is the formalization of normative structures in knowledge bases. However, the utilization of these knowledge bases is still limited. In the AuReLeE project, effective methods for general automation of normative reasoning processes are developed and implemented. To this end, computational decision procedures will be designed. The project will also design and implement a dedicated system that combines the developed decision procedures with a flexible approach to import and re-use existing knowledge bases for their employment as underlying contexts for normative reasoning. AuReLeE is conducted at the University of Luxembourg and will contribute key insights for combining highly efficient reasoning methods with practically usable compliance checking tools.

Automated Reasoning with Legal Entities (AuReLeE)

https://aurelee.net/

Acronym:	AuReLeE
PI:	Alexander STEEN
Funding:	Fonds National de la Recherche - CORE - Core Junior
Duration:	1 Mar 2021 – 1 Feb 2023
Members:	• Alexander STEEN (Principal Investigator) • David FUENMAYOR PELAEZ (Research and Development

Specialist)

Description

The goal of the project Automated Reasoning with Legal Entities (AuReLeE) is to provide effective and general means for the automation of normative reasoning processes based on legal knowledge bases. To this end, the project will design and implement a dedicated system that combines efficient decision procedures with a flexible approach to import and re-use existing knowledge bases for their employment as underlying contexts for the normative reasoning tasks. The results of AuReLeE hence allow the full utilization of the existing legal knowledge bases' potential for compliance checking.

Future-Proofing Privacy in Secure Electronic Voting

Acronym:	FP2
PI:	Johannes MUELLER
Funding:	Fonds National de la Recherche - CORE - Core Junior
Duration:	1 Jan 2021 – 31 Dec 2023
Member:	Johannes MUELLER (Principal Investigator)

Stateful Zero-Knowledge

Acronym:	SZK
PI:	Alfredo RIAL
Funding:	Fonds National de la Recherche - CORE - Core Junior
Duration:	1 Mar 2018 – 28 Feb 2021
Members:	• Alfredo RIAL (Principal Investigator) • Peter Y A RYAN (Local Scientific Advisor)

Description

A zero-knowledge (ZK) proof system allows a prover to prove statements to a verifier without revealing secret information. The goal of this project is to define, construct and analyse protocols for stateful zero-knowledge (SZK). SZK is defined as the task of keeping state information between prover and verifier in a ZK proof system. We view the state as a data structure where the prover stores each piece of data at a certain position.

Our definitions must ensure the following: (1) data in the state is hidden from

the verifier, (2) the prover can read and write data at positions while hiding both the data and the positions, and (3) a piece of data read from the state at a position equals the last piece of data stored at that position.

Our constructions for SZK will allow the prover to prove statements about the positions read or written. We will use SZK as building block in protocols for data collection and analysis, which are useful to protect privacy while allowing the release of statistics about data. These protocols are of interest in a lot of settings, e.g. e-commerce, location-based services and smart metering and billing. Thanks to the strong privacy properties offered by SZK, we will be able to design protocols for tasks that before could not be realized while fully protecting user privacy.

B.15 FNR - Industrial Fellowships Projects

Application of Near Field Technology in Commercial Vehicle Tire Monitoring System

Acronym:	NFT
Reference:	R-AGR-3426-10
PI:	Thomas ENGEL
Funding:	Fonds National de la Recherche - Industrial Fellowships
Budget:	51.000,00 €
Duration:	15 Sep 2018 – 15 Sep 2022
Members:	• Thomas ENGEL (Principal Investigator) • Anne OCHSENBEIN (Project Coordinator) • Stefanie OESTLUND (Project Coordinator) • Mathieu VIAU-COURVILLE (Project Coordinator) • Ahmad RIDA (Doctoral Candidate)
Area:	Communicative Systems
Partner:	Goodyear S.A.

Description

This project addresses the advantages of using near-field based automotive systems in applications where RFID based systems cannot function properly, proposing an automotive tire identification and diagnose system to use on fleet commercial vehicles.

The project will research other capabilities of near-field (NF) technology as a replacement for wire based communication between the tractor and trailer, providing the driver and possibly the control center with crucial information

about tire conditions. This is the first study on the use of NF in automotive safety systems as well as the first automotive application using low frequency NF. It will look at the various advantages of the use of NF in such an application, and possibility extend this research to initiate major innovation in the automotive industry using this technology.

B.16 FNR - INTER Projects

An integrated approach to study the delegation of decision-making to autonomous agents in socio-technicalsystems

Acronym:	DELICIOS
PI:	Jean BOTEV
Funding:	Fonds National de la Recherche - INTER
Budget:	867.141,00 €
Duration:	1 Nov 2019 – 31 Oct 2023
Members:	• Jean BOTEV (Principal Investigator) • Ningyuan SUN (Doctoral Candidate)
Areas:	• Computational Sciences • Security, Reliability and Trust in Information Technology
Partners:	• Ghent University • Vrije Universiteit Brussel

Description

In this age of ubiquitous digital interconnectivity, we may envisage that humans will increasingly delegate their social, economic or data-related transactions to an autonomous agent, for reasons of convenience or complexity. Although the scientific knowledge to create such systems appears to be available, this transformation does not appear to become commonplace soon, except maybe the use of basic digital assistants. We aim to explore if this is due to the lack of knowledge about human trust and acceptance of artificial autonomous delegates that make decisions in their place or even how these delegates should be designed. We study these questions using computational agents models that are validated in a series of behavioural experiments defined around the public goods game. We investigate when and how the autonomous agent may evolve from observer, over decision support to a delegate with full autonomy in decision-making. Using VR and AR technologies, we will investigate if the representation in which the agent is experienced influences trust. All the technology-oriented research is checked against socio-technology acceptance theories through an intricate

collaboration with experts in social sciences. The results of this fundamental research will allow us to explore important questions related to the intelligence and interface of the envisioned agents, and lay the foundation for new types of online markets that brings autonomous agents into real-world applications.

Analysis and Protection of Lightweight Cryptographic Algorithms

https://www.fnr.lu/projects/analysis-and-protection-of-lightweight-cryptographic-algorithms/

Acronym:	APLICA
PI:	Alexei BIRYUKOV
Funding:	Fonds National de la Recherche - INTER
Duration:	1 Jan 2021 – 31 Dec 2023
Members:	• Alexei BIRYUKOV (Principal Investigator) • Johann GROSZSCHÄDL (Researcher) • Anne OCHSENBEIN (Project Coordinator)
Areas:	• Computer Science & ICT Security • Information Security • Security, Reliability and Trust in Information Technology
Partners:	• Gregor Leander • Ruhr-Universität Bochum

Description

The Internet of Things (IoT) represents the next phase of the evolution of the Internet towards a network that integrates the physical world into the virtual world. In the near future, the vast majority of devices connected to the Internet will not be classical computers like PCs, laptops, or smart phones, but miniature sensor nodes, actuators, and various other kinds of “smart” devices with computation and communication capabilities. This evolution will create a strong demand for lightweight cryptographic algorithms that are suitable for devices with extreme resource constraints such as RFID tags. Recently, the US National Institute of Standards and Technology (NIST) announced an initiative to standardize lightweight hash functions and authenticated encryption schemes in an open process with public evaluation. The mission of the APLICA project is to contribute to the evaluation of the more than 50 candidate algorithms submitted to the NIST by analyzing their theoretical and practical security properties. More concretely, APLICA will contribute to the development of new cryptanalytic techniques (including new software tools for cryptanalysis) that can be

applied to lightweight authenticated encryption algorithms and hash functions, and to the design and implementation of new countermeasures against side-channel attacks, in particular differential power analysis, that are suitable for resource-constrained IoT devices. Both topics have the potential to create significant real-world impact since the NIST-standardized algorithms will likely get deployed in billions of devices.

Results

The APLICA project started in January 2021 as a joint research effort between the CryptoLux group of the University of Luxembourg (UL) and the Workgroup for Symmetric Cryptography of the Ruhr-University Bochum (RUB). Its main goals are (i) to evaluate the security of lightweight symmetric cryptosystems, in particular the candidate algorithms (and eventual standards) of the currently-ongoing Lightweight Cryptography (LWC) standardization project of the NIST and (ii) to support the candidates submitted by UL and RUB. The security evaluation takes into account both classical cryptanalysis (i.e., the analysis of the security of an algorithm in a mathematical sense) and their robustness against physical attacks (i.e., analysis under assumption that an attacker can observe certain implementation-related properties of a cryptographic algorithm while it is executed on a device, such as the execution time or power consumption).

In 2021, the APLICA team at UL achieved three major results; the first two are in the area of (classical) cryptanalysis, while the third falls into the area of efficient and secure implementation of lightweight cryptosystems to resist physical attacks. (i) The APLICA team gained new insights into the security of WARP, a lightweight block cipher that can serve as replacement for AES128 without changing the mode of operation. WARP is extremely energy-efficient and currently the smallest 128-bit block cipher in terms of silicon area. The project team developed key-recovery attacks on WARP based on differential cryptanalysis in single and related-key settings. It was demonstrated that searching for differential trails for up to 20 rounds of WARP is possible, with the first 19 having optimal differential probabilities. (ii) The project team developed a new cryptanalytic tool for differential cryptanalysis, called meet-in-the-filter (MiF). It is suitable for ciphers with a slow or incomplete diffusion layer such as the ones based on Addition-Rotation-XOR (ARX). The main idea of the MiF technique is to stop the difference propagation earlier in the cipher, allowing to use differentials with higher probability. (iii) The project team improved the state-of-the-art in efficient masking of the Advanced Encryption Standard (AES). Masking is a very popular mitigation against Differential Power Analysis (DPA), which is a form of physical attack that aims to break the link between the internal intermediate values and the measurements by applying secret sharing techniques internally throughout the execution. The project team developed a new method to efficiently compute a side-channel protected AES using the masking scheme described by Rivain and Prouff.

Brainsourcing for Affective Attention Estimation

Acronym:	BANANA
PI:	Luis LEIVA
Funding:	Fonds National de la Recherche - INTER
Budget:	800.307,00 €
Duration:	1 Oct 2021 – 30 Sep 2024
Member:	Luis LEIVA (Principal Investigator)
Partners:	• Opole University of Technology • Universitat Jaume I • University of Helsinki

Description

Attention estimation and annotation are tasks aimed at revealing which parts of some content are likely to draw the users' interest. Previous approaches have tackled these incredibly challenging tasks using a variety of behavioral signals, from dwell-time to clickthrough data, and computational models of visual correspondence to these behavioral signals. Today, these signals are leveraged by a myriad of online services to personalize social media, search engine results, recommender systems, and even in supporting critical decision making, such as financial or medical data. However, the signals that all these services are based on are rough estimations of the real underlying attention and affective preferences of the users. Indeed, users may attend to some content simply because it is salient, but not because it is really interesting, or simply because it is outrageous. In contrast, project BANANA will use brain-computer interfaces (BCIs) to infer users' preferences and their attentional correlates towards visual content, as measured directly from the human brain. We aim for a scientific breakthrough by proposing the first-of-its-kind affective visual attention annotation via brainsourcing, i.e. crowdsourced BCI signal acquisition. First, our approach will allow accurate estimation of user preferences, attention allocation, and –critically– the affective component of attention, directly measured from the natural and implicit brain potentials evoked in response to users experiencing digital contents. Then, we will utilize the resulting data in a crowdsourcing setting to reveal how multiple users react to different stimuli and how their attention and affective responses are distributed. These collective responses will produce unified, consistent measures as a result. Our technology will be used in several downstream tasks such as segmentation of users' attention while looking at images, identification of key events, and video summarisation. We will pilot BANANA with different user groups to test and prove its effectiveness, using objective benchmarks and evaluation strategies.

Intelligent aNd orcheStrated securIty and privacy-aware slicing for 5G and beyond veHicular neTworks

Acronym:	5G-INSIGHT
PI:	Thomas ENGEL
Funding:	Fonds National de la Recherche - INTER
Budget:	1.300.041,00 €
Duration:	1 Feb 2021 – 31 Jan 2024
Member:	Thomas ENGEL (Principal Investigator)
Area:	Computer Science & ICT Security
Partners:	• LIST - Luxembourg Institute of Science & Technology • Université Gustave Eiffel • Université de Bourgogne - Franche - Comté (UBFC) • Université de La Rochelle

Description

Network slicing is considered as the key technology of an agile Vehicle-to-everything deployment. However, most deployments in Europe focus on evaluating the network performance and ignore the security and privacy aspects, notably in a cross-border scenario.

Building on key 5G technologies (SDN, NFV) and machine learning algorithms (federated and deep learning), 5G-INSIGHT aims at (a) proposing new techniques for road and network traffic prediction, thus allowing the early detection of intrusions and anomalies within 5G vehicular slices, (b) enforcing security-by-design and privacy-preserving slicing policies for attack mitigation and personal data anonymization, and (c) developing resource orchestration and management across multiple potential providers using federated slicing. Proposed approaches will be validated by simulations as well as by a demonstration platform (proof-of-concept) that integrates the specific characteristics of the France-Luxembourg cross-border area.

Intelligent orchestrated security and privacy-aware slicing for 5G and beyond vehicular networks

Acronym:	5G-INSIGHT
Reference:	R-AGR-3925-10
PI:	Thomas ENGEL
Funding:	Fonds National de la Recherche - INTER
Budget:	1.649.301,00 €
Duration:	1 Apr 2021 – 31 Mar 2024
Members:	• Thomas ENGEL (Principal Investigator)

- Stefanie OESTLUND (Project Coordinator)
- Abdelwahab BOUALOUACHE (Research Associate)

Area: Computer Science & ICT Security

Partners:
- Université Gustave Eiffel
- Université de Bourgogne
- Université de La Rochelle

Description

The tremendous technological developments in the automotive industry today are mainly fuelled by the development of vehicle-to-everything (V2X) communication capabilities and new automated driving features. Given their intrinsic requirements in terms of ultra-low latency and ultra-high reliable connectivity under high-mobility conditions, these features will only be unlocked over the long run with the large-scale adoption of 5G technologies. Among them, network slicing is considered as the key technology of an agile V2X use-case deployment, ensuring network flow isolation, resource assignment, and network scalability. However, while most deployments in Europe focus on evaluating the resulting network performance, security and privacy challenges associated with this technology have not been much investigated, notably in a cross-border scenario. Building on key 5G technologies (SDN, NFV) and machine learning algorithms (federated and deep learning), 5G-INSIGHT aims at: (a) proposing new techniques for road and network traffic prediction, thus allowing the early detection of intrusions and anomalies within 5G vehicular slices; (b) enforcing security-by design and privacy-preserving slicing policies for attack mitigation and personal data anonymization respectively; and (c) developing resource orchestration and management across multiple potential providers using federated slicing. The project will validate the proposed approaches by implementing simulations as well as a demonstration platform (Proof-of-concept) that will integrate the specific characteristics of the France-Luxembourg cross-border area.

Results

Network slicing is considered as the key technology of an agile Vehicle-to-everything (V2X) use-case deployment. However, most deployments in Europe focus on evaluating the network performance and ignore the security and privacy aspects, notably in a cross-border scenario. 5G-INSIGHT (ANR-FNR project) aims to fill this gap by building novel security mechanisms ranging from attack detection to attack mitigation leveraging novel tools and paradigms such as those based on Machine-Learning (ML), particularly federated and deep learning, to Blockchains and Deception Security, all while considering the specific but very sensitive (in terms of security) case of cross-border areas (i.e., the France-Luxembourg border-crossing case).

5G-INSIGHT has started in April 2021. The SECAN-lab team is responsible to coordinate Luxembourg activities in this project. We will provide mechanisms

to detect vehicular slicing attacks and design blockchain-based mechanisms to mitigate them as well. In 2021, the SECAN-lab team has contributed to study the requirements of the 5G-INSIGHT use cases. Our team is currently working with the consortium to finalize the study on attacks and vulnerabilities of the use cases and possible attack scenarios to implement for the generation of datasets. Besides, we have developed a novel federated learning-based solution for detecting passive mobile attackers in V2X.

Personalized Explainable Artificial Intelligence for decentralized agents with heterogeneous knowledge

Acronym:	EXPECTATION
PI:	Leon VAN DER TORRE
Funding:	Fonds National de la Recherche - INTER
Budget:	946.005,00 €
Duration:	1 Jan 2021 – 31 Dec 2023
Member:	Leon VAN DER TORRE (Principal Investigator)
Area:	Computer Science & ICT Security
Partners:	• Ozyegin University • University of Applied Sciences and Arts Western Switzerland • Università di Bologna

Description

Explainable AI (XAI) has emerged in recent years as a set of techniques and methodologies aiming at explaining machine learning (ML) models, and enabling humans to understand, trust, and manipulate the outcomes produced by artificial intelligent entities effectively. Although these initiatives have advanced over the state of the art, several challenges still need to be addressed to apply XAI in real-life scenarios adequately. In particular, two key aspects that need to be addressed are the personalization of XAI and the ability to provide explanations in decentralized environments where heterogeneous knowledge is prevalent. Firstly, personalization of XAI is particularly relevant, due to the diversity of backgrounds, contexts, and abilities of the subjects receiving the explanations generated by AI-systems (e.g., patients and healthcare professionals). Henceforth, the need for personalization must be coped with the imperative need for providing trusted, transparent, interpretable, and understandable outcomes from ML processing. Secondly, the emergence of diverse AI systems collaborating on a given set of tasks relying on heterogeneous datasets opens to questioning how explanations can be combined or integrated, considering that they emerge from different knowledge assumptions and processing pipelines. In this project, we want to address those two challenges, leveraging on the

multi-agent systems (MAS) paradigm, in which decentralized AI agents will extract and inject symbolic knowledge from/in ML-predictors, which, in turn, will be dynamically shared composing custom explanations. The proposed approach combines inter-agent, intra-agent, and human-agent interactions to benefit from both the specialization of ML agents and the establishment of agent collaboration mechanisms, which will integrate heterogeneous knowledge/explanations extracted from efficient black-box AI agents. The project includes the validation of the personalization and heterogeneous knowledge integration approach through a prototype application in the domain of food and nutrition monitoring and recommendation, including the evaluation of agent-human explainability, and the performance of the employed techniques in a collaborative AI environment.

Secure Voting Technologies

Acronym:	SeVoTe
PI:	Peter Y A RYAN
Funding:	Fonds National de la Recherche - INTER
Duration:	1 Oct 2016 – 30 Sep 2021
Members:	• Peter Y A RYAN (Principal Investigator) • Marie-Laure ZOLLINGER (PhD student) • Peter Browne Roenne (Research Associate)

Description

The goal of this research project is to provide significant advances on the issues that appear in modern voting and e-voting systems, with a particular focus on the following aspects: Rigorous expression of the security properties intended from and/or exhibited by a voting system, in order to both improve our understanding of what can be achieved in general, and of the properties, and potential weaknesses, of actual systems. Further, the design of voting systems and components thereof (cryptographic schemes, ...), that offer, firstly, a more effective balance between coercion-resistance and, secondly, usability and improved robustness, resilience to incidents, and more effective dispute resolution procedures.

Secure, Usable and Robust Cryptographic Voting Systems

Acronym:	SURCVS
PI:	Peter Y A RYAN
Funding:	Fonds National de la Recherche - INTER

Duration:	1 Nov 2018 – 31 Oct 2022
Members:	• Peter Y A RYAN (Principal Investigator) • Sjouke MAUW (Collaborator) • Jun PANG (Collaborator)
Areas:	• Computer Science & ICT Security • Security, Reliability and Trust in Information Technology
Partner:	Norwegian University of Science and Technology

Description

This project will investigate the security of voting systems and increase our assurance in state-of-the-art voting systems. We have
identified three specific areas which are critical in progressing towards adoption of modern voting systems to the benefit of society.

User confidence: Most users are not interested in the cryptographic details, but user acceptance relies on an understanding of the processes involved. Voting systems must be designed so that voters believe in their security and integrity.

Security proofs: In the cryptographic community it is now routine to provide a mathematical security proof for algorithms and protocols. This is not typically the case for electronic voting systems deployed today. Obtaining such proofs for typical complex voting systems will require innovative proof methods.

Long-term security: Electronic records will be protected by cryptography, but they will be public and must remain secure into the future. A specific long-term threat against most existing voting system is quantum computers. This project will address each of these areas. We will contribute to increased confidence in our voting systems, and thereby also in the integrity of the electoral process. Our emphasis on security proofs for voting systems will improve the overall assurance of voting systems, both directly and by establishing a scientific standard in the field of voting systems.

This project will also generate new knowledge with regard to cryptographic protocols, in particular about protocols involving humans and the practicability of automatic verification for complicated, real-world protocols.

Results

Within 2021, the following papers have been published:

- S. Baloglu, S. Bursuc, S. Mauw, J. Pang. Election Verifiability Revisited: Automated Security Proofs and Attacks on Helios and Belenios. In 34th IEEE Computer Security Foundations Symposium – CSF 2021, Proceedings in IEEE Computer Society, pp. 1– 15, 2021. Presented at CSF 2021, Dubrovnik, Croatia, June 2021 (online).
- S. Baloglu, S. Bursuc, S. Mauw, J. Pang. Provably Improving Election Verifiability in Belenios. In 6th International Joint Conference on Electronic Voting –

E-VOTE-ID 2021, Lecture Notes in Computer Science, volume 12900, pp. 1–16, 2021. Presented at E-VOTE-ID 2021, Bregenz, Austria, October 2021 (online).

Moreover, one paper is submitted for review:

- S. Baloglu, S. Bursuc, S. Mauw, J. Pang. Election Verifiability in Receipt-free Voting Protocols. Submitted to 35th IEEE Computer Security Foundations Symposium – CSF 2022, under review.

Spin and bias in Language Analyzed in News and Text

Acronym:	SLANT
PI:	Sjouke MAUW
Funding:	Fonds National de la Recherche - INTER
Duration:	1 Mar 2020 – 28 Feb 2023
Members:	• Sjouke MAUW (Principal Investigator) • Sviatlana HOEHN (Research Associate)

Description

There is a growing concern about misinformation or biased information in public communication, be it in traditional media or social forums. While automating fact checking has received a lot of attention recently, the problem of fair information is much larger and much more fundamental. It includes insidious forms like biased presentation of events and discussion and their interpretation. To fully analyse and the problem, an interdisciplinary approach is called for. One needs tools and techniques from Linguistics, to study the structure of texts and the relationships between words and sentences, from Game and Decision Theory, to study the strategic reasoning built into the presentation of texts and their individual interpretation and also from Machine Learning and AI, to automatically detect biased text and develop algorithms to de-bias them.

The SLANT project aims at characterising bias in textual data, either intended (eg. in public reporting), or unintended (eg. in writing aiming at neutrality). An abstract model of biased interpretation will be complemented and concretised using work on discourse structure, semantics and interpretation. We will find relevant lexical, syntactic, stylistic or rhetorical differences through an automated but explainable comparison of texts with different biases on the same subject. This will be based on a dataset of news media coverage from a diverse set of sources. We will also explore how our results can help alter bias in texts or remove it from automated representations of texts.

Results

The following paper has been published within 2021:

- Sviatlana Höhn, Nicholas Asher, and Sjouke Mauw. Examining linguistic biases in Telegram with a game theoretic analysis. In Proc. 3rd Multidisciplinary International Symposium on Disinformation in Open Online Media (MISDOOM'21), volume 12887 of LNCS, pages 16-32, Oxford, UK, 2021. Springer-Verlag.

