DCS | DEPARTMENT OF COMPUTER SCIENCE
uni.lu UNIVERSITY OF LUXEMBOURG

FACULTY OF SCIENCE, TECHNOLOGY AND MEDICINE

Department of Computer Science

Activity Report 2020

DCS | DEPARTMENT OF COMPUTER SCIENCE

Department of Computer Science

Activity Report 2020

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

Department of Computer Science
Activity Report 2020

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:	07-06-2021
Note:	This report was created using LaTeX with a template based on previous work by Sebastien Varrette.

Preface

Dear reader,

This annual report synthesizes the progress and activities of the Department of Computer Science in 2020, 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 more than 165 full-time equivalent members involved in both teaching and research activities.

In 2020, the department showed its resilience against the disrupting effects of the Covid pandemic. On short notice, the department was able to successfully organize its teaching duties online and research activities continued mostly as planned. All members of our department did an excellent job in continuing their work under new side conditions.

This year marks the official transformation of the CSC research unit into the Department of Computer Science. To coordinate the responsibilities that come with the status of a department, Nicolas Navet was nominated as the department's first Head of Teaching. We completed the hiring process of two new professors in Machine Learning and Human Computer Interaction. Excellence of our teaching was recognized by the UL teaching award 2020 for Martin Theobald and Alfredo Capozucca. Further, the year was characterised by the UL teaching evaluation and preparation for the accreditation of three of our study programs The initial feedback of both seem to indicate a very positive outcome. Our research activities have led to many publications in top journals and conferences and have also led to significant outreach in the academic and societal context.

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^{2}DH 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 2020 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 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^{2}DH, 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 composition 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 Professors, 12 PostDoc researchers, as well as to 12 Doctoral students. 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, Big Data, and Robotics.

The collaboration with the **Interdisciplinary Centres SnT, LCSB, and C^{2}DH** as well as with the **Luxembourg School of Finance (LSF)** and the **Departments of Law and Humanities**, the involvement with the **High Performance Computing facility** (HPC), and the collaboration with the **Computational Sciences initiative** reflect ILIAS's significance for Luxembourg's strategic priorities and future.

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

- **Big Data**: 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.
- **Information Theory and Stochastic Inference**: the main research topics here are Signal Processing, Error-Correcting Codes, and Probabilistic Graphical Models.
- **Knowledge Discovery and Mining**: 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**: 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**: 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 RoboLab or within the Robo-Football Team, and prepare them for new upcoming disciplines in Artificial Intelligence, Machine Learning, and beyond. We are in contact to the *Luxembourgish Ethics Council* concerning the questions to *Artificial Intelligence and Ethics*.

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

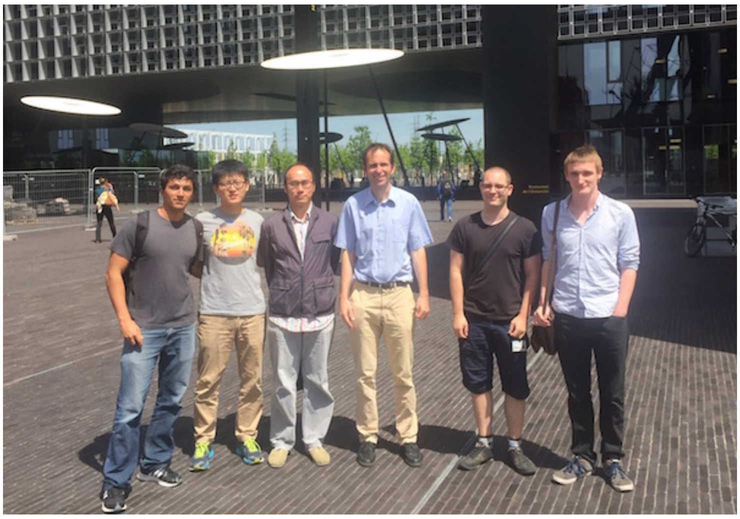
Our research on Advanced Software and Systems (LASSY) can be structured into five partly overlapping dimensions: modelling, methodology, computing paradigms, dependability (including security) and main application domains.

- 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 2020

- 3 publications at top-tier conferences in cryptography (Eurocrypt, Crypto *2)

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

- Jean-Sébastien Coron, Agnese Gini: A Polynomial-Time Algorithm for Solving the Hidden Subset Sum Problem. CRYPTO (2) 2020: 3-31

  We describe an efficient algorithm for solving a 20 year old problem.

- Sonia Belaïd, Jean-Sébastien Coron, Emmanuel Prouff, Matthieu Rivain, Abdul Rahman Taleb. Random Probing Security: Verification, Composition, Expansion and New Constructions. CRYPTO (1) 2020: 339-368

We describe an efficient countermeasure against side-channel attacks.

- Jean-Sébastien Coron, Aurélien Greuet, Rina Zeitoun. Side-Channel Masking with Pseudo-Random Generator. EUROCRYPT (3) 2020: 342-375

  We describe an efficient countermeasure against side-channel attacks.

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) crypto.

Summary of the group's achievements in 2020

Despite the Covid situation and having part of the group split off to form the new IRISC group headed by Dr Lenzini, the group still has a successful year. Notably the group landed a role in the EuroQCI project to develop an infrastructure for secure communication with key establishment using quantum protocols over satellites.

1. Research projects:
   (a) New FNR CORE Junior project "FP2: Future-Proofing Privacy in Secure Electronic Voting"
   (b) The Horizon 2020 FutureTPM project ended successfully, with high praise from the reviewers.
   (c) New FNR COVID-19 Fast Track project SmartExit: Facilitating optimal containment and exit strategies with minimal disclosure access control and tracking
   (d) New FNR CORE project EquiVox: Secure, Quantum-Safe, Practical Voting Technologies
2. The project on COVID containment strategies, included an appearance by Prof Ryan in the media: https://delano.lu/d/detail/news/it-time-luxembourg-adopted-contact-tracing-app/212118 and Prof Jamroga's keynote talk "Facilitating optimal containment and exit strategies with minimal

disclosure access control and tracking." Anti-Covid: Informatics in Mitigation of Covid-19, 22-23 June 2020, virtual.

3. Marie-Laure Zollinger defended her doctoral thesis and was awarded the Excellent Doctoral Thesis Award.
4. Ehsan Estaji's PhD Colloquium presentation was awarded best PhD presentation at E-Vote-ID 2020
5. Software:
   (a) AVXECC (High-throughput elliptic curve cryptography software using Advanced Vector Extensions)
   (b) MsATL (MonoSat for Alternating-time Temporal Logic)
   (c) STV (STrategic Verifier)

The Verifiable Voting Workshop in association with Financial Crypto, founded by Ryan in 2016, had its fifth, successful edition. The APSIA Quantum Lab grow to nine researchers.

Courses taught: Information Security Basics, Security Modelling and Principles of Security Engineering. Dr Mestel proposed, and had accepted, a new MISC course on "Advanced Computing" to start summer semester 2021. The group also contributed to the supervision and evaluation of several 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 2020

1. Hao Cheng, Johann Großschädl, Peter B. Rønne, Peter Y. A. Ryan: Lightweight Post-quantum Key Encapsulation for 8-bit AVR Microcontrollers. CARDIS 2020: 18-33
2. Najmeh Soroush, Vincenzo Iovino, Alfredo Rial, Peter B. Rønne, Peter Y. A. Ryan: Verifiable Inner Product Encryption Scheme. Public Key Cryptography (1) 2020: 65-94
3. Vincenzo Iovino, Alfredo Rial, Peter B. Rønne, Peter Y. A. Ryan: Universal Unconditional Verifiability in E-Voting without Trusted Parties. CSF 2020: 33-48

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 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 two PhD students, Alessandro Temperoni and Mauro Dalle Lucca Tosi, as well as three post-doctoral researchers, Dr. Jeremie Dauphin, Dr. Maciej Skorski and Dr. Vinu Venugopal. Two more PhD students are jointly supervised in the context of a new FNR-PRIDE doctoral training unit (DTU) on “Data-Driven Computational Modeling and Applications”, of which Martin Theobald serves as a co-PI. Two of the above post-doc positions are currently 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 is intended to make the broad area of Artificial Intelligence accessible to a larger audience in Luxembourg. While the COVID19 crisis certainly also affected our group in the past year, our research activities continued to focus on the following three main areas:

(1) Information Extraction & Knowledge-Base Construction

In collaboration with the Max-Planck-Institute in Saarbruecken, 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 will further intensify 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.

(2) Probabilistic & Temporal Databases

A second research focus lies in the development of probabilistic and temporal database models and systems. The team was involved in the development of the Trio probabilistic database system at Stanford University, which was the first principled approach to couple data uncertainty with relational data by using SQL as a query language. Further ongoing research activities (in collaboration with Michael Böhlen, University of Zurich) are in the context of temporal database models that now also fully support the afore-described probabilistic extensions. Further ongoing collaborations in this domain are with Northeastern University (Wolfgang Gatterbauer) and the University of Antwerp (Floris Geerts). Moreover, Martin Theobald served as PC co-chair of the “27th International Symposium on Temporal Representation and Reasoning” (TIME 2020), which was held (virtually) in Bozen/Bolzano, Italy, on September 23-25, 2020.

(3) Distributed Graph Databases

We recently developed the TriAD distributed graph engine, which is one of the fastest currently available engines for RDF data and SPARQL queries. TriAD is purely based on in-memory index structures and implements its own custom communication protocol, based on asynchronous message passing, which outperforms MapReduce-based protocols by several orders of magnitude. Recent extensions of TriAD also support more general graph-pattern queries, including the new SPARQL 1.1 specification.

As a follow-up project at the University of Luxembourg, we intensively worked on the development of our new AIR asynchronous stream-processing engine over the past year, which carries over a number of concepts from TriAD 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 include the investigation of Deep Learning techniques directly into this stream-processing platform.

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

We intensively employed the recent 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 supervised two Master theses in the above areas and contributed to more than 420 hours of teaching in 2020. Moreover, Martin Theobald has received a Teaching Award by the University of Luxembourg (one out of two which were awarded within the faculty) in 2020. The group also actively contributes to the curriculum of a new Master program in Data Science, which is intended to launch in the Winter Term of 2021, with two lectures in the areas of “Cloud Computing & NoSQL Databases” and “Big Data Analytics”.

Summary of the group’s achievements in 2020

1. Yan Wu, Jinchuan Chen, Plarent Haxhidauti, Vinu E. Venugopal, Martin Theobald: Guided Inductive Logic Programming: Cleaning Knowledge Bases with Iterative User Feedback. GCAI 2020: 92-106

2. Vinu E. Venugopal, Martin Theobald, Samira Chaychi, Amal Tawakuli: AIR: A Light-Weight Yet High-Performance Dataflow Engine based on Asynchronous Iterative Routing. SBAC-PAD 2020: 51-58

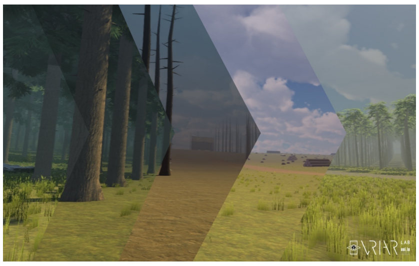
3. Emilio Muñoz-Velasco, Ana Ozaki, Martin Theobald: 27th International Symposium on Temporal Representation and Reasoning (TIME 2020), LIPIcs 178, Schloss Dagstuhl - Leibniz-Zentrum für Informatik 2020, ISBN 978-3-95977-167-2

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 2020



By the end of 2020, the COaST group counted 5 members (1 professor, 1 senior researcher, 1 post-doc, 2 PhD candidates), and 8 publications. The group's research in the context of the ongoing projects DELICIOS and Forest SaVR appeared in renowned academic publications and was presented at various international conferences and scientific events, winning a best demo/presentation award. The H2020 FET Open project ChronoPilot was funded with Dr. Botev as a PI. The 3 million euro project involves a consortium of five European universities. Furthermore, a collaborative project between the VR/AR Lab and the C^{2}DH for a digital treasure hunt in the context of the upcoming Légionnaires exhibition at the Musée Dräi Echelen was launched. Besides, members of the group were involved in the organization of various international scientific events and conferences such as IEEE ACSOS, SAOS/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, as well as guest lecturing abroad. Christian Grévisse successfully defended his PhD thesis.

Three most important publications in 2020

1. **Jean Botev, Adriano Viegas Milani.** Forest SaVR – A Virtual-Reality Application to Raise Awareness of Deforestation. In Proc. 17th GI VR/AR Workshop (VAR), pp.1-4, 2020. Best Demo/Poster Award.
   Deforestation is a serious issue affecting climate and contributing to global warming. This paper presents Forest SaVR, an interactive virtual-reality (VR) application where users can explore a realistic forest environment to experience the various stages and effects of deforestation immersively. The stages range from healthy over cleared to cultivated, and the direct VR experience allows to reconnect and reengage users with contexts that would otherwise remain abstract.

2. **Christian Grévisse, Carina Martins Gomes, Steffen Rothkugel.** AR4OER – A Semantic Platform for Open Educational Augmented Reality Re-

sources. In Proc. 22nd IEEE International Symposium on Multimedia (ISM), pp.227-232, 2020.
Augmented reality (AR) experiences in the classroom permit new ways of interaction and visualization and increase student motivation and engagement. This paper discusses a platform for heterogeneous AR experiences provided as Open Educational Resources (OER) with semantically enriched metadata, reducing the need for costly hardware specific to certain scientific domains. Different scenarios can be integrated through a lose coupling in third-party apps.

3. **Ningyuan Sun, Jean Botev**. Intelligent Adaptive Agents and Trust in Virtual and Augmented Reality. In Proc. 19th IEEE International Symposium on Mixed and Augmented Reality (ISMAR), pp.303-305, 2020.
Intelligent adaptive agents (IAA) can significantly facilitate everyday tasks and are increasingly finding their way into many aspects of daily life. This paper takes a multidisciplinary perspective on trust formation between users and IAA in virtual and augmented reality (VR/AR). The experiential and immersive character of these technologies particularly allows for new ways of interaction and requires systemizing the design of IAA in future VR/AR settings.

4.5 Communication and Information Theory (Cain)

Head of research group: Prof. Dr. Ulrich Sorger

The Cain group is a small research group both in the ILIAS, and the ComSys institutes. It is a part of the SECAN-Lab, too. There are frequent collaborations and exchanges with researchers from other groups like Bouvry's Parallel Computing and Optimisation Group (PCOG), Engel's Security and Networking Lab (SECAN-Lab), or Biryukov's cryptology research group (CryptoLUX). New cooperation started at the end of 2018 with the group of Prof. Viti (Mobilab). The core expertise of the group are mathematical principles behind the efficient encoding of information and the realisation of reliable error-free digital communication systems.

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 2020

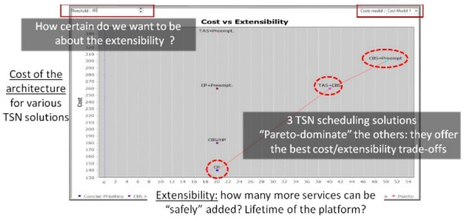
In 2020 the CRTES group comprised 5 members (1 professor, 1 research scientist, 3 PhD students) and had 9 peer-reviewed publications published or accepted. The group's members have taught 5 courses, both at the Bachelor (professional and academic) and Master levels, and supervised 5 Bachelor semester projects (BSP). Prof. Navet serves since July 2020 as deputy head of the department in charge of teaching. He was in the defense board of 3 Phd thesis, 3 Phd supervisory committees and TPC member of 4 conferences.

Most of our work in 2020 was in the field of E/E architecture design and real-time communication networks. Our work aims to further automate the design activities based on constraints and goals. We have been exploring an approach rooted in computational thinking where system designers break down the general multi-dimensional design problem into smaller problems that algorithmics tools can solve in a near optimal way. 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. We also studied how to enhance the design-space exploration (DSE) by guiding the search algorithms based on domain knowledge capturing practical topological constraints as well as security and reliability requirements. Motivated by the need of "fail operational" in automated driving systems, we quantified the reliability / costs trade-offs of different data redundancy solutions that can be implemented with IEEE 802.1CB-2017, which is the IEEE Time-Sensitive-Networking (TSN) standard that supports data redundancy.

Three most interesting publications in 2020

1) T. Hu, I. Cibrario Bertolotti, N. Navet, L. Havet, "Automated Fault Tolerance Augmentation in Model-Driven Engineering for CPS", Computer Standards & Interfaces, Elsevier, vol. 70, June 2020. We propose an approach implemented in an open-source model-transformation framework which allows system designers to decouple functional and non-functional concerns, and express dependability properties at design time using domain-specific languages. The functional control models are then automatically "augmented" with dependability mechanisms while preserving their real-time behavior. The practicality of the approach is demonstrated with the automated implementation of

N-Version Programming in the CPAL model-driven engineering workflow.



Cost/Extensibility trade-offs of different E/E architecture candidate solutions

2) O. Creighton, N. Navet, P. Keller, J. Migge, ”Early-stage topological and technological choices for TSN-based communication architectures”, 2020 IEEE Standards Association (IEEE-SA) Ethernet & IP @ Automotive Technology Day, Munich, September 14-18, 2020. In this joint work with BMW, we explore the ability of algorithmic tools to synthesize Ethernet-based architectures based on a minimal fixed core Ethernet TSN topology, design goals, design constraints, assumptions about next generation applications and data from past projects capturing part of the OEM domain knowledge.

3) T.L. Mai, N. Navet, ”Deep Learning to Predict the Feasibility of Priority-Based Ethernet Network Configurations”, technical report in submission. 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. Even when using ensembles of 32 GNN models, the speedup factor over schedulability analysis ranges from 77 to 1715 in our testing sets, which will facilitate the implementation of DSE algorithms in the design of E/E architectures.

4.7 Critical and Extreme Security and Dependability (CritiX)

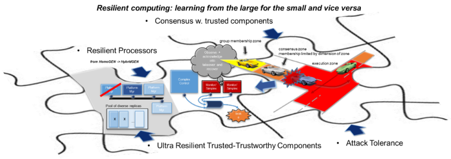
Head of research group: Prof. Dr. Paulo Esteves-Veríssimo (PJV) (until Oct. 2020), Prof. Dr. Marcus Völp

The CritiX lab (https://wwwen.uni.lu/snt/research/critix) was set up in September 2014 at SnT. The group investigates and develops paradigms and techniques for defeating extreme adversary power and sustaining perpetual and unattended operation. CritiX focusses on four scientific priorities, focal points of the PEARL programme: 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 2020


Resilient computing: learning from the large for the small and vice versa
• Consensus w. trusted components
• Resilient Processors
from HomoGEN -> HybridGEN
Platform Mgr
Platform Mgr
Platform Mgr
Platform Mgr
Pool of diverse replicas
x
x
...
Complex Control
Observe + acknowledge into takeover and recover
Monitor/ Simplex
Monitor/ Simplex
brake
group membership zone
consensus zone
membership limited by dimension of zone
execution zone
• Ultra Resilient Trusted-Trustworthy Components
• Attack Tolerance

Despite the pandemic, to which CritiX contributed with the logically centralized, physically distributed PriLok epidemic tracing infrastructure, an architecture fully realizable within the scope of the regulated part of our mobile communication infrastructure, CritiX has seen an immense success in finished Doctoral thesis and PhD defenses. Out of the three candidates that finished, all were nominated and two received the University of Luxembourg Outstanding Thesis Award: Dr. Diego Kreuz for his thesis on Logically Centralized Security for Software-Defined Networking, and Dr. Ivana Vukotic, for her thesis on a Formal Framework for Verifying Implementations of Byzantine Fault-Tolerant Protocols Under Various Models, a work, preeminent scientist Prof. Zachary Tatlock (Washington University and co-inventor of the Verdi interactive theorem prover) thought was impossible. This is while continuing our successful contribution to the state of the art through publication in high-ranked workshops, conferences and journals.

Although the INTEL Labs partnership ended, CritiX is still in contact with INTEL's product division about a technology transfer of our iBFT protocol, which outperforms the seminal hybrid-BFT protocol MinBFT by 3 orders of magnitude. CritiX signed a new partnership with Huawei on the Cyber Intrusion Resilience for Control Systems of Intelligent Vehicles. A significant highlight was the organisation of the 32nd Euromicro Conference on Real-Time Systems, where recently appointed Prof. Völp served as program chair, putting SnT on the map of real-time and embedded systems research. CritiX further contributed to placing SnT's and the University of Luxembourg's security and resilient computing expertise into the European Cybersecurity Atlas, by contributing to two of in total four Cybersecurity Competence Networks in H2020. This is in addition to the H2020 project ADMORPH to which Prof. Völp contributes with his research on threat adaptive control 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 crypto currencies, smart contracts, and other emerging areas in information security, privacy, and anonymity. Further information about the group is available at https://www.cryptolux.org.

Summary of the group's achievements in 2020

In 2020 the CryptoLux group consisted of 6 members (1 full professor, 1 research and development specialist (shared), 1 postdoc, and 4 Ph.D. students), who published 12 papers in major international journals and conference proceedings. Two Ph.D. students (Daniel Feher and Sergei Tikhomirov) defended their Ph.D. thesis and continued to work in the CryptoLux group as postdocs. The FNR CORE project FinCrypt, which deals with financial cryptography, entered its third year. In addition, the UL-internal research project FDISC (”Future Directions in Symmetric Cryptography”) was successfully completed in 2020. Professor Biryukov served on the technical program committee of several international conferences, including ACNS, CBT, and FC (Financial Crypto). The postdoctoral researcher Qingju Wang was a member of the editorial board of the IACR journal ”Transactions on Symmetric Cryptography (ToSC)”. CryptoLux members taught various courses in the bachelor and master programs and supervised student projects.

Most interesting achievements in 2020

1. The authenticated encryption algorithm Schwaemm and the hash function Esch (both based on the SPARKLE permutation) are currently in the second round of the Lightweight Cryptography 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. In 2020, the CryptoLux group extended the SPARKLE family by a lightweight block cipher and a tweakable block cipher. In addition, the group developed highly optimized Assembler implementations of SPARKLE for 8-bit AVR and 32-bit ARM microcontrollers, which made Schwaemm the performance leader among all 2nd-round candidates.

2. In the course of the FinCrypt project, the CryptoLux group demonstrated that the Lightning Network (LN), a second-layer payment protocol built atop of a blockchain-based cryptocurrency like Bitcoin, has some exploitable privacy gaps. Concretely, the group showed how an attacker can deanonymize LN channel balances (i.e., user accounts on LN) through ”probing,” i.e., by sending payments of varying sizes to determine the distribution of funds in each channel. This research has significant real-world implications since it allows an attacker to discover how much Bitcoin a channel held. On the constructive side, the group proposed two approaches that allow the LN to (partially) overcome these issues and achieve a better trade-off between privacy and routing efficiency.

3. As part of the research activities of the FDISC project, the CryptoLux group advanced the state of research on the division property, a distinguishing

property introduced by Todo (EUROCRYPT 2015) for the cryptanalysis of block ciphers. One of these advancements is the discovery of links between the division property and several variants of the cube attack. Furthermore, the group proposed a new modeling method for the three-subset division property without unknown subset. In addition, an algebraic formulation of the division property was introduced along with a technique called monomial prediction, which enabled improved attacks against the stream cipher Trivium.

Top academic publications

1. Christof Beierle, Alex Biryukov, Luan Cardoso dos Santos, Johann Großschädl, Léo Perrin, Aleksei Udovenko, Vesselin Velichkov, Qingju Wang. Alzette: A 64-Bit ARX-box (Feat. CRAX and TRAX). Advances in Cryptology – CRYPTO 2020, vol 12172 of Lecture Notes in Computer Science 12172, pp. 419-448, Springer Verlag, 2020.
2. Ward Beullens, Tim Beyne, Aleksei Udovenko, Giuseppe Vitto. Cryptanalysis of the Legendre PRF and Generalizations.
IACR Transaction on Symmetric Cryptology, vol. 2020, no. 1, pp. 313-330, May 2020.
3. Yonglin Hao, Gregor Leander, Willi Meier, Yosuke Todo, Qingju Wang. Modeling for Three-Subset Division Property Without Unknown Subset - Improved Cube Attacks Against Trivium and Grain-128AEAD. Advances in Cryptology – EUROCRYPT 2020, vol. 12105 of Lecture Notes in Computer Science 12105, pp. 466-495, Springer Verlag, 2020.

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 2020: Qin Ma (research scientist) 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 2020

In 2020, the team published the findings of the lightweight modeling research (initiated in 2018) in the 16th European Conference on Modelling Foundations and Applications (see reference [1] below), culminating in a entirely web-based tool named Fudomo (available at fudomo.uni.lu). The framework itself was taught in the 2020 edition of the model-driven software development course of the MICS programme with several students developing projects based on the Fudomo tool.

In 2020, Qin Ma participated in the research activities of the FMDE research group led by Prof. Kelsen. More specifically, the focus has been on the design, implementation, and dissemination of a light-weight modeling framework (FUDOMO) for domain modeling and model-to-text transformations. In parallel, she continued her collaboration with colleagues from the University of Duisburg-Essen and from the Mexico Autonomous Institute of Technology in the field of smart grids, whereby conceptual modeling languages and model-based analysis techniques are used in tandem to enable strategic analysis of blockchain-based smart grid initiatives. In addition, two new threads have also been initiated within the collaboration during the course of 2020: (1) applying cognitive linguistic lens (such as conceptual blending) for the analysis of ICT concepts, and (2) enhancing the validation capabilities of enterprise modeling method engineering platform ADOxx with a light-weight formal method Alloy.