B.17 FNR - INTER MOBILITY Projects

Deontic logic for Artificial Intelligence

Acronym:	DLAI
PI:	Leon VAN DER TORRE
Funding:	Fonds National de la Recherche - INTER MOBILITY
Budget:	121.528,00 €
Duration:	1 Sep 2020 – 31 Aug 2021
Member:	Leon VAN DER TORRE (Principal Investigator)
Area:	Computer Science & ICT Security

Description

Deontic logic is the field of logic that is concerned with obligation, permission, and related concepts. Typically, a deontic logic uses OA to mean it is obligatory that A, and PA to mean it is permitted that A. As explained in the handbook of deontic logic and normative systems, the history of deontic logic has developed from monadic obligations in Von Wright's SDL, via dyadic obligations in preference-based semantics of DSDL, and its representation by ordering-source-based Kratzer systems, to norm-based semantics. As is well known, there is a striking similarity between on the one hand ordering source-based semantics, preference-based semantics and norm-based semantics, and on the other hand the three classes of Makinson's overview of non-monotonic logic: pivot- based systems, preference-based systems, and rule-based systems.

B.18 FNR - OPEN Projects

Deontic Logic for Epistemic Rights

Acronym:	DELIGHT
PI:	Leon VAN DER TORRE
Funding:	Fonds National de la Recherche - OPEN
Budget:	840.114,00 €
Duration:	1 Mar 2021 – 29 Feb 2024
Member:	Leon VAN DER TORRE (Principal Investigator)
Partners:	• Freie Universitat Berlin • Google Research Amsterdam • Universite de Rennes 1 • University of Bergen • Zhejiang University

Description

Practical and social reasoning is used in the foundations of explainable Artificial Intelligence for the design and engineering of legal and ethical reasoners, and the control and governance of intelligent autonomous systems. DELIGHT investigates deontic logics reasoning about epistemic rights such as the right to know, the freedom of thought and the right to believe, the right to not know, the right to not be misled, or the right to truth. We develop new deontic logics yielding a comprehensive formal analysis of epistemic rights and related legal and ethical concepts, and new reasoning methods to infer which duties follow from these rights, and whether concrete situations in real-life normative systems comply with these rights. Moreover, we evaluate and validate our formal framework using COVID-19 pandemic related legislation and policies in various cultures and legal traditions. Finally, we provide interactive theorem provers to experiment with these new logics, formal models of epistemic rights, and AI applications. These new logics and reasoning systems together with the applied methodology will set the stage for future knowledge representation and reasoning projects in the deontic logic community and develop key technology for AI applications using practical and social reasoning.

B.19 FNR - POC Projects

Swarm Intelligent Mission systeMS

http://simms.lu

Acronym:	SIMMS

PI:	Grégoire DANOY
Funding:	Fonds National de la Recherche - POC
Budget:	338.860,00 €
Duration:	1 Feb 2019 – 30 Apr 2021
Members:	• Grégoire DANOY (Principal Investigator) • Pascal BOUVRY (Scientific and Technology Mentoring) • Pierre-Yves HOUITTE (Research and Development Specialist)
Area:	Intelligent and Adaptive Systems

Description

SIMMS brings a set of innovative algorithms to create a distributed (swarm) intelligence that allows autonomous, highly effective, cost efficient, and coordinated undertaking of missions by mobile vehicles, principally drones. This plug-and-play A.I. (Artificial Intelligence) technology, in the form of a 'smart box', can be used and tailored to all sorts of monitoring, securitisation, rescue or tracking missions. The smart box is compatible with major brands of mobile robots and drones, such as Parrot, DJI, etc.

The integration of SIMMS' proprietary A.I. technology with off-the-shelf sensorial and visualisation technology results in the fully autonomous and coordinated execution of swarm missions The use of swarms of from two to tens of autonomous robots, results in the opportunity to cover greater areas, achieve missions in a fast and efficient way, a higher accuracy and reliability and above all a much more cost effective deployment of technology.

Results

The project has permitted to enhance the commercialization potential of the technology thanks to multiple significant advances:

- Technology: SIMMS PoC permitted to transition from theoretical swarming models validated using simulations and academic drones to the demonstrator of SIMMS MVP on professional drones.
- Business development: SIMMS business model has evolved based on the feedback of prospects and the evolution of the competition. We indeed moved from an a single hardware/software based solution (i.e., swarming in a box) to the additional possibility of a 100% software solution (i.e., focused on the AI model) that would permit to interface our swarming intelligence software module with new drone smart boxes that recently appeared on the market.
- SIMMS identity: development of SIMMS identity and branding through its website, professional explainer video and promotional material.

B.20 FNR - PRIDE Projects

Security and Privacy for System Protection

Acronym:	PRIDE: SPsquared
Reference:	R-AGR-3125
PI:	Sjouke MAUW
Funding:	Fonds National de la Recherche - PRIDE
Budget:	3.037.120,00 €
Duration:	1 Oct 2016 – 30 Jun 2023
Members:	• Sjouke MAUW (Principal Investigator) • Alexei BIRYUKOV (Collaborator) • Jean-Sébastien CORON (Collaborator) • Thomas ENGEL (Collaborator) • Jacques KLEIN (Collaborator) • Gabriele LENZINI (Collaborator) • Christian MULLER (Collaborator) • Jun PANG (Collaborator) • Peter Y A RYAN (Collaborator) • Radu STATE (Collaborator) • Olga GADYATSKAYA (Research Associate)
Areas:	• Computer Science & ICT Security • Security, Reliability and Trust in Information Technology
Partners:	• David Naccache • Université de Paris - II

Description

The proposed Doctoral Training Unit (DTU) focuses on information security and privacy, including its storage, processing and transmission. Our Security and Privacy for System Protection (SP2) research program is set up by the leading researchers of DCS research unit and the Interdisciplinary Centre SnT at the University of Luxembourg. The SP2 program is designed to provide a high-quality research environment for PhD students and to strengthen the links between fundamental and applied research. In particular, research is organized in an interdisciplinary way along five themes where the most critical and pressing research challenges will be addressed:

1. Number Theory, Cryptography and Cryptographic Protocols;
2. Implementation of Cryptography;
3. Internet Privacy;

4. System Security;
5. Socio-Technical Security.

In addition to the research program, our DTU offers a comprehensive training and career development program, with a strong quality control framework, that will not only ensure a high quality scientific output but also prepare our students for an excellent future career in academia, industry and governmental environment. We believe that our DTU's contributions will have a significant scientific, economical and societal impact and will realize strategic priorities of the involved institutions.

Results

During 2021, the following submissions are made under the project:

- Z. Zhong, C. Li, J. Pang. Personalised Meta-path Generation for Heterogeneous Graph Neural Networks. Submitted to European Conference on Machine Learning and Prin- ciples and Practice of Knowledge Discovery, under review.
- Z. Zhong, G. Gonzalez, D. Grattarola, J. Pang. Unsupervised Heterophilous Network Embedding via r-Ego Network Discrimination. Submitted to IEEE Transactions on Neural Networks and Learning Systems, under review.
- Z. Zhong, C. Li, J. Pang. Multi-grained Semantics-aware Graph Neural Networks. Submitted to IEEE Transactions on Knowledge and Data Engineering, under review.
- R. Horne, S. Mauw, S. Yurkov. Whenever a privacy property fails a formula describes an attack: A Complete and Compositional Verification Method for the Applied π- Calculus. Submitted to Theoretical Computer Science Journal, Elsevier, 2022, under review.
- R. Horne, S. Mauw, S. Yurkov. Unlinkability of an Improved Key Agreement Protocol for EMV 2nd Gen Payments. Submitted to IEEE Computer Security Foundations Symposium 2022, under review.

B.21 FNR (Luxembourg)/NCBiR (Poland) Projects

Socio-Technical Verification of Information Security and Trust in Voting Systems

Acronym:	STV
PI:	Peter Y A RYAN
Funding:	FNR (Luxembourg)/NCBiR (Poland)
Duration:	1 Sep 2019 – 31 Aug 2022
Members:	• Peter Y A RYAN (Principal Investigator)

- Wojciech JAMROGA (Research Associate)
- Gabriele LENZINI (Senior Researcher)

B.22 ONRG - NICOP Projects

Heterogeneous multi-swarms of UNmanned auTonomous systEms for mission Deployment

Acronym:	HUNTED
PI:	Pascal BOUVRY
Funding:	Office of Naval Research Global - Naval International Cooperative Opportunities in Science and Technology
Budget:	413.000,00 €
Duration:	15 Aug 2018 – 14 Aug 2021
Members:	• Pascal BOUVRY (Principal Investigator) • Grégoire DANOY (Co-Investigator) • Daniel STOLFI ROSSO (Research Associate)
Areas:	• Intelligent and Adaptive Systems • Security, Reliability and Trust in Information Technology

Description

The HUNTED project proposes a new generation of mobility models for autonomous and heterogeneous UAS swarms that combines a bio-inspired cooperative approach with the power of chaotic dynamics and adaptive clustering. These disruptive models will stand out thanks to a first of its kind integration of state-of-the-art solutions that will permit to optimize the missions' objectives and resilience while ensuring unpredictable yet deterministic trajectories in the different swarm levels.

Results

The surveillance system has been extended to a multi-swarm one where UAVs, Unmanned Ground Vehicles (UGVs), and Unmanned Marine Vehicles (UMVs) collaborate to achieve early detection of escapers from a restricted area. A new chaotic mobility model called CROMM-MS (Chaotic Rössler Mobility Model for Multi-Swarms) was introduced with the aim of patrolling and detecting individuals escaping from a restricted area. We have proposed the parameterisation of CROMM (Chaotic Rössler Mobility Model) in order to address heterogeneous multi-swarms (UAVs, UGVs and UMVs) where early detection has priority over coverage. A new Competitive Coevolutionary Genetic Algorithm (CompCGA)

was designed to optimise the vehicles' trajectories as well as the escapers' evasion ability using a predator-prey approach. These results were published in the Frontiers in Robotics and AI journal [71].

The optimisation of pheromone communication between UAVs evolving as a swarm for surveillance applications has been tackled. More precisely a genetic algorithm (GA) was proposed to optimize the exchange of pheromone maps used in a novel parameterized version of the CACOC (Chaotic Ant Colony Optimisation for Coverage) mobility model named CACOC+. The objective is to keep good performance values even when there is no pheromone data shared between UAVs. Experiments are conducted using realistic simulations, which additionally permit the assessment of the impact of packet loss ratios on the performance of the surveillance system, in terms of reliability and area coverage. Initial results have been accepted as a short paper in GECCO 2021 [194] and next results have been submitted as a full paper to the Special Session on Swarms of UAVs (SUAV 2021) as part of the 13th International Conference on Computational Collective Intelligence (ICCCI 2021) [193].

A novel mobility system called CONSOLE (CONcentric Swarm mObiLity modEl) has been proposed to address surveillance tasks using a UAV swarm. This new swarm-based surveillance system arranges UAVs in concentric security rings and uses solutions of chaotic systems as well as virtual pheromones to improve early intruder detection. An Evolutionary Algorithm (EA) was specially designed and tuned for optimising the CONSOLE's parameters and its performance was compared with five state-of-the-art mobility models, namely MAMM, MAMM2, CROMM, CACOC, and CACOC+. The results of our experiments demonstrated that CONSOLE not only performed better than its competitors, but also that using just eight UAVs as members of the surveillance swarm is enough to achieve detection rates greater than 99.7% and average detection distances greater than 26 meters, reducing the cost and complexity of the whole system. The new CONSOLE model and its experimental validation have been published in the Swarm Intelligence journal (impact factor 2.556) [73].

Theoretical simulations have been conducted using Hunted SIM, a simulation model developed for the HUNTED project. Initially based on Python and then ported to C++, it permits to implement different mobility models using also different types of vehicles. Pheromones, attractors, as well as intruders and collision avoidance algorithms are also included. Hunted SIM has also been extended to multi-swarm systems. An article on the Hunted SIM and the different UAS swarming mobility models it includes has been accepted and presented to the 4th International Workshop on Synergy of Parallel Computing, Optimization and Simulation (PaCOS 2020) as part of The 2020 International Conference on High Performance Computing & Simulation (HPCS 2020).

Realistic simulations have been conducted using the multi-physics robot simulator ARGoS which permits to accurately simulate the UAS physics but also the data transmission model.

B.23 UL Projects

Decentralized global decision-making over dynamic networks of proactive engines

Acronym:	Proactive PhD 4
PI:	Denis ZAMPUNIERIS
Funding:	University of Luxembourg
Duration:	1 Nov 2019 – 1 Nov 2022
Members:	• Denis ZAMPUNIERIS (Principal Investigator) • Parisa MAHYA (Doctoral Candidate) • Sandro REIS (Research assistant)

Description

Proactive Computing is a recent research field, which aims at the development of new IT systems and software applications that work in a more autonomic way for the user's interests. Based on predefined scenarios, the system decides alone about its actions for reacting in a swift and best appropriate way to the changes in its environment, without the command of human beings. Implementing such complex systems into large and/or complex real-world environments often requires one to connect several proactive engines over a dynamic network, for multiple reasons such as geographic proximity of the engines with sensors or actuators, specific computing capacities in engines, redundancy of engines for safer robustness, etc. Each proactive engine taking its decisions locally and acting on its immediate surrounding only, it becomes necessary to add on top of this architecture, a distributed logic for decision-making based on the communication possibilities offered by the network and the computation power embedded in each node. This logic should allow the system of systems to apply uniform management rules and strategies to achieve its global objectives, to deal with potential conflicts between local decisions or their effects, and to pursue goals dedicated to some global optimization purposes.

Proactive computing paradigm applied to the programming of robotic systems

Acronym:	Proactive PhD 3
PI:	Denis ZAMPUNIERIS
Funding:	University of Luxembourg
Duration:	1 Oct 2019 – 1 Oct 2022

Members:
- Denis ZAMPUNIERIS (Principal Investigator)
- Samira CHAYCHI (Doctoral Candidate)
- Sandro REIS (Research assistant)

Description

Proactive Computing is a recent research field which aims at the development of new IT systems and software applications that work in a more autonomic way for the user's interests. Based on predefined scenarios, the system decides alone about its actions for reacting in a the swift and best appropriate way to the changes in its environment, without the command of human beings. The user is no more involved in a continuous interactive loop with the system but is now placed on top of it: he/she is solicited by the system only if the system cannot act by itself.

Nowadays most of the robotic systems are programmed using traditional imperative or object-oriented languages, possibly augmented with real-time, sensor-based and event-based frameworks. This approach leads to intricate code where the pursue of objectives and needs for system management is mixed.

We propose to oppose to this approach, by programming a robotic system with a set of proactive scenarios running in parallel, each one devoted either to a part of the objectives or to some specific system control. This would lead to a better separation of concerns in the code, and consequently to easier development and maintenance. The challenges are numerous and the thesis will concentrate on a few of them, to be decided with the candidate.

B.24 UL and Esch2022 Projects

AI & Art Pavilion

PI: Leon VAN DER TORRE

Funding: University of Luxembourg, Esch2022

Duration: 1 Jun 2020 – 31 Dec 2022

Members:
- Leon VAN DER TORRE (Principal Investigator)
- Amro NAJJAR (Researcher)
- Daniel KARPATI (Project Coordinator)

B.25 UL and External Organisation Funding Projects

A Semantic Search Engine for the Retrieve of Similar Patterns in Luxembourgish Texts

http://acc.uni.lu/strips

Acronym:	STRIPS
PI:	Christoph SCHOMMER
Funding:	University of Luxembourg, External Organisation Funding
Duration:	15 Jan 2018 – 14 Jan 2021
Members:	• Christoph SCHOMMER (Principal Investigator) • Joshgun SIRAJZADE (Researcher)
Area:	Intelligent and Adaptive Systems
Partner:	RTL

Description

The aim of STRIPS is to develop a toolbox of semantic search algorithms for Luxembourgish. We want to implement search algorithms to retrieve and to monitor, e.g., temporal patterns of named entities in Luxembourgish texts. The term semantic, hereby, does not only refer to the usage of keywords or Bag-of-Words like names or geographic identifiers, but fosters also on more complex structures like, for example, on concepts (e.g., topics or themes) and a document's sentiment (e.g., a positive or a negative polarity of the document). The main focus of STRIPS lies in the linguistic processing of texts written in Luxembourgish (particularly stemming, use of phonetic dictionaries and tagged word list for Luxembourgish; Part-of-speech-tagged text corpus), in similarity learning aspects to allow fuzziness in search queries, and in the identification of temporal cross-dependencies inside the Luxembourgish text corpus. To validate the project, we have given heterogeneous text sources (official news items and user-contributed comments) by RTL.

Project Members:

- Prof Dr Peter Gilles
- Prof Dr Christoph Schommer
- Dr Joshgun Sirajzade
- Dr Christoph Purschke
- MSc. Daniela Gierschek
- Thanks to the students from the 1GSO-Abschlussklasse des Lycée Nic-Biever, Dudelange.

- Thanks to the students from the école privée Sainte-Sophie, Luxembourg-Kirchberg.

Prospective students: Anna Felix (Master), Rosito Gerbo (Erasmus Mundus, Torino, Italy).

Former participants: Elisabeth Joy (Department of Computer Science), Elida van Nierop (Department of Mathematics), Rik Lamesch (Department of Mathematics)

Publications:

- Joshgun Sirajzyade, C. Schommer The LuNa Open Toolbox for the Luxembourgish Language. In Conference Proceedings Advances in Data Mining, Applications and Theoretical Aspects. New York (2019).
- Joshgun Sirajzade, Daniela Gierschek, Christoph Schommer and Peter Gilles. Component analysis of adjectives in Luxembourgish for detecting sentiments. Computational Linguistics in the Netherlands (CLIN 29) (2019).
- Daniela Gierschek. Automatic Detection of Sentiment in Luxembourgish User Comments. CL-Postersession at the 41st Annual Conference of the German Linguistic Society (2019).
- Daniela Gierschek, Peter Gilles, Christoph Purschke, Christoph Schommer, Joshgun Sirajzade. A Temporal Warehouse for Modern Luxembourgish Text Collections. DH Benelux (2019).
- Elida van Nierop. Improving LDA Topic Modelling using word embeddings. Master Thesis (2018).
- Joshgun Sirajzade, Christoph Schommer. Mind and Language. AI in an Example of Similar Patterns of Luxembourgish Language. Proceedings International Conference on Artificial Intelligence and Humanities. Seoul, Korea (2018).
- Daniela Gierschek. Automatic Detection of Emotions in Luxembourgish User Comments. PhD Forum at the European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases (ECML-PKDD) 2018.
- Ekaterina Kamlovskaya, Christoph Schommer, Joshgun Sirajzade. A Dynamic Associative Memory for Distant Reading. Proceedings International Conference on Artificial Intelligence and Humanities. Seoul, Korea (2018).
- Joshgun Sirajzade. Korpusbasierte Untersuchung der Wortbildungsaffixe im Luxemburgischen. Technische Herausforderungen und linguistische Analyse am Beispiel der Produktivität. Zeitschrift für Wortbildung = Journal of Word Formation (2018), 2(1).

In the press:

- Wéi si se geduecht: Positiv? Negativ? Neutral? RTL Kultur news (16 December 2019). Luxemburger Wort. 24 April 2019: Luxemburgish ganz Digital: Schnëssen und Strips: So funktioniert moderne Sprachforschung an der Universität Luxemburg. von Birgit Pfaus-Ravida

B.26 External Organisation Funding Projects

CAN bus reverse engineering through Machine Learning

Acronym:	Xee/Elocity
PI:	Thomas ENGEL
Funding:	External Organisation Funding
Duration:	1 Nov 2020 – 31 Oct 2021
Member:	Thomas ENGEL (Principal Investigator)

Model Based Design for Real Time Multicore Embedded Platforms in Industrial Motion Control System

PI:	Tingting HU
Funding:	External Organisation Funding
Budget:	28.000,00 €
Duration:	15 Feb 2019 – 30 Apr 2021
Members:	• Tingting HU (Principal Investigator) • Nicolas NAVET (Supervisor / Scientific Advisor)
Areas:	• Computational Sciences • Software and Systems

Description

The research activity focuses on the redesign of the firmware architecture of the existing Robox-designed R execution environment. The innovative aspects of the project are the use of a model-based design language (MBD) from the early design stages and support of multi-core processors. The MBD will not be used as an implementation language due to real-time performance considerations. Instead, its main application areas will be:

- Test different design choices before their implementation.
- Perform timing analysis of the new firmware architecture.
- Provide a formal architectural reference for the implementation.

The design activity can be divided into two parts:

1. Analysis of existing system and new user requirement

- Thorough analysis of the existing design, focusing on components essential for the new design, and identification of critical points in the existing design that may have negative impacts on the performance.

- Gathering and discussion of new and changed user requirements, with respect to the existing design.

2. Design of the new firmware architecture and validation by simulation

- Re-design of the Robox firmware architecture for multi-core platforms, based on the analysis of the existing system and the new user requirements. The new design will be formally specified with the CPAL model-based design language.
- Exploration and comparison of different design alternatives by means of the simulation capability provided by the CPAL execution engine, with key timing information (such as task cycle time, deadline, execution time, etc) provided by Robox.
- Analysis and confirmation of design scalability, especially task scheduling and synchronization, to 2-, 4-, and 8-core processors by means of the multi-interpreter feature of CPAL, exploiting our past experience with multisource software on multicore ECUs. This activity will be carried out based on the information of selected candidate scheduling policies and synchronization mechanisms.

B.27 Undefined Funding Source Projects

Advanced Methods of Quantization, Compression and Learning in Artificial Intelligence

Acronym:	Com-in-AI
PI:	Vladimir DESPOTOVIC
Budget:	189.588,00 €
Duration:	1 Sep 2020 – 31 Aug 2022
Member:	Vladimir DESPOTOVIC (Principal Investigator)
Area:	Computer Science & ICT Security
Partner:	University of Nis, Faculty of Electronic Engineering

Description

Decreasing computational complexity and memory resources are of particular importance for implementation of AI algorithms in portable and edge computing devices with limited memory and processing power. Related research in this area is still in early stage and deserves further investigation; therefore our project will contribute by proposing innovative methods of compression and quantization of deep neural network (DNN) parameters (weights, biases, activations) and deep features. The goal of the project is to develop a state-of-the-art DNN model with a high performance not only on the hardware commonly used

for AI applications, but also on devices with limited computational resources and thus enabling them to support energy demanding and memory constraint applications. In order to achieve these goals, the project proposes an integrated approach to quantization and compression of DNN parameters, based on statistical modeling of data per layers, as well as data subsets within layers and adaptation of the quantizers on the statistical characteristics of the input data. Moreover, from the exploration of the compression and quantization effects in DNNs with regard to their performance, the benchmark of our methodology will be defined. The researchers' interdisciplinary competences ensure successful development of innovative quantization, compression and learning methodologies that will enable reducing the complexity of AI algorithms and its much wider usage. The results obtained within this project will find a wide range of applications in both academia and industry, particularly in numerous latency-critical services.

Automated GDPR compliance checking of documents and processes

Acronym:	icomplai
PI:	Tomer LIBAL
Budget:	199.158,00 €
Duration:	1 May 2021 – 30 Apr 2023
Member:	Tomer LIBAL (Principal Investigator)
Area:	Computer Science & ICT Security

Description

Since the introduction of the GDPR in 2018, privacy law compliance checking has gained much importance, both financially and ethically. Despite that, a relatively small number of software exists, which can help in this process. Moreover, the current software solutions suffer from several problems, such as inexplainability and nontransparency, which restricts their usability in practice. The icomplai project utilizes technologies that are widely used in high-risk domains, such as train control, for providing an easy-to-use, fully automatic, transparent and explainable interface for privacy law compliance checking of various documents and processes

Co-creating resIlient and susTaInable food systEms towardS FOOD2030

Acronym:	CITIES2030

PI: Thomas ENGEL

Duration: 1 Jun 2020 – 31 May 2024

Member: Thomas ENGEL (Principal Investigator)

Area: Computer Science & ICT Security

Partners:
- AG FUTURA TECHNOLOGII DOOEL SKOPJE
- AYUNTAMIENTO DE QUART DE POBLET
- Academia Romana - Filiala Iasi
- BIOZOON GMBH
- COMUNE DI VICENZA
- Cité de l'agriculture
- Correlate AS
- EPC - EUROPEAN PROJECT CONSULTING -SRL
- EREVNITIKO IDRIMA P.L.
- FUNDACION SOCIALINNOLABS
- FUNDINGBOX RESEARCH APS
- FUTURE FOOD INSTITUTE
- INAGRO, PROVINCIAAL EXTERN VERZELFSTANDIGD AGENTSCHAP IN PRIVAATRECHTELIJKE VORM VZW
- ISTANBUL AVRUPA ARASTIRMALARI DERNEGI
- ITC - INOVACIJSKO TEHNOLOSKI GROZD MURSKA SOBOTA
- Into Seinäjoki Ltd
- Inventivna rjesenja
- KATHOLIEKE HOGESCHOOL VIVES ZUID
- LATVIJAS LAUKU FORUMS
- MATIS OHF
- MUNICIPIUL IASI
- Magistrat der Stadt Bremerhaven
- Mestna obcina Murska Sobota
- PROAGRIA ETELA-POHJANMAA RY
- Primelayer, Unipessoal, Lda
- RIGAS TEHNISKA UNIVERSITATE
- Razvojna agencije Grada Velika Gorica - VE-GO-RA
- SMART & LEAN HUB OY
- STAD BRUGGE
- STICHTING VU
- UNION OF CYPRUS COMMUNITIES
- UNIVERSITA CA' FOSCARI VENEZIA
- UNIVERSITA IUAV DI VENEZIA
- UNIVERSITE DU LUXEMBOURG
- Universidad Politecnica de Madrid
- VEJLE KOMMUNE
- VEREIN ZUR FORDERUNG DES TECHNOLOGIETRANSFERS AN DER HOCHSCHULE BREMERHAVEN EV
- VIDZEMES PLANOSANAS REGIONS
- Waterford Institute of Technology
- ZDRUZENIE PLATFORMA ZA ZELEN RAZVOJSKOPJE

Description

Urban food systems and ecosystems (UFSE) demand immediate action. CITIES2030 innovative approach have a great opportunity to attract the best researchers, entrepreneurs, civil society leaders, cities and all agents of the UFSE as well. The main goal of CITIES2030 is to create a future proof and effective UFSE via a connected structure centered in the citizen, built on trust, with partners encompassing the entire UFSE. CITIES2030 commit to work towards the transformation and restructuring of the way systems produce, transport and supply, recycle and reuse food in the 21st century. CITIES2030 vision is to connect short food supply chains, gathering cities and regions, consumers, strategic and complement industry partners, the civil society, promising start-ups and enterprises, innovators and visionary thinkers, leading universities and research across the vast diversity of disciplines addressing UFSE, including food science, social science and big data. CITIES2030 actively encourage the participation of citizens by delivering a trusted UFSE, moving consumers from being passive recipients to active engagement and motivated change agents. This objective is achieved via multiple tools delivered by CITIES2030 such as the CRFS Alliance, a community of practice supported by a digital platform, reaching all over Europe and beyond. This approach will enable innovation actions and enhancements on a pan-European scope with a global reach. Cities and regions will improve resilience and sustainability, and their leadership will create short food supply chain and ecosystems enabling local investments, trans-borders and transnational deployment. A blockchain-based data-driven UFSE management platform will secure intelligence and coordination actions by delivering an accurate, almost real-time digital twin of the whole supply chain, e.g. from production to waste management, but also on key enablers of resilience and sustainability.

Machine Learning & Arts: The Smart Photo Booth

Acronym:	Machine Learning & Arts: The Smart Photo Booth
PI:	Christoph SCHOMMER
Budget:	50.830,00 €
Duration:	1 Jan 2021 – 31 Dec 2021
Member:	Christoph SCHOMMER (Principal Investigator)

Description

Artificial Intelligence (AI) is no longer only part of science fiction. In recent years, the rapid rise of AI has been simultaneously stunning, promising, sometimes disappointing —and could also be perceived as scary. Views on AI are diverging from experts claiming ”Fear artificial stupidity, not artificial intelligence!” to prominent scientists (e.g. Stephen Hawking) raising their voice to the grave dangers AI could cause to our very existence. What is certain, that

AI-driven technologies are part of our everyday life and the more we democratise the knowledge on these technologies the better we are equipped to look for answers both as a society and as individuals. To start with, AI is symptomatic of the Fourth Industrial Revolution and is the most important of several disruptive technologies. There is a clear need for clarity and understanding of what AI entails today, in order to demystify it and comprehend its impact on our lives, and also, to understand and mitigate its risks. A group of AI researchers and science communicators have teamed up to develop a playful and interactive intelligent machine - the SMART PHOTO BOOTH - where the users can experiment with AI and learn about how intelligent machines are trained. The Smart Photo Booth is designed to guide the user to engage with an AI algorithm via manipulating images. Our photo booth will be similar to an interactive Snapchat filter, allowing the user to generate their very own digital portrait in a chosen style of a specific art movement. Hence, the Smart Photo Booth will be very intuitive and appealing to the general public and particularly for teenagers, it is the perfect medium to teach AI, not only for those who are already technology drawn, but also to publics of diverging interests, backgrounds and gender. The Smart Photo Booth will be adapted and presented in two different venues: a) Space 1 - workshops in the Scienteens Lab at UL for STEM (science, technology, engineering and mathematics) high school students in Luxembourg (April-July 2021); b) Space 2 - permanent exhibition in the Luxembourg Science Center for a wide range of audiences - children, teenagers, and families (August-December 2021). In 2022 we plan to have the Smart Photo Booth exhibited for the whole year in the AI & Art Pavilion. The Pavilion, supported by the Esch 2022 European Capital of Culture, will be providing various interactive programs and a series of exhibitions for all kinds of visitors for the duration of Esch 2022. To implement this project, we have an interdisciplinary team of computer scientists and artists, and are partnering with different organizations for the dissemination strategy: the Scienteens Lab (https://wwwen.uni.lu/lcsb/scienteens_lab), the Luxembourg Science Center (https://www.science-center.lu/) and the European Capital of Culture Esch2022 (https://esch2022.lu/en). By partnering with successful and established 'science in society' initiatives we ensure proper dissemination of the project. Plus, it will allow for the sustainability of the project beyond this proposal.

National Competence Centres in the framework of EuroHPC

Acronym:	EUROCC
PI:	Pascal BOUVRY
Budget:	200.125.000,00 €
Duration:	1 Sep 2020 – 31 Aug 2022
Member:	Pascal BOUVRY (Principal Investigator)
Area:	Computer Science & ICT Security

Partners:
- LUXINNOVATION
- Luxprovide

Description

The EuroCC activity will bring together the necessary expertise to set up a network of National Competence Centres in HPC across Europe in 31 participating, member and associated states, to provide a broad service portfolio tailored to the respective national needs of industry, academia and public administrations. All of this to support and increase strongly the national strengths of High Performance Computing (HPC) competences as well as High Performance Data Analytics (HPDA) and Artificial Intelligence (AI) capabilities and to close existing gaps to increase usability of these technologies in the different states and thus provide a European excellence baseline.

Appendix C

Representational Activities

C.1 Conference Committee Memberships

11th IEEE Workshop Parallel / Distributed Combinatorics and Optimization (PDCO 2021)

https://pdco2021.sciencesconf.org

Location: Portland, United States of America, 17 May 2021 – 21 May 2021.

Participating Members:

- Grégoire DANOY (Co-Chair)
- Pascal BOUVRY (Steering Committee Member)
- Sébastien VARRETTE (Program Committee Member)

13th International Conference on Quality of Multimedia Experience (QoMEX 2021)

Location: Montréal (virtual), Canada, 14 Jun 2021 – 17 Jun 2021.

Participating Members:

- Jean BOTEV (Program Committee Member)

13th International Workshop on Immersive Mixed and Virtual Environment Systems (MMVE 2021)

Location: Istanbul, Turkey, 28 Sep 2021 – 1 Oct 2021.

Participating Members:

- Jean BOTEV (Steering Committee Member, Program Committee Member)

14th International Conference on Security for Information Technology and Communications (SECITC 2021)

https://secitc.eu

Location: Online, 25 Nov 2021 – 26 Nov 2021.

Participating Members:

- Johann GROSZSCHÄDL (Program Committee Member)

14th International Conference on Security for Information Technology and Communications (SECITC 2021)

http://secitc.eu/about-us/

Location: online, Romania, 25 Nov 2021 – 26 Nov 2021.

Participating Members:

- Christian FRANCK (Reviewer)

15th International Working Conference on Variability Modelling of Software-Intensive Systems (VAMOS 21)

https://vamos2021.fh-krems.ac.at/

Location: Online, 9 Feb 2021 – 11 Feb 2021.

Participating Members:

- Maxime CORDY (Program Committee Member)

16th European Conference on Symbolic and Quantitative Approaches to Reasoning with Uncertainty

https://ecsqaru.utia.cas.cz/

Location: Prague, Czechia, 21 Feb 2021 – 24 Feb 2021.

Participating Members:

- Emil WEYDERT (Program Committee Member)

17th IEEE International Workshop on Factory Communication Systems (WFCS'2021)

https://konferenzen.jku.at/wfcs2021/

Location: Vienna, Austria, 9 Jun 2021 – 11 Jun 2021.

Description: WFCS is the largest IEEE conference especially dedicated to communications for (industrial) automation systems. Its aim is to provide a forum for researchers, developers and practitioners to review and discuss most recent trends in the area and share innovative research directions.

Participating Members:

- Nicolas NAVET (Program Committee Member)

17th International Conference on Information Security and Cryptology (INSCRYPT 2021)

https://cst.qd.sdu.edu.cn/inscrypt_2021

Location: Online, 12 Aug 2021 – 14 Aug 2021.

Participating Members:

- Qingju WANG (Program Committee Member)

17th International Workshop on Security and Trust Management (STM 2021)

https://www.nics.uma.es/stm2021/

Location: Darmstadt, Germany, 8 Oct 2021.

Description: STM (Security and Trust Management) is a working group of

ERCIM (European Research Consortium in Informatics and Mathematics). STM 2021 is the seventeenth workshop in this series and will be held virtually at Darmstadt, Germany, in conjunction with the 26th European Symposium On Research in Computer Security (ESORICS 2021). The workshop seeks submissions from academia, industry, and government presenting novel research on all theoretical and practical aspects of security and trust in ICTs.

Participating Members:

- Sjouke MAUW (Program Committee Member)

18th International Conference on Principles of Knowledge Representation and Reasoning KR 2021

Location: Hanoi, Vietnam, 6 Nov 2021 – 12 Nov 2021.

Participating Members:

- Wojciech JAMROGA (Program Committee Member)

18th International Conference on Security and Cryptography

https://secrypt.scitevents.org/Home.aspx?y=2021

Location: NA, Luxembourg, 6 Jul 2021 – 8 Jul 2021.

Description: SECRYPT is an annual international conference covering research in information and communication security. The 18th International Conference on Security and Cryptography (SECRYPT 2021) seeks submissions from academia, industry, and government presenting novel research on all theoretical and practical aspects of data protection, privacy, security, and cryptography. Papers describing the application of security technology, the implementation of systems, and lessons learned are also encouraged. Papers describing new methods or technologies, advanced prototypes, systems, tools and techniques and vision papers indicating future directions are also encouraged.

Participating Members:

- Sjouke MAUW (Program Committee Member)

19th International Conference on Applied Cryptography and Network Security (ACNS 2021)

https://sulab-sever.u-aizu.ac.jp/ACNS2021/index.html

Location: Kamakura, Japan, 21 Jun 2021 – 24 Jun 2021.

Participating Members:

- Alexei BIRYUKOV (Program Committee Member)

19th International Conference on Applied Cryptography and Network Security (ACNS 2021)

https://sulab-sever.u-aizu.ac.jp/ACNS2021/index.html

Location: Kamakura, Japan, 21 Jun 2021 – 24 Jun 2021.

Description: The 19th International Conference on Applied Cryptography and Network Security (ACNS 2021) will be held in Kamakura, Kanagawa, Japan on 21-24 June 2021. The proceedings of ACNS 2021 will be published by Springer in the LNCS series. ACNS is an annual conference focusing on current developments that advance the areas of applied cryptography, cyber security (including network and computer security) and privacy. The goal is to represent both academic research works as well as developments in industrial and technical frontiers. Submissions may focus on the modelling, design, analysis (including security proofs and attacks), development (e.g. implementations), deployment (e.g. system integration), and maintenance (e.g. performance measurements, usability studies) of algorithms, protocols, standards, implementations, technologies devices, systems standing in relation with applied cryptography, cyber security and privacy, while advancing or bringing new insights to the state of the art.

Participating Members:

- Sjouke MAUW (Program Committee Member)

19th International Workshop on Non-Monotonic Reasoning

https://sites.google.com/view/nmr2021/home

Location: online, Vietnam, 3 Nov 2021 – 5 Nov 2021.

Participating Members:

- Emil WEYDERT (Program Committee Member)

1st Training School on Language in the Human-Macine Era

https://lithme.eu

Location: Avila, Spain, 4 Oct 2021 – 8 Oct 2021.

Description: 'Language in the Human-Machine Era' (https://lithme.eu/) aims to prepare the field of linguistics for imminent changes in the way we use technology to communicate. From immersive augmented reality to super-intelligent chatbots, in the near future we will be communicating in very different ways. This will present significant challenges for all areas of linguistics and language research; and so we must all adapt, whether or not we know much about technology right now! LITHME is here to raise awareness of these challenges, and to prepare linguistics and its sub-disciplines for what is to come. Our fully funded training school is open to any eligible researcher who is interested to explore how the widespread use of new and emerging technologies might influence their research. No technological expertise is required, only an interest in exploring the possible effects of these near future advances in language technology.

Participating Members:

- Sviatlana HOEHN (Program Committee Member)

2021 IEEE Conference on Dependable and Secure Computing (DSC)

http://nsclab.org/dsc2021/

Location: Fukushima, Japan, 30 Jan 2021 – 2 Feb 2021.

Description: The IEEE Conference on Dependable and Secure Computing solicits papers, posters, practices, and experiences for presenting innovative research results, problem solutions, and new challenges in the field of dependable and secure computing. The whole spectrum of IT systems and application areas, including hardware design and software systems, with stringent relevant to dependability and security concerns are of interest to DSC. Authors are invited to submit original works on research and practice of creating, validating, deploying, and maintaining dependable and secure systems. The scope of DSC includes, but is not limited to, the following topics.

Participating Members:

- Sjouke MAUW (Program Committee Member)

2021 Mining Software Repositories Conference

https://2021.msrconf.org/

Location: Online, 17 May 2021 – 19 May 2021.

Participating Members:

- Yves LE TRAON (Program Committee Member)

20th IEEE International Conference on Trust Security and Privacy in Computing and Communications (TrustCom 2021)

https://trustcom2021.sau.edu.cn/index.jsp?urltype=tree.TreeTempUrl&wbtreeid=1001

Location: Shenyang, China, 20 Oct 2021 – 22 Oct 2021.

Description: The conference aims at bringing together researchers and practitioners in the world working on trusted computing and communications, with regard to trust, security, privacy, reliability, dependability, survivability, availability, and fault tolerance aspects of computer systems and networks, and providing a forum to present and discuss emerging ideas and trends in this highly challenging research field.

Participating Members:

- Sjouke MAUW (Program Committee Member)

20th International Joint Conference on Autonomous Agents and Multi-Agent Systems AAMAS 2021

Location: London (virtual), United Kingdom, 3 May 2021 – 7 May 2021.

Participating Members:

- Wojciech JAMROGA (Organizing Committee/Scholarship Co-Chair, Program Committee member of the Blue Sky Ideas Track)

20th Workshop on Privacy in the Electronic Society (WPES 2021)

https://wpes2021.di.unimi.it/index.php?pageid=home

Location: Luxembourg, Luxembourg, 15 Nov 2021.

Description: The need for privacy-aware policies, regulations, and techniques has been widely recognized. This workshop discusses the problems of privacy in the global interconnected societies and possible solutions. The 2021 Workshop, held in conjunction with the ACM CCS conference, is the twentieth in a yearly forum for papers on all the different aspects of privacy in today's electronic society. The workshop seeks submissions from academia, industry, and government presenting novel research on all theoretical and practical aspects of electronic privacy, as well as experimental studies of fielded systems. We encourage submissions from other communities such as law and business that present these communities' perspectives on technological issues.

Participating Members:

- Sjouke MAUW (Program Committee Member)

21st IEEE International Working Conference on Source Code Analysis and Manipulation

http://www.ieee-scam.org/2021/

Location: Online, 27 Sep 2021 – 28 Sep 2021.

Participating Members:

- Matthieu JIMENEZ (Program Committee Member, Proceeding Chair)

22nd International Conference on Cryptology in India (INDOCRYPT 2021)

https://indocrypt2021.lnmiit.ac.in

Location: Jaipur, India, 13 Dec 2021 – 15 Dec 2021.

Participating Members:

- Qingju WANG (Program Committee Member)

24th Annual International Conference on Information Security and Cryptology (ICISC 2021)

https://www.icisc.org/static/pastconferences

Location: Seoul, South Korea, 1 Dec 2021 – 3 Dec 2021.

Participating Members:

- Johann GROSZSCHÄDL (Program Committee Member)

24th International Symposium on Formal Methods (FM 2021)

http://lcs.ios.ac.cn/fm2021/

Location: Beijing, China, 20 Nov 2021 – 26 Nov 2021.

Description: FM 2021 is the 24th international symposium in a series organized by Formal Methods Europe (FME), an independent association whose aim is to stimulate the use of, and research on, formal methods for software development. The symposia have been notably successful in bringing together researchers and industrial users around a programme of original papers on research and industrial experience, workshops, tutorials, reports on tools, projects, and ongoing doctoral work. FM 2021 will be both an occasion to celebrate and a platform for enthusiastic researchers and practitioners from a diversity of backgrounds to exchange their ideas and share their experience.

FM 2021 will highlight the development and application of formal methods in a wide range of domains including software, cyber-physical systems and integrated computer-based sys- tems. We are in particular interested in the application of formal methods in the areas of systems-of-systems, security, artificial intelligence, human-computer interaction, manufac- turing, sustainability, power, transport, smart cities, healthcare, biology. We also welcome papers on experiences from application of formal methods in industry, and on the design and validation of formal methods tools.

Participating Members:

- Jun PANG (Publicity co-Chair)

25th ACM International Systems and Software Product Line Conference (SPLC 2021)

https://splc2021.net/

Location: Online, 6 Sep 2021 – 9 Sep 2021.

Participating Members:

- Maxime CORDY (Program Committee Member)

25th International Conference on Financial Cryptography and Data Security (FC 2021)

https://fc21.ifca.ai/index.php

Location: Online, 1 Mar 2021 – 5 Mar 2021.

Participating Members:

- Alexei BIRYUKOV (Program Committee Member)

26th European Symposium on Research in Computer Security (ESORICS 2021)

https://esorics2021.athene-center.de/index.php

Location: Darmstadt, Germany, 4 Oct 2021 – 8 Oct 2021.

Description: Computer security is concerned with the protection of information and computing systems in environments where there is a possibility of intrusion or malicious action. The aim of ESORICS is to further the progress of research in computer security by establishing a European forum for bringing together researchers in this area, by promoting the exchange of ideas with system developers and by encouraging links with researchers in related areas.

Progressively organised in a series of European countries, the symposium is confirmed as the European research event in computer security. Since its inception in 1990, ESORICS has been hosted in a series of European countries and has established itself as the premiere European research event in computer security.

Participating Members:

- Sjouke MAUW (Program Committee Member)

26th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA'2021)

https://2021.ieee-etfa.org/

Location: Västerås, Sweden, 7 Sep 2021 – 10 Feb 2021.

Description: ETFA 2021 is the 26th Annual Conference of the IEEE Industrial Electronics Society (IES) focusing on the latest developments and new technologies in the field of industrial and factory automation. The conference aims to disseminate novel ideas and emerging trends, research results and practical achievements. ETFA 2021 will be held September 7-10, 2021 at Aros Congress Center in Västerås, Sweden.

ETFA 2021 is a unique opportunity to network, build up partnerships and exchange ideas with both industry leaders and a variety of experienced researchers, developers and practitioners from several industries, research institutes, and academia.

Participating Members:

- Nicolas NAVET (Program Committee Member)
- Tingting HU (Sub-reviewer)

28th International Conference on Automated Deduction (CADE)

https://www.cs.cmu.edu/~mheule/CADE28/

Location: online, United States of America, 11 Jul 2021 – 16 Jul 2021.

Participating Members:

- Alexander STEEN (Workshops and Tutorials Chair)

28th International Workshop on Fast Software Encryption (FSE 2021)

https://fse.iacr.org/2021/

Location: Beijing, China, 21 Mar 2021 – 25 Mar 2021.

Participating Members:

- Qingju WANG (Program Committee Member)

29th IEEE/ACM International Conference on Program Comprehension (ICPC 2021)

https://conf.researchr.org/home/icpc-2021

Location: Online, 18 May 2021 – 21 May 2021.

Participating Members:

- Mike PAPADAKIS (Program Committee Member)

29th International Conference on Real-Time and Network Systems (RTNS'2021)

https://rtns2021.univ-nantes.fr/

Location: Nantes, France, 7 Apr 2021 – 9 Apr 2021.

Description: RTNS covers a wide-spectrum of topics in real-time and embedded systems, including, but not limited to:

- Real-time applications design and evaluation: automotive, avionics, space, railways, telecommunications, process control, multimedia.
- Real-time aspects of emerging smart systems: cyber-physical systems and emerging applications, real-time big data, real-time edge/fog and cloud computing, smart grid.
- Real-time system design and analysis: real-time tasks modeling, task/message scheduling, evaluation, mixed-criticality systems, Worst-Case Execution Time (WCET) analysis, quality of service, security.
- Software technologies for real-time systems: model-driven engineering, programming languages, compilers, WCET-aware compilation and parallelization strategies, middleware, Real-Time Operating Systems, virtualization, hypervisors.
- Formal specification and verification: application of formal models, such as model checking, satisfiability modulo theories or constraint programming, to solve real-time problems.
- Real-time distributed systems: fault tolerance, time synchronization, task/messages allocation, adaptability and reconfiguration, publisher/sub-

scriber protocols, distributed real-time database.
- Real-time networks: Networks on Chip (NoC), wired and wireless sensor and actuator networks, Time-Sensitive Networks (TSN), industrial IoT, SDN, 5G, end-to-end latency analysis.
- Hardware support for real-time systems: hardware/software co-design, power/temperature-aware techniques, design of predictable hardware, multi-core and many-core platforms, hardware accelerators, cache related issues, interconnect and memory.