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 in the model-driven software development course of the MICS program, and supervised a S1 BSP project in the BICS program. Qin Ma was also an external reviewer of the AIS conference AMCIS 2020.

Christian Glodt worked on upgrading the existing Atom-based Fudomo tool to work as a web application that can be used from a browser without installing any other software. He also maintained and improved ”Accord”, the research information database of the DCS. 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 (or other achievements) in 2020

1. Kelsen, P., Ma, Q., & Glodt, C. (2020). A Lightweight Modeling Approach Based on Functional Decomposition. Journal of Object Technology, 19(2), 15.
   This publication summarizes our work on example-driven modeling using the Fudomo approach as well as the associated tool of the same name.

2. de Kinderen, S., Ma, Q., & Kaczmarek-Heß, M. (2020, November). Towards Extending the Validation Possibilities of ADOxx with Alloy. In IFIP Working Conference on The Practice of Enterprise Modeling (pp. 138-152). Springer, Cham.

3. de Kinderen, S., Kaczmarek-Heß, M., Ma, Q., & Razo-Zapata I. 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, Enterprise Modelling and Information Systems Architectures - International Journal of Conceptual Modeling (EMISAJ), accepted, 2020.

4.10 Individual and Collective Reasoning Group (ICR)

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

ICR is an interdisciplinary research group in the Dept. of Computer Science. At UL it collaborates a.o. with Digital History, HCI, Psychology, Philosophy, and Law. There are extensive links with leading research institutions all over the world, e.g. Stanford, TU Vienna, and the Institute of Logic and Cognition at the prestigious Zhejiang University in China. Businesswise, ICR is a major partner of LuxAI, its highly successful spinoff.

ICR investigates the theoretical foundations and the computational modeling of high-level cognitive tasks characteristic for intelligent agents, like reasoning, learning/ revision, judgment, explanation, and argumentation. Specific research areas are Normative reasoning in multi-agent contexts (Deontic logics, Social robotics, Explain-able AI, AI-Ethics), Legal Informatics/AI, Logics for Artificial Intelligence (semantics, deduction, computation), and Reasoning under uncertainty, e.g. defeasible inference, formal argumentation, and knowledge/belief dynamics. ICR is furthermore a driving force of the AI-Robolab of the DCS.

Summary of the group's achievements in 2020

In 2020, ICR hosted (altogether) 20 researchers: 1 full professor, 2 visiting professors, 1 research scientist, 9 post-docs, 7 PhD students, as well as bachelor/master students, e.g. in the AIRobolab.

2 students finished their PhD in 2020, 2 postdocs got a permanant job in Academia. ICR is involved in the MSCA ITN program LAST-JD-RIoE (Joint Int. Doctoral Degree in Law, Science, and Technology - Rights of the Internet of Everything), and started teaching for the Int. Space Master with the course Law, Science, and Technology. In the context of ECAI2020, ICR organized the first ESA-CLAIRE online conf. on Space&AI with top keynote speakers and panelists (spaceandai.ijs.si). A paper by Libal and Steen won the best paper award at the major legal informatics event IRIS 2020. A paper by Dauphin et al. got the best student paper award at COMMA 2020.

ICR also launched the AI & Art Pavilion, a big cross-disciplinary outreach project involving artists, researchers and students, co-funded by Esch2022, UL, and a FNR PSP (Kick-off Sep.25). A framework agreement created the foundation for ZLAIRE, the ”Zhejiang-Luxembourg University Joint Lab on Advanced Intelligent Systems and REasoning”, based on the long-standing cooperation between Prof. B. Liao and ICR.

Last but not least, ICR-members have been very succesful in winning projects: AURELEE (FNR junior CORE), DELIGHT (FNR OPEN), ADELE (EU Justice), INDIGO (NORFACE Governance), DILLAN (FNR PRIDE), EXPECTATION (EU CHIST-ERA), C21(FNR IPBG), ICOMPLAI (FNR JUMP PoC), PaCT (FNR JUMP PATHFINDER).

Most important publications in 2020

1. **C. Benzmüller, X. Parent, L. van der Torre**. *Designing normative theories for ethical and legal reasoning: LogiKEy framework, methodology, and tool support.* Artif. Intell. 287, 103348 (2020).
2. **J. Dauphin, T. Rienstra, L. van der Torre**. *A Principle-Based Analysis of Weakly Admissible Semantics.* Proc. of COMMA 2020, pp.167-178.
3. **T. Libal, A. Steen**. *NAI: Towards Transparent and Usable Semi-Automated Legal Analysis.* Proc. of the 23. Int. Rechtsinformatik Symposium (IRIS 2020), pp. 265-272.
4. **R. Markovich**. *Understanding Hohfeld and Formalizing Legal Rights: the Hohfeldian Conceptions and Their Conditional Consequences.* Studia Logica 108 - Special Issue Permission, Obligations and Beyond, ed. by O. Roy and P. Kulicki, 2020, pp. 129–158.

4.11 Knowledge Discovery and Mining (MINE)

Head of research group: Prof. Christoph Schommer

The MINE research group follows a multidisciplinary research approach. MINE contributes to areas that primarily address the application of Artificial Intelligence, particularly, Machine Learning and Natural Language Processing (Sentiment Analysis, Topic Modeling). **More information:** ilias.uni.lu/mine, giraffe.lu

In this context, we cooperate with colleagues across the faculties (C2DH, LCSB, Departments of Linguistics, Cognitive Science, Life Sciences, Philosophy, and others) as well as with industrial partners like RTL, IEE, and Post. **Further Highlights of 2020** are: organization of the AI4Health Lecture Series, Prof. Schommer's invited teaching activities at FU Berlin and Singapore University, various collaborations with schools in Dudelange and Kirchberg, 10 academic courses given at UL, and the final theses defences of 7 Master students and 2 PhD candidates (Denis Montigny: UC London, Robert Mbala: U Louvain).

Current staff: Prof. Dr. Christoph Schommer, Dr. Vladimir Despotovic, Dr. Juliana Stropp (Marie Curie), Dr. Joshgun Sirajzade, MSc. Ekaterina Kamlovskaya (PhD), MSc. Federico Galli (PhD; with U Bologna), MSc. Aliona Codrean (PhD), MSc. Alejandro Campos Raboso (PhD; European Investment Bank), MSc. Nina Hosseini-Kivanani (PhD), Msc. Daniel Karpati (PhD), Isabelle Schroeder (Secretarian).

Research Projects (2020)

- J. Sirajzade, C. Schommer: STRIPS – A Semantic Search Toolbox for the Retrieve of Similar Patterns in Luxembourgish Documents. With RTL (05/2017 – 04/2020).
- J. Sirajzade, C. Schommer: Deep Mining with COVID19-Data Warehouse. FNR (07/2020 – 12/2020).
- V. Despotovic: Detection by Cough and Voice Analysis. FNR (07/2020 – 04/2021).
- V. Despotovic: Multi-task, Multilingual, Multi-modal Language Generation. EU COST.
- V. Despotovic: Network on Privacy-Aware Audio and Video-Based Applications for Active and Assisted Living (GoodBrother). EU COST.

Selected Publications in 2020

1. J. Sirajzade, D. Gierschek, C. Schommer: An Annotation Framework for Luxembourgish Sentiment Analysis. LREC 2020.
2. J. Sirajzade, Daniela Gierschek, Christoph Schommer: Component Analysis of Adjectives in Luxembourgish for Detecting Sentiments. LREC 2020.
3. V. Despotovic, T. Skovranek, C. Schommer: Speech Based Estimation of Parkinson's. Disease Using Gaussian Processes and Automatic Relevance Determination, Neurocomputing, Elsevier, Vol. 401.
4. E. Kamlovskaya, C. Schommer: Using word embeddings to explore the Aboriginality discourse in a corpus of Australian Aboriginal autobiographies. In: Synergies 2020.
5. C. Schommer: The potential of Language Technology and AI. Invited Keynote Talk, European Language Resource Coordination (ELRC).

Selected appearances in Press, Radio, and TV (2020)

- C. Schommer: Wie kontrolléiert meng Daten? RTL TV Kloertext, moderated by Caroline Mart. /30.01.
- C. Schommer: in Cheryl Cadamuro: "KI, ein zweischneidiges Schwert", Revue.lu /20.01.
- C. Schommer: Luxemburger Wort: Eine Doktorarbeit zu beginnen ist (relativ) leicht. p. 10. /28.03.
- C. Schommer: Radio Podcast, Radio 100,7: Kënne Roboteren an Zukunft Mënschen ersetzen? /12.06.
- C. Schommer: Video Podcast, RTL Today: DeepFakes technology. /09.07

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 2020

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 first BiCS ”Turing” Promotion The development of a new bachelor has been led by the Messir group since 2015. After five years of successful development the BiCS represent 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. Jahic Benjamin; Guelfi Nicolas; Ries, Benoît. “Specifying key-properties to improve the recognition skills of neural networks”. Proceedings of the 2020 European Symposium on Software Engineering, published by ACM. This paper introduces an extended software engineering method for dataset augmentation to improve neural networks by satisfying the customer’s requirements. It introduces the notion of key-properties to describe the neural network’s recognition skills that is illustrated through

an experimentation on a case study on the recognition of the state of a digital meter counter.

2. The post-proceedings of the first international workshop on Frontiers in Software Engineering Education (FISEE 2019, Villebrumier, France, November 11–13, 2019) was published as a volume of the Springer Lecture Notes in Computer Science (LNCS). Insights about the relevance effects of teaching nowadays DevOps, as well as the use of standards to define DevOps-oriented curricula were published in different peer-reviewed venues.

3. Capozucca Alfredo; Guelfi Nicolas. ”Analysing the SWECOM Standard for Designing a DevOps Education Programme”. In Proceedings ”Frontiers in Software Engineering Education”. FISEE 2019. Lecture Notes in Computer Science (LNCS). Developing academic education programmes for software engineers is a difficult task. This paper is a first attempt to introduce a standard based development process to derive a DevOps education programme for graduate education. It is introduced as a generic process mainly based on the SWECOM standard. This process is applied to generate a proposal for a significant DevOps graduate academic programme definition in a comprehensive and, most importantly, in a skill oriented manner.

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 2020

At the end of 2020, PCOG counted 18 members (1 professor, 5 research scientists, 4 postdocs, 7 PhD students, 1 R&D Specialist) and produced a total of 18 peer-reviewed publications (4 journal articles, and 14 conference articles). In 2020, one PhD student defended his thesis entitled «Performance Evaluation and Modelling of SaaS Web Services in the Cloud».

PCOG has run three research projects in 2020. The "Digital Trust in Smart ICT" research programme with the ILNAS, 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, 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 also participates in the new NVidia joint AI lab of Luxembourg with Digital Luxembourg,SnT, LCSB and LIST, providing advanced research support on GPU/AI workflows.

PCOG acquired three new research projects in 2020: (1) the second ILNAS/ANEC Research Programme (2021-2024) which will focus on three new pillars (Aerospace, ICT and Construction) in line with Luxembourg's National Standardization Strategy 2020-2030; (2) FNR CORE ADARS (Automating the Design of Autonomous Robot Swarms) on the development of novel hyper-heuristic approaches to automatically generate efficient swarming behaviours for distributed aerospace and space systems (2021-2024); and (3) the STAREBEI STAIRS (A Sustainable and Trustworthy AI Recommitment System) project (2021) funded by the European Investment Bank (EIB).

PCOG team members taught in several Bachelor, Master and PhD programs (BICS, BINFO, MICS, 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 2021, 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 2020

1. **E. Kieffer, G. Danoy, M. R. Brust, P. Bouvry, and A. Nagih.** Tackling large-scale and combinatorial bi-level problems with a genetic programming hyper-heuristic. IEEE Transactions on Evolutionary Computation, 24(1):44–56, Feb 2020.

2. **D. H. Stolfi, M. R. Brust, G. Danoy, and P. Bouvry.** Emerging inter-swarm collaboration for surveillance using pheromones and evolutionary techniques. Sensors, 20(9):2566, 2020.

3. **S. Mahon, S. Varrette, V. Plugaru, F. Pinel and P. Bouvry.** Performance

Analysis of Distributed and Scalable Deep Learning,*2020 20th IEEE/ACM International Symposium on Cluster, Cloud and Internet Computing (CCGRID),* Melbourne, VIC, Australia, 2020, pp. 760-766, doi: 10.1109/CCGrid49817.2020.00-13.

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, pervasive and/or autonomic software systems for several 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 2020

Apart from their regular research and publication work and their participation in 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.

Most interesting publications in 2020

1. **Gilles Neyens and Denis Zampuniéris. Proactive Middleware for Fault Detection and Advanced Conflict Handling in Sensor Fusion.** In Proc. International Conference on Artificial Intelligence and Soft Computing, Zakopane (Poland), 2019.
   Robots traditionally have a wide array of sensors that allow them to react to the environment and make appropriate decisions. These sensors can give incorrect or imprecise data due to malfunctioning or noise. Sensor fusion methods try to overcome some of these issues by using the data coming from different sensors and combining it. However, they often don't take sensor malfunctioning and a priori knowledge about the sensors and the environment into account, which can produce conflicting information for the robot to work with. In this paper, we present an architecture and process in order to overcome some of these limitations based on a proactive rule-based system.

2. **Gilles Neyens and Denis Zampuniéris. Proactive Model for Handling Conflicts in Sensor Data Fusion Applied to Robotic Systems.** In Proc. International Conference on Software Technologies, Prague (Czech Republic), 2019.
   Robots have to be able to function in a multitude of different situations

and environments. To help them achieve this, they are usually equipped with a large set of sensors whose data will be used in order to make decisions. However, the sensors can malfunction, be influenced by noise or simply be imprecise. Existing sensor fusion techniques can be used in order to overcome some of these problems, but we believe that data can be improved further by computing context information and using a proactive rule-based system to detect potentially conflicting data coming from different sensors. In this paper, we will present the architecture and scenarios for a generic model taking context into account.

Top academic publication in 2020

Alexandre Frantz and Denis Zampuniéris. Separation of Concerns Within Robotic Systems Through Proactive Computing. In Proc. IEEE International Conference on Robotic Computing, November 2020.

In this paper, we first introduce a possible new model for designing and implementing software in robotic systems. This model is based on proactive scenarios, coded through dynamic sets of condition-action rules. Each scenario embeds the required rules and can be assembled dynamically with others, allowing the proactive system to achieve a unique objective or behavior and instruct the robot accordingly. Furthermore, a scenario is not aware of the existence of the other scenarios. In fact, it only contains information about a predefined central scenario, which oversees global decision making. In addition, each scenario knows where to enter its suggestions, thus allowing for a high degree in terms of separating concerns and modularity of code. Consequently, allowing easier development, testing and optimization of each scenario independently, possible reuse in different robots, and finally, a faster achievement of robust and scalable robotics software.

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 2020

In 2020, SECAN-Lab conducted research in the scope of 10 publicly and industry-funded projects. Besides continuing our work in the large EU projects 5G-DRIVE and 5G-MOBIX collaborating with major international players in the automotive and communication technology such as BMW, Daimler, and Siemens, we were able to further intensify our relationship with the automotive industry: The results of our initial work on a security testbed with Honda resulted in the successful FNR BRIDGES proposal SETICA, which allows us addressing Time-Sensitive-Networking (TSN) Security in collaboration with Honda Research. Moreover, a collaboration with ITK Engineering (a Bosch Company) on Automotive Security topics has been initiated aiming at joint Master and PhD supervision. Furthermore, the CITIES2030 project submitted to the EU H2020 program was accepted for funding. The project aims at creating future-proof and effective urban food systems and ecosystems via a connected structure centered on the citizen and built on trust. SECAN-Lab will work on security, privacy and data analytics aspects involved in the end-to-end tracking of the food supply chain.

We successfully completed the two FNR projects PETIT and CONTACT based on which two of our team members, Wladimir De La Cadena and Antonio Di Maio, obtained their PhD degrees. The PETIT project advanced the state-of-the-art of Privacy-Enhancing Techniques (PETs) targeting the future Internet and creating solid fundamentals for systems that empower users with tools for strengthening their anonymity. Results of PETIT were presented in top-ranked conferences including ACM CCS 2020 and IEEE NCA 2020. The CONTACT project aimed at advancing the state-of-the-art of Vehicular Communication by developing a set of communication techniques that are able to provide high levels of QoS in Vehicular Networks, despite the very challenging and unstable conditions of the wireless communication channels. The results of the project have been published in the scope of 28 conference/workshop papers, 7 journal articles, 1 poster, 1 demo, and 1 book chapter.

Despite the COVID crisis, we were able to extend our team and strengthen our collaborations with excellent academic institutions. Amirhossein Adavoudi joined our team to intensify our work on privacy-enhancing technologies and application-driven cryptographic protocols. Furthermore, Dr. Andy Rupp, the Deputy Head of the team, was invited to become an external Principal Investigator with the Competence Center for Applied Security Technology (KASTEL) at the Karlsruhe Institute of Technology (KIT) in Germany.

In terms of academic contributions, the SECAN-Lab team was also very successful in 2020 with more than 20 publications in international workshops, conferences, and journals. Team members were involved in the organizational or technical program committees of 7 international conferences and workshops, including the IEEE Global Communications Conference (GLOBECOM) 2020 and the IEEE Consumer Communications & Networking Conference (CCNC) 2020.

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. Furthermore, Dr.

Stefan Schiffner was organizing the 15th IFIP Summer School on Privacy and Identity Management as a Co-Chair.

Three most interesting publications in 2020

1. W. De la Cadena, A. Mitseva, J. Hiller, J. Pennekamp, S. Reuter, J. Filter, T. Engel, K. Wehrle, A. Panchenko. TrafficSliver: Fighting Website Fingerprinting Attacks with Traffic Splitting. In Proceedings of CCS'20: 2020 ACM SIGSAC Conference on Computer and Communications Security, Virtual Event, USA, November 9-13, 2020.

   Website fingerprinting (WFP) aims to infer information about the content of encrypted and anonymized connections by observing patterns of data flows based on the size and direction of packets. By collecting traffic traces at a malicious Tor entry node — one of the weakest adversaries in the attacker model of Tor — a passive eaves-dropper can leverage the captured meta-data to reveal the websites visited by a Tor user. To limit the exposure of Tor users to WFP, we propose novel lightweight WFP defenses, TrafficSliver, which successfully counter today's WFP classifiers with reasonable bandwidth and latency overheads and, thus, make them attractive candidates for adoption in Tor. Through user-controlled splitting of traffic over multiple Tor entry nodes, TrafficSliver limits the data a single entry node can observe and distorts repeatable traffic patterns exploited by WFP attacks. We show that our network-layer defense reduces the accuracy from more than 98% to less than 16% for all state-of-the-art WFP attacks without adding any artificial delays or dummy traffic. By sending single HTTP requests for different web objects over distinct Tor entry nodes, our application-layer defense reduces the detection rate of WFP classifiers by almost 50 percentage points.

2. W. De la Cadena, D. Kaiser, A. Panchenko, T. Engel. Out-of-the-box Multipath TCP as a Tor Transport Protocol: Performance and Privacy Implications. In Proceedings of the 19th IEEE International Symposium on Network Computing and Applications (NCA) 2020, USA, November 24-27, 2020.

   The transport design of Tor - the most popular anonymization network - has been identified as a key factor responsible for its performance unfairness. In Tor, traffic from multiple users is multiplexed in a single TCP connection between two relays. While this has positive effects on privacy, it negatively influences performance and is characterized by unfairness as TCP congestion control gives all the multiplexed Tor traffic as little of the available bandwidth as it gives to every single TCP connection that competes for the same resource. To counter this, we propose to use multipath TCP (MPTCP). It allows for better resource utilization and increases throughput of the Tor traffic to a fairer extent. Our evaluation in real-world settings shows that using out-of-the-box MPTCP leads to 15% performance gain. We analyze the privacy implications of MPTCP in Tor settings and discuss potential threats and mitigation strategies.

3. V. Fetzer, M. Hoffmann, M. Nagel, A. Rupp, R. Schwerdt. P4TC - Provably-Secure yet Practical Privacy-Preserving Toll Collection. In Proceedings of the 20th Privacy Enhancing Technologies Symposium (PETS) 2020, Virtual Event, July 13–17, 2020.

   Electronic toll collection (ETC) is widely used all over the world not only to finance our road infrastructures, but also to realize advanced features like congestion management and pollution reduction by means of dynamic pricing. Unfortunately, existing systems rely on user identification and allow tracing a user's movements. Several abuses of this personalized location data have already become public. In view of the planned European-wide interoperable tolling system EETS and the new EU General Data Protection Regulation, location privacy becomes of particular importance.

   In this paper, we propose a flexible security model and crypto protocol framework designed for privacy-preserving toll collection in the most dominant setting, i.e., Dedicated Short Range Communication (DSRC) ETC. A major challenge in designing the framework at hand was to combine provable security and practicality, where the latter includes practical performance figures and a suitable treatment of real-world issues, like broken onboard units etc. To the best of our knowledge, our work is the first in the DSRC setting with a rigorous security model and proof and arguably the most comprehensive formal treatment of ETC security and privacy overall. Additionally, we provide a prototypical implementation on realistic hardware which already features fairly practical performance figures. An interaction between an onboard unit and a road-side unit is estimated to take less than a second allowing for toll collection at full speed assuming one road-side unit per lane.

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,
- data mining and deep learning in social networks,
- malware detection and mobile systems security,
- security of cyber-physical socio-technical systems,
- trust management,
- software security (e.g., vulnerability detection),
- space informatics.

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 2020

In 2020, the SaToSS group counted 23 researchers (1 professor, 1 senior researcher, 10 postdocs, 12 PhD students). Currently the group runs one Junior CORE project (PrivDA on privacy in social networks), three FNR INTER projects (AlgoReCell on models of biological networks, SURCVS on secure voting systems and SLANT on security modelling in NLP), one UL-funded project (SEC-PBN on modeling with probabilistic Boolean networks), two FNR PRIDE projects (SP-squared on deep learning and DRIVEN on social analysis) and two AFR projects (PriML on privacy in machine learning and ATTEST on security in IoT). The group has also secured funding for a research associate position within a project co-funded by European Space Agency (ESA) and UL which will start in 2021. In 2020, the group has successfully graduated three PhD candidates. SaToSS has been actively involved in teaching and student supervision for bachelor and master programs in Computer Science (BINFO, BICS, MICS, MSSI).

Three most interesting publications in 2020

1. Fine-grained Code Coverage Measurement in Automated Black-box Android Testing. **Aleksandr Pilgun**, Olga Gadyatskaya, Yury Zhauniarovich, Stanislav Dashevskyi, Artsiom Kushniarou, and **Sjouke Mauw**, in ACM Transactions on Software Engineering Methodology, 2020. To identify buggy or even malicious third-party Android applications, novel frameworks for automated black-box testing and dynamic analysis are being developed. Code coverage is one of the most common metrics for evaluat-

ing effectiveness of these frameworks, and used as a fitness function for guiding evolutionary and fuzzy testing techniques. However, there are no reliable tools for measuring fine-grained code coverage in black-box Android app testing. We present the Android Code coVerage Tool, ACVTool for short, that instruments Android apps and measures the code coverage in the black-box setting at the class, method and instruction granularities. ACVTool has successfully instrumented 96.9% of apps in our experiments. It introduces a negligible instrumentation time overhead, and its runtime overhead is acceptable for automated testing tools. We show in a large-scale experiment with Sapienz, a state-of-art testing tool, that the fine-grained instruction-level code coverage provided by ACVTool helps to uncover a larger number of faults.

2. Active re-identification attacks on periodically released dynamic social graphs. **Xihui Chen**, Ema Këpuska, **Sjouke Mauw**, and **Yunior Ramírez-Cruz**, in Proceedings of the 25th European Symposium On Research In Computer Security (ESORICS) 2020. Active re-identification attacks pose a serious threat to privacy-preserving social graph publication. Active attackers create fake accounts to enforce structural patterns that can be used to re-identify legitimate users on published anonymised graphs, even without additional background knowledge. So far, this type of attacks has only been studied in the scenario where the inherently dynamic social graph is published once. In this paper, we present the first active reidentification attack in the more realistic scenario where a dynamic social graph is periodically published. Our new attack leverages tempo-structural patterns, created by a dynamic set of sybil nodes, for strengthening the adversary. We evaluate our new attack through a comprehensive set of experiments on real-life and synthetic dynamic social graphs. We show that our new attack substantially outperforms the most effective static active attack in the literature by increasing success probability by at least two times and efficiency by at least 11 times. Moreover, we show that, unlike the static attack, our new attack remains at the same level of efficiency as the publication process advances. Additionally, we conduct a study on the factors that may thwart our new attack, which can help design dynamic graph anonymisation methods displaying a better balance between privacy and utility.

3. Logic Beyond Formulas: A Proof System on Graphs. **Matteo Acclavio**, **Ross Horne**, and Lutz Straßburger, in Proceedings of the 35th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS) 2020. A proof system that operates on graphs instead of formulas is presented in this paper. We begin our quest with the well-known correspondence between formulas and cographs, which are undirected graphs that do not have P4 (the fourvertex path) as vertex-induced subgraph; and then we drop that condition and look at arbitrary (undirected) graphs. The consequence is that we lose the tree structure of the formulas corresponding to the cographs. Therefore we cannot use standard proof theoretical methods that depend on that tree structure. In order to overcome this difficulty, we use a modular decomposition of graphs and some techniques from deep inference where inference rules do not rely on the main connective of a formula. For our proof system we show the admissibility of cut and a

generalization of the splitting property. Finally, we show that our system is a conservative extension of multiplicative linear logic (MLL) with mix, meaning that if a graph is a cograph and provable in our system, then it is also provable in MLL+mix.