Participating Members:

- Nicolas NAVET (Program Committee Member)
- Tingting HU (Sub-reviewer)

29th International Joint Conference on Artificial Intelligence and 17th Pacific Rim International Conference on Artificial Intelligence IJCAI-PRICAI 2020

Location: Yokohama (virtual), Japan, 7 Jan 2021 – 15 Jan 2021.

Participating Members:

- Nicolas GUELFI (Program Committee Member)
- Wojciech JAMROGA (Program Committee Member)
- Tomer LIBAL (Program Committee Member)
- Réka MARKOVICH (Program Committee Member)
- Alexander STEEN (Program Committee Member)

2nd ACM/IEEE International Conference on Automation of Software Test AST 2021

https://conf.researchr.org/home/ast-2021

Location: Online, 28 May 2021 – 29 May 2021.

Participating Members:

- Yves LE TRAON (Program Committee Member)

2nd IEEE International Conference on Autonomic Computing and Self-Organizing Systems (ACSOS 2021)

Location: Washington, DC, United States of America, 27 Sep 2021 – 1 Oct 2021.

Participating Members:

- Jean BOTEV (Steering Committee Member, Program Committee Member, General Chair)

2nd International Symposium on Emerging Information Security and Applications (EISA 2021)

https://eisa.compute.dtu.dk/2021/

Location: Copenhagen, Denmark, 12 Nov 2021 – 13 Nov 2021.

Description: With recent evolution of adversarial techniques, intrusions have become more complex that may threaten the security of various assets regarding information and applications. In addition, coordinated intrusions like worm outbreak can continue to be a major threat to information, system and network security in the near future. The popularity of Internet may generate a large volume of different types of sensitive information. Therefore, there is a need for emerging techniques, theories and applications to protect information and practical security.

Participating Members:

- Sjouke MAUW (Program Committee Member)

2nd Workshop on Secure Cryptographic Implementation (SCI 2021)

https://sci.ittc.ku.edu/2021/index.html

Location: Online, 23 Jun 2021.

Participating Members:

- Johann GROSZSCHÄDL (Program Committee Member)

30th International Joint Conference on Artificial Intelligence IJCAI 2021

Location: Montreal, Canada, 21 Aug 2021 – 26 Aug 2021.

Participating Members:

- Réka MARKOVICH (Program Committee Member)
- Alexander STEEN (PC Member)
- Wojciech JAMROGA (Senior Program Committee member)

33rd Benelux Conference on Artificial Intelligence and the 30th Belgian Dutch Conference on Machine Learning (BNAIC/BeneLearn2021)

https://bnaic2021.uni.lu

Location: Esch-sur-Alzette, Luxembourg, 10 Nov 2021 – 12 Nov 2021.

Description: BNAIC/BeneLearn 2021 is the reference AI & ML conference for Belgium, Netherlands & Luxemburg.

Participating Members:

- Sviatlana HOEHN (Main organizer)

33rd Benelux Conference on Artificial Intelligence and the 30th Belgian Dutch Conference on Machine Learning (BNAIC/BENELEARN 2021)

Location: Belval, Luxembourg, 10 Nov 2021 – 12 Nov 2021.

Description: BNAIC/BeneLearn 2021 is the reference AI & ML conference for Belgium, Netherlands & Luxemburg.

This year, the 33rd Benelux Conference on Artificial Intelligence and the 30th Belgian Dutch Conference on Machine Learning (BNAIC/BENELEARN 2021) are organized as a joint conference by the University of Luxembourg, under the auspices of the Faculty of Science, Technology, and Medicine (FSTM) and the Interdisciplinary Lab for Intelligent and Adaptive Systems (ILIAS), and the IT for Innovative Services (ITIS) research department from the Luxembourg Institute of Science and Technology.

Participating Members:

- Samira CHAYCHI (Organising Committee)
- Réka MARKOVICH (Track chair and PC member)

33rd IFIP International Conference on Testing Software and Systems (ICTSS 21)

http://ictss2021.cs.ucl.ac.uk/

Location: Online, 10 Nov 2021 – 11 Nov 2021.

Participating Members:

- Mike PAPADAKIS (Program Committee Member)

34th IEEE Computer Security Foundations Symposium

Location: Online, Croatia, 21 Jun 2021 – 25 Jun 2021.

Participating Members:

- Johannes MUELLER (Program Committee Member)

34th International Conference on Legal Knowledge and Information Systems JURIX 2021

https://jurix2021.mruni.eu/

Location: Vilnius, Lithuania, 8 Dec 2021 – 10 Dec 2021.

Participating Members:

- Réka MARKOVICH (Program Committee Member)

35th AAAI Conference on Artificial Intelligence (AAAI-21)

https://aaai.org/Conferences/AAAI-21/

Location: Online, 2 Feb 2021 – 9 Feb 2021.

Description: 35th AAAI Conference on Artificial Intelligence (AAAI-21)

Participating Members:

- Yves LE TRAON (Program Committee Member)

35th Annual IFIP WG 11.3 Conference on Data and Applications Security and Privacy (DBSec 2021)

https://wpsites.ucalgary.ca/dbsec2021/

Location: Calgary, Canada, 19 Jul 2021 – 20 Jul 2021.

Description: DBSec is an annual international conference covering research in data and applications security and privacy.

Participating Members:

- Sjouke MAUW (Program Committee Member)

36th IEEE/ACM International Conference on Automated Software Engineering

Location: Online, 14 Nov 2021 – 20 Nov 2021.

Participating Members:

- Matthieu JIMENEZ (Technical Program Committee Member)

37th International Conference on Software Maintenance and Evolution

https://icsme2021.github.io/

Location: Online, 27 Sep 2021 – 1 Oct 2021.

Participating Members:

- Maxime CORDY (Track / Working Group Chair, Program Committee Member)
- Yves LE TRAON (General Chair)
- Mike PAPADAKIS (General Chair)

3rd International Workshop on EXplainable and TRAnsparent AI and Multi- Agent Systems (EXTRAAMAS 2022)

https://extraamas.ehealth.hevs.ch/index.html

Location: London, United Kingdom, 3 May 2021 – 7 May 2021.

Description: EXTRAAMAS 2021 is a forum to discuss and disseminate research on explainable artificial intelligence with a particular focus on cross-disciplinary perspectives.

Participating Members:

- Sviatlana HOEHN (Publicity Chair)

42nd ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI 2021)

https://pldi21.sigplan.org/venue/pldi-2021-venue

Location: Online, 20 Jun 2021 – 26 Jun 2021.

Participating Members:

- Maxime CORDY (Artefact track Porgram Committee member)

42nd IEEE Real-Time Systems Symposium (RTSS 2021)

http://2021.rtss.org/

Location: Dortmund, Germany, 7 Dec 2021 – 10 Dec 2021.

Description: The IEEE Real-Time Systems Symposium (RTSS) is the premier conference in the field of real-time systems and is a venue for researchers and practitioners to showcase innovations covering all aspects of real-time systems, including theory, design, analysis, implementation, evaluation, and experience. RTSS '21, celebrating the 42nd anniversary of the event, continues the trend of making RTSS an expansive and inclusive event, striving to embrace new and emerging areas of real-time systems research. It will be held in a virtual format on December 7-10, 2021.

Participating Members:

- Tingting HU (Program Committee Member)

43rd international conference on software engineering (ICSE21)

https://conf.researchr.org/home/icse-2021

Location: Online, 25 May 2021 – 28 May 2021.

Participating Members:

- Yves LE TRAON (Program Committee Member)
- Mike PAPADAKIS (Program Committee Member)

4th International Conference on Logic and Argumentation (CLAR)

https://easychair.org/smart-program/CLAR2021/

Location: Hangzhou, China, 20 Oct 2021 – 22 Oct 2021.

Participating Members:

- Réka MARKOVICH (Program Committee Member)
- Alexander STEEN (Program Committee Member)
- Emil WEYDERT (Program Committee Member)

5th IEEE Workshop on Security and Privacy on the Blockchain (S&B 2021)

https://ieeesb.org/index.html

Location: Online, 7 Sep 2021.

Participating Members:

- Alexei BIRYUKOV (Program Committee Member)

5th International Workshop on Cryptocurrencies and Blockchain Technology (CBT 2021)

https://www.00.cbt.gold.upc.edu/cbt/cbt2021

Location: Darmstadt, Germany, 8 Oct 2021.

Participating Members:

- Alexei BIRYUKOV (Program Committee Member)

7th Workshop on "Critical Automotive applications: Robustness & Safety" (CARS)

http://cars2021.astus.se/

Location: Munich, Germany, 13 Sep 2021.

Description: The CARS workshop is a forum focusing on architecture, methods and development techniques for safety-related automotive embedded systems and applications. The 7th edition of CARS is collocated with EDCC 2021.

Participating Members:

- Nicolas NAVET (Program Committee Member)

7th Workshop On The Security Of Industrial Control Systems & Of Cyber-Physical Systems (CyberICPS 2021)

https://www.ds.unipi.gr/cybericps2021/

Location: Darmstadt, Germany, 4 Oct 2021 – 8 Oct 2021.

Description: CyberICPS is the result of the merging of the CyberICS and WOS-CPS workshops that were held for the first time in conjunction with ESORICS 2015.

Cyber-physical systems (CPS) are physical and engineered systems that interact with the physical environment, whose operations are monitored, coordinated, controlled and integrated by information and communication technologies. These systems exist everywhere around us, and range in size, complexity and criticality, from embedded systems used in smart vehicles, to SCADA systems in smart grids to control systems in water distribution systems, to smart transportation systems, to plant control systems, engineering workstations, substation equipment, programmable logic controllers (PLCs), and other Industrial Control Systems (ICS). These systems also include the emerging trend of Industrial Internet of Things (IIoT) that will be the central part of the fourth industrial revolution.

Participating Members:

- Sjouke MAUW (Technical Program Committee Member)

8th IEEE/ACM International Conference on Mobile Software Engineering and Systems 2021

https://conf.researchr.org/home/mobilesoft-2021

Location: Online, 17 May 2021 – 19 May 2021.

Participating Members:

- Yves LE TRAON (Program Committee Member)

8th International Conference on Future Internet of Things and Cloud (FiCloud 2021)

https://www.ficloud.org/2021/

Location: Online, Italy, 23 Aug 2021 – 25 Aug 2021.

Participating Members:

- Qin MA (PC Member)

8th International Conference on Metaheuristics and Nature Inspired Computing (META 2021)

https://meta2021.sciencesconf.org

Location: Marrakech, Morocco, 27 Oct 2021 – 30 Oct 2021.

Participating Members:

- Grégoire DANOY (Programme Chair)
- Pascal BOUVRY (Program Committee Member)

9th International Conference on Human-Agent Interaction (HAI 2021)

Location: Nagoya, Japan, 9 Nov 2021 – 11 Nov 2021.

Participating Members:

- Jean BOTEV (Session Chair)

ACM Conference on Conversational User Interfaces (CUI)

Location: Online, United States of America, 27 Jul 2021 – 29 Jul 2021.

Participating Members:

- Mateusz DUBIEL (PC Member)

ACM Conference on Designing Interactive Systems (DIS):

Location: Online, United States of America, 28 Jun 2021 – 2 Jul 2021.

Participating Members:

- Luis LEIVA (PC Member)

ACM Conference on Human Factors in Computing Systems

Location: Yokohama, Japan, 8 May 2021 – 13 May 2021.

Participating Members:

- Luis LEIVA (PC Member)

ACM Conference on Intelligent User Interfaces (IUI)

Location: College Station, TX, United States of America, 13 Apr 2021 – 17 Apr 2021.

Participating Members:

- Luis LEIVA (PC Member, Associate Chair)

ACM Conference on Web Search and Data Mining (WSDM)

Location: Jerusalem, Israel, 8 Mar 2021 – 12 Mar 2021.

Participating Members:

- Luis LEIVA (PC Member)

ACM International Conference on Multimodal Interaction (ICMI)

Location: Montréal & Online, Canada, 18 Oct 2021 – 22 Oct 2021.

Participating Members:

- Luis LEIVA (PC Member)

ACM SIGIR Conference on Research and Development in Information Retrieval (SIGIR)

Location: Online, United States of America, 11 Jul 2021 – 15 Jul 2021.

Participating Members:

- Luis LEIVA (PC Member)

ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA21)

https://conf.researchr.org/home/issta-2021

Location: Online, 11 Jul 2021 – 17 Jul 2021.

Participating Members:

- Mike PAPADAKIS (Track / Working Group Chair, Program Committee Member)
- Maxime CORDY (Artefact track Porgram Committee member)

AIFA 2021

https://wwwen.uni.lu/university/events/aifa21_ai_and_the_future_of_arts

Location: Belval-Université, Luxembourg, 28 Sep 2021 – 30 Sep 2021.

Description: From 28 to 30 September 2021, AIFA21 will take place at the Belval campus of the University of Luxembourg as a free hybrid event, participation on site under covidcheck: https://covid19.public.lu/en/covidcheck.html

As part of the overall AI Pavilion project (for Esch2022), numerous experts from the field of AI and the arts will explore the increasing interactions between the two fields and address a wide range of topics. AIFA21 is a multidisciplinary event that aims to discuss and explore future developments, opportunities and risks of AI, for example:

- What is the role of AI as a tool for creating art in the visual and performing arts?
- What kind of AI technology is used and how is it used?
- How does AI as technology become a material component of a work of art?
- How do AI utopias and dystopias influence contemporary art production?
- What role does AI play in the development of contemporary art?
- Is AI a stronger vector of artistic interdisciplinarity?

- How can artists inspire or trigger scientific and technological innovation in AI?

On 28 September, AIFA21 will be officially opened at 13.45 by Prof. Dr. Jean-Marc Schlencker, Dean of the Faculty of Science, Technology, and Medicine at the University's Computational Creativity Hub (Maison du Savoir, Administration building, Ground floor). Please join us on-site or online (links for the online event are provided below).

Participating Members:

- Christoph SCHOMMER (Keynote speaker)

Artificial Intelligence and Ethics Workshop at KI2021: 44th German Conference on Artificial Intelligence.

https://ki2021-ai-ethics.github.io/

Location: Berlin+virtual, Germany, 27 Sep 2021.

Participating Members:

- David FUENMAYOR PELAEZ (Invited Speaker)

AuReLeE kickoff workshop

https://aurelee.net/kickoff/

Location: online, Luxembourg, 27 May 2021.

Participating Members:

- Alexander STEEN (Organizing Chair)

Benelux Conference on Artificial Intelligence and Belgian-Dutch Conference on Machine Learning (BNAIC/BeneLearn)

Location: Esch-sur-Alzette, Luxembourg, 10 Nov 2021 – 12 Nov 2021.

Participating Members:

- Luis LEIVA (Programme Chair)
- Mateusz DUBIEL (PC Member)
- Luis LEIVA (PC Member)

BNAIC/BENELEARN

https://bnaic2021.uni.lu/

Location: Belval, Luxembourg, 10 Nov 2021 – 12 Nov 2021.

Description:

This year, the 33rd Benelux Conference on Artificial Intelligence and the 30th Belgian Dutch Conference on Machine Learning (BNAIC/BENELEARN 2021) are organized as a joint conference by the University of Luxembourg, under the auspices of the Faculty of Science, Technology, and Medicine (FSTM) and the Interdisciplinary Lab for Intelligent and Adaptive Systems (ILIAS), and the IT for Innovative Services (ITIS) research department from the Luxembourg Institute of Science and Technology.

BNAIC/BENELEARN 2021 will be held on-site under CovidCheck regulations, as a three-day event: from Wednesday 10 to Friday 12 November 2021. BNAIC/BENELEARN 2021 will include invited speakers, research presentations, posters, and demonstrations. The three-day conference will provide ample opportunity for interaction between academics and businesses: academics are also encouraged to join the business sessions and vice versa.

Participating Members:

- Marharyta ALEKSANDROVA (Session Chair)
- Amro NAJJAR (Track Chair & Local Organization Chair)

CAST IT-Security Award

https://cast-forum.de/workshops/programm/301

Location: Darmstadt, Germany, 25 Nov 2021.

Description:

CAST-Förderpreis IT-Sicherheit 2021

Auch in diesem Jahr verleiht der CAST e.V. den Förderpreis IT-Sicherheit 2021 an Autorinnen und Autoren herausragender Abschluss- und Studienarbeiten auf dem Gebiet der IT-Sicherheit. Gefragt sind innovative Ideen, interessante Ergebnisse, neue Sichtweisen und Wege, die aktuelle und relevante Themen

der IT-Sicherheit adressieren.

Participating Members:

- Andy RUPP (Jury Member)

Digital Around the World

https://digitalaroundtheworld.org/digital-around-the-world-2021/

Location: Virtual, Luxembourg, 20 Oct 2021 – 21 Oct 2021.

Description: The second edition of the Digital Around the World conference was held from October 20 to 21, 2021.

Once again, we digitally toured the world in 24 hours non-stop. We started from Europe and crossed the Atlantic to Brazil, the USA, through Asia and Africa

The event was very successful gathering 600 participants from 53 countries from all around the world. For 26 hours around 100 top-level speakers presented their knowledge and visions on emerging technologies and digital transformation, making this virtual event really magnificent.

Participating Members:

- Latif LADID (Co-Chair)

e ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE 21)

https://2021.esec-fse.org/

Location: Online, 19 Aug 2021 – 28 Aug 2021.

Participating Members:

- Mike PAPADAKIS (Track / Working Group Chair)
- Maxime CORDY (Program Committee Member)
- Yves LE TRAON (Doctoral Symposium program committee)

EUNIC - EU NAtional Institutes of Culture: The Future of Living

https://www.bozar.be/en/calendar/future-living-day-2

Location: Brussels, Belgium, 19 Oct 2021 – 20 Oct 2021.

Description: **The future of living with AI**

No one can predict the future of society in coexistence with machines, but it should be clear that our future will be much more predictable if we responsibly decide today what kind of future we want. A society led by elites is simply not sustainable, so **we have no choice but to build an inclusive world that becomes more sustainable, safe and ethical, also with the help of incredibly capable technology**. Properly thought-out algorithms, collaborative technology, data democracy, and other tools that can be moderated with the help of artificial intelligence should create a better future for humanity and the ecosystem in which it lives. Invited to this panel, experts in computer science, urbanism, and think tanks on technology and society will talk about the challenges of the society of the future and will jointly discuss our chances of taking the right path to a better tomorrow, today.

Participating Members:

- Christoph SCHOMMER (Keynote speaker)

Eurocrypt 2021

https://eurocrypt.iacr.org/2021/

Location: Zagreb, Croatia, 17 Oct 2021 – 21 Oct 2021.

Description: Eurocrypt 2021.

Participating Members:

- Jean-Sébastien CORON (Program Committee Member)

EXTRAAMAS20201

Location: London, United Kingdom, 3 May 2021 – 7 May 2021.

Description: The 3rd International Workshop on **EX**plainable and **TRA**nsparent **AI** and **M**ulti-**A**gent **S**ystems (EXTRAAMAS 2021) is a forum to discuss and disseminate research on explainable artificial intelligence with a particular focus on cross-disciplinary perspectives. This edition of the workshop has two particular focus topics with the ultimate goal to strengthen bleeding-edge foundational and applied research:

1. XAI in Action: Applied perspectives.
EXTRAAMAS explicitly encourages the submission of applied research and demonstration papers. To further facilitate applied perspectives, EXTRAAMAS will organize a panel of industry experts. The panel will be guided to discuss a set of – sometimes provocative questions – in interaction with the audience.

2. Explainable Reasoning in Face of Contradictions: Cross-disciplinary Perspectives.
To facilitate basic research questions that lie at the heart of the AAMAS community, EXTRAAMAS explicitly encourages submissions on symbolic approaches to explainable AI and explainable agency. The corresponding EXTRAAMAS session will be kicked off by a keynote by Dov Gabbay, Augustus De Morgan Professor Emeritus of Logic at the Department of Informatics, King's College London & Professor Emeritus at Bar-Ilan University, Israel. **Selected papers will be invited to a special issue in the Journal of Applied Logics - IfCoLoG Journal of Logics and their Applications.**

Participating Members:

- Amro NAJJAR (Programme Chair)
- Jérémie DAUPHIN (Program Committee Member)

Future of PI: Challenges and Perspectives of Personal Identification

https://futureofpi.github.io/2021/

Location: Vienna, Austria, 6 Sep 2021.

Description: The Future of PI workshop took place on **2021, Sep 6** and was co-located with EuroS&P 2021 (~~Vienna virtual, Sep 7–10).~~

Every day, billions of users demonstrate various aspects about themselves to digital service providers with the help of digital Identity Management (IdM) systems. The involved technologies range from simple passwords to user certificates, anonymous credentials and the ubiquitous Single Sign-On systems. These approaches can be categorized along multiple axes, including how a digital identity is defined or acquired, the level of trust required towards third parties like identity providers, the amount of privacy protection, whether trusted hardware is assumed, the degree of user involvement that is necessary, or the deployment overhead. While these categories seem not inherently mutually exclusive, existing approaches arguably provide satisfactory solutions only according to some of them — and a broadly convincing solution is still lacking.

The goal of this workshop is to bring together academic researchers from various IdM-related domains, as well as practitioners, to improve the understanding of the current state and directions of IdM research, and identify open challenges towards secure and usable solutions. Discussions are fostered by a combination of selected and invited talks delivered by recognized experts in their respective fields, who review current digital IdM systems, highlight shortcomings in existing approaches, and identify new paths to resolve them.

Participating Members:

- Andy RUPP (Program Committee Member)

Global IEEE 5G-IoT Summit

http://www.5gsummit.org/dubai/

Location: Dubai, United Arab Emirates, 14 Dec 2021.

Description: As Internet usages are proliferating, communications networks are faced with new shortcomings. Future networks will have to support in 2020 mobile traffic volumes 1000 times larger than today and a spectrum crunch is anticipated. Wireless access rates are today significantly lower than those of fixed access, which prevents the emergence of ubiquitous low cost integrated access continuum with context independent operational characteristics. Communication networks energy consumption is growing rapidly, especially in the radio part of mobile networks. The proliferation of connected devices makes it very difficult to maintain similar performance characteristics over an ever larger portfolio of technologies and requirements (i.e.Ultra High Definition TV vs. M2M, IoT). Heterogeneity of access technologies entails unsustainable cost with increasing difficulties to integrate an ever larger set of resources with reduced OPEX. Network infrastructure openness is still limited. It prevents the emergence of integrated OTT (cloud)-network integration with predictable end to end performance characteristics, and limits the possibility for networks to become programmable infrastructures for innovation with functionalities exposed to developers' communities.

This 5G SUMMIT focuses on exploring and elucidating all facets of the next generation of IPv6, 5G, IoT, Cloud Computing, Blcokchain technology, business and societal gaps and challenges between the current 3G-4G-LTE access-only Internet models and the proper vision of 5G, evolutionary or revolutionary, to go beyond just access by embracing and facilitating the upfront integration of all new technologies (IOT, SDN/NFV, Cloud Computing, ..) to be user-transparent, app-oriented, service-ready, ubiquitous and lowest cost.

Some of the worldwide 5G experts have been invited and attracted to share their state-of-the-art knowledge with the emerging 5G community in the UAE and around the world in view of facilitating the worldwide harmonization of research and best practices for deployment of viable user scenarios in the global

5G ecosystem, the built-in security and privacy by design in 5G, and explore the different ways to enable Internet protocols over the next generation of empowered devices in order to reach convergence and end to end transparency led by the IEEE 5G Future Networks Initiative T which is supporting technically this event.

Participating Members:

- Latif LADID (Co-Chair)

IE2021 - 17th International Conference on Intelligent Environments

https://www.mdx.ac.ae/ie2021

Location: Dubai, United Arab Emirates, 21 Jun 2021 – 24 Jun 2021.

Description: The International Conference on Intelligent Environments (IE) is in its seventeenth year and is now recognized as a major annual venue in the area. IE, that has been hosted all around the world, offers a truly international forum and welcomes contributions from all technically active regions of the planet.

Intelligent environments refer to physical spaces in which information and communication technologies and sensing technologies are woven in order to create interacting spaces enhancing occupants' experience. The ultimate objective of such environments is to enrich users' activities, but also to allow users to manage them and be aware of their capabilities.

IE is a multidisciplinary event welcoming contribution from a diversity of relevant areas including sensing, networking, human-computer interaction, artificial intelligence, software engineering, context-awareness, internet of things, pervasive and ubiquitous computing, etc. This as an asset of the conference, responding to the complexity of systems developed today and their embedding into society.

Participating Members:

- Denis ZAMPUNIERIS (Program Committee Member)

IEEE 5G & Blockchain Summit

https://www.5gsummit.org/5GBlockChain/

Location: Venice, Italy, 23 Sep 2021 – 24 Sep 2021.

Description: Blockchain and Distributed systems have always presented com-

plex challenges, and technology trends are in many ways making the software designer's job more difficult. In particular, today's systems must successfully handle: - Privacy: Regulations such as the General Data Protection Regulation (GDPR) for Europe and the California Consumers Privacy Act (CCPA) require much stronger security for personal data, and that system owners must delete all personal data based on a user's request or completion of a transaction. - Access control complexity: Modern access control often uses rules that depend on data from sources outside the organization, requiring high performance networks with data integrity guarantees. - "Internet of Things" and ubiquitous sensor nodes: Data sources can include building sensors, smart watches, medical sensors, and many other sensor types. In short, systems must handle more data from disparate sources, and at the same time be responsive to new and emerging privacy and data retention requirements. Recent developments in distributed ledger technology (DLT) have been applied to some of these challenges, with only limited success. A key problem is the immutability property of blockchain (the most prominent form of DLT), which conflicts with the requirement to allow deletion of user data. There are many critical use cases in the health sector and the food supply sector. The Cities2030 project will look at the food supply chain with end to end tracking and tracing from the farm to the fork using Blockchain with compliance to GDPR.

Participating Members:

- Latif LADID (Chair)
- Thomas ENGEL (Honorary Chair)

IEEE 5G for CAM

https://www.5gsummit.org/CAM/

Location: Brussels, Belgium, 11 May 2021 – 12 May 2021.

Description: In the context of the European 5G Action Plan, the mobility vertical, spanning road, rail, water ways and coastal maritime, including a multimodality component, has been singled out as a driver of the European Single Digital Market. The main societal objectives of Connected and Automated Mobility (CAM) are Safer Rides (enhanced road safety), More Efficient Rides (lower emissions and reduced congestion) and Connected Rides (infotainment). But the impact of CAM on jobs and growth, as well as on global competitiveness, will be paramount. This will be achieved by building a complete ecosystem around infrastructure, equipment and services on top of 5G advanced connectivity, whilst mutualizing the huge investments in mobile and fixed broadband. Considerable effort and funding (from Horizon 2020) has been put into large-scale testing and validation, and even pre-deployment, of 5G namely in cross-border segments of Trans-European Transport Corridors. The objective is now to move towards large-scale deployment across the Continent. This first 5G for CAM conference will bring together a variety of EU-funded projects in the

area of CAM, to share their experiences and present results with a view towards deployment. As Horizon 2020 is open to International participation, the event will also provide an opportunity to address a broader global perspective.

Participating Members:

- Latif LADID (Co-Chair)

IEEE 5G World Forum

https://entrepreneurship.ieee.org/session/2021-5g-world-forum/

Location: Montreal, Canada, 13 Oct 2021 – 15 Oct 2021.

Description: The theme for this global 5G event is 5G and Beyond: A Comprehensive Look at Future Networks. The conference will bring together contributors who have been cultivating future networks technology; and applications for the benefit of society. It will emphasize novel architectures that support not only traditional mobile broadband technology but also vertical industry.

Participating Members:

- Abdelwahab BOUALOUACHE (Technical Program Committee Member)
- Latif LADID (Founding Co-Chair)

IEEE Congress on Evolutionary Computation (CEC 2021)

https://cec2021.mini.pw.edu.pl

Location: Krakow, Poland, 28 Jun 2021 – 1 Jul 2021.

Participating Members:

- Grégoire DANOY (Program Committee Member)

IEEE Global Telecommunications Conference

https://globecom2021.ieee-globecom.org/

Location: Madrid, Spain, 7 Dec 2021 – 11 Dec 2021.

Description: The 2021 IEEE Global Communications Conference (GLOBECOM)

will be held in Madrid, Spain, from 7 -11 December 2021. Themed "Connecting Cultures around the Globe," this flagship conference of the IEEE Communications Society will feature a comprehensive high-quality technical program including 12 symposia, selected areas in communications track and a variety of tutorials and workshops. IEEE GLOBECOM 2021 will also include an attractive Industry program aimed at practitioners, with keynotes and panels from prominent research, industry and government leaders, business and industry panels, and vendor exhibits.

Participating Members:

- Abdelwahab BOUALOUACHE (Technical Program Committee Member)

IEEE International Conference on Communications

https://icc2021.ieee-icc.org/

Location: Montreal, Canada, 14 Jun 2021 – 23 Jun 2021.

Description: The IEEE International Conference on Communications (ICC) has been the flagship event of the IEEE Communications Society since 1965. ICC is one of the IEEE Communications Society's two flagship conferences dedicated to driving innovation in nearly every aspect of communications.

The Theme of the ICC 2021 Conference is "**CONNECTIVITY – SECURITY – PRIVACY**". The ICC 2021 Conference attracts and brings together thousands of the world's industry leaders, scientists, academics, engineering professionals, policy makers, and government officials. For participants it promises to stimulate the scientific exchange of ideas, the identification of future trends in communications, and the illumination of business opportunities to attend, present, demonstrate, and share the results of latest research and development on latest leading-edge technologies in Communications and take away with them the new challenges learned from the conferences.

Participating Members:

- Abdelwahab BOUALOUACHE (Technical Program Committee Member)

IEEE International Conference on Software Security and Reliability (QRS21)

https://qrs21.techconf.org/

Location: Online, 6 Dec 2021 – 10 Dec 2021.

Participating Members:

- Mike PAPADAKIS (Program Committee Member)

IEEE International Conference on Software Testing Verification and Validation (ICST) 2021

https://icst2021.icmc.usp.br/

Location: Online, 12 Apr 2021 – 16 Apr 2021.

Participating Members:

- Mike PAPADAKIS (Steering Committee Member)
- Yves LE TRAON (Program Committee Member)
- Mike PAPADAKIS (Program Committee Member, Publication and Web Chair)

IEEE International Mediterranean Conference on Communications and Networking

https://meditcom2021.ieee-meditcom.org/

Location: Athens, Greece, 7 Sep 2021 – 10 Sep 2021.

Description: The IEEE Communications Society is proud to launch IEEE MeditCom, a NEW annual conference for the Mediterranean region!

The inaugural IEEE International Mediterranean Conference on Communications and Networking (MeditCom) will take place 7-10 September 2021 in Athens, Greece.

IEEE MeditCom will bring together visionaries in academia, research labs and industry from all over the world to the shores of the Mediterranean Sea, with programming that will address many of the outstanding challenges that exist in the areas of communications and networking. The conference will solicit research papers on a wide range of research topics, spanning both theoretical and systems research along with vertical technologies. Known as the "cradle of Western civilization", IEEE MeditCom participants will also have an opportunity to explore this exciting and dynamic region with its rich history and beauty.

Participating Members:

- Abdelwahab BOUALOUACHE (Technical Program Committee Member)

IEEE International Smart Cities Conference

https://attend.ieee.org/isc2-2021/

Location: Virtual, Luxembourg, 7 Sep 2021 – 10 Sep 2021.

Description: The **IEEE International Smart Cities Conference** is the flagship IEEE Smart Cities event which brings together practitioners, city policymakers & administrators, infrastructure operators, industry representatives and researchers to present technologies and applications, share their experiences & views with current and future Smart Cities applications. The conference includes keynote and panel session discussions, tutorials given by experts on state-of-the-art topics, and special sessions on emerging topics with the aim of complementing the regular program.

Participating Members:

- Ion TURCANU (Technical Program Committee Member)

IEEE Vehicular Networking Conference

https://ieee-vnc.org/2021/

Location: Virtual, Luxembourg, 10 Nov 2021 – 12 Nov 2021.

Description: Now in its 13th year, VNC has been the primary venue for people interested in vehicular communication to meet.

When VNC 2020 had to move online, we had high hopes to run VNC 2021 at least in a hybrid format so that at least parts of the community could meet in Ulm, Germany, and enjoy the conference on-site. Unfortunately, the course of global **pandemic development requires us to move to a pure online format once more**. Reasons for this step are that Germany is in the middle of a fourth wave with unclear predictions for autumn but mostly that we collected feedback from our community and learned that a majority of prospective participants and authors would be blocked from on-site attendance either due to international trans-continental travel restrictions or due to organizational travel policies.

We therefore decided that IEEE VNC 2021 will be exclusively online and we are committed to optimize the conference for the best online experience possible. Building on our experience from last year (which received a lot of positive comments), we will try to enhance this even more and hope to see many of you participating in our virtual conference.

Participating Members:

- Ion TURCANU (Technical Program Committee Member)

IFIP Summer School on Privacy and Identity Management

https://ifip-summerschool2021.uni.lu/

Location: Belval, Luxembourg, 16 Aug 2021 – 20 Aug 2021.

Description: In 2021, the University of Luxembourg at its Belval campus will welcome you to the 16th IFIP Summer School on Privacy and Identity Management. This years topic is "It's complicated: Exploring the relationship between cybersecurity and privacy, and improving training and awareness" We will take a holistic approach to society and technology and support interdisciplinary exchange through keynote and plenary lectures, tutorials, workshops, and research paper presentations. In particular, participants' contributions that combine technical, legal, regulatory, socio-economic, social or societal, political, ethical, anthropological, philosophical, or psychological perspectives are welcome. The interdisciplinary character of the work is fundamental to the School.

Participating Members:

- Stefan SCHIFFNER (Chair)

IFIP TC13 International Conference on Human-Computer Interaction (INTERACT)

Location: Bari, Italy, 30 Aug 2021 – 3 Sep 2021.

Participating Members:

- Luis LEIVA (PC Member)

INTERNATIONAL CONFERENCE ON OPTIMIZATION AND LEARNING (OLA2021)

https://ola2021.sciencesconf.org

Location: Catania, Italy, 21 Jun 2021 – 23 Jun 2021.

Participating Members:

- Pascal BOUVRY (Program Committee Member)
- Matthias R. BRUST (Program Committee Member)

- Grégoire DANOY (Program Committee Member)

International Conference on the Applications of Evolutionary Computation (EvoApps)

http://www.evostar.org/2021/

Location: Sevilla, Spain, 7 Apr 2021 – 9 Apr 2021.

Participating Members:

- Grégoire DANOY (Program Committee Member)

International Conference on Wireless on Demand Network Systems and Service

http://2021.wons-conference.org/

Location: Virtual, Luxembourg, 9 Mar 2021 – 11 Mar 2021.

Description: Wireless on-demand network systems and services have become pivotal in shaping our future networked world. Starting as a niche application over Wi-Fi, they can now be found in mainstream technologies like Bluetooth LE, LTE Direct and Wireless LANs, and have become the cornerstone of upcoming networking paradigms including mesh and sensor networks, cloud networks, vehicular networks, disruption tolerant and opportunistic networks, and in-body networks.

The challenges of this exciting research field are numerous. Examples include how to make smart use of these novel technologies when multiple technologies or a mix of permanent services and on-demand networking opportunities are available to a network node, how to provide robust services in highly dynamic environments, how to efficiently employ and operate heavily resource-constrained devices, and how to develop robust and lightweight algorithms for self-organization and adaptation. Finally, there are many application-specific challenges.

WONS, now in its sixteenth edition, is a high quality forum to address these challenges. WONS aims to provide a global platform for rich interactions between experts in their fields, discussing innovative contributions in a stimulating environment.

Participating Members:

- Ion TURCANU (Technical Program Committee Member)

International Workshop on Logical Aspects in Multi-Agent Systems and Strategic Reasoning LAMAS & SR 2021

Location: London (virtual), United Kingdom, 3 May 2021 – 4 May 2021.

Participating Members:

- Wojciech JAMROGA (Program Committee Member)

IV Ibero-American Congress of Smart Cities - ICSC-CITIES 2021

http://icsc-cities2021.com/

Location: Cancún, Mexico, 29 Nov 2021 – 1 Dec 2021.

Description: **Smart Cities** are the result of the increasingly urgent need to orient our lives towards sustainability. Therefore, these cities use infrastructure, innovation and technology to improve the quality of life of their citizens.

Being a strategic issue that brings new challenges, the organizers invites the academic community to participate in the IV Ibero-American Congress of Smart Cities (ICSC-CITIES 2021). The congress will be a discussion forum to create synergies among different research groups to favor the development of Smart Cities. Authors are invited to register and submit manuscripts, and contribute to knowledge development and integration in different scenarios.

ICSC-CITIES 2021 will take place on November 29-December 01, 2021 in Cancún, México with the sponsorship of the Ibero-American Program of Science and Technology for Development (CYTED).

Main topics: sustainability, mobility, energy efficiency, governance

Participating Members:

- Daniel STOLFI ROSSO (Program Committee Member)

Joint Logic Workshop: Logic in Computer Science and Deduction Systems

https://kwarc.info/events/GI2020/index.html

Location: online, Germany, 26 Mar 2021.

Participating Members:

- Alexander STEEN (Program Committee Co-Chair)

JSEET 2021 - Joint Track on Software Engineering Education and Training at the 43rd IEEE/ACM International Conference on Software Engineering (ICSE)

Location: Madrid (Virtual Event), Spain, 23 May 2021 – 29 May 2021.

Participating Members:

- Nicolas GUELFI (Program Committee Member)

Les Rendez-Vous de l'UNESCO

https://bnl.public.lu/fr/actualites/communiques/2021/les_rendez-vous_de_l_unesco.html

Location: Luxembourg, Luxembourg, 25 Feb 2021 – 2 Dec 2021.

Description: La Commission Luxembourgeoise pour la coopération avec l'UNESCO et la Bibliothèque nationale du Luxembourg invitent à leur cycle de conférences dans le cadre des « Rendez-Vous de l'UNESCO ».

Le thème central du cycle est cette année :
« Mankind and Media. Rethinking the Roles in the Age of Information »

Les dernières années ont en outre montré clairement qu'on est fortement dépendant de la transmission des informations vite et performante : on demande toujours plus de données, plus d'informations, plus de connectivité.

Mais peut-on conserver une vue d'ensemble dans ce flux d'information hyperrapide ? Peut-on encore contrôler la transformation des informations par les médias numériques ? Où en est l'humain devant l'évolution exponentielle des technologies, de l'intelligence artificielle et du commerce de nos données ? Qui reste à l'origine de l'information et qui comment nous l'interprétons ?

Les conférences traitent cette thématique en différentes perspectives. Le 25 février, Prof. Dr. Christoph Schommer de l'Université du Luxembourg fera l'ouverture en posant la question : L'intelligence Artificielle? Où en sommes-nous ? Il abordera les possibilités, chances et risques de ces nouvelles technologies. 4 journalistes se réuniront le 22 avril et discuteront, animés par Josée Hansen, la transmission d'informations et l'objectivité dans le temps des « Fake News » et du « Click Bait ». Dr. Manuela di Franco nous introduira le 1er juillet dans le monde des dessins animés et se penchera sur leur rôle dans la transmission des messages subliminaux et propagandistes. Ian di Toffoli et Prof. Dr. Lukas K. Sosoe s'entretiendront le 30 septembre sur les problèmes et limites de l'éthique dans le monde digital. Qu'il ne faut pas oublier l'art dans la transmission des

messages nous rappelleront les 4 artistes qui poursuivront le 2nd décembre, dans la dernière table ronde de ce cycle modérée par Dr. Nora Schleich, le rôle de la liberté artistique face à la libre expression des opinions. Que peut et même doit faire l'art ?

La Bibliothèque nationale du Luxembourg aménagera pour chacune de ces soirées, qui auront lieu toujours jeudi à 19hrs, une salle assez grande pour assurer la réunion en présence physique et, le cas échéant, en respect des restrictions actuelles.

25.02.2021 Der Mensch und die Künstliche Intelligenz. Wo stehen wir? (DE) - COMPLÈT
Un entretien avec Prof. Christoph Schommer, modéré par Dr. Nora Schleich, traduit en anglais

22.04.2021 Medienpluralismus – Eng Garantie fir Demokratie am 21. Joerhonnert? (LU)
Une table-ronde avec François Aulner, Pia Oppel, Christoph Bumb et Jean-Louis Siweck, modérée par Josée Hansen

01.07.2021 Transmission of Information via Specific Media – Propagandistic Messages in Comics (EN)
Une présentation de Dr. Manuela di Franco, traduit en français

30.09.2021 L'Ethique dans la société de l'Information (FR)
Un discours avec Prof. Lukas Sosoe, modéré par Ian de Toffoli, traduit en anglais

02.12.2021 Artistesch Fräiheet a Meenungsfräiheet (LU)
Une table-ronde avec Justine Blau, Dr. Cédric Kayer, Filip Markiewicz et Anne Simon., modérée par Dr. Nora Schleich

Participating Members:

- Christoph SCHOMMER (Keynote speaker)

Lifelike Computing Systems Workshop (LIFELIKE 2021)

Location: Prague (virtual), Czechia, 19 Jul 2021 – 23 Jul 2021.

Participating Members:

- Jean BOTEV (Co-Chair)

Mensch und Computer (MuC)

Location: Ingolstadt, Germany, 5 Sep 2021 – 8 Sep 2021.

Participating Members:

- Luis LEIVA (PC Member, Associate Chair)

Online IoT Week

https://iotweek.org/online-iot-week-2021-2/

Location: Virtual, Luxembourg, 30 Aug 2021 – 3 Sep 2021.

Description:

NEXT-GENERATION IOT FOR A SUSTAINABLE FUTURE

The 10th edition of the IoT Week, held online from August 30 to September 3, 2021, was focused on defining the Next Generation of IoT for a Sustainable Future.

For the first time, the IoT Week conference was organized as an online event. Our virtual floor hosted numerous thought leaders from across the globe from all facets of the tech industry. More than 160 speakers shared their standings on the latest development and the future of IoT and digital transformation. The whole event was very lively with 41 sessions, workshops, and panel discussions with 500 participants daily.

Participating Members:

- Latif LADID (Co-Chair)

PHDS IN LOGIC XII

https://www.mi.fu-berlin.de/phdsinlogic2020/

Location: Berlin+virtual, Germany, 8 Sep 2021 – 10 Sep 2021.

Participating Members:

- Alexander STEEN (Invited Speaker)

Plate Forme Intelligence Artificielle

https://pfia2021.fr/programme/

Location: Bordeaux, France, 28 Jun 2021 – 2 Jul 2021.

Participating Members:

- Marharyta ALEKSANDROVA (Invited Speaker)

Privacy Enhancing Technologies

https://petsymposium.org/cfp21.php

Location: Sydney, Australia, 12 Jun 2021 – 16 Jun 2021.

Description: The annual **Privacy Enhancing Technologies Symposium (PETS)** brings together privacy experts from around the world to present and discuss recent advances and new perspectives on research in privacy technologies. Papers undergo a journal-style reviewing process, and accepted papers are published in the journal *Proceedings on Privacy Enhancing Technologies (PoPETs)*.

PoPETs, a scholarly, open-access journal for research papers on privacy, provides high-quality reviewing and publication while also supporting the successful PETS community event. PoPETs is published by Sciendo, part of De Gruyter, which has over 260 years of publishing history. PoPETs does not have article processing charges (APCs) or article submission charges.

Participating Members:

- Andy RUPP (Program Committee Member)

RSA Conference Cryptographers' Track (CT-RSA)

https://sites.google.com/site/ctrsa2021/

Location: San Francisco, United States of America, 17 May 2021 – 20 May 2021.

Description: CT-RSA, or Cryptographers' Track RSA Conference, is the venue for scientific papers on cryptography within the RSA Conference. The RSA Conference is the main trade show for the security industry; over 40,000 people attend the exhibition floor, keynote addresses, events, seminars, training events and the various technical tracks. CT-RSA is the track devoted to scientific papers on cryptography. As such CT-RSA is a great venue to ensure that scientific results not only get published to the wider cryptologic community, but also get exposed to technical attendees from industry, government and wider afield.

Participating Members:

- Andy RUPP (Program Committee Member)

SEENG 2021 the Third International Workshop on Software Engineering Education for the Next Generation as component at the 43rd IEEE/ACM International Conference on Software Engineering (ICSE)

Location: Madrid (Virtual Event), Spain, 24 May 2021.

Participating Members:

- Nicolas GUELFI (Program Committee Member)

SIGNIS Workshop at GlobeCom 2021

https://globecom2021.ieee-globecom.org

Location: Madrid, Spain, 7 Dec 2021 – 11 Dec 2021.

Participating Members:

- Pascal BOUVRY (Program Committee Member)
- Grégoire DANOY (Program Committee Member)
- Frederic PINEL (Program Committee Member)
- Arijit ROY (Workshop Organiser / Co-Organiser)

Southern African Conference on Artificial Intelligence Research (SACAIR 2021)

https://2021.sacair.org.za/

Location: online, South Africa, 6 Dec 2021 – 10 Dec 2021.

Participating Members:

- Réka MARKOVICH (Program Committee Member)

Special Session on Commonsense knowledge reasoning and programming in Artificial Intelligence at ACIIDS 2021

https://aciids.pwr.edu.pl/2021/

Location: Online, 7 Apr 2021 – 11 Apr 2021.

Participating Members:

- Pascal BOUVRY (Co-Chair)
- Matthias R. BRUST (Co-Chair)
- Grégoire DANOY (Co-Chair)

SUAV 2021: Special Session on Swarms of UAVs at ICCCI 2021

https://iccci.pwr.edu.pl/2021/

Location: Rhodes, Greece, 29 Sep 2021 – 1 Oct 2021.