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 is a SnT group that 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)
- Multi-objective reasoning and optimization
- Model-driven data analytics (on top of Models@run.time)
- Information Retrieval and Data mining to collect knowledge
- Mobile Security, malware detection, prevention and dissection

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, Smart Grid and Smart Home infrastructures, and the latest paradigms of databases.

Summary of the group's achievements in 2020

SerVal has been successful in several dimensions in 2020, despite the split of the team with the creation of the spin-off group TruX, the number of researchers has been maintained to around 35 researchers. However, the group scientific production has dropped with only 15 papers (compared to 35 in 2019) published in top venues such as FSE, ICSE, Empirical Software Engineering, KDD, WWW etc. In addition to the split of the team, this can be explained by the fact many PhD students are at the start of their thesis and also by the loss of the structural FSTM maitre assistant position that was not renewed for Prof. Le Traon. The ratio of permanent researchers is thus very low (3 for a team of 35 persons). Still, two PhD students defended in 2020. The two projects with Paypal are continued, as well as new projects with BGL BNP Paribas. A couple of FNR Projects have been funded (CORE, Junior). The team received a Best Paper award for their paper on "Data-driven Simulation and Optimization for Covid-19 Exit Strategies" published at KDD Covid track. Dr. Papadakis and Prof. Le Traon are organising the International Conference on Software Maintenance and Evolution 2021 (ICSME 21). Prof. Le Traon has been nominated vice-director of the SnT research center in January 2020.

Main publications and achievements in 2020

1. Data-driven Simulation and Optimization for Covid-19 Exit Strategies. KDD 2020: Salah Ghamizi, Renaud Rwemalika, Maxime Cordy, Lisa Veiber, Tegawendé F. Bissyandé, Mike Papadakis, Jacques Klein, Yves Le Traon (Best Paper)

   The rapid spread of the Coronavirus SARS-2 is a major challenge that led almost all governments worldwide to take drastic measures to respond to the tragedy. Chief among those measures is the massive lockdown of entire countries and cities, which beyond its global economic impact has created some deep social and psychological tensions within populations. While the adopted mitigation measures (including the lockdown) have generally proven useful, policymakers are now facing a critical question: how and when to lift the mitigation measures? A carefully-planned exit strategy is indeed necessary to recover from the pandemic without risking a new outbreak. Classically, exit strategies rely on mathematical modeling to predict the effect of public health interventions. Such models are unfortunately known to be sensitive to some key parameters, which are usually set based on rules-of-thumb.

2. Mining Fix Patterns for FindBugs Violations. IEEE Trans. Software Eng. 47(1): 165-188 (2021): Kui Liu, Dongsun Kim, Tegawendé F. Bissyandé, Shin Yoo, Yves Le Traon:

   Several static analysis tools, such as Splint or FindBugs, have been proposed to the software development community to help detect security vulnerabilities or bad programming practices. However, the adoption of these tools is hindered by their high false positive rates. Tthere is lack of a systematic way to investigate the distributions on existing violations and fixed ones in the wild, that can provide insights into prioritizing violations for developers, and an effective way to mine code and fix patterns which can help developers easily understand the reasons of leading violations and how to fix them. In this paper, we first collect and track a large number of fixed and unfixed violations across revisions of software. The empirical analyses reveal that there are discrepancies in the distributions of violations that are detected and those that are fixed, in terms of occurrences, spread and categories, which can provide insights into prioritizing violations. To automatically identify patterns in violations and their fixes, we propose an approach that utilizes convolutional neural networks to learn features and clustering to regroup similar instances. We then evaluate the usefulness of the identified fix patterns by applying them to unfixed violations. The results show that developers will accept and merge a majority (69/116) of fixes generated from the inferred fix patterns.

3. Selecting fault revealing mutants. Empir. Softw. Eng. 25(1): Thierry Titcheu Chekam, Mike Papadakis, Tegawendé F. Bissyandé, Yves Le Traon, Koushik Sen.

   Mutant selection refers to the problem of choosing, among a large number of mutants, the (few) ones that should be used by the testers. In view of this, we investigate the problem of selecting the fault revealing mutants, i.e., the mutants that are killable and lead to test cases that uncover unknown program faults. We formulate two variants of this problem: the fault revealing mutant selection and the fault revealing mutant prioritization. We argue and show that these problems can be tackled through a set of 'static' program features and propose a machine learning approach, named FaRM, that learns to select and rank killable and fault revealing mutants. Experimental results involving 1,692 real faults show the practical benefits of our approach in both examined problems. Our results show that FaRM achieves a good trade-off between application cost and effectiveness (measured in terms of faults revealed). We also show that FaRM outperforms all the existing mutant selection methods, i.e., the random mutant sampling, the selective mutation and defect prediction (mutating the code areas pointed by defect prediction). In particular, our results show that with respect to mutant selection, our approach reveals 23% to 34% more faults than any of the baseline methods, while, with respect to mutant prioritization, it achieves higher average percentage of revealed faults with a median difference between 4% and 9% (from the random mutant orderings).

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 with common labs with the Electrical Engineering. The group is devoted to 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 2020

In 2020, the PhD works were focused towards research on hosting capacity enhancement for photovoltaic generation distributed in grids, failsafe curtailment and protection. For the complete subsets of radial and meshed MV-grid configurations both overcurrent and overvoltage constraints need to be respected. Control-dynamics results for a newly developed control strategy implementation have been pursued, in view of large-scale integration of PV in the national grid, as planned in the National Energy and Climate Plan (NECP), laying the ground for cooperative control methods including droops and fairly distributed curtailment. The complete subset analysis guarantees supply security within the tolerances required, while maintaining reconfiguration freedom of the grid operator. With large-scale photovoltaic distributed generation in the Gigawatt range, the supply security of the grid requires closer attention. To identify and overcome bottlenecks due to overloading of substation transformers and overloading of lines for large-scale integration of PV plants, measures to avoid cost-intensive network reinforcement are identified according to current grid codes and grid code enhancement.

Cooperation with Eurosolar and the Swiss Solar Agency have been continued with Prof. Sachau as member of the Norman Foster committee and the European Solarprize committee. Cooperation with the JRC Ispra has been reinforced contributing to the field of EU electrical energy security and Luxembourg's NECP.

In the frame of the Visiting Scientist Agreement with 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 grid. As previous scientific officer of DG Research, Brussels and of the EC-JRC Energy Institute, being acquainted with the long-term European policy framework and prospects for energy research and demonstration, he has prepared the addendum for Monitoring of Subgrid Storage Integration, complementing the European PV Monitoring Guidelines, in cooperation with Luxembourg's grid operator, it's Haute Commissariat Protection Nationale and the Market Regulator. Spatial and temporal aggregation of key data on progress towards climate-neutrality has been aligned with the principles of Eurostat.

4.19 Team Leprévost

Head of research group: Prof. Dr. Franck Leprévost

Summary of the group's achievements in 2020

A series of organizational events occurred during the year 2020. The departure of Nicolas Bernard (in December 2019) on the one hand and the arrival (in September 2019) of Raluca Chitic as a PhD student on the other hand had an impact on this year's activities. On the top of all, like everyone, we had 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 at image recognition. A series of results led to the publication in particular of a conference paper (Best Paper Award) and a journal paper on these subjects. Additional articles were published as well with international collaborators. A tutorial book was also written during the confinement, and released on time for the start of the academic year in September 2020.

DCS asked Prof Leprévost to coordinate the DCS cluster activities in the context of the teaching evaluation 2020. This task, covering most of 2020 and part of 2021, was timely demanding, but led to a positive evaluation (as of February 2021). The CET of Mrs. Chitic met during summer 2020, and gave a positive evaluation of her work.

Most important talks:

- R. Chitic: Presentation of paper (1), 24 March 2020 - 12th Asian Conference, ACIIDS 2020 Phuket (Thailand) (23-26 March 2020).

- F. Leprévost: Keynote Conference ”Cryptology in pre- and post-quantum times”, 17 November 2020 - 2nd International Conference ”Digital Industry: State and Development Prospects 2020” - GloSIC-2020, Chelyabinsk (Russia) (15-18 November 2020).

List of published articles

1. Raluca Chitic, Nicolas Bernard and Franck Leprévost: “A proof of concept to deceive humans and machines at image classification with evolutionary algorithms”. Intelligent Information and Database Systems – 12th Asian Conference, ACIIDS 2020 Phuket, Thailand, March 23-26, 2020, Proceedings Part II, p. 467-480. LNAI 12034, Springer, Eds. Ngoc Thanh Nguyen, Kietikul Jearanaitanakij, Ali Selamat, Bogdan Trawinski, Suphamit Chittayasothorn.
2. Raluca Chitic, Nicolas Bernard and Franck Leprévost: “Evolutionary algorithms deceive humans and machines at image classification: An extended proof of concept on two scenarios”. To appear in the Journal of Information and Telecommunication. http://dx.doi.org/10.1080/24751839.2020.1829388
3. Panissara Thanapol, Kittichai Lavangnananda, Frédéric Pinel, Pascal Bouvry, Franck Leprévost: “Reducing Overfitting and Improving Generalization in Training Convolutional Neural Network (CNN) under Limited Sample Sizes in Image Recognition”. Proc. of the 5th. Inter. Conf. on Information Technology (InCIT 2020), 21st – 22nd October 2020, Bangsaen, Thailand, p. 300-305.
4. Jorge Cortés-Mendoza, Andrei Tchernykh, Mikhail Babenko, Luis Bernardo Pulido-Gaytan, Gleb Radchenko, Franck Leprévost, Xinheng Wang, Arutyun Avetisyan: ”Privacy-preserving logistic regression as a cloud service based on residue number system”. Proc. of the 6th. Russian Supercomputing Days (RusSCD’2020), 21-22 September 2020, Moscow, Russia, p. 598-610.

Best paper Award: The paper (1) was granted Best Paper Award of the conference.

List of publications - Books:

- Franck Leprévost : « How Big is Big? How Fast is Fast? A Hands-On Tutorial on Mathematics of Computation ». (September 2020) Ed. Amazon. ISBN 9798642630556

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. In joint work with his assistant Jim Barthel, a revised paper on specific properties of integral binary quadratic forms has been submitted for publication. A joint article on ”New constructions of Verifiable Delay Functions” has been submitted to ESORICS2020, after rejection revised and re-submitted to CANS2020 (status currently pending). 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 solve the new conjecture with a large-scale computation. A paper describing the results is currently pending.

Research on the Simultaneous Chinese Remaindering (S-CRT), a generalization of the well-known Chinese Remainder Theorem popular in number theory, has been continued. A new graph-based algorithm for finding certain solutions of the S-CRT has been implemented in a proof-of-concept version and is currently tested in practice to better understand its practical usability (very large, directed graphs are involved in the algorithm). During this research, it became clear that techniques used in the solution algorithm for S-CRT show strong similarities with other number-theoretic problems like integer factorization or possibly even the discrete logarithm problem modulo primes. A first proof-of-concept implementation of a new integer factoring algorithm has been done and indicates that several practical algorithmic questions still require further optimization, before a practically relevant algorithm can be published.

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 2020 due to the Corona virus. A time intensive programme assessment and self-reflection on the strengths and weaknesses of both programmes was done as part of the “Evaluation 2020”. In addition, the preparation for the accreditation of both Bachelor programmes, done by ACQUIN and foreseen for January 2021, required an enormous workload during the year 2020.

CHAPTER 5

Organizational Structure

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

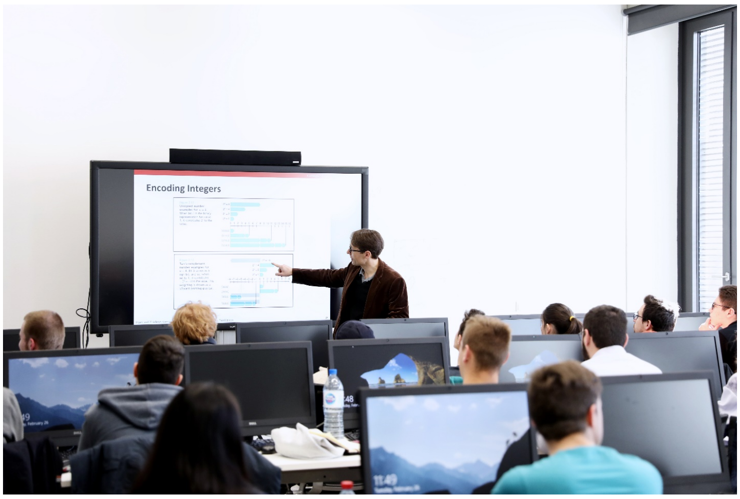
- The department is meant to be responsible for research and education performed by its members. The head of the department is therefore responsible for both.
- The head is seconded by a vice-head, who is able to take over all the head's responsibilities whenever needed, e.g. due to temporary absence 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 6.5) 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 6.6) 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 6.7) and at the master level (MISSM see section 6.3), that are run 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 section 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. In 2020, 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. DCS members Martin Theobald and Alfredo Capozucca received the 2020 UL teaching award as a recognition for their excellence in teaching, after three previous teaching awards for DCS members over years 2019 and 2018.

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 200 doctoral candidates, 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 five 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 2020 there were around 90 students from more than 30 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. 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, professors from renowned partner universities, and industrial experts having significant experience working in the space sector. In the fourth semester of the master, the students will work on their Master thesis which can also be done in collaboration with an external partner such as a company or an agency. In order to gain additional work experience, students are also encouraged to do a voluntary internship in a space company.

In 2020 there were around 20 students from more than 10 countries in the ISM.

6.5 Bachelor in Computer Science (BiCS)

The Computer Science and Communication research offers a bachelor program in computer science (BiCS) that welcomed its first promotion in September 2017. The study programme aims at bringing the theoretical and practical skills needed to successfully pursue studies in a Master programme related to Computer Science at the University of Luxembourg or any other world-class university or school.

The main strengths of the BiCS are:

- Programme designed from the international standard ACM / IEEE CS 2013.
- Pedagogy based on acquisition by practice through research and development projects.
- Scientific quality to enhance interest and strengths in science and technology for the future.
- Applied multilingualism for effective integration into the Luxembourgish or international labor 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 computer science engineers and researchers. It mainly uses project-based learning as a signature pedagogy which is in line with the University's drive for "research-based teaching".

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

- Support business incubation for selected BiCS students
- Host selected BSP (Bachelor Semester Projects)
- Develop industrial collaborations
- 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.

The BiCSLab axes are:

- Senseware: Software engineering for intelligent and augmented environments. Interdisciplinary (learning, robotics, virtual & augmented reality)
- Greenware: Systemic approach to resilient ecosystems (permaculture). Software & Hardware (co-)development of IT solutions for permaculture
- Software: General development tools and method for the BicsLab axes. Hosts any project on software development not included in the other axes.

The figures for academic year 2019/2020 are:

- 90 total applicants: 24% female, 76% male
- admission rate: 63%
- high school degrees: 85% classic, 15% vocational & other
- high school country: 44% Luxembourg, 18% Greater region, 38% others
- 96 currently registered to the program: 38 first year, 28 second year, 30 third year

6.6 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 2020-2021, a total of 159 students are registered within the BINFO program (64 in the first year, 48 in the second, and 47 students in the third year). The number of BINFO graduates in 2020 is 26. More information on the programme can be found at https://binfo.uni.lu.

During the year 2020, an in-depth analysis of internal processes and a self-reflection about the strengths and weaknesses of the programme was done as contribution to the "Evaluation 2020". In addition, a complete documentation of all processes and quality insurance activities in the programme was developed for an ongoing programme accreditation process (evaluation committee site visit planned for January 2021).

6.7 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 acknowledgement 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 re-

quired 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 2020-2021, a total of 27 students are registered within the BINFO-CEP program (13 in the first, 14 students in the second/third year). The number of BINFO-CEP graduates in 2020 is 10. More information on the programme can be found at https://binfo-cep.uni.lu.

During the year 2020, an in-depth analysis of internal processes and a self-reflection about the strengths and weaknesses of the programme was done as contribution to the "Evaluation 2020". In addition, a complete documentation of all processes and quality insurance activities in the programme was developed for an ongoing programme accreditation process (evaluation committee site visit planned for January 2021).

6.8 Certificate Smart ICT for business innovation

The purpose of this certificate is to train in a year's time, including classes, seminars and an internship, professionals from the ICT sector who want to -further-develop their Smart ICT skills and maybe embrace new career opportunities in positions like Digital Strategy Consultant, Smart ICT Consultant, Innovation Manager, Standards Manager, Head of Innovation, Head of Digital Strategy or Entrepreneur (start-up company). The certificate aims at enhancing the skills of ICT professionals and reinforcing the position of Luxembourg in the field of Smart ICT by offering its students a broad view of Smart ICT concepts and tools at their disposal to develop their sense of innovation.

Students who successfully complete the University certificate will be able to: identify and decode the high potential of Smart ICT concepts for business and innovation; analyse the challenges of digital trust and information security; identify participants and goals in the standardisation process; and cater for the current and future issues and standardisation needs in ICT areas such as digital intelligence (ICT Governance), smart platforms (Cloud Computing, Smart Cities, Green ICT), and smart interactions (Internet of Things, Smart Cyber Physical Systems & Robotics, Big data and Analytics, Digital Trust).

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	4	A.1 (p.55)
Book Chapters	3	A.2 (p.56)
Journal Articles	57	A.3 (p.56)
Conference Papers	135	A.4 (p.62)
Theses	27	A.5 (p.76)
Total	*226*	

Table A.1: Overview of publications per category

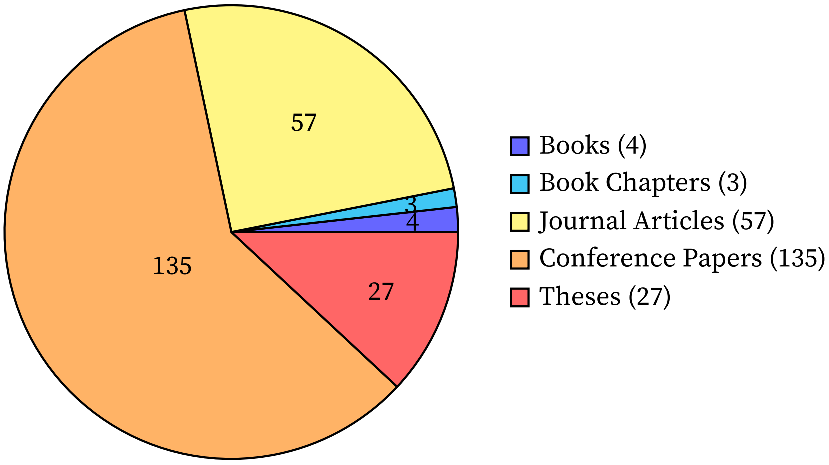


Figure A.1: Distribution of Types of Publications

A.1 Books

[1] Jean-Michel Bruel, Alfredo Capozucca, Manuel Mazzara, Bertrand Meyer, Alexandr Naumchev, and Andrey Sadovykh, eds. *Fron-*

tiers in Software Engineering Education. Springer, 2020. ISBN: 978-3-030-57662-2. DOI: 10.1007/978-3-030-57663-9. URL: http://hdl.handle.net/10993/44259.

[2] Franck Leprevost. *How big is big? How fast is fast? A Hands-On Tutorial on Mathematics of Computation*. Amazon, 2020. ISBN: 9798642630556. URL: http://hdl.handle.net/10993/45079.

[3] Emilo Muñoz-Velasco, Ana Ozaki, and Martin Theobald, eds. *27th International Symposium on Temporal Representation and Reasoning, TIME 2020, September 23-25, 2020, Bozen-Bolzano, Italy*. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020. ISBN: 978-3-95977-167-2. URL: http://hdl.handle.net/10993/45324.

[4] Jun Pang and Lijun Zhang, eds. *Proceedings of the 6th International Symposium on Dependable Software Engineering. Theories, Tools, and Applications*. Springer, 2020. ISBN: 978-3-030-62821-5. URL: http://hdl.handle.net/10993/44699.

A.2 Book Chapters

[5] Evgeny Bobrov, Antonio Bucchiarone, Alfredo Capozucca, Nicolas Guelfi, Manuel Mazzara, Alexandr Naumchev, et al. “DevOps and Its Philosophy: Education Matters!” In: *Microservices: Science and Engineering*. Ed. by Nicola Dragoni, Schahram Dustdar, and Patricia Lago. Springer International Publishing, 2020, pp. 349–361. ISBN: 9783030316457. DOI: 10.1007/978-3-030-31646-4_14. URL: http://hdl.handle.net/10993/42393.

[6] Esther David, Rabbi S. David, Dov M. Gabbay, and Uri J. Schild. “Talmudic Norms Approach to Mixtures with a Solution to the Paradox of the Heap: A Position Paper”. In: *Beyond Faith and Rationality*. Springer, 2020, pp. 173–193. URL: http://hdl.handle.net/10993/46682.

[7] Arianna Rossi and Monica Palmirani. “What’s in an Icon? Promises and Pitfalls of Data Protection Iconography”. In: *Data Protection and Privacy: Data Protection and Democracy*. Ed. by Ronald Leenes, Dara Hallinan, Serge Gutwirth, and Paul de Hert. Hart Publishing, 2020, pp. 59–92. ISBN: 9781509932740. URL: http://hdl.handle.net/10993/39922.

A.3 Journal Articles

[8] Andrea Baiocchi and Ion Turcanu. “Age of Information of One-Hop Broadcast Communications in a CSMA Network”. In: *IEEE Communications Letters* 25 (2020), pp. 294–298. DOI: 10.1109/LCOMM.2020.3022090. URL: http://hdl.handle.net/10993/44167.

[9] Christof Beierle, Alex Biryukov, Luan Cardoso Dos Santos, Johann Großschädl, Léo Paul Perrin, Aleksei Udovenko, et al. “Lightweight AEAD and Hashing using the Sparkle Permutation Family”. In: *IACR Transactions on Symmetric Cryptology* 2020 (2020), pp. 208–261. DOI: 10.13154/tosc.v2020.iS1.208-261. URL: http://hdl.handle.net/10993/41993.

[10] Kirstie Bellman, Jean Botev, Ada Diaconescu, Lukas Esterle, Christian Gruhl, Chris Landauer, et al. "Self-improving System Integration: Mastering Continuous Change". In: *Future Generation Computer Systems* (2020). DOI: 10.1016/j.future.2020.11.019. URL: http://hdl.handle.net/10993/46306.

[11] Christoph Benzmüller, Ali Farjami, David Fuenmajor, Paul Joseph Yves Meder, Xavier Parent, Alexander Steen, et al. "LogiKEy Workbench: Deontic Logics, Logic Combinations and Expressive Ethical and Legal Reasoning (Isabelle/HOL Dataset)". In: *Data in Brief* 33 (2020). DOI: 10.1016/j.dib.2020.106409. URL: http://hdl.handle.net/10993/45489.

[12] Christoph Benzmüller, Xavier Parent, and Leon van der Torre. "Designing normative theories for ethical and legal reasoning: LogiKEy framework, methodology, and tool support". In: *Artificial Intelligence* 287 (2020), p. 103348. URL: http://hdl.handle.net/10993/46383.

[13] Alex Biryukov and Daniel Feher. "ReCon: Sybil-Resistant Consensus from Reputation". In: *Pervasive and Mobile Computing* (2020). DOI: 10.1016/j.pmcj.2019.101109. URL: http://hdl.handle.net/10993/41325.

[14] Ahto Buldas, Olga Gadyatskaya, Aleksandr Lenin, Sjouke Mauw, and Rolando Trujillo Rasua. "Attribute evaluation on attack trees with incomplete information". In: *Computers and Security* 88 (2020). DOI: 10.1016/j.cose.2019.101630. URL: http://hdl.handle.net/10993/41590.

[15] Alfredo Capozucca and Nicolas Guelfi. "Analysing the SWECOM Standard for Designing a DevOps Education Programme". In: *In: Bruel JM., Capozucca A., Mazzara M., Meyer B., Naumchev A., Sadovykh A. (eds) Frontiers in Software Engineering Education. FISEE 2019. Lecture Notes in Computer Science* 12271 (2020), pp. 133–150. DOI: 10.1007/978-3-030-57663-9_10. URL: http://hdl.handle.net/10993/44258.

[16] Giovanni Casini, Luigi Di Caro, Guido Governatori, Valentina Leone, and Réka Markovich. "Mining and Reasoning with Legal Texts – MIREL 2019". In: *CEUR Workshop Proceedings* (2020). URL: http://hdl.handle.net/10993/46698.

[17] Xihui Chen, Sjouke Mauw, and Yunior Ramirez Cruz. "Publishing Community-Preserving Attributed Social Graphs with a Differential Privacy Guarantee". In: *Proceedings on Privacy Enhancing Technologies* 2020 (2020), pp. 131–152. DOI: 10.2478/popets-2020-0066. URL: http://hdl.handle.net/10993/44465.

[18] Ioana Raluca Chitic, Franck Leprevost, and Nicolas Bernard. "Evolutionary algorithms deceive humans and machines at image classification: An extended proof of concept on two scenarios". In: *Journal of Information and Telecommunication* (2020). URL: http://hdl.handle.net/10993/44665.

[19] Marcello D'Agostino, Dov M. Gabbay, and Sanjay Modgil. "Normality, non-contamination and logical depth in classical natural deduction". In: *Studia Logica* 108 (2020), pp. 291–357. URL: http://hdl.handle.net/10993/46681.