Participating Members:

- Grégoire DANOY (Co-Chair)

Summer School on Verification Technology Systems and Applications (VTSA 2021)

https://resources.mpi-inf.mpg.de/departments/rg1/conferences/vtsa21/

Location: Liege, Belgium, 11 Oct 2021 – 15 Oct 2021.

Description: The summer school on verification technology, systems & applications takes place at the University of Liege, Sart-Tilman Campus from October 11 - October 15, 2021. We believe that all three aspects verification technology, systems & applications strongly depend on each other and that progress in the area of formal analysis and verification can only be made if all three aspects are considered as a whole. Our five speakers Gilles Audemard, Cezara Dragoi, Christoph Haase, Leslie Lamport, and Josef Widder stand for this view in that they represent and will present a particular verification technology and its implementation in a system in order to successfully apply the approach to real world verification problems.

Participating Members:

- Jun PANG (Organising Committee)

Symposium on Search Based Software Engineering (ssbse 21)

https://conf.researchr.org/home/ssbse-2021

Location: Online, 11 Oct 2021 – 12 Oct 2021.

Participating Members:

- Mike PAPADAKIS (Steering Committee Member, Program Committee Member)

The 13th Asian Conference on Machine Learning

Location: Virtual Event., China, 17 Nov 2021 – 19 Nov 2021.

Participating Members:

- Alessandro TEMPERONI (Attendant)

The 5th IEEE International Conference on Agents (IEEE ICA2021)

https://sites.google.com/view/ieeeica2021/home

Location: online, Japan, 13 Dec 2021 – 15 Dec 2021.

Participating Members:

- Liuwen YU (Keynote speaker)

The First International Workshop on Logics for New-Generation Artificial Intelligence (LNGAI 2021)

https://www.xixilogic.org/events/lngai2021/

Location: Hangzhou, China, 18 Jun 2021 – 20 Jun 2021.

Participating Members:

- Réka MARKOVICH (Program Committee Member)

The Genetic and Evolutionary Computation Conference (GECCO 2021)

https://gecco-2021.sigevo.org/HomePage

Location: Lille, France, 10 Jul 2021 – 14 Jul 2021.

Participating Members:

- Grégoire DANOY (Program Committee Member)

The Genetic and Evolutionary Computation Conference (GECCO 2021)

https://gecco-2021.sigevo.org/

Location: Lille, France, 10 Jul 2021 – 14 Jul 2021.

Description: The Genetic and Evolutionary Computation Conference (GECCO) presents the latest high-quality results in genetic and evolutionary computation since 1999. Topics include: genetic algorithms, genetic programming, ant colony optimization and swarm intelligence, complex systems (artificial life, robotics, evolvable hardware, generative and developmental systems, artificial immune systems), digital entertainment technologies and arts, evolutionary combinatorial optimization and metaheuristics, evolutionary machine learning, evolutionary multiobjective optimization, evolutionary numerical optimization, real world applications, search-based software engineering, theory and more.

Participating Members:

- Daniel STOLFI ROSSO (Program Committee Member)

TPTP Tea Party

http://tptp.org/TPTP/TPTPTParty/2021a/

Location: online, United States of America, 9 Dec 2021.

Participating Members:

- Alexander STEEN (Invited Speaker)

C.2 Doctoral Thesis Defense Committee Memberships

Emilie Allart, University of Lille

Date: 26 Jan 2021
Location: Lille, France

PhD Defense Jury Members:

- Jun PANG (Member)

Eva Andersen, University of Luxembourg

Date: 28 May 2021
Location: Luxembourg, Luxembourg

PhD Defense Jury Members:

- Christoph SCHOMMER (Chairman)
- Christoph SCHOMMER (Co-supervisor)

Nikolaos ANTONIADIS, University of Luxembourg

Date: 26 May 2021
Location: Esch sur Alzette, Luxembourg

PhD Defense Jury Members:

- Nicolas NAVET (Chairman)

Carlo Brunetta, Chalmers University of Technology

Date: 27 Aug 2021
Location: Gothenburg, Sweden

PhD Defense Jury Members:

- Andy RUPP (Member)

Nacha Chondamrongkul, University of Auckland

Date: 17 Mar 2021
Location: Auckland, New Zealand

PhD Defense Jury Members:

- Jun PANG (Member)

Wladimir Augusto De La Cadena Ramos, University of Luxembourg

Date: 11 Jan 2021
Location: Luxembourg, Luxembourg

PhD Defense Jury Members:

- Ulrich SORGER (Chairman)
- Thomas ENGEL (Supervisor)

PhD Defense Jury External Partners:

- George Danezis (Member)
- Andriy Pachenko (Vice-chairman)
- Thorsten Ries (Member)

Antonio Fiscarelli, University of Luxembourg

Date: 17 Jun 2021
Location: Esch-sur-Alzette, Luxembourg

PhD Defense Jury Members:

- Pascal BOUVRY (Supervisor)
- Grégoire DANOY (Member)

PhD Defense Jury External Partners:

- Thomas Stützle (Vice-chairman)
- Christophe VERBRUGGEN (Member)

Federico Galli, University of Luxembourg

Date: 28 May 2021
Location: Luxembourg, Luxembourg

PhD Defense Jury Members:

- Christoph SCHOMMER (Supervisor)
- Christoph SCHOMMER (Supervisor)

Federico Galli, University of Luxembourg

Date: 28 May 2021
Location: Bologna, Italy

PhD Defense Jury Members:

- Christoph SCHOMMER (Supervisor)

PhD Defense Jury External Partners:

- Giovanni de Cristofaro (Member)

- Hans Micklitz (Chairman)
- Dino Pedreschi (Member)
- Giovanni Sartor (Supervisor)

Lucio Idone, UC London

Date: 29 Mar 2021
Location: London, United Kingdom

PhD Defense Jury Members:

- Christoph SCHOMMER (Chairman)

PhD Defense Jury External Partners:

- Guido Germano (Supervisor)
- Jessica James (Examiner)
- Philip Treleaven (Supervisor)

Ekaterina Kamlovskaya, University of Luxembourg

Date: 28 Oct 2021
Location: Belval-Université, Luxembourg

PhD Defense Jury Members:

- Martin THEOBALD (Chairman)
- Christoph SCHOMMER (Supervisor)

PhD Defense Jury External Partners:

- Christof Schoech (Member)
- Nina Tahmasebi (Member)

Valentina Leone, University of Luxembourg

Date: 28 May 2021
Location: Belval-Université, Luxembourg

PhD Defense Jury Members:

- Martin THEOBALD (Supervisor)
- Christoph SCHOMMER (Other)

Luca Notarnicala, University of Luxembourg

Date: 6 Jul 2021
Location: Luxembourg, Luxembourg

PhD Defense Jury Members:

- Jean-Sébastien CORON (Co-supervisor)

Nader Samir Labib, University of Luxembourg

Date: 5 Oct 2021
Location: Esch-sur-Alzette, Luxembourg

PhD Defense Jury Members:

- Ulrich SORGER (Chairman)
- Grégoire DANOY (Supervisor)
- Pascal BOUVRY (Expert)
- Matthias R. BRUST (Member)

PhD Defense Jury External Partners:

- Frédéric Guinand (Vice-chairman)
- Jean-Philippe Humbert (Member)

Khachatur Torchyan, University of Luxembourg

Date: 11 Nov 2021
Location: Esch-sur-Alzette, Luxembourg

PhD Defense Jury Members:

- Thomas ENGEL (Chairman)
- Juergen SACHAU (Supervisor)

C.3 Awards

Best Paper Award at QRS'21, 10 Dec 2021

Recipients: Alexandre BARTEL, Yves LE TRAON, Mike PAPADAKIS
The paper "CONFUZZION: A Java Virtual Machine Fuzzer for Type Confusion Vulnerabilities" received the best paper award from the 21st IEEE International Conference on Software Quality Reliability and Security. The paper presents a novel fuzzing technique targeting confusion vulnerabilities within the Java Virtual Machine.

Best Paper Award for "Lightweight EdDSA Signature Verification for the Ultra-Low-Power Internet of Things", 19 Dec 2021

Recipients: Christian FRANCK, Johann GROSZSCHÄDL
Best paper award at "ISPEC 2021: The 16th International Conference on Information Security Practice and Experience".

Best paper awards at ACSAC 2021, 8 Dec 2021

Recipients: Hailong HU, Jun PANG
The paper titled by "Stealing machine learning models: Attacks and counter-

measures for generative adversarial networks" was awarded the best paper in the 37th Annual Computer Security Applications Conference (ACSAC'21).

BM 2nd Award of Scientific Excellence at PAAMS 2021., 1 Oct 2021

Recipient: Amro NAJJAR
Second Award: "Experiments on User-centered control of lights in open-plan office spaces using IoT devices and Distributed Constraint Optimization" by FAROUSI Nuha, ATRACHE Meryem, STAHL Christoph, and NAJJAR Amro

Fellowship of the TAILOR Connectivity Fund, 28 Sep 2021

Recipient: Réka MARKOVICH

Outstanding Reviewer Recognition at ICMI'21, 22 Oct 2021

Recipient: Luis LEIVA

Outstanding Reviewer Recognition at MobileHCI'21, 1 Oct 2021

Recipient: Luis LEIVA

Reviewer Recognition at INTERACT'21, 3 Sep 2021

Recipient: Luis LEIVA

Standards+Innovation young researcher Award, 28 May 2021

Recipient: Saharnaz ESMAEILZADEH DILMAGHANI
Standards+Innovation Young Researcher award presented annually to an individual student, under 30 years of age, based on the work done for academic theses, doctoral dissertations or other university research project addressing standardization.

Winner Ideation Camp, 3 Mar 2021

Recipient: Amirhossein ADAVOUDI JOLFAEI
Ideation Camp is an intensive workshop focusing on students' personal growth, higher employability and learning new skills. After attending this workshop, students are often motivated to open their own enterprises. There have been six editions on campus with a total of 550 registrations, 265 participants and 234 experienced mentors. Some successful entrepreneurs that have resulted out of Ideation Camp series include: EdTech companies CheckMath and EduGamiTec; social start-ups GoldenMe and Visibility STEM Africa; FoodTech start-up Happy Local and GreenTech company OurChoice.

The first Ideation Camp of 2021 went ahead in full virtual mode and united 50 participants and 53 mentors.

This first online Ideation Camp of the University's Entrepreneurship Programme was as action-packed and challenging as previous six editions and brought forward start-up ideas in areas such as technology, fashion or the food industry.

The winning team of the Ideation Camp 7 is Homemade Eats, an online platform that connects cooks with people passionate about great homemade food. The team was formed around the idea of Maroun Altekly, student in the Master in Entrepreneurship and Innovation. Inspired by his mother's great cooking and opportunities related to selling it to foodies, Maroun decided to build a business model around this demand. "I learned so much through working hard under pressure during this event, and thanks to the fantastic mentorship provided by Guardian Angels," says Maroun. "This success is a result of coordinated work of my team: founder of Happy Local and Bachelor student in applied information technology Sam Abdi, doctoral candidate Amirhossein Adavoudi Jolfaei, as well as Mariusz Ludwikowski who is student in the Interdisciplinary Space Master, and Marius Smintina who studies business economics". The winning team is awarded a free fellowship by the Founder Institute Luxembourg and the University of Luxembourg Incubator. Homemade Eats team is now looking to bring their business idea to life with a help of the Venture Mentoring Service of the University.

C.4 Media Appearances

AI & Arts. Workshop (BattleRoyal Berlin + rethink Berlin)

https://esch2022.uni.lu/projects/aiart/

Interview (Internet), 12 Nov 2021
Members: Christoph SCHOMMER
see https://esch2022.uni.lu/projects/aiart/

Mise à l'honneur de deux étudiants du programme de recherche ILNAS-Université du Luxembourg 2017-2020 (ILNAS)

https://portail-qualite.public.lu/fr/actualites/normes-normalisation/2021/mise-a-honneur-etudiants-programme-recherche-ilnas-universite-luxembourg-2017-2020.html

Article (Internet), 11 Nov 2021
Members: Saharnaz ESMAEILZADEH DILMAGHANI, Nader SAMIR LABIB
Mené de concert par l'Université du Luxembourg/*Interdisciplinary Centre for Security, Reliability and Trust* (SnT) et l'ILNAS, le programme de recherche « Normalisation technique pour une utilisation fiable dans le domaine "*Smart*

ICT" » (2017-2020) a vu deux de ses doctorants mis à l'honneur en 2021.

Standards+Innovation Awards (Standards+Innovation)

https://www.standardsplusinnovation.eu/awards

Article (Internet), 1 Nov 2021
Members: Saharnaz ESMAEILZADEH DILMAGHANI
DILMAGHANI Saharnaz - Young researcher winner 2021

Young Researcher presented annually to an individual student, under 30 years of age, based on the work done for academic theses, doctoral dissertations or other university research project addressing standardization.

Luxembourg to lead Europe's first Master's programme on HPC (Luxembourg Trade & Invest)

https://www.tradeandinvest.lu/news/luxembourg-to-lead-europes-first-masters-programme-on-hpc/

Article (Internet), 28 Oct 2021
Members: Pascal BOUVRY

Master en HPC à l'Université du Luxembourg (Soluxions magazine)

https://www.soluxions-magazine.com/master-hpc-universite-du-luxembourg/

Article (Internet), 13 Oct 2021
Members: Pascal BOUVRY

University of Luxembourg to Lead First Pan-European Master's Programme in HPC (HPC Wire)

https://www.hpcwire.com/off-the-wire/university-of-luxembourg-to-lead-first-european-masters-programme-in-hpc/

Article (Internet), 13 Oct 2021
Members: Pascal BOUVRY
A consortium of European partners led by the University of Luxembourg has been selected by the EuroHPC Joint Undertaking to design and implement the first pan-European High Performance Computing (HPC) pilot Master's programme. From Autumn 2022, the consortium will offer courses providing students with outstanding career perspectives in the rapidly expanding field of HPC.

Premier master en HPC l'an prochain à l'Uni (Paperjam)

https://paperjam.lu/article/premier-master-en-hpc-an-proch

Article (Internet), 12 Oct 2021
Members: Pascal BOUVRY
L'Université du Luxembourg accueillera l'an prochain le premier master en «high performance computing». Une pièce essentielle dans la stratégie digitale.

University of Luxembourg to lead the first pan-European Master's programme in HPC (EuroHPC)

https://eurohpc-ju.europa.eu/press-release/university-luxembourg-lead-first-pan-european-masters-programme-hpc

Article (Internet), 12 Oct 2021
Members: Pascal BOUVRY
A consortium of European partners led by the University of Luxembourg has been selected by the EuroHPC Joint Undertaking to design and implement the first pan-European High Performance Computing (HPC) pilot Master's programme. From Autumn 2022, the consortium will offer courses providing students with outstanding career perspectives in the rapidly expanding field of HPC.

Saharnaz Dilmaghani, doctorante au SnT, remporte le prix Standards+Innovation du CEN-CENELEC dans la catégorie "Jeune chercheur" (Gouvernement.lu)

https://gouvernement.lu/fr/actualites/toutes_actualites/communiques/2021/10-octobre/08-prix-cen-cenelec.html

Article (Internet), 8 Oct 2021
Members: Saharnaz ESMAEILZADEH DILMAGHANI, Nader SAMIR LABIB
Lors de la cérémonie de remise des prix Standards+Innovation du CEN (Comité européen de normalisation) -CENELEC (Comité européen de normalisation électrotechnique) qui s'est tenue le 5 octobre 2021, Saharnaz Dilmaghani a remporté le prix "Young Researcher". Cette récompense représente une reconnaissance importante de ses travaux de recherche et de sa contribution à la normalisation pour le Luxembourg. Elle est également le fruit du travail de l'ensemble de l'équipe de recherche qui a accompagné Saharnaz Dilmaghani tout au long de son doctorat et qui s'est impliquée dans la normalisation technique internationale via la mise en œuvre du programme de recherche conjoint entre l'Université du Luxembourg/SnT et l'ILNAS.

Depuis 2019, dans le cadre de leur Plan Innovation, le CEN et le CENELEC décernent chaque année les prix Standards+Innovation, visant à récompenser la contribution des chercheurs et des innovateurs aux travaux de normalisation.

Cette année, Saharnaz Dilmaghani et Nader Samir Labib, tous deux doctorants de l'Interdisciplinary Centre for Security, Reliability and Trust (SnT) dans le cadre du programme de recherche conjoint entre l'Université du Luxembourg/SnT et l'ILNAS, étaient nominés dans la catégorie "Jeune chercheur" (Young Researcher) du CEN-CENELEC Standards+Innovation Award.

Von Mausklicks und Datenschutz (Revue)

https://issuu.com/revue26/docs/revue_2021-30

Interview (Magazine), 28 Jul 2021
Members: Luis LEIVA

The future of living (EUNIC - EU National Institutes for Culture)

https://www.youtube.com/embed/BRiqOR-p7cc

Interview (Internet), 22 Jul 2021
Members: Christoph SCHOMMER
see

https://www.youtube.com/embed/BRiqOR-p7cc

New chatbot can explain apps and show you how they access hardware or data (Aalto University Featured Press Release)

https://www.aalto.fi/en/news/new-chatbot-can-explain-apps-and-show-you-how-they-access-hardware-or-data

News (Internet), 1 Jul 2021
Members: Luis LEIVA
Chatbots have already become a part of our everyday lives with their quick and intuitive way to complete tasks like scheduling and finding information using natural language conversations. Researchers at Aalto University have now harnessed the power of chatbots to help designers and developers develop new apps and allow end users to find information on the apps on their devices.

Interview Duerchbléck Zukunft, elo!? (Fondatioun Zentrum fir politesch Bildung)

https://www.youtube.com/watch?v=FOKu0G8b0pk&feature=youtu.be

Interview (Internet), 14 Jun 2021
Members: Christoph SCHOMMER

AI for ethical and legal debates (Spotlight on Young Researchers, FNR)

https://www.fnr.lu/research-with-impact-fnr-highlight/spotlight-ai-for-ethical-legal-debates/

Article (Internet), 1 May 2021
Members: Alexander STEEN

ILNAS: Retour en vidéo sur « Technical Standardisation for Trustworthy ICT, Aerospace, and Construction » (2021-2024) (Chambre des Métiers Luxembourg)

https://www.cdm.lu/news/fiche/newsnew/news/retour-en-video-sur-le-demarrage-du-programme-de-recherche-technical-standardisation-for-trustworthy-ict-aerospace-and-construction-deuxieme-partie-2021-2024

Interview (Internet), 4 Mar 2021
Members: Pascal BOUVRY
Depuis 2017, l'ILNAS et l'Université du Luxembourg, via son Centre interdisciplinaire pour la sécurité, la fiabilité et la confiance (SnT), ont établi un partenariat visant à rapprocher la normalisation technique et la recherche scientifique.

Nous vous proposons de découvrir, au travers de deux vidéos, les résultats du premier programme de recherche qui vient de s'achever « Normalisation technique pour une utilisation fiable dans le domaine "Smart ICT" » (2017-2020) et les ambitions du nouveau programme de recherche « Technical Standardisation for Trustworthy ICT, Aerospace, and Construction » (2021-2024). La première vidéo, portant sur la période 2017-2020, est disponible ici. Dans la seconde vidéo, disponible ci-dessous (vidéo en anglais avec sous-titres en français), les principaux architectes de ces programmes vous présentent les objectifs pour 2021-2024.

Ist die KI für oder gegen die Menschheit? (Les cycles de l'UNESCO)

Interview (Radio), 25 Feb 2021
Members: Christoph SCHOMMER
Invited evening talk at the National Library of Luxembourg. 25 February 2021, 19h00. Moderated by Simone Beck (National Library) and Dr Nora Schleich (host). The evening talk was recorded and parts of it will be broadcasted by Radio 100,7.

The evening talk itself was organised as an interview, in which the host (Nora Schleich) commented on aspects wrt AI.

Jury member of AI newcomers Award (Gesellschaft für Informatk - Internet Site)

https://kicamp.org/ki-newcomerinnen

Review (Internet), 1 Feb 2021
Members: Alexander STEEN
"AI newcomers" (KI-Newcomer*innen), an award presented by the German federal ministry on education and research (BMBF) and the German Informatics Society (GI)

Video retrospect on the results of the « Normalisation technique pour une utilisation fiable dans le domaine “Smart ICT” » research program (ITNation)

https://itnation.lu/news/video-retrospect-on-the-results-of-the-normalisation-technique-pour-une-utilisation-fiable-dans-le-domaine-smart-ict-research-program/

Interview (Internet), 22 Jan 2021
Members: Matthias R. BRUST, Saharnaz ESMAEILZADEH DILMAGHANI, Chao LIU, Nader SAMIR LABIB
Since 2017, ILNAS and the University of Luxembourg, via the Interdisciplinary Centre for Security, Reliability and Trust (SnT), have set up a partnership aimed at bringing the worlds of technical standardization and scientific research closer together. Through two successive videos, we invite you to discover the results of the first such research program, « Normalisation technique pour une utilisation fiable dans le domaine “Smart ICT” » (2017-2020), and the ambitions of the upcoming one, *Technical Standardisation for Trustworthy ICT, Aerospace, and Construction* » (2021-2024). In the first video, available below (in English, with French subtitles), the team from the University of Luxembourg involved in the 2017-2020 program share their experience and explain how their research work and technical standardization were mutually enhanced .

The ILNAS/UL Research program and Education about Standardization (ILNAS)

https://www.youtube.com/watch?v=Yp0uA90Tgn4

Interview (Internet), 22 Jan 2021
Members: Matthias R. BRUST, Saharnaz ESMAEILZADEH DILMAGHANI, Chao LIU, Nader SAMIR LABIB
Depuis 2017, l’ILNAS et l’Université du Luxembourg, via son Centre interdisciplinaire pour la sécurité, la fiabilité et la confiance (SnT), ont établi un partenariat visant le rapprochement des mondes de la normalisation technique et de la recherche scientifique. L’équipe de l’Université du Luxembourg impliquée dans le programme de recherche « Normalisation technique pour une utilisation fiable dans le domaine ”Smart ICT” » (2017-2020) vous fait part de son expérience, et explique comment la normalisation technique a enrichi ses travaux de recherche et réciproquement.

Retour en vidéo sur les résultats du programme de recherche « Normalisation technique pour une utilisation fiable dans le domaine ”Smart ICT” (ILNAS)

https://portail-qualite.public.lu/fr/actualites/normes-normalisation/2021/video-resultats-programme-de-recherche-normalisation-technique-utilisation-fiable-domaine-smart-ict-partie-2017-2020.html

Interview (Internet), 21 Jan 2021
Members: Matthias R. BRUST, Saharnaz ESMAEILZADEH DILMAGHANI, Chao LIU, Nader SAMIR LABIB
Depuis 2017, l'ILNAS et l'Université du Luxembourg, via son Centre interdisciplinaire pour la sécurité, la fiabilité et la confiance (SnT), ont établi un partenariat visant le rapprochement des mondes de la normalisation technique et de la recherche scientifique. Découvrez, au travers de deux vidéos, les résultats du premier programme de recherche « Normalisation technique pour une utilisation fiable dans le domaine ”Smart ICT” » (2017-2020) et les ambitions du nouveau programme de recherche *Technical Standardisation for Trustworthy ICT, Aerospace, and Construction* » (2021-2024). Dans la première vidéo, disponible ci-dessous (vidéo en anglais avec sous-titres en français), l'équipe de l'Université du Luxembourg impliquée dans le programme de recherche 2017-2020 vous fait part de son expérience, et explique comment la normalisation technique a enrichi ses travaux de recherche et réciproquement.