[20] Vladimir Despotovic, Tomas Skovranek, and Christoph Schommer. "Speech Based Estimation of Parkinson's Disease Using Gaussian Processes and Automatic Relevance Determination". In: *Neurocomputing* 401 (2020), pp. 173–181. DOI: 10.1016/j.neucom.2020.03.058. URL: http://hdl.handle.net/10993/42898.

[21] Huimin Dong, Réka Markovich, and Leon van der Torre. "Developing AI Logic for Social Reasoning". In: *Journal of Zhejiang University* (2020). URL: http://hdl.handle.net/10993/46391.

[22] Vinu Ellampallil Venugopal and P Sreenivasa Kumar. "Difficulty-level modeling of ontology-based factual questions". In: *Semantic Web – Interoperability, Usability, Applicability* (2020). URL: http://hdl.handle.net/10993/45328.

[23] Saharnaz Esmaeilzadeh Dilmaghani, Apivadee Piyatumrong, Grégoire Danoy, Pascal Bouvry, and Matthias R. Brust. "Innovation Networks from Inter-organizational Research Collaborations". In: *Heuristics for Optimization and Learning* (2020), pp. 361–375. URL: http://hdl.handle.net/10993/45895.

[24] Valerie Fetzer, Max Hoffmann, Matthias Nagel, Andy Rupp, and Rebecca Schwerdt. "P4TC - Provably-Secure yet Practical Privacy-Preserving Toll Collection". In: *Proceedings on Privacy Enhancing Technologies* 2020 (2020), pp. 62–152. DOI: 10.2478/popets-2020-0046. URL: http://hdl.handle.net/10993/46295.

[25] Dov M. Gabbay. "Introducing Abstract Argumentation with Many Lives". In: *Journal of Applied Logic* 2631 (2020), p. 295. URL: http://hdl.handle.net/10993/46679.

[26] Jun Gao, li li li, Tegawendé François D Assise Bissyande, and Jacques Klein. "Understanding the Evolution of Android App Vulnerabilities". In: *IEEE Transactions on Reliability* (2020). DOI: 10.1109/TR.2019.2956690. URL: http://hdl.handle.net/10993/41509.

[27] Ziya Alper Genç, Vincenzo Iovino, and Alfredo Rial. ""The Simplest Protocol for Oblivious Transfer" Revisited". In: *Information Processing Letters* (2020). DOI: 10.1016/j.ipl.2020.105975. URL: http://hdl.handle.net/10993/44182.

[28] Yujuan Gui, Mélanie H. Thomas, Pierre Garcia, Mona Karout, Rashi Halder, Alessandro Michelucci, et al. "Pituitary Tumor Transforming Gene 1 Orchestrates Gene Regulatory Variation in Mouse Ventral Midbrain During Aging". In: *Frontiers in Genetics* (2020). DOI: 10.3389/fgene.2020.566734. URL: http://hdl.handle.net/10993/44345.

[29] Yonglin Hao, Lin Jiao, Chaoyun Li, Willi Meier, Yosuke Todo, and Qingju Wang. "Links between Division Property and Other Cube Attack Variants". In: *IACR Transactions on Symmetric Cryptology* (2020). URL: http://hdl.handle.net/10993/42851.

[30] Max Hoffmann, Michael Klooß, Markus Raiber, and Andy Rupp. "Black-Box Wallets: Fast Anonymous Two-Way Payments for Constrained Devices". In: *Proceedings on Privacy Enhancing Technologies* 2020 (2020), pp. 165–194. DOI: 10.2478/popets-2020-0010. URL: http://hdl.handle.net/10993/46294.

[31] Kai Hu, Qingju Wang, and Meiqin Wang. “Finding Bit-Based Division Property for Ciphers with Complex Linear Layers”. In: *IACR Transactions on Symmetric Cryptology* (2020). URL: http://hdl.handle.net/10993/42849.

[32] Tingting Hu, Ivan Cibrario Bertolotti, Nicolas Navet, and Lionel Havet. “Automated Fault Tolerance Augmentation in Model-Driven Engineering for CPS”. In: *Computer Standards & Interfaces* 70 (2020). DOI: 10.1016/j.csi.2020.103424. URL: http://hdl.handle.net/10993/41575.

[33] Llio Humphreys, 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* (2020), pp. 1–41. URL: http://hdl.handle.net/10993/46385.

[34] Wojciech Jamroga, Beata Konikowska, Damian Kurpiewski, and Wojciech Penczek. “Multi-valued Verification of Strategic Ability”. In: *Fundamenta Informaticae* 175 (2020), pp. 207–251. DOI: 10.3233/FI-2020-1955. URL: http://hdl.handle.net/10993/45852.

[35] Wojciech Jamroga, Wojciech Penczek, Teofil Sidoruk, Piotr Dembiński, and Antoni Mazurkiewicz. “Towards Partial Order Reductions for Strategic Ability”. In: *Journal of Artificial Intelligence Research* 68 (2020), pp. 817–850. DOI: 10.1613/jair.1.11936. URL: http://hdl.handle.net/10993/45851.

[36] Asad Javed, Jérémy Robert, Keijo Heljanko, and Kary Främling. “IoTEF: A Federated Edge-Cloud Architecture for Fault-Tolerant IoT Applications”. In: *Journal of Grid Computing* (2020). DOI: 10.1007/s10723-019-09498-8. URL: http://hdl.handle.net/10993/44467.

[37] Pierre Kelsen, Qin Ma, and Christian Glodt. “A Lightweight Modeling Approach Based on Functional Decomposition”. In: *Journal of Object Technology* 19 (2020), 15:1–22. URL: http://hdl.handle.net/10993/44826.

[38] Nida Khan, Bilal Kchouri, Nissar Ahmad Yatoo, Zsofia Kräussl, Anass Patel, and Radu State. “Tokenization of Sukuk: Ethereum Case Study”. In: *Global Finance Journal* (2020). DOI: 10.1016/j.gfj.2020.100539. URL: http://hdl.handle.net/10993/43222.

[39] Emmanuel Kieffer, Grégoire Danoy, Matthias R. Brust, Pascal Bouvry, and Anass Nagih. “Tackling Large-Scale and Combinatorial Bi-Level Problems With a Genetic Programming Hyper-Heuristic”. In: *IEEE Transactions on Evolutionary Computation* 24 (2020), pp. 44–56. DOI: 10.1109/TEVC.2019.2906581. URL: http://hdl.handle.net/10993/43995.

[40] 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* (2020). URL: http://hdl.handle.net/10993/46368.

[41] Anil Koyuncu, Kui Liu, Tegawendé François D Assise Bissyande, Dongsun Kim, Jacques Klein, Martin Monperrus, et al. "FixMiner: Mining relevant fix patterns for automated program repair". In: *Empirical Software Engineering* (2020). DOI: 10.1007/s10664-019-09780-z. URL: http://hdl.handle.net/10993/44172.

[42] li li li, Jun Gao, Tegawendé François D Assise Bissyande, Lei Ma, Xin Xia, and Jacques Klein. "CDA: Characterising Deprecated Android APIs". In: *Empirical Software Engineering* 24 (2020), pp. 1–41. DOI: 10.1007/s10664-019-09764-z. URL: http://hdl.handle.net/10993/45771.

[43] Tomer Libal and Alexander Steen. "NAI: Towards Transparent and Usable Semi-Automated Legal Analysis". In: *Jusletter IT* 27 Mai 2020 (2020). DOI: 10.38023/2eb63e02-f13e-45f5-9a7b-d7fe55e42c6c. URL: http://hdl.handle.net/10993/44995.

[44] Jun Pang and Chenyi Zhang. "Preface for the special issue of the 12th International Symposium on Theoretical Aspects of Software Engineering (TASE 2018)". In: *Science of Computer Programming* 187 (2020), p. 102375. URL: http://hdl.handle.net/10993/42848.

[45] Soumya Paul, Cui Su, Jun Pang, and Andrzej Mizera. "An efficient approach towards the source-target control of Boolean networks". In: *IEEE/ACM Transactions on Computational Biology and Bioinformatics* 17 (2020), pp. 1932–1945. DOI: 10.1109/TCBB.2019.2915081. URL: http://hdl.handle.net/10993/40583.

[46] Zoran Peric, Bojan Denic, and Vladimir Despotovic. "Gaussian source coding based on variance-mismatched three-level scalar quantisation using Q-function approximations". In: *IET Communications* 14 (2020), pp. 594–602. DOI: 10.1049/iet-com.2019.0431. URL: http://hdl.handle.net/10993/42600.

[47] Aleksandr Pilgun, Olga Gadyatskaya, Yury Zhauniarovich, Stanislav Dashevskyi, Artsiom Kushniarou, and Sjouke Mauw. "Fine-grained Code Coverage Measurement in Automated Black-box Android Testing". In: *ACM Transactions on Software Engineering and Methodology* 29 (2020), pp. 1–35. DOI: 10.1145/3395042. URL: http://hdl.handle.net/10993/44477.

[48] Julien Polge, Jérémy Robert, and Yves Le Traon. "A Case Driven Study of the Use of Time Series Classification for Flexibility in Industry 4.0". In: *Sensors* 20 (2020). DOI: 10.3390/s20247273. URL: http://hdl.handle.net/10993/45334.

[49] Julien Polge, Jérémy Robert, and Yves Le Traon. "Permissioned Blockchain Frameworks in the Industry: A Comparison". In: *ICT Express* (2020). DOI: 10.1016/j.icte.2020.09.002. URL: http://hdl.handle.net/10993/44257.

[50] Jérémy Robert, Sylvain Kubler, and Sankalp Ghatpande. "Enhanced Lightning Network (off-chain)-based micropayment in IoT ecosystems". In: *Future Generation Computer Systems* (2020). DOI: 10.1016/j.future.2020.05.033. URL: http://hdl.handle.net/10993/44267.

[51] Martin Rosalie, Emmanuel Kieffer, Matthias R. Brust, Grégoire Danoy, and Pascal Bouvry. “Bayesian optimisation to select Rössler system parameters used in Chaotic Ant Colony Optimisation for Coverage”. In: *Journal of Computational Science* 41 (2020), p. 101047. DOI: 10.1016/j.jocs.2019.101047. URL: http://hdl.handle.net/10993/43994.

[52] Arianna Rossi and Gabriele Lenzini. “Making the Case for Evidence-based Standardization of Data Privacy and Data Protection Visual Indicators”. In: *Journal of Open Access to Law (JOAL)* 8 (2020). URL: http://hdl.handle.net/10993/41863.

[53] Arianna Rossi and Gabriele Lenzini. “Transparency by Design in Data-Informed Research: a Collection of Information Design Patterns”. In: *Computer Law and Security Review* 37 (2020). DOI: 10.1016/j.clsr.2020.105402. URL: http://hdl.handle.net/10993/41864.

[54] Arianna Rossi and Monica Palmirani. “Can Visual Design Provide Legal Transparency? The Challenges for Successful Implementation of Icons for Data Protection”. In: *Design Issues* 36 (2020), pp. 82–96. DOI: 10.1162/desi_a_00605. URL: http://hdl.handle.net/10993/44451.

[55] Alexander Steen. “Extensional Paramodulation for Higher-Order Logic and its Effective Implementation Leo-III”. In: *KI – Künstliche Intelligenz* 34 (2020), pp. 105–108. DOI: 10.1007/s13218-019-00628-8. URL: http://hdl.handle.net/10993/40799.

[56] Daniel Stolfi Rosso, Matthias R. Brust, Grégoire Danoy, and Pascal Bouvry. “Emerging Inter-Swarm Collaboration for Surveillance Using Pheromones and Evolutionary Techniques”. In: *Sensors* 20 (2020), p. 2566. DOI: 10.3390/s20092566. URL: http://hdl.handle.net/10993/44183.

[57] Syi, Gábor Hamp, and Réka Markovich. “Legal Data Actions”. In: *Jusletter IT* (2020). URL: http://hdl.handle.net/10993/46400.

[58] Pierre Talbot, Éric Monfroy, and Charlotte Truchet. “Modular Constraint Solver Cooperation via Abstract Interpretation”. In: *Theory and Practice of Logic Programming* 20 (2020), pp. 848–863. DOI: 10.1017/S1471068420000162. URL: http://hdl.handle.net/10993/44545.

[59] Thierry Titcheu Chekam, Mike Papadakis, Tegawendé François D Assise Bissyande, Yves Le Traon, and Koushik Sen. “Selecting fault revealing mutants”. In: *Empirical Software Engineering* (2020). URL: http://hdl.handle.net/10993/42674.

[60] Ion Turcanu, Pierpaolo Salvo, Andrea Baiocchi, Francesca Cuomo, and Thomas Engel. “A Multi-Hop Broadcast Wave Approach for Floating Car Data Collection in Vehicular Networks”. In: *Vehicular Communications* (2020). DOI: 10.1016/j.vehcom.2020.100232. URL: http://hdl.handle.net/10993/41779.

[61] Tao Xie, Zhi Jin, Xuandong Li, Gang Huang, Hausi Muller, Jun Pang, et al. “Preface (Special section on software systems 2020)”. In: *Journal of Computer Science and Technology* 35 (2020), pp. 1231–1233. DOI: 10.1007/s11390-020-0006-4. URL: http://hdl.handle.net/10993/44914.

[62] Alexander Yakubov, Wazen Shbair, Nida Khan, Radu State, Christophe Medinger, and Jean Hilger. “BlockPGP: A Blockchain-based Framework for PGP Key Servers”. In: *International Journal of Networking and Computing* 10 (2020), pp. 1–24. URL: http://hdl.handle.net/10993/41991.

[63] Marc van Zee, Dragan Doder, Leon van der Torre, Mehdi Dastani, Thomas Icard, and Eric Pacuit. “Intention as commitment toward time”. In: *Artificial Intelligence* 283 (2020), p. 103270. URL: http://hdl.handle.net/10993/46384.

A.4 Conference Papers

[64] Faouzi Amrouche, Sofiane Lagraa, Raphaël Frank, and Radu State. “Intrusion detection on robot cameras using spatio-temporal autoencoders: A self-driving car application”. In: *91st IEEE Vehicular Technology Conference, VTC Spring 2020, Antwerp, Belgium, May 25-28, 2020*. 2020. URL: http://hdl.handle.net/10993/43949.

[65] Nikolaos Antoniadis, Maxime Cordy, Angelo Sifaleras, and Yves Le Traon. “Preventing Overloading Incidents on Smart Grids: A Multiobjective Combinatorial Optimization Approach”. In: *Communications in Computer and Information Science*. Springer, Cham, 2020, pp. 269–281. ISBN: 978-3-030-41913-4. DOI: 10.1007/978-3-030-41913-4_22. URL: http://hdl.handle.net/10993/41329.

[66] Davide Basile, Maurice Ter Beek, Maxime Cordy, and Axel Legay. “Tackling the equivalent mutant problem in real-time systems: the 12 commandments of model-based mutation testing”. In: *SOFTWARE PRODUCT LINE CONFERENCE*. 2020. DOI: 10.1145/3382025.3414966. URL: http://hdl.handle.net/10993/45568.

[67] Ringo Baumann, Dov M. Gabbay, and Odinaldo Rodrigues. “Forgetting an Argument”. In: *Proceedings of the AAAI Conference on Artificial Intelligence*. 2020, pp. 2750–2757. URL: http://hdl.handle.net/10993/46680.

[68] Christof Beierle, Alex Biryukov, Luan Cardoso Dos Santos, Johann Groszschädl, Léo Perrin, Aleksei Udovenko, et al. “Alzette: A 64-Bit ARX-box (Feat. CRAX and TRAX)”. In: *Advances in Cryptology – CRYPTO 2020, 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17-21, 2020, Proceedings, Part III*. Ed. by Daniele Micciancio and Thomas Ristenpart. Springer Verlag, 2020, pp. 419–448. ISBN: 978-3-030-56876-4. DOI: 10.1007/978-3-030-56877-1_15. URL: http://hdl.handle.net/10993/44281.

[69] Evgeny Bobrov, Antonio Bucchiarone, Alfredo Capozucca, Nicolas Guelfi, and Sergey Masyagin. “Teaching DevOps in Academia and Industry: Reflections and Vision”. In: *Software Engineering Aspects of Continuous Development and New Paradigms of Software Production and Deployment*. Ed. by Jean-Michel Bruel, Manuel Mazzara, and Bertrand Meyer. Springer International Publishing, 2020, pp. 1–14. ISBN: 9783030393069. URL: http://hdl.handle.net/10993/42391.

[70] Jean Botev. “Self-Integration in Mediated-Reality Systems: a Socio-Technical Perspective”. In: *Proceedings of the 1st IEEE International Conference on Autonomic Computing and Self-Organizing Systems (ACSOS)*. 2020. URL: http://hdl.handle.net/10993/43891.

[71] Jean Botev and Francisco J. Rodríguez Lera. “Immersive Telepresence Framework for Remote Educational Scenarios”. In: *Proceedings of the 22nd International Conference on Human-Computer Interaction (HCI International)*. 2020. URL: http://hdl.handle.net/10993/41713.

[72] Jean Botev and Adriano Viegas Milani. “Forest SaVR – A Virtual-Reality Application to Raise Awareness of Deforestation”. In: *Proceedings of the 17th GI VR/AR Workshop (VAR)*. 2020. URL: http://hdl.handle.net/10993/43892.

[73] Abdelwahab Boualouache, Ridha Soua, and Thomas Engel. “SDN-based Misbehavior Detection System for Vehicular Networks”. In: *2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*. 2020. URL: http://hdl.handle.net/10993/42449.

[74] Abdelwahab Boualouache, Ridha Soua, and Thomas Engel. “Toward an SDN-based Data Collection Scheme for Vehicular Fog Computing”. In: *IEEE International Conference on Communications ICC'2020*. 2020. URL: http://hdl.handle.net/10993/42547.

[75] Colin Boyd, Thomas Haines, and Peter Roenne. “Vote Selling Resistant Voting”. In: *Financial Cryptography and Data Security - FC 2020 International Workshops, AsiaUSEC, CoDeFi, VOTING, and WTSC, Kota Kinabalu, Malaysia February 14, 2020, Revised Selected Papers*. Springer, 2020, pp. 345–359. DOI: 10.1007/978-3-030-54455-3_25. URL: http://hdl.handle.net/10993/45356.

[76] Xavier Boyen, Thomas Haines, and Johannes Mueller. “A Verifiable and Practical Lattice-Based Decryption Mix Net with External Auditing”. In: *Computer Security - ESORICS 2020 - 25th European Symposium on Research in Computer Security, ESORICS 2020, Guildford, UK, September 14-18, 2020, Proceedings, Part II*. 2020. DOI: 10.1007/978-3-030-59013-0_17. URL: http://hdl.handle.net/10993/45497.

[77] Joachim Breitner and Maciej Skorski. “Explicit Renyi Entropy for Hidden Markov Models”. In: *Explicit Renyi Entropy for Hidden Markov Models*. 2020. URL: http://hdl.handle.net/10993/45875.

[78] Matthias R. Brust, Pascal Bouvry, Grégoire Danoy, and El-Ghazali Talbi. “Design Challenges of Trustworthy Artificial Intelligence Learning Systems”. In: *Intelligent Information and Database Systems - 12th Asian Conference ACIIDS 2020, Phuket, Thailand, March 23-26, 2020, Companion Proceedings*. Springer, 2020, pp. 574–584. DOI: 10.1007/978-981-15-3380-8_50. URL: http://hdl.handle.net/10993/43996.

[79] Alessio Buscemi, German Castignani, Thomas Engel, and Ion Turcanu. “A Data-Driven Minimal Approach for CAN Bus Reverse Engineering”. In: *3rd IEEE Connected and Automated Vehicles Symposium, Victoria, Canada, 4-5 October 2020*. 2020. DOI: 10.1109/CAVS51000.2020.9334650. URL: http://hdl.handle.net/10993/44180.

[80] Davide Calvaresi, Jean-Gabriel Piguet, Jean-Paul Calbimonte, Timotheus Kampik, Amro Najjar, Guillaume Gadek, et al. “Ethical Concerns and Opportunities in Binding Intelligent Systems and Blockchain Technology”. In: *Highlights in Practical Applications of Agents, Multi-Agent Systems and Trust-worthiness. The PAAMS Collection - International Workshops of PAAMS 2020, L’Aquila, Italy, October 7-9, 2020, Proceedings*. Springer, 2020, pp. 5–16. DOI: 10.1007/978-3-030-51999-5_1. URL: http://hdl.handle.net/10993/46007.

[81] Ramiro Daniel Camino, Christof Ferreira Torres, Mathis Baden, and Radu State. “A Data Science Approach for Honeypot Detection in Ethereum”. In: *2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. 2020. URL: http://hdl.handle.net/10993/43195.

[82] Guido Cantelmo, Piergiorgio Vitello, Bogdan Toader, Constantinos Antoniou, and Francesco Viti. “Inferring Urban Mobility and Habits from User Location History”. In: *Transportation Research Procedia*. Vol. 47. Elsevier, 2020, pp. 283–290. URL: http://hdl.handle.net/10993/47413.

[83] Tong Cao, Jiangshan Yu, Jérémie Decouchant, Xiapu Luo, and Paulo Verissimo. “Exploring the Monero Peer-to-Peer Network”. In: *Financial Cryptography and Data Security 2020, Sabah, 10-14 February 2020*. 2020. URL: http://hdl.handle.net/10993/42573.

[84] Fernando Kaway Carvalho Ota, Jorge Augusto Meira, Cyril Cassagnes, and Radu State. “Mobile App to SGX Enclave Secure Channel”. In: *2019 IEEE International Symposium on Software Reliability Engineering Workshops*. 2020. DOI: 10.1109/ISSREW.2019.00081. URL: http://hdl.handle.net/10993/44341.

[85] Fernando Kaway Carvalho Ota, Jorge Augusto Meira, Raphaël Frank, and Radu State. “Towards Privacy Preserving Data Centric Super App”. In: *2020 Mediterranean Communication and Computer Networking Conference, Arona 17-19 June 2020*. IEEE, 2020. ISBN: 978-1-7281-6248-5. DOI: 10.1109/MedComNet49392.2020.9191550. URL: http://hdl.handle.net/10993/44340.

[86] Cyril Cassagnes, Lucian Andrei Trestioreanu, Clement Joly, and Radu State. “The rise of eBPF for non-intrusive performance monitoring”. In: *IEEE Xplore*. 2020, p. 7. DOI: 10.1109/NOMS47738.2020.9110434. URL: http://hdl.handle.net/10993/43564.

[87] Boonyarit Changaival, Grégoire Danoy, Kliazovich, Frédéric Guinand, Matthias R. Brust, Jedrzej Musial, et al. “NGAP: a novel hybrid metaheuristic algorithm for round-trip carsharing fleet planning”. In: *GECCO ’20: Genetic and Evolutionary Computation Conference, Companion Volume, Cancún, Mexico, July 8-12, 2020*. ACM, 2020, pp. 259–260. DOI: 10.1145/3377929.3389941. URL: http://hdl.handle.net/10993/43998.

[88] Xihui Chen, Ema Kepuska, Sjouke Mauw, and Yunior Ramirez Cruz. “Active Re-identification Attacks on Periodically Released Dynamic Social Graphs”. In: *Computer Security - ESORICS 2020*. Ed. by Liqun Chen, Ninghui Li, Kaitai Liang, and Steve Schneider. 2020, pp. 185–205. DOI: 10.1007/978-3-030-59013-0_10. URL: http://hdl.handle.net/10993/44270.

[89] Raluca Ioana Chitic, Nicolas Bernard, Franck Leprévost, and Iona Raluca Chitic. “A proof of concept to deceive humans and machines at image classification with evolutionary algorithms”. In: *Proceedings of ACIIDS 2020*. Springer, 2020, pp. 467–480. URL: http://hdl.handle.net/10993/42259.

[90] Yi Ting Chua, Simon Parkin, Matthew Edwards, Daniela Oliveira, Stefan Schiffner, Gareth Tyson, et al. “Identifying Unintended Harms of Cybersecurity Measures”. In: *Proceedings of ECRIME 2019*. Institute of Electrical and Electronics Engineers, 2020. URL: http://hdl.handle.net/10993/41702.

[91] Maxime Cordy, Mike Papadakis, and Axel Legay. “Statistical Model Checking for Variability-Intensive Systems”. In: *FUNDAMENTAL APPROACHES TO SOFTWARE ENGINEERING, Dublin 22-25 April 2020*. 2020. URL: http://hdl.handle.net/10993/45705.

[92] Jean-Sébastien Coron, Sonia Belaid, Emmanuel Prouff, Matthieu Rivain, and Abdul Rhaman Taleb. “CRYPTO 2020”. In: *CRYPTO 2020*. 2020. URL: http://hdl.handle.net/10993/46424.

[93] Jean-Sébastien Coron and Agnese Gini. “A Polynomial-Time Algorithm for Solving the Hidden Subset Sum Problem”. In: *Advances in Cryptology – CRYPTO 2020*. Springer International Publishing, 2020, pp. 3–31. ISBN: 978-3-030-56880-1. DOI: 10.1007/978-3-030-56880-1_1. URL: http://hdl.handle.net/10993/44119.

[94] Jean-Sébastien Coron, Aurelien Greuet, and Rina Zeitoun. “Eurocrypt 2020”. In: *Eurocrypt 2020*. 2020. URL: http://hdl.handle.net/10993/46425.