Interview mat Daniel Weyler: Schule der Zukunft – Mensch oder Roboter, welche Lehrkraft darf es denn sein? (Zentrum fir politesch Bildung)

Interview (Magazine), 13 Jan 2021
Members: Christoph SCHOMMER
Interview mat Daniel Weyler: **Schule der Zukunft – Mensch oder Roboter, welche Lehrkraft darf es denn sein?**

C.5 Guest Researchers

The following guest researchers were invited to the DCS:

Lutz Straßburger

Period: 1 Aug 2021 – 4 Aug 2021
Hosted by: Matteo ACCLAVIO, Ross James HORNE

Dr Juliana STROPP (University Madrid)
Period: 1 Dec 2019 – 30 Jun 2021
Hosted by: Christoph SCHOMMER
Reason: PostDoc, EU Marie Curie. Title: TAXON-TIME **Rediscovering biodiversity using big data to trace taxonomic knowledge through time.**

Prof. Dr. Je Sen Teh (Universiti Sains Malaysia)
Period: 15 Nov 2021 – 14 May 2022
Hosted by: Alexei BIRYUKOV

C.6 Visits

The following visits by DCS members to external organisations took place:

Matteo ACCLAVIO
Institution: Université de Montpellier
Location: Montpellier, France
Period: 13 Jan 2021 – 16 Jan 2021.

Matteo ACCLAVIO
Institution: University of Birmingham
Location: Birmingham, United Kingdom
Period: 3 Sep 2021 – 10 Sep 2021.

Matteo ACCLAVIO
Institution: University of Birmingham
Location: Birmingham, United Kingdom
Period: 21 Oct 2021 – 2 Nov 2021.

Matteo ACCLAVIO
Institution: Université de Montpellier
Location: Montpellier, France
Period: 22 Dec 2021 – 23 Dec 2021.

Matteo ACCLAVIO
Institution: INRIA-Saclay
Location: Palaisseau, France
Period: 24 Dec 2021.

Ross James HORNE

Institution: Inria-Saclay and LIX-Ecole Poly- technique
Location: Paris, France
Period: 1 Apr 2021 – 8 Apr 2021.

Réka MARKOVICH

Institution: CNR ISTI
Location: Pisa, Italy
Period: 27 Sep 2021 – 26 Oct 2021.

Juergen SACHAU

Institution: European Commission Joint Research Centre
Location: Ispra, Italy
Period: 1 Oct 2019 – 31 Mar 2021.

Alexander STEEN

Institution: Freie Universität Berlin
Location: Berlin, Germany
Period: 2 Aug 2021 – 9 Aug 2021.
Reason: Research visit to Prof. Christoph Benzmüller and Prof. Geoff Sutcliffe (visiting professor at FU Berlin), cooperation towards proof standardization.

Alexander STEEN

Institution: Schloss Dagstuhl
Location: Wadern, Germany
Period: 12 Sep 2021 – 17 Sep 2021.
Reason: Participation in Dagstuhl seminar on ”Integrated Deduction” (Seminar 21371).

Alexander STEEN

Institution: FAU University Erlangen-Nuremberg
Location: Erlangen, Germany
Period: 18 Nov 2021 – 19 Nov 2021.
Reason: Research cooperation and guest lecture of Alexander Steen with Prof. Axel Adrian in the domain of AI & Law.

Appendix D

Software

Accord

https://accord.uni.lux

License: Internal use only

Members: Christian GLODT (Analyst, Architect, Designer, Developer, Tester)

Description: Accord is a the successor to the CSC Information System and is intended to provide services to all FSTM research units. It manages research information and allows the automatic generation of reports and websites.

Changes: Small improvements and bug fixes have been applied to Accord in 2021.

ADTool

http://satoss.uni.lu/software/adtool

License: free use

Members: Sjouke MAUW (Analyst)

Description: The attack–defense tree language formalizes and extends the attack tree formalism. It is a methodology to graphically analyze security aspects of scenarios. With the help of attributes on attack–defense trees, also quantitative analysis can be performed. As attack–defense tree models grow, they soon become intractable to be analyzed by hand. Hence computer support is desirable. Software toll, called the ADTool, has been implemented as a part of the ATREES project to support the attack–defense tree methodology for security modeling. The main features of the ADTool are easy creation, efficient editing, and quantitative analysis of attack–defense trees. The tool is available at http://satoss.uni.lu/software/adtool. The tool was realized by Piotr Kordy and

its manual was written by Patrick Schweitzer.

Algorithms for Probabilistic Argumentation

License: Creative Common

Members: Leon VAN DER TORRE (Architect)

Description: We developed efficient algorithms for computing probabilistic argumentation. These algorithms were implemented in Java, and tested on a machine with an Intel CPU running at 2.26 GHz and 2.00 GB RAM. Please refer to the following paper in details.

1. Beishui Liao, Kang Xu, Huaxin Huang. Formulating Semantics of Probabilistic Argumentation by Characterizing Subgraphs: Theory and Empirical Results, Jurnal of Logic and Computation, to appear. http://arxiv.org/abs/1608.00302

AMT: Assessment Management Tool

License: to be defined

Members: Alfredo CAPOZUCCA (Analyst), Nicolas GUELFI (Analyst), Thibault Jean Angel SIMONETTO (Developer)

Description: AMT: Assessment Management Tool is a software to assess an observed element (e.g. course, student) according to an evaluation model. Each evaluation model uses one or multiple scale(s) to evaluate the observed element. The development of this tool was initiated in the context of a Bachelor in Informatics (BINFO)'s thesis and it's still under construction. Currently, there exists only a beta version available to internal members of the group.

ASSA-PBN

http://satoss.uni.lu/software/ASSA-PBN/

License: free use

Members: Andrzej MIZERA (Designer), Jun PANG (Analyst)

Description: ASSA-PBN is a tool specially designed for approximate steady-state analysis of large probabilistic Boolean networks (PBNs). The approximate steady-state analysis is crucial for large PBNs, which naturally arise in the domain of Systems Biology. ASSA-PBN provides different solutions for different

size PBNs. In particular, ASSA-PBN provides the two-state Markov chain approach and the Skart approach for large PBNs. The latest version of the package was released in Nov. 2014 and is available from http://satoss.uni.lu/software/ASSA-PBN/.

at-decorator

https://github.com/vilena/at-decorator/tree/master/CSP_decorator

License: GNU General Public License v3.0

Members: Sjouke MAUW (Designer)

Description: **at-decorator** is a tool designed to compute values for an attack tree (fully decorate an attack tree) given some available data points and predicates on data values (relationships between attack tree node values). In contrast to the standard bottom-up approach, our tool does not require to have all leaf node values available to fully decorate a tree.

The tool is available as open source, and it utilizes Constraint Programming and the Z3 theorem prover. The tool is available here https://github.com/vilena/at-decorator/tree/master/CSP_decorator

AVXECC

License: GPLv3

Members: Hao CHENG (Developer), Johann GROSZSCHÄDL (Developer)

Description: High-throughput elliptic curve cryptography software using Advanced Vector Extensions.

BiCS Management Tool (BMT)

https://messir.uni.lu/bmt/login

License: to be defined

Members: Nicolas GUELFI (Analyst), Alen JAHIC (Developer), Benoit RIES (Analyst)

Description: Development of the BiCS Management Tool, a web application for managing the BiCS Semester Projects.

BiCS Website

License: to be defined

Members: Nicolas GUELFI (Analyst), Benoit RIES (Analyst)

Description: The modern website should be a first entrance door for the new Bachelor. People from outside should get all information around the Bachelor and the projects done within the BiCSLab. One the one hand, our goal is to make the Bachelor visible to the World and attract people to enrol inside the Bachelor. On the other hand, we would like to make our projects visible to the outside, to attract industrial partners for proposing projects within the BiCS and the BiCSLab. Student's can work on these projects within their BiCS Semester Project course in cooperation with the industrial partners.

BlockSci

http://github.com/cryptolu/BlockSci

License: GNU General Public License Version 3

Members: Daniel FEHER (Developer)

Description: A high-performance tool for Zcash blockchain science and exploration.

CABEAN

License: Apache License

Members: Jun PANG (Designer)

Description: CABEAN is a software tool for the control of asynchronous Boolean networks, which are often used to model gene regulatory networks. CABEAN is freely available. The newest version of CABEAN is 2.0.0, updated on October 26, 2020.

CABEAN provides the following methods to solve the six source-target control problems: the minimal one-step instantaneous source-target control (OI); the minimal one-step temporary source-target control (OT); the minimal one-step permanent source-target control (OP); attractor-based sequential instantaneous source-target control (ASI); attractor-based sequential temporary source-

target control (AST); attractor-based sequential permanent source-target control (ASP). CABEAN provides the following target control methods: instantaneous target control (ITC); temporary target control (TTC); permanent target control (PTC).

CheckMasks: formal verification of side-channel countermeasures for cryptographic implementations

https://github.com/coron/checkmasks

License: GPL v2

Members: Jean-Sébastien CORON (Designer)

Description: This is an implementation in Common Lisp of the techniques described in the paper:

[Cor17b] Jean-Sebastien Coron. Formal Verification of Side-Channel Countermeasures via Elementary Circuit Transformations. IACR eprint archive. https://eprint.iacr.org/2017/879.pdf

Generic verification of security properties:

- Generic verification of the t-SNI of multiplication-based refreshing
- Generic verification of the t-SNI of multiplication
- Generic verification of some properties of RefreshMasks: lemmas 5, 6, 7, 8 of [Cor17a], and Lemma 3 from [CRZ18].
- Generic verification of the t-SNI property of the Boolean to arithmetic conversion algorithm from [Cor17a].

Polynomial-time verification fo security properties:

- Poly-time verification of the t-SNI of multiplication-based refreshing [Cor17b, Lemma 3]
- Poly-time verification of some properties of RefreshMasks: [Cor17b, Lemma 4] corresponding to [Cor17a, Lemma6], and [Cor17b, Lemma 5] corresponding to [Cor17a, Lemma 5]
- Poly-time verification of the t-SNI of multiplication [Cor17b, Lemma 6]

Automatic generation of security proof:

- Automatic poly-time verification of t-SNI of multiplication-based refreshing, and of the two previous properties of RefreshMasks.

References:

[Cor17a] Jean-Sebastien Coron. High-order conversion from boolean to arithmetic masking. Proceedings of CHES 2017.

[CRZ18] Jean-Sébastien Coron, Franck Rondepierre, Rina Zeitoun. High Order

Masking of Look-up Tables with Common Shares. To appear at TCHES 2018. IACR Cryptology ePrint Archive 2017: 271 (2017)

Coco Müller

License: Proprietary

Members: Sviatlana HOEHN (Supervisor)

Description: Practicing foreign language conversation with a machine may have multiple advantages: a machine does not judge, a machine is always available and accessible from everywhere. In this project we focus on language understanding and generation for German as a communication language for non-native speakers.

CollaTrEx

License: N/A

Members: Jean BOTEV (Architect)

Description: CollaTrEx is framework for collaborative context-aware mobile exploration and training. It is particularly designed for the in-situ collaboration within groups of learners performing together diverse educational activities to explore their environment in a fun and intuitive way.

Aside from employing both absolute and relative spatio-temporal context for determining the available activities, different buffering levels are an important conceptual feature supporting seamless collaboration in spite of temporary connection losses or when in remote areas.

CollaTrEx comprises a prototypical front-end implementation for tablet devices, as well as a web-based back-end solution for the creation and management of activities which can be easily extended to accommodate both future technologies and novel activity types.

DBVerify

http://satoss.uni.lu/software/DBVerify/

License: Open source

Members: Sjouke MAUW (Designer)

Description: DBVerify is a set of Tamarin implementation of several state-of-

the-art distance-bounding protocols as well as their MSC representation. It intends to show the usage of the causality-based verication methodology proposed in our paper ”Distance-Bounding Protocols: Verication without Time and Location” (published at IEEE S&P’18). It was developed by Zach Smith (ZS) and Jorge Toro-Pozo (JT).

Disputool

https://disputool.uni.lu/

License: Free use

Members: Shohreh HADDADAN (Developer)

Description: This website was created as a demonstration of my research project: ”Argument mining in political debates data”. It contains the annotated dataset with argument components(Claim/Premise) divided by date and year.

The neural network model with the best results trained on identifying argument components is also integrated in this website so that users can interact and test the model. This demo website is going to be improved with more visualizations including topic model visualizations soon.

E4L: Energy for Life

License: to be defined

Members: Alfredo CAPOZUCCA (Architect), Phillip DALE (Developer), Michele MELCHIORRE (Developer)

Description: E4L: Energy for Life is a web application aimed at helping people to calculate their daily energy consumption, and allow them to compare between days, and between people. In this manner, users input information using pictures that best fit their daily experience, and then the tool compares the persons data, to Luxembourg, European, and World averages. Thus, the tool is supposed to help people understand better energy or how much they use. The development of this web application forms the core of a larger educational and research concept. This work is done in collaboration with the Laboratory for Energy Materials (LEM).

ELRA Language Corpus

License: LC/ELDA/DISTR-S/2014-11/001-UNILU

Members: Sviatlana HOEHN (Architect), Christoph SCHOMMER (Designer)

Description: The *deL1L2IM* corpus, created between May and August 2012 and last updated in August 2014, has been collected within the framework of a PhD project (Mrs. Sviatlana Höhn, geb. Danilava) on the development of a learning method implying conversations with an artificial companion. This PhD work is presented as a qualitative investigation of instant messaging dialogues on a long-term basis (four months) between advanced learners of German and German native speakers, chatting about whatever topic they wish.

The dataset is composed of 72 dialogues, each of them having a duration of 20 to 45 minutes. The whole corpus contains ca. 52,000 words and 4,800 messages and has a file size of 0,5 Mb. Nine pairs of participants – i.e. nine learners and four native speakers – were required, with 8 dialogues per pair.

The interactions have undergone linguistic analysis whereby the annotation will be performed only on repair/correction sequences (incomplete learner error annotation). The goal of the project was to create an application for language modelling and to improve learner language applications, tutoring softwares and dialogue systems.

The corpus is delivered in one written text file (in XML format, customized under TEI P5).

ePassport Vulnerability Demonstration

https://github.com/bboyifeel/passport_relay_guide

License: Apache License

Members: Ross James HORNE (Architect), Sjouke MAUW (Architect)

Description: We have a repository containing code to demonstrate vulnerabilities discovered in ePassports. Two modified readers are used for such demonstrations. One acts as a fake reader who relays information to a fake ePassport in another location. Both can be installed on an Android phone with RFC capabilities. The attack has been disclosed responsibly.

Excalibur

https://messir.uni.lu/confluence/display/EXCALIBUR/Excalibur

License: Eclipse Public License 1.0

Members: Alfredo CAPOZUCCA (Developer), Nicolas GUELFI (Developer), Benoit RIES (Developer)

Description: Excalibur is a tool supporting the Messir methodology, a Scientific Method for the Software Engineering Master, used in Software Engineering Lectures at bachelor and master levels.

Excalibur tool covers the phase of Requirements Analysis and its main features are requirements analysis specification (its own DSL), requirements report generation (latex/pdf) and requirements simulation (prolog). It relies on Eclipse technologies as XText for textual specification and Sirius for graphical views of the textual specifications.

It is available here: http://messir.uni.lu

FELICS

https://github.com/cryptolu/FELICS

License: GNU General Public License Version 3

Members: Luan CARDOSO DOS SANTOS (Developer), Johann GROSZSCHÄDL (Developer)

Description: FELICS is an open-source framework for the fair and consistent evaluation of lightweight cryptographic primitives on 8-bit AVR, 16-bit MSP430, and 32-bit ARM Cortex-M microcontrollers. Further information about FELICS can be found on the CryptoLux Wiki at https://www.cryptolux.org/index.php/FELICS.

Findel

https://github.com/cryptolu/findel

License: GNU General Public License Version 3

Members: Alexei BIRYUKOV (Designer), Sergei TIKHOMIROV (Developer)

Description: Findel (Financial Derivatives Language) is a domain-specific language that implements the composable approach to modeling financial derivatives on the Ethereum platform. For more information on Findel see paper "Findel: Secure Derivative Contracts for Ethereum".

Fudomo

https://fudomo.uni.lu/

License: MIT

Members: Christian GLODT (Designer, Developer, Tester), Pierre KELSEN (Tester, Supervisor)

Description: Implementation of a model transformation approach based on functional decomposition, including a web-based modeling environment as well as command-line tools and libraries. The web-based modeling environment is available at https://lassy-fmde.github.io/try-fudomo/.

Changes: Numerous improvements have been made to try-fudomo in 2021.

I/O Logic Workbench

License: GNU General Public License v3.0 only

Members: Alexander STEEN (Developer)

Description: The I/O Logic Workbench is aimed at providing a browser-based automated reasoning system for various I/O logics. In short, the system allows you to input a set of norms and an input (the description of the current situation), and provides automated means for inferring whether a certain formula can be derived as an obligation from this.

J-NERD/J-REED

https://people.mpi-inf.mpg.de/~datnb/

License: BSD

Members: Martin THEOBALD (Architect)

Description: Open-source information extraction libraries

Légionnaires Rallye

https://www.legionnaires.lu/

License: N/A

Members: Jean BOTEV (Designer), Claude Marc OHLHOFF (Developer)

Description: The Légionnaires Rallye is a mobile game engaging players in a digital treasure hunt around Luxembourg City. It was developed in collaboration with the Luxembourg Centre for Contemporary and Digital History (C^2DH), to promote the Légionnaires exhibition (June 30, 2021 - February 28, 2022) at the Musée Dräi Eechelen. The game extends the exhibition outside the museum walls, allowing players to learn about the history of the Luxembourgish légionnaires while solving riddles and walking around the city.

Changes: Mobile web application.

LEO-III

https://github.com/leoprover/Leo-III

License: BSD

Members: Alexander STEEN (Developer)

Description: An automated theorem prover for classical higher-order logic (with choice).

Leo-III [SWB16] is an automated theorem prover for (polymorphic) higher-order logic which supports all common TPTP dialects, including THF, TFF and FOF as well as their rank-1 polymorphic derivatives [SWB17]. It is based on a paramodulation calculus with ordering constraints and, in tradition of its predecessor LEO-II [BP15], heavily relies on cooperation with external (mostly first-order) theorem provers for increased performance. Nevertheless, Leo-III can also be used as a stand-alone prover without employing any external cooperation.

Leo-III won the 2nd place in the world championships in higher-order automated theorem proving.

Changes: Leo-III is an automated theorem prover for (polymorphic) higher-order logic which supports all common TPTP dialects, including THF, TFF and FOF as well as their rank-1 polymorphic derivatives. It is based on a paramodulation calculus with ordering constraints and, in tradition of its predecessor LEO-II, heavily relies on cooperation with external (mostly first-order) theorem

provers for increased performance. Nevertheless, Leo-III can also be used as a stand-alone prover without employing any external cooperation. It is now in version 1.6.

Minor updates in 2021 (see https://github.com/leoprover/Leo-III/releases/tag/v1.6):

- Small fixes in proof output when injective functions are present
- Added preliminary support for ground arithmetic
- Bump to Scala language version 2.13.5
- This version was used in CASC-28 (http://tptp.org/CASC/28/).

Lightning-Privacy

https://sites.google.com/view/lightning-privacy/home

License: GNU General Public License Version 3

Members: Sergei TIKHOMIROV (Developer)

Description: The scripts and data used for the paper ”A Quantitative Analysis of Security, Anonymity and Scalability for the Lightning Network”.

MiCS Management System

http://demos.uni.lux/mics

License: non-redistributable, for internal use only

Members: Christian FRANCK (Analyst, Architect), Christian GLODT (Designer, Developer, Tester)

Description: An internal web-based tool developed for the management of modules, courses and profiles of the Master in Information and Computer Sciences. Developed by Christian Glodt.

Changes: Work has been started on a feature allowing to import data from ACME files.

MinUS

http://satoss.uni.lu/software/MinUS

License: free use

Members: Jun PANG (Analyst)

Description: This tool, MinUS, integrates the technologies of trajectory pattern mining with the state-of-the art research on discovering user similarity with trajectory patterns. Specifically, with MinUS, we provide a platform to manage movement datasets, and construct and compare users trajectory patterns. Tool users can compare results given by a series of user similarity metrics, which allows them to learn the importance and limitations of different similarity metrics and promotes studies in related areas, e.g., location privacy. Additionally, MinUS can also be used by researchers as a tool for preliminary process of movement data and parameter tuning in trajectory pattern mining. The tool is available at http://satoss.uni.lu/software/MinUS.

Model Decomposer

License: free to use, binary redistribution permitted

Members: Christian GLODT (Architect, Developer), Qin MA (Analyst)

Description: An Eclipse plugin that implements a generic model decomposition technique which is applicable to Ecore instances and EP models, and is described in a paper published in the proceedings of the FASE 2011 conference.

MouseFaker

https://github.com/luileito/mousefaker

License: MIT

Members: Luis LEIVA (Developer)

Description: A web browser extension that anonymizes your mouse movements to prevent user profiling.

MsATL (MonoSat for Alternating-time Temporal Logic)

License: MIT License

Members: Wojciech JAMROGA (Designer)

Description: MsATL is a prototype tool for deciding the satisfiability of Alternating-time Temporal Logic (ATL) with imperfect information. MsATL combines SAT Modulo Monotonic Theories solvers with existing ATL model checkers: MCMAS and STV. The tool can deal with various semantics of ATL, including perfect and imperfect information, and can handle additional practical requirements. MsATL can be applied for synthesis of games that conform to a given specification, with the synthesized game often being minimal.

Primes-Backdoor

https://github.com/cryptolu/primes-backdoor

License: GPLv3

Members: Giuseppe VITTO (Developer)

Description: The Primes-Backdoor repository contains a SageMath implementation of the prime generation procedure and factorization attack detailed in the paper “Factoring Primes to Factor Moduli: Backdooring and Distributed Generation of Semiprimes”.

Protocol implementation of Dining Cryptographers Networks (DC-nets)

https://gitlab.uni.lu/cfranck/dcnets

License: (C) University of Luxembourg

Members: Christian FRANCK (Developer)

Description: This project is about a practical implementation of Dining Cryptographers Networks based on the research that can be found on our project homepage (https://dcnets.readthedocs.io).