[95] Jean-Sébastien Coron, Luca Notarnicola, and Gabor Wiese. “Simultaneous Diagonalization of Incomplete Matrices and Applications”. In: *Proceedings of the Fourteenth Algorithmic Number Theory Symposium (ANTS-XIV), edited by Steven Galbraith, Open Book Series 4, Mathematical Sciences Publishers, Berkeley, 2020*. Vol. 4. MSP, 2020, pp. 127–142. URL: http://hdl.handle.net/10993/45537.

[96] Jorge Cortés-Mendoza, Andrei Tchernykh, Mikhail Babenko, Luis Bernardo Pulido-Gaytan, Gleb Radchenko, Franck Leprevost, et al. “Privacy-Preserving Logistic Regression as a Cloud Service Based on Residue Number System”. In: *6th Russian Supercomputing Days, Moscow 21-22 September 2020*. Ed. by Vladimir Voevodin and Sergey Sobolev. Springer, 2020, pp. 598–610. DOI: 10.1007/978-3-030-64616-5_51. URL: http://hdl.handle.net/10993/45091.

[97] Marcos Cramer and Jérémie Dauphin. “A First Approach to Argumentation Label Functions”. In: *Computational Models of Argument - Proceedings of COMMA 2020, Perugia Italy, September 4-11, 2020*. IOS Press, 2020, pp. 159–166. DOI: 10.3233/FAIA200501. URL: http://hdl.handle.net/10993/45746.

[98] Aditya Shyam Shankar Damodaran and Alfredo Rial. “UC Updatable Databases and Applications”. In: *12th International Conference on Cryptology*. 2020. URL: http://hdl.handle.net/10993/42984.

[99] Aditya Shyam Shankar Damodaran and Alfredo Rial. “Unlinkable Updatable Databases and Oblivious Transfer with Access Control”. In: *25th Australasian Conference on Information Security and Privacy*. 2020. URL: http://hdl.handle.net/10993/43250.

[100] Grégoire Danoy, Didier El Baz, Vincent Boyer, Bernabé Dorronsoro, Laurence T. Yang, and Keqin Li. “IEEE Workshop on Parallel / Distributed Combinatorics and Optimization (PDCO 2020)”. In: *2020 IEEE International Parallel and Distributed Processing Symposium Workshops, IPDPSW 2020, New Orleans, LA, USA, May 18-22, 2020*. IEEE, 2020, p. 489. DOI: 10.1109/IPDPSW50202.2020.00089. URL: http://hdl.handle.net/10993/44000.

[101] Grégoire Danoy, Jun Pang, and Sutcliffe. “Proceedings of the 6th Global Conference on Artificial Intelligence (GCAI 2020)”. In: *6th Global Conference on Artificial Intelligence*. Easychair, 2020. URL: http://hdl.handle.net/10993/43132.

[102] Stanislav Dashevskyi, Yury Zhauniarovich, Olga Gadyatskaya, Aleksandr Pilgun, and Hamza Ouhssain. “Dissecting Android Cryptocurrency Miners”. In: *CODASPY ’20: Tenth ACM Conference on Data and Application Security and Privacy, New Orleans LA USA, March 2020*. ACM, 2020, pp. 191–202. ISBN: 978-1-4503-7107-0. DOI: 10.1145/3374664.3375724. URL: http://hdl.handle.net/10993/45293.

[103] Jérémie Dauphin, Tjitze Rienstra, and Leon van der Torre. “A Principle-Based Analysis of Weakly Admissible Semantics”. In: *Computational Models of Argument - Proceedings of COMMA 2020, Perugia Italy, September 4-11, 2020*. IOS Press, 2020, pp. 167–178. DOI: 10.3233/FAIA200502. URL: http://hdl.handle.net/10993/44735.

[104] Vladimir Despotovic and Tomas Skovranek. “Fractional Linear Prediction Toolbox for MATLAB”. In: *Proc. of 21th International Carpathian Control Conference (ICCC)*. IEEE, 2020, pp. 1–6. ISBN: 978-1-7281-1952-6. DOI: 10.1109/ICCC49264.2020.9257227. URL: http://hdl.handle.net/10993/44835.

[105] Jintai Ding, Doug Emery, Johannes Mueller, Peter Y A Ryan, and Vonn Kee Wong. “Post-Quantum Anonymous Veto Networks”. In: *E-Vote-ID 2020*. 2020. URL: http://hdl.handle.net/10993/45495.

[106] Gabriel Duflo, Grégoire Danoy, El-Ghazali Talbi, and Pascal Bouvry. “Automated design of efficient swarming behaviours: a Q-learning hyper-heuristic approach”. In: *GECCO ’20: Genetic and Evolutionary Computation Conference, Companion Volume, Cancún, Mexico, July 8-12, 2020*. ACM, 2020, pp. 227–228. DOI: 10.1145/3377929.3390026. URL: http://hdl.handle.net/10993/43999.

[107] Gabriel Duflo, Grégoire Danoy, El-Ghazali Talbi, and Pascal Bouvry. “Automating the Design of Efficient Distributed Behaviours for a Swarm of UAVs”. In: *IEEE Symposium Series on Computational Intelligence, Canberra 1-4 December 2020*. IEEE, 2020, pp. 489–496. DOI: 10.1109/SSCI47803.2020.9308355. URL: http://hdl.handle.net/10993/46504.

[108] Briag Gerard Benjamin Dupont, Christian Franck, and Johann Groszschädl. “Fast and Flexible Elliptic Curve Cryptography for Dining Cryptographers Networks”. In: *Mobile, Secure, and Programmable Networking, 6th International Conference, MSPN 2020, Paris, France, October 28–29, 2020, Revised Selected Papers*. Ed. by Samia Bouzefrane, Maryline Laurent, Selma Boumerdassi, and Renault Eric. Springer Verlag, 2020, pp. 89–109. ISBN: 978-3-030-67549-3. DOI: 10.1007/978-3-030-67550-9_7. URL: http://hdl.handle.net/10993/46390.

[109] Maria Eichlseder, Lorenzo Grassi, Reinhard Lüftenegger, Morten Øygarden, Christian Rechberger, Markus Schofnegger, et al. “An Algebraic Attack on Ciphers with Low-Degree Round Functions: Application to Full MiMC”. In: *26th Annual International Conference on the Theory and Application of Cryptology and Information Security - ASIACRYPT 2020*. 2020. URL: http://hdl.handle.net/10993/44163.

[110] Vinu Ellampallil Venugopal and Martin Theobald. “Benchmarking Synchronous and Asynchronous Stream Processing Systems”. In: *Benchmarking Synchronous and Asynchronous Stream Processing Systems*. ACM, 2020, pp. 322–323. DOI: 10.1145/3371158.3371206. URL: http://hdl.handle.net/10993/45325.

[111] Vinu Ellampallil Venugopal, Martin Theobald, Samira Chaychi, and Amal Tawakuli. “AIR: A Light-Weight Yet High-Performance Dataflow Engine based on Asynchronous Iterative Routing”. In: *AIR: A Light-Weight Yet High-Performance Dataflow Engine based on Asynchronous Iterative Routing*. IEEE, 2020, pp. 51–58. ISBN: 978-1-7281-9924-5. URL: http://hdl.handle.net/10993/45326.

[112] Saharnaz Esmaeilzadeh Dilmaghani, Matthias R. Brust, Grégoire Danoy, and Pascal Bouvry. “Local Community Detection Algorithm with Self-defining Source Nodes”. In: *Complex Networks & Their Applications IX*. Springer, Cham, 2020, pp. 200–210. URL: http://hdl.handle.net/10993/45897.

[113] Saharnaz Esmaeilzadeh Dilmaghani, Matthias R. Brust, Grégoire Danoy, Natalia Cassagnes, Johnatan Pecero, and Pascal Bouvry. “Privacy and Security of Big Data in AI Systems:A Research and Standards Perspective”. In: *2019 IEEE International Conference on Big Data (Big Data), 9-12 December 2019*. IEEE, 2020. ISBN: 978-1-7281-0858-2. URL: http://hdl.handle.net/10993/42478.

[114] Ehsan Estaji, Thomas Haines, Kristian Gjoesteen, Peter Roenne, Peter Y A Ryan, and Najmeh Soroush. “Revisiting Practical and Usable Coercion-Resistant Remote E-Voting”. In: *Electronic Voting - 5th International Joint Conference, E-Vote-ID 2020, Bregenz, Austria, October 6-9, 2020, Proceedings*. Springer, 2020, pp. 50–66. DOI: 10.1007/978-3-030-60347-2_4. URL: http://hdl.handle.net/10993/46105.

[115] Christof Ferreira Torres, Mathis Steichen, Robert Norvill, Beltran Fiz Pontiveros, Hugo Jonker, and Sjouke Mauw. “ÆGIS: Shielding Vulnerable Smart Contracts Against Attacks”. In: *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security (ASIA CCS ’20), October 5–9, 2020, Taipei, Taiwan*. 2020. URL: http://hdl.handle.net/10993/42957.

[116] Christof Ferreira Torres, Mathis Steichen, and Radu State. “Towards Usable Protection Against Honeypots”. In: *IEEE International Conference on Blockchain and Cryptocurrency, Toronto, Canada 3-6 May 2020*. 2020. URL: http://hdl.handle.net/10993/43052.

[117] Alexandre Frantz and Denis Zampunieris. “Separation of Concerns Within Robotic Systems Through Proactive Computing”. In: *Proceeding of the 4th IEEE International Conference on Robotic Computing*. IEEE, 2020, pp. 197–201. ISBN: 978-1-7281-5237-0. DOI: 10.1109/IRC.2020.00039. URL: http://hdl.handle.net/10993/44762.

[118] Dov M. Gabbay, Ross James Horne, Sjouke Mauw, and Leon van der Torre. “Attack-Defence Frameworks: Argumentation-Based Semantics for Attack-Defence Trees.” In: *Graphical Models for Security - 7th International Workshop*. 2020. DOI: 10.1007/978-3-030-62230-5_8. URL: http://hdl.handle.net/10993/45491.

[119] Olga Gadyatskaya and Sjouke Mauw. “Attack-Tree Series: A Case for Dynamic Attack Tree Analysis”. In: *Proc.\ 6th International Workshop on Graphical Models for Security (GraMSec’19)*. Springer, 2020, pp. 7–19. URL: http://hdl.handle.net/10993/42498.

[120] Jun Gao, li li li, Pingfan Kong, Tegawendé François D Assise Bissyande, and Jacques Klein. “Borrowing your enemy’s arrows: the case of code reuse in android via direct inter-app code invocation”. In: *ESEC/FSE 2020: Proceedings of the 28th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering*. Association for Computing Machinery, 2020. DOI: 10.1145/3368089.3409745. URL: http://hdl.handle.net/10993/45769.

[121] Américo Gaudín, Gabriel Madruga, Carlos Rodríguez, Santiago Iturriaga, Sergio Nesmachnow, Claudio Paz, et al. “Autonomous Flight of Unmanned Aerial Vehicles Using Evolutionary Algorithms”. In: *High Performance Computing*. Springer International Publishing, 2020, pp. 337–352. ISBN: 978-3-030-41005-6. URL: http://hdl.handle.net/10993/42822.

[122] Salah Ghamizi, Maxime Cordy, Martin Gubri, Mike Papadakis, Andrey Boystov, Yves Le Traon, et al. “Search-based adversarial testing and improvement of constrained credit scoring systems”. In: *ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE ’20), November 8-13, 2020*. 2020. URL: http://hdl.handle.net/10993/45695.

[123] Salah Ghamizi, Maxime Cordy, Mike Papadakis, and Yves Le Traon. “FeatureNET: Diversity-driven Generation of Deep Learning Models”. In: *International Conference on Software Engineering (ICSE)*. 2020. URL: http://hdl.handle.net/10993/44547.

[124] Salah Ghamizi, Renaud Rwemalika, Maxime Cordy, Lisa Veiber, Tegawendé François D Assise Bissyande, Mike Papadakis, et al. “Data-driven simulation and optimization for covid-19 exit strategies”. In: *Data-driven simulation and optimization for covid-19 exit strategies*. Association for Computing Machinery, 2020, pp. 3434–3442. ISBN: 9781450379984. DOI: 10.1145/3394486.3412863. URL: http://hdl.handle.net/10993/45706.

[125] Christian Grevisse, Carina Martins Gomes, and Steffen Rothkugel. "AR4OER: A Semantic Platform for Open Educational Augmented Reality Resources". In: *Proceedings of the 2020 IEEE International Symposium on Multimedia*. IEEE, 2020. ISBN: 978-1-7281-8697-9. DOI: 10.1109/ISM.2020.00047. URL: http://hdl.handle.net/10993/44912.

[126] Christian Grevisse and Steffen Rothkugel. "An SKOS-Based Vocabulary on the Swift Programming Language". In: *The Semantic Web – ISWC 2020*. Springer, 2020, pp. 244–258. DOI: 10.1007/978-3-030-62466-8_16. URL: http://hdl.handle.net/10993/44592.

[127] Thomas Haines, Olivier Pereira, and Peter Roenne. "Short Paper: An Update on Marked Mix-Nets: An Attack, a Fix and PQ Possibilities". In: *Financial Cryptography and Data Security - FC 2020 International Workshops, AsiaUSEC, CoDeFi, VOTING, and WTSC, Kota Kinabalu, Malaysia February 14, 2020, Revised Selected Papers*. Springer, 2020, pp. 360–368. DOI: 10.1007/978-3-030-54455-3_26. URL: http://hdl.handle.net/10993/45357.

[128] Yonglin Hao, Gregor Leander, Willi Meier, Yosuke Todo, and Qingju Wang. "Modeling for Three-Subset Division Property without Unknown Subset and Improved Cube Attacks". In: *39th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2020), Croatia 10-14 May 2020*. 2020. URL: http://hdl.handle.net/10993/43040.

[129] Sviatlana Hoehn and Kerstin Bongard. "Heuristic Evaluation of COVID-19 Chatbots". In: *Proceedings of CONVERSATIONS 2020*. 2020. DOI: 10.1007/978-3-030-68288-0_9. URL: http://hdl.handle.net/10993/44913.

[130] Ross James Horne. "Session Subtyping and Multiparty Compatibility Using Circular Sequents". In: *In 31st International Conference on Concurrency Theory (CONCUR 2020)*. 2020, pp. 12:1–12:22. URL: http://hdl.handle.net/10993/44394.

[131] Ross James Horne, Matteo Acclavio, and Lutz Straßburger. "Logic Beyond Formulas: A Graphical Proof System". In: *LICS '20: Proceedings of the 35th Annual ACM/IEEE Symposium on Logic in Computer Science*. 2020, pp. 38–52. URL: http://hdl.handle.net/10993/44426.

[132] Kai Hu, Siwei Sun, Meiqin Wang, and Qingju Wang. "An Algebraic Formulation of the Division Property: Revisiting Degree Evaluations, Cube Attacks, and Key-Independent Sums". In: *26th Annual International Conference on the Theory and Application of Cryptology and Information Security- ASIACRYPT 2020*. Springer, 2020. URL: http://hdl.handle.net/10993/44162.

[133] Junhao Huang, Zhe Liu, Zhi Hu, and Johann Groszschädl. "Parallel Implementation of SM2 Elliptic Curve Cryptography on Intel Processors with AVX2". In: *Information Security and Privacy, 25th Australasian Conference, ACISP 2020, Perth, WA, Australia, November 30 - December 2, 2020, Proceedings*. Ed. by Joseph K. Liu and Hui Cui. Springer Verlag, 2020, pp. 204–224. ISBN: 978-3-030-55303-6. DOI: 10.1007/978-3-030-55304-3_11. URL: http://hdl.handle.net/10993/46416.

[134] Vincenzo Iovino, Alfredo Rial, Peter Roenne, and Peter Y A Ryan. "(Universal) Unconditional Verifiability in E-Voting without Trusted Parties". In: *2020 IEEE 33rd Computer Security Foundations Symposium*. 2020. URL: http://hdl.handle.net/10993/44191.

[135] Benjamin Jahic, Nicolas Guelfi, and Benoit Ries. "Specifying key-properties to improve the recognition skills of neural networks". In: *Proceedings of the 2020 European Symposium on Software Engineering*. Association for Computing Machinery, 2020. ISBN: 9781450377621. DOI: 10.1145/3393822.3432332. URL: http://hdl.handle.net/10993/44492.

[136] Wojciech Jamroga, Yan Kim, Damian Kurpiewski, and Peter Y A Ryan. "Towards Model Checking of Voting Protocols in Uppaal". In: *Proceedings of the Fifth International Joint Conference on Electronic Voting E-VOTE-ID 2020*. Springer, 2020. DOI: 10.1007/978-3-030-60347-2_9. URL: http://hdl.handle.net/10993/46367.

[137] Wojciech Jamroga, Damian Kurpiewski, and Vadim Malvone. "Natural Strategic Abilities in Voting Protocols". In: *Proceedings of the 10th International Workshop on Socio-Technical Aspects in Security STAST 2020*. Springer, 2020. URL: http://hdl.handle.net/10993/45849.

[138] Ekaterina Khramtsova, Christian Hammerschmidt, Sofiane Lagraa, and Radu State. "Federated Learning For Cyber Security: SOC Collaboration For Malicious URL Detection". In: *IEEE International Conference on Distributed Computing Systems (ICDCS)*. 2020. URL: http://hdl.handle.net/10993/44927.

[139] Sybren de Kinderen, Qin Ma, and Monika Kaczmarek-Heß. "Towards Extending the Validation Possibilities of ADOxx with Alloy". In: *Lecture Notes in Business Information Processing 400*. Springer, 2020, pp. 138–152. ISBN: 978-3-030-63478-0. URL: http://hdl.handle.net/10993/44999.

[140] Niklas Kolbe, Pierre-Yves Vandenbussche, Sylvain Kubler, and Yves Le Traon. "LOVBench: Ontology Ranking Benchmark". In: *Proceedings of The Web Conference 2020 (WWW '20)*. 2020. DOI: 10.1145/3366423.3380245. URL: http://hdl.handle.net/10993/42990.

[141] Augusto Wladimir de La Cadena Ramos, Daniel Kaiser, Andriy Panchenko, and Thomas Engel. "Out-of-the-box Multipath TCP as a Tor Transport Protocol: Performance and Privacy Implications". In: *19th IEEE International Symposium on Network Computing and Applications (IEEE NCA 2020)*. 2020. URL: http://hdl.handle.net/10993/44663.

[142] Augusto Wladimir de La Cadena Ramos, Asya Mitseva, Jens Hiller, Jan Pennekamp, Sebastian Reuter, Julian Filter, et al. "TrafficSliver: Fighting Website Fingerprinting Attacks with Traffic Splitting". In: *27th ACM Conference on Computer and Communications Security (CCS '20)*. 2020. URL: http://hdl.handle.net/10993/44415.

[143] Sofiane Lagraa and Radu State. "Process mining-based approach for investigating malicious login events". In: *IEEE/IFIP Network Operations and Management Symposium, Budapest, Hungary, April 20-24, 2020*. 2020. URL: http://hdl.handle.net/10993/43588.

[144] Li Li, Jun Gao, Pingfan Kong, Haoyu Wang, Mengyu Huang, Yuanfang Li, et al. “Knowledgezooclient: Constructing knowledge graph for android”. In: *The 3rd International Workshop on Advances in Mobile App Analysis*. 2020. URL: http://hdl.handle.net/10993/45770.

[145] Yongjian Li, Taifeng Cao, David Jansen, Jun Pang, and Xiaotao Wei. “Accelerated verification of parametric protocols with decision trees”. In: *Proceedings of the 38th International Conference on Computer Design (ICCD)*. IEEE, 2020, pp. 397–404. DOI: 10.1109/ICCD50377.2020.00073. URL: http://hdl.handle.net/10993/45214.

[146] Tomer Libal. “A Meta-level Annotation Language for Legal Texts”. In: *Lecture Notes in Computer Science*. Springer, 2020. ISBN: 978-3-030-44637-6. URL: http://hdl.handle.net/10993/45477.

[147] Tomer Libal and Alexander Steen. “NAI: Towards Transparent and Usable Semi-Automated Legal Analysis”. In: *Verantwortungsbewusste Digitalisierung, Tagungsband des 23. Internationalen Rechtsinformatik Symposions IRIS 2020*. Ed. by Erich Schweighöfer, Walter Hötzendorfer, Franz Kummer, and Ahti Saarenpää. Editions Weblaw, 2020, pp. 265–272. ISBN: 978-3-96698-589-5. URL: http://hdl.handle.net/10993/42684.

[148] Tomer Libal and Alexander Steen. “Towards an Executable Methodology for the Formalization of Legal Texts”. In: *Logic and Argumentation. CLAR 2020*. Ed. by Mehdi Dastani, Huimin Dong, and Leon van der Torre. Springer, 2020, pp. 151–165. ISBN: 978-3-030-44637-6 || 978-3-030-44638-3. DOI: 10.1007/978-3-030-44638-3_10. URL: http://hdl.handle.net/10993/42688.

[149] Tomer Libal and Tereza. “Towards Automating Inconsistency Checking of Legal Texts”. In: *Towards Automating Inconsistency Checking of Legal Texts*. 2020. URL: http://hdl.handle.net/10993/45476.

[150] Tomer Libal, Leon van der Torre, Dov Gabbay, and Matteo Pascucci. “A bimodal simulation of defeasibility in thenormative domain”. In: *CEUR Workshop Proceedings*. 2020. URL: http://hdl.handle.net/10993/45478.

[151] Hilder Vitor Lima Pereira. “Efficient AGCD-Based Homomorphic Encryption for Matrix and Vector Arithmetic”. In: *Applied Cryptography and Network Security*. Springer International Publishing, 2020, pp. 110–129. ISBN: 978-3-030-57808-4. URL: http://hdl.handle.net/10993/44996.

[152] Kui Liu, Shangwen Wang, Anil Koyuncu, Kisub Kim, Tegawendé François D Assise Bissyande, Dongsun Kim, et al. “On the Efficiency of Test Suite based Program Repair: A Systematic Assessment of 16 Automated Repair Systems for Java Programs”. In: *42nd ACM/IEEE International Conference on Software Engineering (ICSE)*. 2020. DOI: 10.1145/3377811.3380338. URL: http://hdl.handle.net/10993/42854.

[153] Tianming Liu, Haoyu Wang, Li Li, Xiapu Luo, Feng Dong, Yao Guo, et al. “MadDroid: Characterizing and Detecting Devious Ad Contents for Android Apps”. In: *Proceedings of The Web Conference 2020*. Association for Computing Machinery, 2020, pp. 1715–1726. ISBN: 9781450370233. DOI: 10.1145/3366423.3380242. URL: http://hdl.handle.net/10993/45320.

[154] Cedric Lothritz, Kevin Allix, Lisa Veiber, Jacques Klein, and Tegawendé François D Assise Bissyande. “Evaluating Pretrained Transformer-based Models on the Task of Fine-Grained Named Entity Recognition”. In: *Proceedings of the 28th International Conference on Computational Linguistics*. 2020, pp. 3750–3760. URL: http://hdl.handle.net/10993/45217.

[155] Wei Ma, Thomas Laurent, Miloš Ojdanić, Thierry Titcheu Chekam, Anthony Ventresque, and Mike Papadakis. “Commit-Aware Mutation Testing”. In: *IEEE International Conference on Software Maintenance and Evolution (ICSME)*. 2020. URL: http://hdl.handle.net/10993/44125.

[156] S. Mahon, Sébastien Varrette, Valentin Plugaru, Frederic Pinel, and Pascal Bouvry. “Performance Analysis of Distributed and Scalable Deep Learning”. In: *20th IEEE/ACM Intl. Symp. on Cluster, Cloud and Internet Computing (CCGrid’20)*. IEEE/ACM, 2020, pp. 760–766. ISBN: 978-1-7281-6095-5. URL: http://hdl.handle.net/10993/43342.

[157] Abdoul Wahid Mainassara Chekaraou, Xavier Besseron, Alban Rousset, Emmanuel Kieffer, and Bernhard Peters. “Predicting near-optimal skin distance in Verlet buffer approach for Discrete Element Method”. In: *10th IEEE Workshop on Parallel / Distributed Combinatorics and Optimization*. 2020. DOI: 10.1109/IPDPSW50202.2020.00093. URL: http://hdl.handle.net/10993/44814.

[158] Gaetano Manzo, Eirini Kalogeiton, Antonio di Maio, Torsten Braun, Maria Rita Palattella, Ion Turcanu, et al. “DeepNDN: Opportunistic Data Replication and Caching in Support of Vehicular Named Data”. In: *21st IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*. 2020, pp. 234–243. DOI: 10.1109/WoWMoM49955.2020.00051. URL: http://hdl.handle.net/10993/43885.

[159] Asya Mitseva, Marharyta Aleksandrova, Thomas Engel, and Andriy Panchenko. “Security and Performance Implications of BGP Rerouting-resistant Guard Selection Algorithms for Tor”. In: *Security and Performance Implications of BGP Rerouting-resistant Guard Selection Algorithms for Tor*. 2020. URL: http://hdl.handle.net/10993/42525.

[160] Asya Mitseva, Thomas Engel, and Andriy Panchenko. “Analyzing PeerFlow – A Bandwidth Estimation System for Untrustworthy Environments”. In: *Analyzing PeerFlow – A Bandwidth Estimation System for Untrustworthy Environments*. 2020. URL: http://hdl.handle.net/10993/42523.

[161] Xian Mo, Jun Pang, and Zhiming Liu. “Higher-order graph convolutional embedding for temporal networks”. In: *Proceedings of the 21st International Conference on Web Information System Engineering (WISE’20)*. Springer, 2020, pp. 3–15. URL: http://hdl.handle.net/10993/44535.

[162] Ludovic Mouline, Maxime Cordy, and Yves Le Traon. “Load approximation for uncertain topologies in the low-voltage grid”. In: *INTERNATIONAL CONFERENCE ON SMART GRID COMMUNICATIONS, 11-13 November 2020*. 2020, pp. 1–6. DOI: 10.1109/SmartGridComm47815.2020.9302940. URL: http://hdl.handle.net/10993/44335.

[163] Johannes Mueller and Thomas Haines. “SoK: Techniques for Verifiable Mix Nets”. In: *IEEE Computer Security Foundations Symposium*. 2020. DOI: 10.1109/CSF49147.2020.00012. URL: http://hdl.handle.net/10993/45022.

[164] Johannes Mueller, Ralf Küsters, Julian Liedtke, Daniel Rausch, and Andreas Vogt. “Ordinos: A Verifiable Tally-Hiding E-Voting System”. In: *IEEE European Symposium on Security and Privacy*. 2020. DOI: 10.1109/EuroSP48549.2020.00022. URL: http://hdl.handle.net/10993/45019.

[165] Artur Niewiadomski, Magdalena Kacprzak, Damian Kurpiewski, Michał Knapik, Wojciech Penczek, and Wojciech Jamroga. “MsATL: a Tool for SAT-Based ATL Satisfiability Checking”. In: *Proceedings of 19th International Conference on Autonomous Agents and Multiagent Systems AAMAS 2020*. 2020. ISBN: 978-1-4503-7518-4. URL: http://hdl.handle.net/10993/45853.

[166] Tiago Oliveira, Jérémie Dauphin, Ken Satoh, Shusaku Tsumoto, and Paulo Novais. “Goal-Driven Structured Argumentation for Patient Management in a Multimorbidity Setting”. In: *Logic and Argumentation - Third International Conference, CLAR 2020 Hangzhou, China, April 6-9, 2020, Proceedings*. Springer, 2020, pp. 166–183. DOI: 10.1007/978-3-030-44638-3_11. URL: http://hdl.handle.net/10993/45743.

[167] Frédéric Pinel, Jian-xiong Yin, Christian Hundt, Emmanuel Kieffer, Sébastien Varrette, Pascal Bouvry, et al. “Evolving a Deep Neural Network Training Time Estimator”. In: *Communications in Computer and Information Science*. Springer, 2020. URL: http://hdl.handle.net/10993/42856.

[168] Sean Rivera, Vijay Gurbani, Sofiane Lagraa, Antonio Ken Iannillo, and Radu State. “Leveraging eBPF to preserve user privacy for DNS, DoT, and DoH queries”. In: *Proceedings of the 15th International Conference on Availability, Reliability and Security*. 2020. DOI: 10.1145/3407023.3407041. URL: http://hdl.handle.net/10993/44402.

[169] François Robinet, Antoine Demeules, Raphaël Frank, Georgios Varisteas, and Christian Hundt. “Leveraging Privileged Information to Limit Distraction in End-to-End Lane Following”. In: *2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC)*. 2020. URL: http://hdl.handle.net/10993/41788.

[170] Peter Roenne, Arash Atashpendar, Gjøsteen Kristian, and Peter Ryan. “Coercion-Resistant Voting in Linear Time via Fully Homomorphic Encryption: Towards a Quantum-Safe Scheme”. In: *Financial Cryptography and Data Security 2019. FC 2019: International Workshops, CIW, VOTING, and WTSC*. Springer, 2020. URL: http://hdl.handle.net/10993/37791.

[171] Azim Roussanaly, Marharyta Aleksandrova, and Anne Boyer. “BacAnalytics: A Tool to Support Secondary School Examination in France”. In: *25th International Symposium on Intelligent Systems (ISMIS 2020)*. 2020. URL: http://hdl.handle.net/10993/42639.

[172] Rudrani Sharma, Christoph Schommer, and Nicolas Vivarelli. “Building up Explainability in Multi-layer Perceptrons for Credit Risk Modeling”. In: *Building up Explainability in Multi-layer Perceptrons for Credit Risk Modeling*. 2020, p. 2. URL: http://hdl.handle.net/10993/44277.

[173] Joshgun Sirajzade, Daniela Gierschek, and Christoph Schommer. "An Annotation Framework for Luxembourgish Sentiment Analysis". In: *Proceedings of the LREC 2020 1st Joint SLTU and CCURL Workshop (SLTU-CCURL 2020)*. Ed. by Laurent Besacier, Sakriani Sakti, Claudia Soria, and Dorothee Beermann. European Language Resources Association (ELRA), 2020, pp. 172–176. ISBN: 979-10-95546-35-1 || 9791095546351. URL: http://hdl.handle.net/10993/43136.

[174] Joshgun Sirajzade, Daniela Gierschek, and Christoph Schommer. "Component Analysis of Adjectives in Luxembourgish for Detecting Sentiments". In: *Proceedings of the LREC 2020 1st Joint SLTU and CCURL Workshop(SLTU-CCURL 2020)*. Ed. by Dorothee Beermann, Laurent Besacier, Sakriani Sakti, and Claudia Soria. European Language Resources Association (ELRA), 2020, pp. 159–166. ISBN: 979-10-95546-35-1 || 9791095546351. URL: http://hdl.handle.net/10993/43137.

[175] Najmeh Soroush, Vincenzo Iovino, Alfredo Rial, Peter Roenne, and Peter Y A Ryan. "Verifiable Inner Product Encryption Scheme". In: *Public-Key Cryptography – PKC 2020*. 2020. URL: http://hdl.handle.net/10993/44190.

[176] Ridha Soua, Maria Rita Palattella, André Stemper, and Thomas Engel. "Enhancing CoAP Group Communication to Support mMTC Over Satellite Networks". In: *IEEE International Conference on Communications (ICC)*. 2020. URL: http://hdl.handle.net/10993/42599.

[177] Alexander Steen and Christoph Benzmüller. "The Higher-Order Prover Leo-III (Highlight paper)". In: *Proceedings of the 24th European Conference on Artificial Intelligence*. IOS Press, 2020, pp. 2937–2938. ISBN: 978-1-64368-100-9. DOI: 10.3233/FAIA200462. URL: http://hdl.handle.net/10993/42687.

[178] Borce Stojkovski and Gabriele Lenzini. "Evaluating ambiguity of privacy indicators in a secure email app". In: *Proceedings of the Fourth Italian Conference on Cyber Security, Ancona Italy, February 4th to 7th, 2020*. Ed. by Michele Loreti and Luca Spalazzi. CEUR-WS.org, 2020, pp. 223–234. URL: http://hdl.handle.net/10993/43267.

[179] Daniel Stolfi Rosso, Matthias R. Brust, Grégoire Danoy, and Pascal Bouvry. "A Cooperative Coevolutionary Approach to Maximise Surveillance Coverage of UAV Swarms". In: *IEEE 17th Annual Consumer Communications & Networking Conference CCNC 2020, Las Vegas, NV, USA, January 10-13, 2020*. IEEE, 2020, pp. 1–6. DOI: 10.1109/CCNC46108.2020.9045643. URL: http://hdl.handle.net/10993/43997.

[180] Daniel Stolfi Rosso, Matthias R. Brust, Grégoire Danoy, and Pascal Bouvry. "Competitive Evolution of a UAV Swarm for Improving Intruder Detection Rates". In: *2020 IEEE International Parallel and Distributed Processing Symposium Workshops, IPDPSW 2020, New Orleans, LA, USA, May 18-22, 2020*. IEEE, 2020, pp. 528–535. DOI: 10.1109/IPDPSW50202.2020.00094. URL: http://hdl.handle.net/10993/44001.

[181] Daniel Stolfi Rosso, Matthias R. Brust, Grégoire Danoy, and Pascal Bouvry. "Optimizing the Performance of an Unpredictable UAV Swarm for Intruder Detection". In: *Optimization and Learning - Third International Conference, OLA 2020, Cádiz, Spain, February 17-19, 2020, Proceedings*.

Springer, 2020, pp. 37–48. DOI: 10.1007/978-3-030-41913-4_4. URL: http://hdl.handle.net/10993/44002.

[182] Cui Su and Jun Pang. “A Dynamics-based Approach for the Target Control of Boolean Networks”. In: *Proceedings of the 11th ACM International Conference on Bioinformatics, Computational Biology and Health Informatics*. ACM Press, 2020, 50:1–50:8. ISBN: 978-1-4503-7964-9. URL: http://hdl.handle.net/10993/44705.

[183] Cui Su and Jun Pang. “Sequential Temporary and Permanent Control of Boolean Networks.” In: *Proceedings of the 18th International Conference on Computational Methods in Systems Biology (CMSB)*. Springer, 2020, pp. 234–251. URL: http://hdl.handle.net/10993/44408.

[184] Ningyuan Sun and Jean Botev. “Intelligent Adaptive Agents and Trust in Virtual and Augmented Reality”. In: *Proceedings of the 19th IEEE International Symposium on Mixed and Augmented Reality (ISMAR)*. 2020. URL: http://hdl.handle.net/10993/46305.

[185] Zeyu Sun, Jie Zhang, Mark Harman, Mike Papadakis, and Lu Zhang. “Automatic Testing and Improvement of Machine Translation”. In: *International Conference on Software Engineering (ICSE)*. 2020. URL: http://hdl.handle.net/10993/41849.

[186] Iraklis Symeonidis and Gabriele Lenzini. “Systematization of threats and requirements for private messaging with untrusted servers. The case of E-mailing and instant messaging”. In: *International Conference on Information Systems Security and Privacy, Malta 25-27 February 2020*. 2020. URL: http://hdl.handle.net/10993/42724.

[187] Panissara Thanapol, Kittichai Lavangnananda, Pascal Bouvry, Frederic Pinel, and Franck Leprevost. “Reducing overfitting and improving generalization in training convolutional neural network under limited sample sizes in image recognition”. In: *5th International Conference on Information Technology, Bangsaen 21-22 October 2020*. 2020, pp. 300–305. URL: http://hdl.handle.net/10993/45107.

[188] Haoye Tian, Kui Liu, Abdoul Kader Kaboreé, Anil Koyuncu, Li Li, Jacques Klein, et al. “Evaluating Representation Learning of Code Changes for Predicting Patch Correctness in Program Repair”. In: *35th IEEE/ACM International Conference on Automated Software Engineering, September 21-25, 2020, Melbourne, Australia*. 2020. URL: http://hdl.handle.net/10993/45494.

[189] Sergei Tikhomirov, Pedro Moreno-Sanchez, and Matteo Maffei. “A Quantitative Analysis of Security, Anonymity and Scalability for the Lightning Network”. In: *Proceedings of 2020 IEEE European Symposium on Security and Privacy (EuroS&P)*. 2020. URL: http://hdl.handle.net/10993/44483.

[190] Thierry Titcheu Chekam, Mike Papadakis, and Yves Le Traon. “Muteria: An Extensible and Flexible Multi-Criteria Software Testing Framework”. In: *ACM/IEEE International Conference on Automation of Software Test (AST) 2020*. 2020. URL: http://hdl.handle.net/10993/44079.

[191] Lisa Veiber, Kevin Allix, Yusuf Arslan, Tegawendé François D Assise Bissyande, and Jacques Klein. “Challenges Towards Production-Ready Explainable Machine Learning”. In: *Proceedings of the 2020 USENIX Conference on Operational Machine Learning (OpML 20)*. USENIX Association, 2020. ISBN: 978-1-939133-15-1. URL: http://hdl.handle.net/10993/44318.

[192] Yan Wu, Jinchuan Chen, Plarent Haxhidauti, Vinu Ellampallil Venugopal, and Martin Theobald. “Guided Inductive Logic Programming: Cleaning Knowledge Bases with Iterative User Feedback”. In: *Guided Inductive Logic Programming: Cleaning Knowledge Bases with Iterative User Feedback*. 2020, pp. 92–106. URL: http://hdl.handle.net/10993/45625.

[193] Liuwen Yu, Réka Markovich, and Leon van der Torre. “Interpretation of Support among Arguments”. In: *Legal Knowledge and Information Systems – Frontiers in Artificial Intelligence and Application Series*. 2020. URL: http://hdl.handle.net/10993/46423.

[194] Chenyi Zhang and Jun Pang. “Characterising probabilistic alternating simulation for concurrent games”. In: *Proceedings of the 14th IEEE Symposium on Theoretical Aspects of Software Engineering (TASE)*. IEEE, 2020, pp. 121–128. DOI: 10.1109/TASE.2020.00025. URL: http://hdl.handle.net/10993/44962.

[195] Zhiqiang Zhong, Yang Zhang, and Jun Pang. “NeuLP: An End-to-End Deep-Learning Model for Link Prediction”. In: *Proceedings of the 21st International Conference on Web Information System Engineering (WISE’20)*. Springer, 2020, pp. 96–108. URL: http://hdl.handle.net/10993/44544.

[196] Marie-Laure Zollinger, Peter Roenne, and Peter Ryan. “Short paper: Mechanized Proofs of Verifiability and Privacy in a paper-based e-voting Scheme”. In: *International Conference on Financial Crypto Workshop on Advances in Secure Electronic Voting*. 2020. URL: http://hdl.handle.net/10993/42392.

A.5 Theses

[197] Ramiro Daniel Camino. “Machine Learning Techniques for Suspicious Transaction Detection and Analysis”. PhD thesis. University of Luxembourg, Luxembourg, Luxembourg, 2020. URL: http://hdl.handle.net/10993/44939.

[198] Andrea Capponi. “Energy-efficient Mobile Crowdsensing Solutions for Smart Cities”. PhD thesis. University of Luxembourg, Esch-sur-Alzette, Luxembourg, 2020. URL: http://hdl.handle.net/10993/46378.

[199] Andrej Dameski. “Foundations of an Ethical Framework for AI Entities: the Ethics of Systems”. PhD thesis. University of Luxembourg, Esch-sur-Alzette, Luxembourg and University of Bologna, Bologna, Italy, 2020. URL: http://hdl.handle.net/10993/45285.

[200] Ali Farjami. “Discursive Input/Output Logic: Deontic Modals, and Computation”. PhD thesis. University of Luxembourg, Luxembourg, 2020. URL: http://hdl.handle.net/10993/44768.

[201] Daniel Feher. “Data Analytics and Consensus Mechanisms in Blockchains”. PhD thesis. University of Luxembourg, Esch-sur-Alzette, Luxembourg, 2020. URL: http://hdl.handle.net/10993/44493.

[202] Ziya Alper Genç. “Analysis, Detection, and Prevention of Cryptographic Ransomware”. PhD thesis. University of Luxembourg, Luxembourg, Luxembourg, 2020. URL: http://hdl.handle.net/10993/44662.

[203] Christian Grevisse. “The ALMA-Yactul Ecosystem: A Holistic Approach for Student-centered Integration of Learning Material”. PhD thesis. University of Luxembourg, Luxembourg, 2020. URL: http://hdl.handle.net/10993/41490.

[204] Yujuan Gui. “Genetic regulators of ventral midbrain gene expression and nigrostriatal circuit integrity”. PhD thesis. University of Luxembourg, Luxembourg, 2020. URL: http://hdl.handle.net/10993/43833.

[205] Abdallah Ali Zainelabden Abdallah Ibrahim. “PERFORMANCE EVALUATION AND MODELLING OF SAAS WEB SERVICES IN THE CLOUD”. PhD thesis. University of Luxembourg, Esch-sur-Alzette, Luxembourg, 2020. URL: http://hdl.handle.net/10993/41839.

[206] Sasan Jafarnejad. “Machine Learning-based Methods for Driver Identification and Behavior Assessment: Applications for CAN and Floating Car Data”. PhD thesis. University of Luxembourg, Esch-sur-Alzette, Luxembourg, 2020. URL: http://hdl.handle.net/10993/42721.

[207] Nida Khan. “Blockchain-enabled Traceability and Immutability for Financial Applications”. PhD thesis. University of Luxembourg, Luxembourg, 2020. URL: http://hdl.handle.net/10993/43941.

[208] Niklas Kolbe. “A Formal Approach to Ontology Recommendation for Enhanced Interoperability in Open IoT Ecosystems”. PhD thesis. University of Luxembourg, Luxembourg, 2020. URL: http://hdl.handle.net/10993/43756.

[209] Anil Koyuncu. “Boosting Automated Program Repair for Adoption By Practitioners”. PhD thesis. University of Luxembourg, Luxembourg, 2020. URL: http://hdl.handle.net/10993/45073.

[210] Diego Kreutz. “Logically Centralized Security for Software-Defined Networking”. PhD thesis. University of Luxembourg, Luxembourg, 2020. URL: http://hdl.handle.net/10993/44608.

[211] Hilder Vitor Lima Pereira. “Homomorphic encryption and multilinear maps based on the approximate-GCD problem”. PhD thesis. University of Luxembourg, Esch-sur-Alzette, Luxembourg, 2020. URL: http://hdl.handle.net/10993/44723.

[212] Abdoul Wahid Mainassara Chekaraou. “Large Scale Parallel Simulation For Extended Discrete Element Method”. PhD thesis. University of Luxembourg, Luxembourg, 2020. URL: http://hdl.handle.net/10993/46418.

[213] Antonio di Maio. "Routing Strategies and Content Dissemination Techniques for Software-Defined Vehicular Networks". PhD thesis. University of Luxembourg, Esch-sur-Alzette, Luxembourg, 2020. URL: http://hdl.handle.net/10993/43560.

[214] Robert Norvill. "Blockchain Technology for Data Sharing in the Banking Sector". PhD thesis. University of Luxembourg, Luxembourg, Luxembourg, 2020. URL: http://hdl.handle.net/10993/44209.

[215] Aleksandr Pilgun. "Instruction Coverage for Android App Testing and Tuning". PhD thesis. University of Luxembourg, Esch-sur-Alzette, Luxembourg, 2020. URL: http://hdl.handle.net/10993/45355.

[216] Amin Sleimi. "AN NLP-BASED FRAMEWORK TO FACILITATE THE DERIVATION OF LEGAL REQUIREMENTS FROM LEGAL TEXTS". PhD thesis. University of Luxembourg, Luxembourg, Luxembourg, 2020. URL: http://hdl.handle.net/10993/45065.

[217] Zachary Daniel Smith. "Design and Verification of Specialised Security Goals for Protocol Families". PhD thesis. University of Luxembourg, Luxembourg, 2020. URL: http://hdl.handle.net/10993/45058.

[218] Cui Su. "Scalable Control of Asynchronous Boolean Networks". PhD thesis. University of Luxembourg, Luxembourg, 2020. URL: http://hdl.handle.net/10993/44771.

[219] Sergei Tikhomirov. "Security and Privacy of Blockchain Protocols and Applications". PhD thesis. University of Luxembourg, Esch-sur-Alzette, Luxembourg, 2020. URL: http://hdl.handle.net/10993/44424.

[220] Itzel Vazquez Sandoval. "A multifaceted formal analysis of end-to-end encrypted email protocols and cryptographic authentication enhancements". PhD thesis. University of Luxembourg, Esch-sur-Alzette, Luxemburgo, 2020. URL: http://hdl.handle.net/10993/44819.

[221] Ivana Vukotic. "Formal Framework for Verifying Implementations of Byzantine Fault-Tolerant Protocols Under Various Models". PhD thesis. University of Luxembourg, Esch sur Alzette, Luxembourg, 2020. URL: http://hdl.handle.net/10993/43529.

[222] Junwei Wang. "On the practical security of white-box cryptography". PhD thesis. Université du Luxembourg, Esch-sur-Alzette, Luxembourg and Université Paris 8, Saint-Denis, France, 2020. URL: http://hdl.handle.net/10993/44291.

[223] Marie-Laure Zollinger. "From Secure to Usable and Verifiable Voting Schemes". PhD thesis. University of Luxembourg, Esch-sur-Alzette, Luxembourg, 2020. URL: http://hdl.handle.net/10993/44422.

Appendix B

Research Projects

This chapter lists research projects that were ongoing during 2018, and whose principal investigator is a DCS member. It is structured to summarize the projects by funding source.

- EC - Erasmus+ - KA2
- EC - H2020
- EU - COST Action
- NLnet - NGI - NGI0 PET Fund
- FNR
- FNR and UL
- FNR - AFR
- FNR - AFR PhD
- FNR - AFR PhD and ILNAS
- FNR - CORE
- FNR - CORE - Core Junior
- FNR - COVID-19 Fast Track
- FNR - Industrial Fellowships
- FNR - INTER
- FNR (Luxembourg)/NCBiR (Poland)
- FNR - POC
- FNR - PRIDE
- ONRG - NICOP
- UL
- UL and Esch2022
- UL and External Organisation Funding
- External Organisation Funding

B.1 EC - Erasmus+ - KA2 Projects

Modernisation of Higher Education in central Asia through new technologies

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 2021
Members:	• Thomas ENGEL (Principal Investigator) • Aurel MACHALEK (Researcher) • Anne OCHSENBEIN (Project Coordinator) • Stefanie OESTLUND (Project Coordinator) • Mathieu VIAU-COURVILLE (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 2020 year of global pandemic crises clearly showed the importance of projects like HiEdTec in the field of higher education. New techniques of distance teaching have to be established, new methods very related to the HiEdTec research area are being used. The main contribution of the University of Luxembourg to the HiEdTec project was to evaluate the progress of the project, especially with the objective to:

- A plan for ensuring the project quality has been created and fulfilled;
- Project evaluation plan for ensuring the project quality has been developed and fully realised;
- Procedures for the evaluation of all project deliverables have been organized, conducted, and reported;
- The results of the project QA activities have been spread among the partners on a regular basis;
- Internal evaluations of the interim and final results of the project have been organized and conducted.
- Meetings have been evaluated and results been reported.

Secondly, the University of Luxembourg continues the work on creating a sustainable academic network and develops a plan for its sustainability after the project end.

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 – 28 Feb 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)
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
- Orange Polska Spolka Akcyjna
- ORION INNOVATIONS PRIVATE COMPANY
- SMARTNET ANONYMI TOURISTIKI KAI KATASKEVASTIKI ETAIREIA PAROCHIS YPIRESION
- Spi
- University of Kent
- University of Surrey
- Vediafi Oy
- VTT, Finland

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

The work carried out in 2020 focused on two aspects:

5G-Drive aims 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. In 2020, Secan-Lab continued its active contribution to this project on two aspects. The first aspect focused on carrying out laboratory tests on the resiliency of V2X and the accuracy of a misbehavior detection system (MDS) according to the test procedures we defined in the first stage of the project. More specifically, the SECAN-lab team has tested the resilience of ITS-G5 and C-V2X to the jamming attacks. The SECAN-lab team has also tested the accuracy of its developed MDS solution to detect grey hole attacks.

In the second aspect, the SECAN-lab team investigated 5G key technologies (software-defined networking (SDN) and multi-access edge computing) and their contribution to the security and privacy of connected vehicles. On the first hand, we exploit the SDN to propose a context-aware MDS. Based on the context, the proposed system can tune security parameters to provide accurate detection with low false positives while being Sybil attack-resistant and compliant with vehicular privacy standards. On the second hand, the Secan-lab has investigated data collection in the context of vehicular Fog Computing (VFC). SDN is also exploited to propose a fully-programmable, self-configurable, and context-aware data collection scheme for VFC. This scheme leverages a stochastic model to dynamically estimate the number of fog stations to be deployed. The proposed scheme provides lower latency and higher resiliency compared to classical data collection schemes.

5G-MOBIX

Acronym:	5G-MOBIX
Reference:	R-AGR-3457-10
PI:	Thomas ENGEL
Funding:	European Commission - Horizon 2020
Budget:	21,410,205.65 €
Duration:	1 Nov 2018 – 31 Oct 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) • Ion TURCANU (Post-Doc)
Area:	Communicative Systems
Partners:	• Aalto Korkeakoulusaatio S.R. • AEVAC - Asociación Española del Vehículo Autónomo Conectado • AKKA Informatique et Systemes • Alsa Grupo, S.L.U.

- ASELSAN Elektronik Sanayi ve Ticaret A.S.
- 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
- Dalian Roiland Technology Co.,Ltd
- Dalian University of Technology
- Datang Telecom Technology
- DEKRA Testing and Certification, S.A.U.
- Eindhoven University of Technology
- Electronics and Telecommunications Research Institute (ETRI)
- Ericsson Arastirma Gelistirme ve Bilisim Hizmetleri A.S.
- Ericsson Hellas
- ERTICO - ITS
- FONDATION PARTENARIAL MOV'EOTEC (VeDecoM)
- Ford Otomotiv Sanayi A.S.
- Fraunhofer Gesellschaft
- Gemeente Helmond
- GT-ARC gemeinnützige GmbH
- HERE Global B.V.
- 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.
- ISEL
- JEFATURA CENTRAL DE TRAFICO
- Korea Automotive Technology Institute (KATECH)
- KPN
- Luxembourg Institute of Science & technology (LIST)
- National Electric Vehicle Sweden (NEVS)
- NEDERLANDSE ORGANISATIE VOOR TOEGEPAST NATUUR-WETENSCHAPPELIJK ONDERZOEK (TNO)
- NOKIA SIEMENS NETWORKS PORTUGAL S.A.
- NOKIA SPAIN S.A.
- Satellite Applications Catapult Limited
- Sensible 4
- Siemens S.A.
- SNETICT
- TASS International
- Technical University of Berlin
- Telefonica
- TIS

- TURKCELL Teknoloji ARGE A.S.
- Universidad de Murcia
- Valeo Schalter und Sensoren GmbH
- VICOMTECH
- VTT, Finland
- 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

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. In 2020, Secan-Lab continued its active contribution to this project. In particular, we participated in dissemination activities through several keynotes and speeches at international conferences/events and lead the international cooperation activities. We contributed to the standardization activities by publishing an ETSI Group Report on “IPv6-based Vehicular Networking (V2X)”: ETSI GR IP6 030 V1.1.1 (2020-10).