The protocol relies on the following techniques:

- Zero-knowledge ciphertext verification based on Pedersen commitments. (https://arxiv.org/abs/1402.2269)
- SICTA-based collision resolution with a throughput of 0.924 packets. (https://arxiv.org/abs/1402.1732)

ReCon

https://github.com/cryptolu/ReCon

License: GNU General Public License Version 3

Members: Alexei BIRYUKOV (Designer), Daniel FEHER (Developer)

Description: ReCon is a Universal Reputation Module for Distributed Consensus Protocols. This is the simulation of the protocol written in Python 2.7 based on the paper "Guru: Universal Reputation Module for Distributed Consensus Protocols".

rio: Reasoner for I/O Logics

https://github.com/aureleeNet/rio

License: BSD-3 clause license

Members: Alexander STEEN (Developer)

scala-tptp-parser

https://github.com/leoprover/scala-tptp-parser/

License: MIT license

Members: Alexander STEEN (Developer)

Selene Cryptographic Library in Python

License: Internal use only

Members: Peter Y A RYAN (Supervisor)

Selene User Interface

License: Internal use only

Members: Marie-Laure ZOLLINGER (Developer)

SemiPrimes

https://github.com/cryptolu/semiprimes

License: GPLv3

Members: Giuseppe VITTO (Developer)

Description: The SemiPrimes repository contains a SageMath and MP-SPDZ implementation of the distributed semiprime generation protocol detailed in the paper “Factoring Primes to Factor Moduli: Backdooring and Distributed Generation of Semiprimes”.

SHA512 optimized for MSP430

https://gitlab.uni.lu/cfranck/sha512_for_msp430

License: (C) University of Luxembourg

Members: Christian FRANCK (Developer), Johann GROSZSCHÄDL (Developer)

Description: Optimized Implementation of SHA-512 for MSP430 Microcontrollers. Details are described in the paper referenced on https://orbilu.uni.lu/handle/10993/49799 .

Sketchnoting

License: N/A

Members: Aryobarzan ATASHPENDAR (Developer), Christian GREVISSE (Architect)

Description: Enhanced sketchnoting (iOS app) for the retrieval and integration of learning material.

Features handwriting recognition and semantic annotation for retrieving resources relevant to the concepts mentioned in the handwritten notes from existing Knowledge Graphs. Drawing recognition enables visual queries, allowing for enhanced search capabilities.

SPARKLE

https://github.com/cryptolu/sparkle

License: GNU General Public License Version 3

Members: Luan CARDOSO DOS SANTOS (Developer), Johann GROSZSCHÄDL (Developer)

Description: SPARKLE is an ARX-based cryptographic permutation suitable for software implementation on 8/16/32-bit microcontrollers. SCHWAEMM and ESCH are an authenticated encryption algorithm and a hash function, respectively, which use the SPARKLE permutation in a sponge construction. This repository contains (i) reference and optimized C implementations of SCHWAEMM and ESCH, (ii) supporting software for the security analysis of SPARKLE, SCHWAEMM, and ESCH, (iii) documentation, (iv) the submission packages for the NIST Lightweight Cryptography competition, and (v) benchmarking results.

Changes: In 2021, the CryptoLux group developed improved Assembler implementations of the SPARKLE permutation for 8-bit AVR and 32-bit ARM microcontrollers, as well as new Assembler implementations for MSP430 and RISC-V.

STV (STrategic Verifier)

License: MIT License

Members: Wojciech JAMROGA (Supervisor)

Description: STV is a prototype tool aimed at verification of strategic abilities in multi-agent systems, and synthesis of strategies that guarantee a given temporal goal. We have significantly extended the tool with support for model reductions.

Two methods are used: (i) checking for equivalence of models according to a handcrafted relation of alternating bisimulation, and (ii) fully automated partial order reduction (POR). We also added a simple model specification language that allows the user to define their own inputs for verification, which was not available in the previous version.

The purpose of the extension is twofold. First, it should facilitate practical verification of MAS, as the theoretical and experimental
results for POR and bisimulation-based reduction suggest. No less importantly, it serves a pedagogical objective. Actual reduction schemes are often difficult to understand. We put emphasis on visualisation of the reductions, so that the tool can be also used in the classroom to show how the reduction works. Finally, checking strategic bisimulation by hand is difficult and prone to errors; here, the user can both see the idea of the bisimulation, and automatically check if it is indeed correct.

TeachDCS: Teaching Load Monitoring System

License: Copyright University of Luxembourg (Default)

Members: Christian FRANCK (Developer)

Description: DCS Teaching Monitoring System (for internal use)

TESMA

License: Eclipse Public License 1.0

Members: Nicolas GUELFI (Analyst), Benjamin JAHIC (Developer), Sandro REIS (Developer), Benoit RIES (Analyst)

Description: Tool for the Specification, Management and Assessment of Teaching Programs.

Nicolas Guelfi, Benjamin Jahic and Benoît Ries, TESMA: Towards the Development of a Tool for Specification, Management and Assessment of Teaching Programs, published in the Proceedings of the 2nd International Conference on Applications in Information Technology (ICAIT-2016)

http://orbilu.uni.lu/handle/10993/28607

TriAD

https://people.mpi-inf.mpg.de/~gurajada/

License: BSD

Members: Martin THEOBALD (Architect)

Description: Open-source, distributed graph database

Whitebox

https://github.com/cryptolu/whitebox

License: GNU General Public License Version 3

Members: Alexei BIRYUKOV (Designer)

Description: This repository contains white-box analysis and implementation tools, in particular proof-of-concept code for the paper ”Attacks and Countermeasures for White-box Designs” by Alex Biryukov and Aleksei Udovenko (ASIACRYPT 2018).

The code is split into three parts:

1. Implementation: Proof-of-concept implementation of AES using the new nonlinear masking scheme.
2. Verification: Code for verifying algebraic security of gadgets.
3. Attacks: Several attacks from the paper.

X64ECC: Elliptic Curve Cryptography for Dining Cryptographers Networks

https://gitlab.uni.lu/cfranck/dcnets

License: (C) University of Luxembourg

Members: Christian FRANCK (Developer), Johann GROSZSCHÄDL (Developer)

Description: Optimized cryptographic library using the techniques described in ”Fast and Flexible Elliptic Curve Cryptography for Dining Cryptographers Networks” (https://orbilu.uni.lu/handle/10993/46390).

XDEM (eXtended Discrete Element Method)

http://luxdem.uni.lu/

License: Internal use only

Members: Bernhard PETERS (Developer), Sébastien VARRETTE (Developer)

Description: The eXtended Discrete Element Method (XDEM), formerly Discrete Particle Method (DPM), is an advanced numerical simulation tool which deals with both motion and chemical conversion of particulate material such as coal or biomass in furnaces. However, predictions of solely motion or conversion in a de-coupled mode are also applicable. The Discrete Particle Method uses object oriented techniques that support objects representing three-dimensional particles of various shapes such as cylinders, discs or tetrahedrons for example, size and material properties. This makes it a highly versatile tool dealing with a large variety of different industrial applications of granular matter. A user interface allows easily extending the software further by adding user-defined models or material properties to an already available selection of materials, properties and reaction systems describing conversion. Thus, the user is relieved of underlying mathematics or software design, and therefore, is able to direct his focus entirely on the application. The Discrete Particle Method is organised in a hierarchical structure of C++ classes and works both in Linux and XP environments also on multi-processor machines. This software is developed by the XDEM research team, led by Prof. Bernhard Peters from the Research Unit in Engineering Science (RUES) in collaboration with the Department of Computer Science.

Yactul

License: N/A

Members: Steffen ROTHKUGEL (Architect)

Description: Yactul is a game-based student response framework for interactive education.

ZettaStreams

https://gitlab.uni.lu/omarcu/zettastreams

License: Apache2

Members: Ovidiu-Cristian MARCU (Developer)

Description: The ZettaStreams prototype is a unified storage and processing architecture for handling key-value and streaming storage and real-time processing. ZettaStreams develops on top of RAMCloud, KerA, DFI, Apache Arrow, Apache Flink.

Changes: ZettaStreams integrated latest RAMCloud, latest Flink, and a branch version of KerA in addition to new developments to support virtual-log replication (see Virtual Log-Structured Storage for High-Performance Streaming at IEEE Cluster 2021). A new deployment with Singularity on uni.lu HPC clusters enables reproducibility and experimental APIs for RDMA usage within ZettaStreams.

Appendix E

Staff Statistics

Note: Statistics in this chapter count staff numbers using FTE (Full-Time Equivalent) units. The FTE number takes into account the occupancy of the position (half-time, full-time or similar), as well as the start or end of the employment of the staff member during the course of the year.

An FTE number of 1.0 indicates a staff member being employed at full time for the duration of the whole year.

E.1 Number of Staff by Category (Full-Time Equivalent)

Category	**Number**
Doctoral Candidate	51.99
Postdoctoral Researcher	35.65
Professor	21.58
Student / Intern	19.64
Research Scientist	17.51
Scientific / Technical Support Staff	12.24
Research Associate	9.74
Administrative Staff	4.76
Research Facilitator	0.70
Project Coordinator	0.50
Technology Transfer Officer	0.12
Total	*174.43*

Table E.1: Number of Staff by Category

E.2 Distribution of Staff by Category

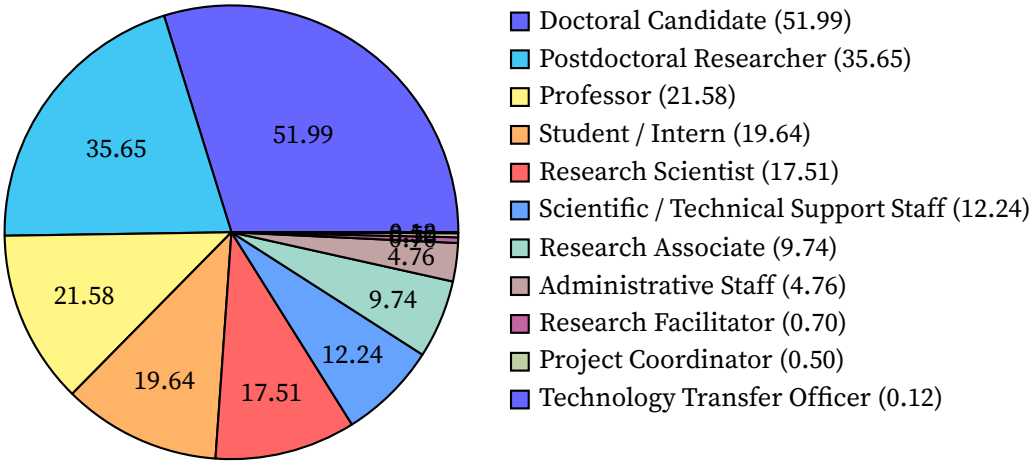


Figure E.1: Staff Distribution

E.3 List of Members by Category

Note: In the following list, staff members without an explicitly shown FTE number implicitly have an FTE number of 1.0.

Category	Last Name	First Name
Professor	BIRYUKOV	Alexei
	BOUVRY	Pascal (0.50 FTE)
	CORON	Jean-Sébastien
	ENGEL	Thomas
	GUELFI	Nicolas
	KELSEN	Pierre
	LE TRAON	Yves
	LEIVA	Luis (0.91 FTE)
	LEPREVOST	Franck
	LOUKAS	Andreas (0.16 FTE)
	MAUW	Sjouke
	MÜLLER	Volker
	NAVET	Nicolas
	PAPADAKIS	Mike
	ROTHKUGEL	Steffen
	RYAN	Peter Y A
	SACHAU	Juergen
	SCHOMMER	Christoph
	SORGER	Ulrich
	STEENIS	Bernard
	THEOBALD	Martin

Category	Last Name	First Name
	VAN DER TORRE	Leon
	ZAMPUNIERIS	Denis
Research Scientist	BOTEV	Jean
	BRUST	Matthias R. (0.79 FTE)
	CAPOZUCCA	Alfredo
	CORDY	Maxime
	DANOY	Grégoire
	DECOUCHANT	Jérémie (0.16 FTE)
	FRANCK	Christian
	HU	Tingting
	JAMROGA	Wojciech
	KIEFFER	Emmanuel
	MA	Qin (0.66 FTE)
	MUELLER	Johannes (0.91 FTE)
	PANG	Jun
	PINEL	Frederic (0.83 FTE)
	RIAL	Alfredo (0.16 FTE)
	RIES	Benoit
	ROENNE	Peter (0.24 FTE)
	RUPP	Andy
	SKROBOT	Marjan (0.75 FTE)
	VARRETTE	Sébastien
	WEYDERT	Emil
Postdoctoral Researcher	ACCLAVIO	Matteo
	ALEKSANDROVA	Marharyta
	BHATIA	Tarunpreet (0.08 FTE)
	BIRYUKOV	Maria
	BOUALOUACHE	Abdelwahab (0.16 FTE)
	BURSUC	Sergiu
	CARNEIRO PESSOA	Tiago (0.80 FTE)
	CHEN	Xihui (0.96 FTE)
	DAUPHIN	Jérémie (0.33 FTE)
	DESPOTOVIC	Vladimir
	DUBIEL	Mateusz (0.29 FTE)
	EBRAHIMI	Ehsan
	ELLAMPALLIL VENUGOPAL	Vinu (0.95 FTE)
	FEHER	Daniel (0.78 FTE)
	GAO	Jun (0.96 FTE)
	GUI	Yujuan (0.53 FTE)
	HASAN	Cengis
	HOEHN	Sviatlana
	HORNE	Ross James
	JIMENEZ	Matthieu
	KIM	Kisub (0.25 FTE)
	KNOKS	Aleks (0.33 FTE)

Category	Last Name	First Name
	KONG	Pingfan (0.71 FTE)
	KOUTSANTONIS	Loizos
	LIBAL	Tomer (0.67 FTE)
	LOMBARD-PLATET	Marius (0.25 FTE)
	MARCU	Ovidiu-Cristian (0.88 FTE)
	MARKOVICH	Réka (0.99 FTE)
	MIZERA	Andrzej
	MUELLER	Johannes (0.08 FTE)
	NAJJAR	Amro
	NOUZRI	Sana
	ROSSI	Arianna
	ROY	Arijit (0.75 FTE)
	RWEMALIKA	Renaud (0.21 FTE)
	SAHU	Rajeev Anand
	SALA	Petra (0.25 FTE)
	SIRAJZADE	Joshgun (0.87 FTE)
	SKROBOT	Marjan (0.24 FTE)
	STEEN	Alexander
	STOLFI ROSSO	Daniel
	TATARINOV	Juliane (0.91 FTE)
	TEH	Je Sen (0.13 FTE)
	TIKHOMIROV	Sergei (0.75 FTE)
	TITCHEU CHEKAM	Thierry (0.04 FTE)
	TOPAL	Ali Osman (0.84 FTE)
	WANG	Qingju
	WASIM	Muhammad Umer (0.87 FTE)
	ZOLLINGER	Marie-Laure (0.79 FTE)
Research Associate	BARTEL	Alexandre (0.19 FTE)
	BOUALOUACHE	Abdelwahab (0.83 FTE)
	CHEN	Xihui (0.04 FTE)
	FOTIADIS	Georgios
	KAISER	Daniel
	KRISHNASAMY	Ezhilmathi
	MESTEL	David
	OSTREV	Dimiter (0.75 FTE)
	RAMIREZ CRUZ	Yunior (0.41 FTE)
	SCHIFFNER	Stefan (0.79 FTE)
	TABATABAEI	Masoud
	TALBOT	Pierre
	TURCANU	Ion (0.75 FTE)
Project Coordinator	OCHSENBEIN	Anne (0.50 FTE)
Technology Transfer Officer	WASIM	Muhammad Umer (0.12 FTE)
Research Facilitator	OESTLUND	Stefanie (0.70 FTE)

Category	Last Name	First Name
Scientific / Technical Support Staff	CARTIAUX	Hyacinthe
	DAUPHIN	Jérémie (0.58 FTE)
	FUENMAYOR PELAEZ	David (0.84 FTE)
	GLODT	Christian
	GROSZSCHÄDL	Johann
	HOUITTE	Pierre-Yves
	LADID	Latif
	MACHALEK	Aurel
	OLLOH	Abatcha
	REIS	Sandro
	SKORSKI	Maciej (0.83 FTE)
	STEMPER	André
	VALETTE	Teddy
Doctoral Candidate	ADAVOUDI JOLFAEI	Amirhossein
	ANTONIADIS	Nikolaos (0.41 FTE)
	ATASHPENDAR	Aryobarzan (0.25 FTE)
	BALOGLU	Sevdenur
	BARTHEL	Jim Jean-Pierre
	BUSCEMI	Alessio
	CARDOSO DOS SANTOS	Luan
	CHAYCHI	Samira
	CHEN	Ninghan
	CHENG	Hao
	CHITIC	Ioana Raluca
	COMBARRO SIMON	Manuel (0.16 FTE)
	DALLE LUCCA TOSI	Mauro
	DAMODARAN	Aditya Shyam Shankar
	DE LA CADENA RAMOS	Augusto Wladimir (0.04 FTE)
	DUFLO	Gabriel
	EL ORCHE	Fatima Ezzahra
	ESMAEILZADEH DILMAGHANI	Saharnaz (0.66 FTE)
	ESTAJI	Ehsan
	FISCARELLI	Antonio Maria (0.16 FTE)
	FOTOUHI	Mahdi (0.25 FTE)
	GAO	Jun (0.04 FTE)
	GARG	Aayush
	GHAMIZI	Salah
	GIL PONS	Reynaldo
	HADDADAN	Shohreh (0.70 FTE)
	HOSSEINI KIVANANI	Nina (0.96 FTE)
	HU	Hailong
	JAHIC	Benjamin

Category	Last Name	First Name
	KALISKI	Adam (0.71 FTE)
	KAMLOVSKAYA	Ekaterina (0.99 FTE)
	KARPATI	Daniel (0.96 FTE)
	KELLER	Patrick
	KIM	Kisub (0.58 FTE)
	KIM	Yan
	KONG	Pingfan (0.28 FTE)
	LI	Xu (0.25 FTE)
	LIU	Chao
	MA	Wei
	MAI	TIEU LONG
	MAKKI	Ayman
	PICARD	Stéven (0.33 FTE)
	QIAO	Lisha (0.91 FTE)
	RAGOT	Adrien (0.70 FTE)
	RIDA	Ahmad
	RWEMALIKA	Renaud (0.79 FTE)
	SALA	Petra (0.74 FTE)
	SAMIR LABIB	Nader (0.66 FTE)
	SOROUSH	Najmeh
	SOUANI	Badr (0.16 FTE)
	STREIT	David D
	SUN	Ningyuan
	TAWAKULI	Amal
	TEMPERONI	Alessandro
	THANAPOL	Panissara
	TORCHYAN	Khachatur (0.58 FTE)
	VAN WIER	Jeroen
	VITTO	Giuseppe
	WANG	Aoran
	XU	Jingjing (0.58 FTE)
	YU	Liuwen
	YURKOV	Semen
	ZAHORANSKY	Valeria
	ZEYEN	Olivier (0.16 FTE)
	ZHONG	Zhiqiang
Administrative Staff	EDWARDSDOTTIR	Helga Fanney
	FINNSSON	
	PECERO SANCHEZ	Johnatan Eliabeth (0.59 FTE)
	PUECH	Andrea (0.80 FTE)
	SCHMITZ	Fabienne
	SCHROEDER	Isabelle (0.50 FTE)
	VANDEVENTER	Arlyne (0.87 FTE)
Student / Intern	AKINYEMI	Opeyemi Priscilla (0.34 FTE)

Category	Last Name	First Name
	ALSAHLI	Malik Ruzayq M (0.83 FTE)
	ANTROPOVA	Daria (0.99 FTE)
	ATASHPENDAR	Aryobarzan (0.08 FTE)
	AVDUSINOVIC	Elmir (0.29 FTE)
	BEGUM	Rubaiya (0.50 FTE)
	BOLOWICH	Alya (0.14 FTE)
	BONTE	Eliott Cyril Michel (0.60 FTE)
	BORGOGNONI	Alex (0.15 FTE)
	BOURSCHEID	Thiago Jorge (0.91 FTE)
	CAO	Rui (0.79 FTE)
	CHEN	Xiao Zhou Gilles (0.11 FTE)
	CHERNAKOV	Pavel (0.50 FTE)
	DE JESUS MATIAS	Flavio (0.10 FTE)
	DE JESUS SOUSA	Tiago Alexandre (0.99 FTE)
	DE PLAEN	Celine (0.07 FTE)
	DERIDDER	Nathan Lennart Vicky (0.29 FTE)
	FATHI	Fatima Zahra (0.95 FTE)
	FERSTLER	Yves Claude (0.39 FTE)
	GAMBOA DOS SANTOS	Léo (0.05 FTE)
	GAREEV	Daniel (0.76 FTE)
	GHARBIN	Prince Yaw (0.13 FTE)
	GOLDBERG	Alexander Linnevers (0.08 FTE)
	HANG	Kevin (0.05 FTE)
	HANI	Moad (0.83 FTE)
	HOFFMANN	Yann (0.08 FTE)
	HOUSSEL	Paul Robert Balthazar (0.05 FTE)
	HUGOT	Simon (0.08 FTE)
	IGHANIAN	Paria (0.42 FTE)
	JAHIC	Alen (0.39 FTE)
	KEHONJIC	Armin (0.25 FTE)
	KUDRYAVTSEVA	Kristina (0.16 FTE)
	KUMAR	Ravindra (0.41 FTE)
	KYRIAZIS	Christos (0.16 FTE)
	LICINA	Esada (0.11 FTE)
	LIMONIER	Joris, Shan, Andre (0.29 FTE)
	MARTINA	Antoine Joseph Dominique (0.50 FTE)
	MILCZAREK	Zofia (0.08 FTE)
	OHLHOFF	Claude Marc (0.52 FTE)

Category	Last Name	First Name
	PEREHUDA	Yevhen (0.63 FTE)
	POLDRUGO	Alex (0.25 FTE)
	RADWAN	Ahmed (0.33 FTE)
	RUZIC	Alen (0.24 FTE)
	SCHROEDER	Quentin (0.08 FTE)
	SHOJAEE	Nooshin (0.95 FTE)
	SOUANI	Badr (0.46 FTE)
	SPADONI	Gabriel Sergio Jalmar (0.27 FTE)
	SURYAVANSHI	Roma (0.17 FTE)
	SUVANTO	Elias (0.22 FTE)
	TANNOURY	Joe (0.08 FTE)
	TOSTES	Guillaume (0.01 FTE)
	VARADHARAJAN	Vanitha (0.74 FTE)
	VIEGAS MILANI	Adriano (0.08 FTE)
	WOLBERT	David (0.06 FTE)
	YOUSEEF	Boghos (0.16 FTE)
	ZEYEN	Olivier (0.42 FTE)
	ZHAKUDAYEVA	Arnagul (0.05 FTE)

Appendix F

List of Acronyms

ComSys: Communicative Systems Laboratory
CSC: Computer Science & Communications
DCS: Department of Computer Science
HPC: High Performance Computing
ILIAS: Interdisciplinary Laboratory for Intelligent and Adaptive Systems
LACS: Laboratory of Algorithmics, Cryptology and Security
LASSY: Laboratory for Advanced Software Systems
SnT: Interdisciplinary Centre for Security Reliability and Trust
UL: University of Luxembourg
FNR: Fonds National de la Recherche Luxembourg

https://dcs.uni.lu

Department of Computer Science (DCS)
University of Luxembourg
Faculty of Science, Technology and Medecine
6, avenue de la Fonte
L-4364 Esch-sur-Alzette
Luxembourg

Administrative Contact:

Isabelle Glemot-Schroeder, Andrea Puech and Fabienne Schmitz
Email: dcs@uni.lu