Co-creating resIlient and susTaInable food systEms towardS FOOD2030

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

Acronym:	CITIES2030
PI:	Thomas ENGEL
Funding:	European Commission - Horizon 2020
Duration:	1 Oct 2020 – 30 Sep 2021
Member:	Thomas ENGEL (Principal Investigator)

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

In October 2020, the University of Luxembourg together with 40 other European partners have started working on the project CITIES2030 "Co-creating resilient and sustainable food towards FOOD2030". Funded by the European Union H2020 research programme for the period 2020-2024, CITIES2030 aims to implement sustainable cities and regions food systems. The main goal of CITIES2030 is to create future proof and effective urban food systems and ecosystems via a connected structure centred on the citizen and built on trust. CITIES2030 commits 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. The Secan-Lab will work on the security, privacy and blockchain for end to end tracing and tracking of the food supply chain. Additonally the Secan-Lab will participate in developing the relevant data-analytics system using the latest technologies.

Future Proofing the Connected World: A Quantum-Resistant Trusted Platform Module

Acronym:	FutureTPM
PI:	Peter Y A RYAN
Funding:	European Commission - Horizon 2020
Duration:	1 Jan 2018 – 31 Dec 2020
Member:	Peter Y A RYAN (Principal Investigator)

Description

The goal of FutureTPM is to design a Quantum-Resistant (QR) Trusted Platform Module (TPM) by designing and developing QR algorithms suitable for inclusion in a TPM. The algorithm design will be accompanied with implementation and performance evaluation, as well as formal security analysis in the full range of TPM environments: i.e. hardware, software and virtualization environments. Use cases in online banking, activity tracking and device management will provide environments and applications to validate the FutureTPM framework.

Results

FutureTPM is an EU H2020 project that was completed in December 31, 2020. The project focuses on the development of a quantum-resistant Trusted Platform Module (TPM). The main progress and contribution of the APSIA group is related to work packages (WP) 2 and 3. The objective of WP2 is to identify, or create new, quantum-resistant cryptographic primitives and protocols to be integrated in a TPM. A final list of recommendations for symmetric and asymmetric primitives and privacy-related protocols to be included in a TPM was reported in the end of 2020, where in the case of asymmetric primitives the selection was based on the third round of NIST's standardisation process. In the case of privacy-related protocols, the focus is on the Direct Anonymous Attestation (DAA) scheme, which is the most well-known functionality of a TPM providing remote attestation, and in particular the quantum-resistant version of the DAA is based on lattice primitives and assumptions (LDAA).

The main objective of WP3 is the security modelling of the TPM and the formal verification of its security properties. Due to the complexity of the TPM we have decided to model the core TPM functionalities instead of looking the TPM as a whole. In particular we have focused on the modelling of the remote attestation service, which is the most commonly used functionality in TPM-based applications. We demonstrate our models in the context of one of the envisioned FutureTPM use cases; namely the Device Management which is led by Huawei partner. The Device Management describes a network infrastructure in which the focus is on the secure identification and management of network devices. Our produced models are based on the "ideal functionalities" of TPM commands that have been defined through appropriate abstractions towards formally verifying the security properties of the executed protocols.

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 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.

B.4 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) • Briag Gerard Benjamin DUPONT (Collaborator)

Description

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

B.5 FNR Projects

Privacy Policy Creation, Certification and Translation

http://www.icomplai.eu

Acronym:	PaCT
PI:	Tomer LIBAL

Funding:	Fonds National de la Recherche
Duration:	1 May 2020 – 31 Oct 2020
Members:	• Tomer LIBAL (Principal Investigator) • Alexander STEEN (Researcher)

Description

Data protection is a bureaucratic but important process. We propose using an existing platform for automated legal reasoning in order to build GDPR-compliant editing, certification and translation tools for the benefit of website owners, auditors and regulators.

B.6 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.7 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.

Tailoring Automated Software Techniques for Real World and Large Scale Software Applications

Acronym:	TASTRA
PI:	Yves LE TRAON
Funding:	Fonds National de la Recherche - Aide à la Formation Recherche
Duration:	15 Jan 2016 – 14 Jan 2020
Member:	Yves LE TRAON (Principal Investigator)

Description

In recent years, there has been much research in the area of automated software testing, leading to the development of interesting testing techniques such as symbolic execution and mutation testing. These techniques are shown in academic research to be quite effective for finding defects in programs. Despite the undisputed potential of those techniques, the problems of their application cost, scalability, operation of software with environment interaction are obstacles to its practical use in real-world programs and environments. The main problems that require attention and hopefully will be resolved by the present project are the design of effective mutations and symbolic execution that will allow the techniques to scale and deal with environmental defects such as configuration errors, network protocols, file systems and concurrency. The present project will 1) Evaluate the level of test confidence or guarantee that should be provided by mutation testing, 2) Design a technique to effectively detect useful mutants, 3) leverage symbolic execution on program environment.

B.8 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.

B.9 FNR - AFR PhD and ILNAS Projects

ILNAS - UL/SnT Research Programme on Digital Trust in Smart ICT

https://smartict.gforge.uni.lu

Acronym:	Smart-ICT
Reference:	R-AGR-3239-10-Z
PI:	Pascal BOUVRY
Funding:	Fonds National de la Recherche - Aide à la Formation Recherche PhD, Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services

Budget:	1,742,000.00 €
Duration:	1 Jan 2017 – 31 Dec 2020
Members:	• Pascal BOUVRY (Principal Investigator) • Grégoire DANOY (Researcher) • Matthias R. BRUST (Post-Doc) • Saharnaz ESMAEILZADEH DILMAGHANI (PhD student) • Chao LIU (PhD student) • Nader SAMIR LABIB (PhD student)
Areas:	• Information Security • Intelligent and Adaptive Systems • Security, Reliability and Trust in Information Technology

Description

Following the successful launch of the University Certificate “Smart ICT for business innovation” in September 2015 and the creation of a new Master’s degree in partnership with the Institut luxembourgeois de la normalisation, de l’accréditation, de la sécurité et qualité des produits et services (ILNAS); the interdisciplinary center for security reliability and trust (SnT) and ILNAS entered a partnership to jointly develop Luxembourg as a European centre of excellence and innovation for secure, reliable, and trustworthy Smart ICT systems and services.

Research Pillars

With emphasis on digital trust for smart ICT and the related standardization efforts, the scientific research in the context of this joint program focuses on the three main pillars of, Big Data & Analytics, Internet-of-Things (IoT), Cloud Computing and has the following objectives:

- ”Smart ICT for business innovation” certificate. The joint research programme is of primary importance at national level, as it will serve to consolidate and sustain the ”Smart ICT for business innovation” certificate, while implementing the project of a new Master in Lifelong Learning in the field ”Smart ICT for Business Innovation”.
- Smart ICT and Standardization. Creating an innovative environment on digital trust for smart ICT and the related standardization efforts with its core pillars Big Data & Analytics, Internet-of-Things (IoT), Cloud Computing.
- Big Data & Analytics. One goal is standardization of annotated clinical data in the context of international biomedical research, with CDISC as an example. Secondly, efficiency and confidentiality of Big Data integration at an international level has to be achieved. Data exchange procedures and formats are needed to improve the efficiency of Big Data sharing and data integration.
- Internet-of-Things (IoT). Standardization in the field of drones is still recent with no final standard yet released. The objective is to investigate the use of UAV drones in the context of homogeneous and heterogeneous drone fleets. Ensuring the proper functioning of the fleet raises new problems of opti-

mization at the level of the communications based on the future dedicated protocols.

- Cloud Computing. The objective is to provide tools for analyzing and comparing prices offered by different Cloud providers. A thorough study of the different pricing methods of suppliers' services is therefore required. Cloud service pricing models will be developed to enable brokers to automatically be determining the best service selection strategy(s) according to customer criteria.

Results

Publications

- Distributed Pareto-based Path Planning Algorithm for Autonomous Unmanned Aerial Vehicles, 2021. 4th International Workshop on Multi-agent Path Finding (WoMAPF20) in conjunction with 29th International Joint Conferences on Artificial Intelligence (IJCAI) N. S. Labib, G. Danoy, M. R. Brust, P. Bouvry. [10993/46217]
- Trustworthiness in IoT - A Standards Gap Analysis on Security, Data Protection and Privacy, 2019. IEEE Conference on Standards for Communications and Networking (CSCN 2019) N. S. Labib, M. R. Brust, G. Danoy, P. Bouvry. [10993/46217]
- A Multilayer Low-Altitude Airspace Model for UAV Traffic Management. *9th ACM Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications (DIVANet '19), 2019.* N. S. Labib, G. Danoy, J. Musial, M. R. Brust, P. Bouvry. [10993/40536]
- Internet of Unmanned Aerial Vehicles—A Multilayer Low-Altitude Airspace Model for Distributed UAV Traffic Management. Sensors, 2019. N. S. Labib, G. Danoy, J. Musial, M. R. Brust, P. Bouvry. [10993/41481]
- White Paper: Data Protection and Privacy in Smart ICT - Scientific Research and Technical Standardization, 2018 [10993/37276]
- On Standardised UAV Localisation and Tracking Systems in Smart Cities - N. Labib, M.R. Brust, G. Danoy, P. Bouvry, Book of abstracts of the 17th Annual STS Conference (Graz), 2018 [10993/37265]
- A Standardized Broker Model in Smart Cities, C. Liu, S. Varrette, G. Danoy, M.R. Brust, P. Bouvry, Book of abstracts of the 17th Annual STS Conference (Graz), 2018 [10993/37479]
- Maya Olszewski, Jeff Meder, Emmanuel Kieffer, Raphaël Bleuse, Martin Rosalie, Grégoire Danoy, and Pascal Bouvry. Template of a Chaotic Attractor . Graph Drawing. 2018 [10993/37764]
- J. Mesit, M.R. Brust, P. Bouvry. Lightweight Key Agreement for Wireless Sensor Networks, IEEE QRS, 2018
- Raphaël Bleuse, Giorgio Lucarelli, and Denis Trystram. Data Movements by Anticipation: Position Paper . Euro-Par Workshops 2018 [10993/37830]
- A.M. Fiscarelli, M.R. Brust, G. Danoy, P. Bouvry, *A Memory-based Label Propagation Algorithm for Community Detection*, Int. C. on Complex Networks and Their Applications (COMPLEX NETWORKS), 2018 [10993/38402]
- C. Liu, P. Bouvry. Optimal Pricing for Socially-aware Usage of Cloud Services. International Conference on Optimization and Learning, OLA 2019

- Transforming Collaboration Data into Network Layers for Enhanced Analytics , S. Dilmaghani, A. Piyatumrong, P. Bouvry, M.R. Brust, International Conference on Optimization and Learning OLA 2019
- M. Rezazad, M.R. Brust, M. Akbari, P. Bouvry, N-M. Cheung*, Detecting Target-Area Link-Flooding DDoS Attacks using Traffic Analysis and Supervised Learning,* Future of Information and Communication Conference (FICC), 2018
- J. Chen, S. Hossain, M.R. Brust, N. Johnson, *A Game Theoretic Analysis of the Twitter Follow-Unfollow Mechanism,* Int. C. on Decision and Game Theory for Security (GameSec), 2018 [↗10993/38696]

Talks

- On 06.07.2018, Prof. Bouvry presented the SnT-ILNAS research and educational programme at the ETSI Workshop at the Technoport in Belval.
- On 09.07.2018, Dr. Brust delivered a talk entitled Toward an innovative and trustworthy ICT Ecosystem for the Smart City at the Int. Workshop on Urban Data Science (UDS 2018) (http://urban.se.rit.edu/2018/index.html) in Bangkok (Thailand).

B.10 FNR - CORE Projects

CONtext and conTent Aware CommunicaTions for QoS support in VANETs

Acronym:	CONTACT
Reference:	R-AGR-0643
PI:	Thomas ENGEL
Funding:	Fonds National de la Recherche - CORE
Budget:	1,346,000.00 €
Duration:	1 Apr 2016 – 31 Mar 2020
Members:	• Thomas ENGEL (Principal Investigator) • Anne OCHSENBEIN (Project Coordinator) • Stefanie OESTLUND (Project Coordinator) • Mathieu VIAU-COURVILLE (Project Coordinator) • Antonio DI MAIO (Doctoral Candidate) • Maria Rita PALATTELLA (Post-Doc) • Ridha SOUA (Post-Doc) • Ion TURCANU (Post-Doc)
Area:	Communicative Systems
Partners:	• CarPostalSwiss • HES-SO Valais • University of Bern

Description

Vehicular Ad hoc Networks (VANETs) have been receiving a lot of interest from academia, automotive industry, and government, as they hold the potential to enable a wide range of applications and services, improving both safety and comfort on the road.

One of the main drivers of vehicular communications is the support for safety applications (e.g. accident, traffic jam notifications), which together with the more recent autonomous and coordinated driving applications require low end-to-end delay and no packet loss. These applications will share the vehicular network resources with services with very different QoS requirements, such as infotainment services (e.g. live video streams, tourist information).

Due to the volatility of the vehicular environment, VANETs are characterized by a dynamic topology, short-lived intermittent wireless connectivity, and a cooperative and decentralized communication paradigm. All these features make the provision of high levels of QoS in VANETs a challenging task. Even more challenging is the support of a very diverse set of QoS requirements, due to the high heterogeneity of existing and prospective vehicular applications. The main existing approaches to QoS provisioning in VANETs either tackle this issue by focusing on a single layer of the network architecture, or focus on enabling a single specific QoS class of service. The CONTACT project aims at enabling Quality of Service (QoS) support in VANETs by taking a multi-pronged, cross-layer approach, by developing a set of communication techniques, which efficiently adapt, at the same time to the highly volatile and unstable vehicular environment, to content attributes and properties, and to application performance requirements. For this purpose, CONTACT will investigate the use of three different emerging approaches: Content-Centric Networking (CCN), Software Defined Networking (SDN), and Floating Content (FC). CCN implies introducing (content) name-based addressing instead of host-based addressing. This can be beneficial for communications in highly mobile network scenarios such as vehicular networks, where host addresses are not very meaningful. SDN, with its centralized view of network resources, may help in handling efficiently dynamic (re)allocation of resources/channels, and distribution of content (e.g., by reducing amount of Geobroadcast messages). Finally, FC techniques could be used to improve content availability for delay tolerant communications. The main idea behind CONTACT is to combine and exploit the advantages offered by CCN, SDN and FC, to offer a variety of QoS levels. The improvements in communication reliability, content availability, and end-to-end delay are pursued by adopting strategies based on the type of content (alerts, driving coordination, informational) as well as on its context attributes (such as location of origin, geographical range of interest, time of validity).

Results

CONTACT project has concluded on 31.03.2020. SECAN-Lab continued its active contribution to the project, focusing mainly on coordinating and preparing the final project report, which has been submitted and accepted by FNR. Overall, the CONTACT project advanced the state of the art by developing a set of communication techniques that are able to provide high levels of QoS in vehicular networks, despite the very challenging and unstable conditions of the wireless communication channels. We demonstrated the benefits of applying the SDN, NDN, and FC paradigms, both individually and as an integrated architecture, to enable QoS support in VANETs. We showed that the centralized architecture of SDN provides a global overview of the vehicular network, which, in turn, helps taking globally optimized decisions with respect to routing, anchor zone dimensioning, privacy preservation, content distribution, etc. We proved that NDN provides a flexible architecture that is best suited for highly dynamic networks, such as vehicular networks. We demonstrated how FC significantly improves content replication in low-density vehicular networks by identifying relevant areas where the content is needed and opportunistically replicating it inside this area. Finally, we showed how integrating these three technologies significantly improves communication reliability and QoS in vehicular networks.

The results of the project have been published in international conferences and scientific journals. Overall, the project consortium published a total of 28 conference/workshop papers, 7 journal articles, 1 poster, 1 demo, and 1 book chapter.

Finally, in 2020, Antonio Di Maio has successfully defended his Ph.D. thesis, which summarizes the results of his work within the CONTACT project.

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 (Post-Doc)
Area:	Communicative Systems
Partner:	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

Today's economy, and by this, citizens of the EU, depend on reliable network and information services. Despite a wide selection of technical protection measures being available, attacks on NIS 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 IT systems in central sectors of the economy are secure. The analysis of 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 be derived and developers can be equipped with guidelines on how to meet the legal requirements with the currently available technologies. However, technology and the law evolve at different speeds hence these interpretations and guidelines need to be dynamic.

As for the objectives of EnCaViBS in 2020, we identified the relevant implementation acts and are in the process of translation. These translations will be gradually published on the project's web portal: https://encavibs.uni.lu. Moreover, we are developing a maturity assessment methodology. Its first version will be online during the first half of 2021. Lastly, the questionnaire for the first round of Delphi interviews has been created and stakeholders have been identified. We have also contributed to the review process of the NIS Directive.

Privacy Enhancing Techniques for Future Internet

Acronym:	PETIT
Reference:	R-AGR-0665
PI:	Thomas ENGEL, Andriy PANCHENKO
Funding:	Fonds National de la Recherche - CORE
Budget:	654,000.00 €
Duration:	1 Sep 2016 – 31 Aug 2020
Members:	• Thomas ENGEL (Principal Investigator) • Andriy PANCHENKO (Principal Investigator) • Anne OCHSENBEIN (Project Coordinator) • Stefanie OESTLUND (Project Coordinator) • Mathieu VIAU-COURVILLE (Project Coordinator) • Augusto Wladimir DE LA CADENA RAMOS (Doctoral Candidate) • Marharyta ALEKSANDROVA (Post-Doc) • Daniel KAISER (Post-Doc) • Mohamed Nizar MSADEK (Post-Doc) • Stefan SCHIFFNER (Post-Doc)
Area:	Communicative Systems
Partner:	University College London

Description

Internet Technology invades almost all spheres of our everyday life. Due to emerging use cases such as online social networks, banking, buildings automation, smart metering, eHealth, and eGovernment, networks are increasingly used to transmit privacy-sensitive data. The volumes of transferred, processed, and stored data are continuously expanding. There is an ever-growing temptation to collect the information once revealed: storage becomes steadily cheaper, data mining increasingly better. As a consequence, privacy on the Internet is attracting more and more attention and has become a serious concern.

The goal of the proposal “Privacy-Enhancing Techniques for Future Internet” (PETIT) is to advance the state-of- the-art in the field of Privacy-Enhancing Techniques (PETs) in order to meet the challenges of the Future Internet and to create solid fundamentals for systems that empower users with tools for strengthening their privacy protection on the Internet. This will be done by analysing existing and developing new methods for privacy-friendly communication and by contributing to a broader understanding of the topic and its primitives within the community of researchers as well as the society. To this end, we will thoroughly analyze the susceptibility of existing PETs with respect to traffic analysis to make them robust against this kind of vulnerability. Afterwards, we will design and analyze methods for network discovery in untrustworthy environments in order to overcome scalability and trustworthiness issues in currently deployed systems. Moreover, we will address the topic of privacy-preserving routing by means of new communication paradigms for emerging protocols and performance-improved path selection metrics for better optimization of available resources and provision of an adequate quality of service.

Privacy-friendly communication is essential for exercising the right to freedom of expression, particularly in those countries that are filtering and censoring access to information. On the other hand, there should be a possibility for law enforcement to persecute criminals that misuse these techniques. Finally, we will address the contradictory issues of censorship resistance and law enforcement in order to harmonize them in future designs. This will help to increase the acceptance and integration of PETs into our daily life to give users the possibility to retain control over their personal data and to mitigate privacy threats and concerns.

Results

In September 2020, we successfully concluded the FNR core project "Privacy-Enhancing Techniques for Future Internet" (PETIT). The PETIT project advanced the state-of-the-art in the field of Privacy-Enhancing Techniques (PETs) meeting challenges of the Future Internet and creating solid fundamentals for systems that empower users with tools for strengthening their privacy protection on the Internet. We analysed existing and developed new methods for privacy-friendly communication and contributed to a broader understanding of the topic and its primitives within the community of researchers as well as the society.

The main focus of PETIT was both thoroughly analysing the susceptibility of existing PETs with respect to traffic analysis and making them robust against this kind of vulnerability. We made advances in the fields of website fingerprinting, network discovery in untrustworthy networks, Tor traffic splitting for performance and protection against traffic-analysis attacks, and privacy-preserving routing. Results were presented in top-ranked conferences including ACM CCS 2020 and IEEE NCA 2020 with a profound impact for other researchers.

PETIT allowed us to establish international research collaborations that are still ongoing and fruitful. The initial PI, Dr.-Ing. Andriy Panchenko, obtained a permanent position as a full professor at the Brandenburg University of Technology, Germany. For the PI, this was a final step of his successful transition from a junior to a senior researcher. Further, Wladimir De La Cadena obtained his PhD degree working on PETIT.

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.

Results

- The related proposal *Give control back to users: personalised privacy-preserving data aggregation from heterogeneous social graphs (HETERS)* was submitted to the 2020 CORE call. The proposal was graded as excellent, although not retained due to the lack of sufficient funds.
- Publications and conference presentations:

  1. X. Chen, S. Mauw, Y. Ramírez-Cruz. Publishing Community-Preserving Attributed Social Graphs with a Differential Privacy Guarantee. Proceedings on Privacy Enhancing Technologies 2020(4):131–152, 2020. Presented at PETS 2020, Montréal, Canada, July 2020 (online).
  2. X. Chen, E. Këpuska, S. Mauw, Y. Ramírez-Cruz. Active Re-identification Attacks on Periodically Released Dynamic Social Graphs. In Computer Security – ESORICS 2020, Lecture Notes in Computer Science 12309, pp. 185–205, 2020. Presented at ESORICS 2020, Surrey, UK, September 2020 (online).

- Submissions:

  1. S. Mauw, Y. Ramírez-Cruz, R. Trujillo-Rasua. Preventing active re-identification attacks on social graphs via sybil subgraph obfuscation. Submitted to Knowledge and Information Systems, under review.

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.

Results

The FNR CORE project Q-CoDe aims to explore whether quantum information processing can help to achieve the cryptographic property of deniability. In 2020, we continued our work on achieving participation-deniability for key-exchange protocols via designated verifier signatures. We also explored the possibility of achieving participation deniability via plaintext-aware encryption. In addition, we studied how plaintext-aware encryption against quantum adversaries can be defined and whether it is achievable.

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.

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
Member:	Peter Y A RYAN (Principal Investigator)

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

The FinCrypt team studied privacy issues of the Lightning Network (LN), which is a payment channel network that was introduced in 2018 to improve the scalability (and also privacy) of permissionless blockchains such as Bitcoin. In particular, the team investigated a privacy shortcoming of the LN, namely the balance probing attack, and evaluated its effects on the real network. It was found that an attacker can easily discover channel balances using probing, which takes under a minute per channel and requires moderate capital commitment and no expenditures (the attacker's funds are only temporarily locked). The team developed a proof-of-concept implementation of the attack for Bitcoin's testnet and came up with two proposals that allow LN to increase its privacy and efficiency, respectively. In a second line of research, the FinCrypt team studied the security of cryptographic accumulator schemes, which allow one to aggregate values of a possibly very large set into a short digest, commonly referred to as the accumulator value. More concretely, the team cryptanalyzed the two accumulator variants proposed by Au et al. at CT-RSA 2009, namely the α-based construction and the Reference String-based (RS-based) construction. For the former the team showed that the non-membership mechanism, designed to allow for more efficiency on the accumulator manager side, has a subtle cryptographic flaw, which enables an adversary to efficiently recover the secret of the accumulator manager, given just several hundred to few thousand non-membership witnesses (regardless of the number of accumulated elements). The second variant is also vulnerable since a group of users is able to compute valid witnesses for unauthorized elements even when the Accumulator manager keeps secret all the information needed to compute such witnesses, i.e. the reference string. Furthermore, the FinCrypt team proposed a Dynamic Universal Accumulator in the Accumulator Manager setting for bilinear groups, which extends previous work by Nguyen (CT-RSA 2005), Au et al. (CT-RSA 2009) and Damgaard and Triandopoulos (Eprint 2008). The new features include support for batch addition and deletion operations as well as a privacy-friendly decentralized batch witness update protocol, where the witness update information is the same for all users. Together with a non-interactive zero-knowledge protocol, these make the proposed scheme suitable as an efficient and scalable Anonymous Credential System, accessible even by low-resource users.

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.11 FNR - CORE - Core Junior Projects

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.

Results

SZK is a FNR CORE (junior track) project whose goal is the design of zero-knowledge proofs of knowledge protocols with state, i.e., where the prover is able to reuse efficiently statements that have already been proven. The project started on 01/03/2018. In 2020, the main focus has been on implementing the SZK protocols that we had designed previously, and also the privacy-preserving applications that use those protocols as a building block.

B.12 FNR - COVID-19 Fast Track Projects

Facilitating optimal containment and exit strategies with minimal disclosure access control and tracking

Acronym:	SmartExit
PI:	Peter Y A RYAN
Funding:	Fonds National de la Recherche - COVID-19 Fast Track
Duration:	1 May 2020 – 31 Oct 2020
Members:	• Peter Y A RYAN (Principal Investigator) • Wojciech JAMROGA (Researcher) • Peter Browne Roenne (Researcher) • David MESTEL (Research Associate) • Marjan SKROBOT (Research Associate)

Description

The SmartExit project's goal was to identify, specifically in the context of Luxembourg, effective strategies and technologies to help contain the Covid-19 outbreak. No less importantly, such strategies should limit the economic and social impact and facilitate an earlier return to normality. This involves firstly identifying the relevant functional and privacy requirements for such technologies, and secondly surveying and evaluating the numerous technologies being developed around the world against these requirements. Given the limited project time and resources, and the fact that already many competing technologies were emerging, it was not proposed to develop yet another approach. Rather, it was envisaged that we should suggest how to adapt a more promising approach to the Luxembourg context.

Information Diffusion in Twitter during the COVID-19 Pandemic: the Case of the Greater Region

Acronym:	PandemicGR
PI:	Jun PANG
Funding:	Fonds National de la Recherche - COVID-19 Fast Track
Duration:	15 May 2020 – 14 Nov 2020
Members:	• Jun PANG (Principal Investigator) • Ninghan CHEN (PhD student) • Zhiqiang ZHONG (PhD student)

Description

The PandemicGR project will address of the challenge of understanding and analysing the information diffusion mechanism in online social media during the COVID-19 pandemic, based on a newly collected and properly anonymised Twitter dataset concentrating on Luxembourg and the greater region. In this project, we aim to (1) achieve in-depth analysis of user engagement and communication patterns during this public health crisis, (2) build a machine learning model to simulate and predict COVID-19 information cascades, and (3) develop an effective classifier to detect misinformation in order to improve information trustworthiness in online social media. The results from the PandemicGR project will have both immediate and medium-term impact for crisis management for bother Luxembourg and the greater region.

Results

- A technical report titled “From #Jobsearch to #Mask: Improving COVID-19 cascade prediction with spillover effects” has published online at arXiv (CoRR abs/2012.07088, 2020).
- A technical report titled “An exploratory study of COVID-19 information on Twitter in the Greater Region” has published online at Big Data and Cognitive Computing (https://doi.org/10.3390/bdcc5010005 2021).

B.13 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.

Results

The project enters its 3rd year with advancements in simulation and analysis, as well as further research into the theoretical background of commercial vehicles tires and the proposed technology.

The Researcher initiated a complex modeling and analysis of the state of the art TPMS solution and its shortcomings using the Finite element method. In parallel, a FEM model of the proposed solution was built to compare against the state of the art. The highly detailed FEM Analysis presented several challenges and required close cooperation with the project's Industry partner Goodyear Tires. Resulting in highly accurate analysis of both systems and their application environment. Several test antennas have been built as part of the upcoming work package, with laboratory tests on the proposed solutions starting in 2021.

Publications are planned for 2021 including conference papers.

B.14 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.

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.

Results

The PhD student Marie-Laure Zollinger, who is funded by the SeVoTe project, successfully defended her thesis in September 2020 and got the excellent thesis award. Several papers were presented e.g. at Voting'20 and submitted in 2020.

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

The close collaboration with Norway and Australia continued in 2020 with a physical meeting in Luxembourg in March 2020 and a digital meeting in September 2020. Several papers in this project has been presented at international conferences in 2020.

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.

B.15 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)

Results

We have made significant progress in the development of verification algorithms and model reduction techniques for analysis of socio-technical systems. In particular, we identified some important problems with the existing semantics of strategic requirements in asynchronous multi-agent systems, and proposed how to deal with the problems. We also continued the development of partial-order reduction methods for model checking of such systems. Last but not least, we developed and implemented a new method of satisfiability checking for strategic properties.

On the more practical side, we have prepared a number of multi-agent models of existing voting protocols, including Pret-a-Voter, Selene, and the postal voting procedure used in the 2020 presidential election in Poland. We used the models to conduct preliminary experiments and identify what further developments are need to do scalable verification in realistic cases. Among other things, we combined this kind of modeling with the idea of natural strategies to propose a formalization of ”usable receipt-freeness” and ”usable voter-verifiability.”

B.16 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 development of SIMMS simulator, directly interfaced with SIMMS control application, has enabled numerous of realistic tests to fine-tuned the swarming model. The whole system received relevant improvements to be managed more efficiently. A new generation of professional drone joins the swarm with the acquisition of the DJI M300.

SIMMS continues to gain in visibility with the addition of a professional video explainer and with the participation to the HEC Liège Business Game. (http://simms.lu/).

B.17 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
Partner:	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

- Gabor Wiese taught the course "Number theory for cryptography" as a part of the DTU training program, granting 0.5 ECTS.
- The paper "NeuLP: An end-to-end deep-learning model for link prediction", co-authored by ZZ and JP, has been published in the proceedings of the 21st International Conference on Web Information System Engineering (WISE'20).

B.18 ONRG - NICOP Projects

Heterogeneous multi-swarms of UNmanned auTonomous systEms for mission Deployment

Acronym:	HUNTED
PI:	Pascal BOUVRY
Funding:	Office of Naval Research Global
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

Inter-swarm collaboration using evolutionary techniques (WP2): The mobility model ABISS (Attractor Based Inter-Swarm collaborationS) developed in the first year of the project has been published in the open access journal Sensors (MDPI - impact factor 3.031) [56]. In this article a new concept of attractors was introduced as a way to foster inter-swarm collaboration whenever a zone is unreachable for a type of UAS.

Bayesian optimization to select Rossler system parameters used in the Chaotic Ant Colony optimisation for Coverage mobility model (WP3): The work on the optimization of the Rossler system for CACOC using a surrogate-based optimization method relying on Bayesian optimization was published in March 2020 in the Journal of Computational Science (Elsevier - impact factor 2.502) [51].

Enhanced Intra-level coordination using cooperative evolutionary techniques (WP3): We have continued developing the inter-swarm coordination model based on the previously developed CACOC (Chaotic Ant Colony optimisation for Coverage) algorithm to manage the mobility for a swarm of Unmanned Aerial Vehicles (UAVs). Concretely, we have defined and optimised a set of parameters, and designed a Cooperative Coevolutionary Genetic Algorithm (CCGA) to optimise each UAV configuration independently. Results have been published in the 2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC 2020) [179].

Collaborative/Competitive Coevolutionary Optimization of a Predator-Prey model (WP3): Building up on the optimized parameters, we have proposed a Predator-Prey model to test our surveillance system in a more realistic scenario. To this end, we have defined an intelligent intruder (prey) model to avoid UAVs (predators). The UAVs' configuration has been optimised using a specifically designed cooperative coevolutionary genetic algorithm (CCGA). Results have been published in the International Conference in Optimization and Learning (OLA2020) [181].

In the next research work, we have additionally optimised the intruders model by performing competitive tournaments for training and testing our specimens. Our results (Table 3) have been published in the 10th IEEE Workshop Parallel / Distributed Combinatorics and Optimization (PDCO 2020) [180].

B.19 UL Projects

A Personalization Framework for Sentiment Categorization with Recurrent Neural Network

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

Acronym:	PERSEUS
PI:	Christoph SCHOMMER
Funding:	University of Luxembourg
Duration:	15 Jan 2016 – 15 Jan 2020
Members:	• Christoph SCHOMMER (Principal Investigator) • Siwen GUO (Doctoral Candidate) • Sviatlana HOEHN (Scientific Advisor)
Area:	Intelligent and Adaptive Systems
Partner:	DFKI

Description

In the research project PERSEUS, we aim at discovering individualities in expressing sentiments in text. To study the diversity between individuals and the consistency in each individual, we have build a personalized framework that takes user-related text from social platforms, such as Twitter and Facebook, and investigates and improves sentiment categorisation by applying Deep Learning techniques. This project researches beyond purely understanding the meaning of text, and focuses on integrating the preference and tendency of users to provide user-sensitive predictions. Aspects of sentiment analysis in chatbots are analysed.

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.

Future Directions in Symmetric Cryptography

Acronym:	FDISC
PI:	Alexei BIRYUKOV
Funding:	University of Luxembourg
Duration:	1 Oct 2017 – 31 Aug 2020
Members:	• Alexei BIRYUKOV (Principal Investigator) • Qingju WANG (Post-Doc)
Area:	Security, Reliability and Trust in Information Technology

Description

Symmetric cryptographic primitives (e.g. block ciphers, hash functions) form an indispensible part of modern security protocols, most notably TLS and IPSec, where they are used for bulk encryption and the verification of message integrity. The emergence of novel application domains for symmetric cryptosystems, such as the Internet of Things (IoT) or digital currencies, has introduced very specific requirements that were not anticipated in the past. FDISC explores new research directions for the design, analysis and implementation of symmetric primitives with the goal of facilitating their deployment in the aforementioned new application domains. The research carried out in the FDISC project consists of two Work Packages (WPs), each involving two tasks. The goal of the first WP is to design and implement a lightweight ARXbased block cipher with provable security guarantees against certain forms of both classical cryptanalysis and side-channel attacks. Thereafter, the second WP aims at designing a provably memory-hard Proof-of-Work (PoW) scheme for digital currencies and developing new approaches for client puzzles suitable for mobile devices.

Results

In 2020, the FDISC team further analyzed the links between the division property and the bias phenomenon of dynamic cube attacks. In addition, considering the best accuracy of the bit-based division property, the team introduced a variant of the three-subset bit-based division property without unknown subset, and proposed an efficient algorithm to recover the superpoly in which the secret keys are involved. The team achieved the best key recovery attacks on the stream cipher TRIVIUM and the authenticated encryption cipher Grain-128 AEAD (published at EUROCRYPT 2020). Another result of the FDISC project concerns the division property of SPN ciphers with a complex matrix as part of the linear layer. Previously, no methods were able to model the division property through complex matrices efficiently and accurately. The team proposed a new approach to solve this problem (published in ToSC) that improves integral distinguishers for several ciphers (e.g. the team re-produced 5-round key-dependent integral distinguishers proposed at CRYPTO 2016, which can not be obtained by any of the previous automatic methods). Furthermore, in a related line of research, the FDISC team formulated the division property by monomials instead of the original subsets, which makes the definition more clean and algebraic, and further simplifies the propagation rules of the division property. Due to these simplifications, it became possible to propose efficient algorithms for enhancing cube attacks based on the division property (published at ASIACRYPT 2020). In the context of Multi-Party Computation (MPC) friendly symmetric ciphers, the team contributed to the construction of the first full-round key recovery attack on MiMC over binary fields, which became possible thanks to a generalization of higher-order differential cryptanalysis (published at ASIACRYPT 2020). Finally, the FDISC team also co-designed a novel lightweight block cipher and a tweakable block cipher based on the ARXbox Alzette, which were both presented at CRYPTO 2020.

High Performance Computing @ UL

http://hpc.uni.lu/

Acronym:	UL HPC
PI:	Pascal BOUVRY, Sébastien VARRETTE
Funding:	University of Luxembourg
Duration:	1 Jul 2007 – 31 Dec 2020
Members:	• Pascal BOUVRY (Principal Investigator) • Sébastien VARRETTE (Principal Investigator) • Frederic PINEL (Researcher) • Emmanuel KIEFFER (Post-Doc) • Hyacinthe CARTIAUX (Technical support) • Valentin PLUGARU (Research and Development Specialist)

Description

With the advent of the technological revolution and the digital transformation that made all scientific disciplines becoming computational nowadays, High Performance Computing (HPC) is increasingly identified as a strategic asset and enabler to accelerate the research performed in all areas requiring intensive computing and large-scale Big Data analytic capabilities.

Therefore since 2007, the University of Luxembourg (UL) has invested tens of millions of euro into its own HPC facilities to responds to the growing needs for increased computing and storage. This enabled its researchers to go beyond the limits of traditional simulation. Furthermore, special focus was laid on the development of large computing power combined with huge data storage capacity to accelerate the research performed in intensive computing and large-scale data analytic (Big Data). This characteristic distinguishes the HPC center at the university from many other HPC facilities, which often concentrate on only one of these two pillars. This makes the UL HPC facility the reference implementation within the country, offering a cutting-edge research infrastructure to Luxembourg public research while serving as edge access to the upcoming Euro-HPC Luxembourg supercomputer.

Nowadays, people from the three faculties and the three Interdisciplinary centres within the UL, are users of this facility. 2019 has seen also the first HPC service contracts signed with industrial partners (Arcelor-Mittal, Ceratizit etc.) and more generally, the University extends access to its HPC resources (i.e., facility and expert HPC consultants) to scientific staff of national public organizations and external partners.

The HPC facility is managed by an expert team under the responsibility of Prof. Pascal Bouvry (Head) and Dr. Sebastien Varrette (Deputy Head), PC for research. The UL HPC platform has kept growing over time thanks to the continuous efforts of the core HPC team (Dr. S. Varrette, V. Plugaru, S. Peter, H. Cartiaux, C. Parisot, Dr. F. Pinel, Dr. E. Kieffer and E. Krishnasamy - contact: hpc-team@uni.lu). Installed in the premises of the University's Centre de Calcul (CDC), it provides in 2019 a total computing capacity of 1,26 PetaFlops (1 PetaFlops = 10^{15} floating point operations per second) across several clusters of compute nodes, and around 10 PetaByte of shared data storage. A total of 756 servers are operated by the team to pilot the HPC platform and the other deployed services for research such as Gforge and GitLab used by hundreds of researchers. This places the HPC center of the University of Luxembourg as one of the major actors in HPC and Big Data for the Greater Region Saar-Lor-Lux. It also consolidates the University's ambition to offer a cutting-edge research infrastructure to Luxembourg public research while serving as edge access to the upcoming Luxembourg MeluXina supercomputer in the EuroHPC context.

From its reputation and national expertise in the HPC and Big Data domains, the University of Luxembourg through its Delegate (Prof. Pascal Bouvry) and Advisor (Dr. Sebastien Varrette), has been chosen by the ministry to represent the country within PRACE (Partnership for Advanced Computing in Europe). The UL is also member of ETP4HPC - European Technology Platform (ETP) in the area of High-Performance Computing (HPC) and involved to support the EuroHPC development in the country, in particular with regards the upcoming Luxembourg MeluXina supercomputer or the implementation of the HPC Competence Center, both scheduled for 2020.

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.20 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.21 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.22 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)

Results

The goal of the collaboration is to implement a tool for CAN Bus reverse engineering based on Machine Learning techniques. CAN Bus is the standard network to connect all electronic sensors within a vehicle. This network not does not offer encryption but, nonetheless, the data format is encoded according to the specific needs of the manufacturer of the vehicle. The goal of this work is to deanonymize this data by adopting data-driven heuristics and employing Machine Learning models.

A first one-year contract was signed with the company in October 2019 and it was renovated in October 2020 (till October 2021).

The collaboration has so far led to two papers, one already published at the IEEE Connected and Automated Vehicles Symposium in 2020.

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.

Networked SCADA Security

Reference:	R-AGR-0435
PI:	Thomas ENGEL
Funding:	External Organisation Funding
Budget:	841,679.00 €
Duration:	1 May 2012 – 30 Jun 2020
Members:	• Thomas ENGEL (Principal Investigator) • Anne OCHSENBEIN (Project Coordinator) • Stefanie OESTLUND (Project Coordinator) • Mathieu VIAU-COURVILLE (Project Coordinator) • Giulia RINALDI (Research assistant) • Florian ADAMSKY (Post-Doc) • Raimondas SASNAUSKAS (Post-Doc) • Ridha SOUA (Post-Doc) • Emilia TANTAR (Post-Doc)
Area:	Communicative Systems
Partner:	CREOS

Description

Researchers from the SECAN-Lab group headed by Prof. Dr. Thomas Engel continue their efforts to make industry control systems more secure and resilient against wide range of networks attacks. Together with the Luxembourg utility company Creos, they search for weaknesses within contemporary SCADA deployments using emulation — a method to analyze real-world systems with a high level of details. To this end, the SCADA team researches methods to stay safe and robust in the presence of network attacks.

Security Analysis Ethernet Testbed

Acronym:	SAET
PI:	Thomas ENGEL
Funding:	External Organisation Funding
Duration:	1 Jan 2020 – 31 Mar 2020
Member:	Thomas ENGEL (Principal Investigator)
Partner:	Honda r&d Europe GmbH

Results

Ethernet has become an attractive candidate technology to extend the capabilities of the next-generation automotive networks. An important part of making Ethernet a promising option for automotive networks is the work done in the IEEE TSN working group. While Ethernet typically just offers a best-effort service, TSN allows deterministic services over Ethernet, which includes guaranteed packet transport with bounded latency, low packet delay variation (jitter), and low packet loss.

However, security aspects, which are also an integral part of making Ethernet succeed as automotive technology, have been neglected so far. While the IEEE specified promising security technologies such as 802.1X (access control) and 802.1AE (MACsec, media access control security), there is no standard combining security technologies with TSN.

In this project, we motivated the need for further research in the field of combining TSN with security technologies by demonstrating several powerful yet easy-to-perform attacks against an unsecured TSN testbed. The results of our attack experiments show that further research in this field is of paramount importance because current technologies like CAN will not be able to cope with future in-car bandwidth needs and, while time-sensitive Ethernet would be a most suitable successor, it first has to be made secure. The results of this project were used in our successful FNR BRIDGES application, which allows us to address TSN security integration in collaboration with Honda Research starting in June 2021.

Appendix C

Representational Activities

C.1 Conference Committee Memberships

10th IEEE Workshop Parallel / Distributed Combinatorics and Optimization (PDCO 2020)

Location: New Orleans, United States of America, 18 May 2020 – 22 May 2020.

Participating Members:

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

10th Workshop on Logical Aspects of Multi-Agent Systems LAMAS 2020

Location: Auckland (virtual), New Zealand, 10 May 2020.

Participating Members:

- Wojciech JAMROGA (Program Committee Member)

11th International Conference on Ambient Systems

http://cs-conferences.acadiau.ca/ant-20/

Location: Warsaw, Poland, 6 Apr 2020 – 9 Apr 2020.

Description: 11th International Conference on Ambient Systems, Networks and Technologies (ANT 2020)

Participating Members:

- Ion TURCANU (PC Member)

12th International Conference on Quality of Multimedia Experience (QoMEX 2020)

Location: Athlone (virtual), Ireland, 26 May 2020 – 28 May 2020.

Participating Members:

- Jean BOTEV (Program Committee Member)

12th International Workshop on Immersive Mixed and Virtual Environment Systems (MMVE 2020)

Location: Istanbul (virtual), Turkey, 8 Jun 2020 – 11 Jun 2020.

Participating Members:

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

13th International Conference on Security for Information Technology and Communications (SECITC 2020)

https://sites.google.com/view/secitc/

Location: Bucharest, Romania, 19 Nov 2020 – 20 Nov 2020.

Participating Members:

- Johann GROSZSCHÄDL (Program Committee Member)

15th International Conference on Deontic Logic and Normative Systems (DEON 2020/2021) [Proceedings Only]

Location: (Virtual), Germany, 1 Jan 2020.

Participating Members:

- Réka MARKOVICH (Program Committee Member)
- Leon VAN DER TORRE (Program Committee Member)

16th IEEE International Workshop on Factory Communication Systems (WFCS'2020)

https://www.cister-labs.pt/wfcs2020/

Location: Porto, Portugal, 27 Apr 2020 – 29 Apr 2020.

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 Conference of Principles of Knowledge Representation (KR2020)

Location: Rhodes (Virtual), Greece, 12 Sep 2020 – 18 Sep 2020.

Participating Members:

- Emil WEYDERT (Program Committee Member)

18th International Conference on Practical Applications of Agents and Multi-Agent Systems (PAAMS 2020)

Location: Virtual, Italy, 6 Oct 2020.

Participating Members:

- Amro NAJJAR (Program Committee Member)

18th International Workshop on Nonmonotonic Reasoning (NMR 2020)

Location: Rhodes (Virtual), Greece, 12 Sep 2020 – 14 Sep 2020.

Participating Members:

- Emil WEYDERT (Program Committee Member)

18th Mediterranean Communication and Computer Networking Conference

https://2020.medcomnet.org/

Location: Arona, Italy, 17 Jun 2020 – 19 Jun 2020.

Description: MedComNet 2020 continues the tradition of the MedHocNet conference series that started in Sardinia in 2006 and was held annually in beautiful locations on the shores of the Mediterranean. This year for the first time the conference will take place on the shores of a lake, in the birth place of Mario Gerla, who was the initiator of this conference series.

MedComNet is a forum for the presentation of new research results in the broad area of wired and wireless communication and computer networking. All aspects of the networking research area will be welcome.

Participating Members:

- Ion TURCANU (PC Member)

19th IEEE International Symposium on Mixed and Augmented Reality (ISMAR 2020)

Location: Recife / Porto de Galinhas (virtual), Brazil, 9 Nov 2020 – 13 Nov 2020.

Participating Members:

- Jean BOTEV (Unknown)

19th International Joint Conference on Autonomous Agents and Multi-Agent Systems AAMAS 2020

Location: Auckland (virtual), New Zealand, 9 May 2020 – 13 May 2020.

Participating Members:

- Amro NAJJAR (Program Committee Member)
- Alexander STEEN (Program Committee Member, Workshop Organiser / Co-Organiser)
- Wojciech JAMROGA (Program Committee member of the Blue Sky Ideas Track)

19th International Semantic Web Conference (ISWC 2019)

Location: Athens (virtual), Greece, 1 Nov 2020 – 6 Nov 2020.

Participating Members:

- Christian GREVISSE (Paper presentation)

19th Workshop on Privacy in the Electronic Society (WPES)

Location: Online, United Kingdom, 9 Nov 2020.

Participating Members:

- Alfredo RIAL (Program Committee Member)

1st IEEE International Conference on Autonomic Computing and Self-Organizing Systems (ACSOS 2020)

Location: Washington, DC (virtual), United States of America, 17 Aug 2020 – 21 Aug 2020.

Participating Members:

- Jean BOTEV (Steering Committee Member, Program Committee Member)
- Ningyuan SUN (Unknown)

1st Workshop on Secure Cryptographic Implementation (SCI 2020)

https://sci.ittc.ku.edu/2020/index.html

Location: Rome, Italy, 21 Oct 2020.

Participating Members:

- Johann GROSZSCHÄDL (Program Committee Member)

2020 Americas Conference on Information Systems

https://amcis2020.aisconferences.org/

Location: (virtual), United States of America, 10 Aug 2020 – 14 Aug 2020.

Participating Members:

- Qin MA (Reviewer)

23rd Annual International Conference on Information Security and Cryptology (ICISC 2020)

http://www.icisc.org/static/pastconferences

Location: Seoul, South Korea, 2 Dec 2020 – 4 Dec 2020.

Participating Members:

- Johann GROSZSCHÄDL (Program Committee Member)

23rd International Conference on the Applications of Evolutionary Computation (EvoApps 2020)

Location: Seville, Spain, 15 Apr 2020 – 17 Apr 2020.

Participating Members:

- Grégoire DANOY (Program Committee Member)

24th European Conference on Artificial Intelligence ECAI 2020

Location: Santiago de Compostela (virtual), Spain, 8 Jun 2020 – 12 Jun 2020.

Participating Members:

- Wojciech JAMROGA (Senior Program Committee member)
- Amro NAJJAR (Reviewer)

24th International Conference on Financial Cryptography and Data Security (FC 2020)

https://fc20.ifca.ai

Location: Kota Kinabalu, Malaysia, 10 Feb 2020 – 14 Feb 2020.

Participating Members:

- Alexei BIRYUKOV (Program Committee Member)

25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA'2020)

http://www.etfa2020.org/

Location: Vienna, Austria, 8 Sep 2020 – 11 Sep 2020.

Description: ETFA focuses on the latest developments and new technologies in the field of industrial and factory automation. The conference aims to 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 (Technical Program Committee Member)

27th International Symposium on Temporal Representation and Reasoning (TIME 2020)

https://drops.dagstuhl.de/opus/volltexte/2020/12967/pdf/lipics-vol178-time2020-complete.pdf

Location: Bozen, Italy, 22 Sep 2020 – 25 Sep 2020.

Description: The 27th International Symposium on Temporal Representation and Reasoning (TIME 2020) was planned to be in Bozen-Bolzano, Italy, from the 23rd to the 24th of September, 2020. However, due to the special circumstances related to COVID-19, the conference was held virtually. This year's edition was organized as a part of the Bolzano Summer of Knowledge (BOSK 2020). TIME is a well-established symposium series that brings together researchers interested in reasoning about temporal aspects of information in all areas of computer science. The symposium aims to be interdisciplinary and to attract attendees from artificial intelligence, database management, logic and verification, and beyond.

Participating Members:

- Martin THEOBALD (Co-Chair)

27th International Workshop on Fast Software Encryption (FSE 2020)

https://fse.iacr.org/2020/

Location: Athens, Greece, 9 Nov 2020 – 13 Nov 2020.

Participating Members:

- Qingju WANG (Program Committee Member)

28th International Conference on Real-Time and Network Systems (RTNS'2020)

https://rtns2020.inria.fr/

Location: Paris, France, 8 Jun 2020 – 10 Jun 2020.

Description: RTNS is a friendly and inclusive conference with a great sense of community that presents excellent opportunities for collaboration. Original unpublished papers on all aspects of real-time systems and networks are welcome. 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 (RTOS), 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/subscriber 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)

32nd IEEE International Conference on Software Engineering Education & Training (CSEE&T 2020)

https://ase.in.tum.de/cseet2020/

Location: Munich, Germany, 9 Nov 2020 – 12 Nov 2020.

Participating Members:

- Benoit RIES (Program Committee Member)

33rd International Conference on Legal Knowledge and Information Systems (JURIX 2020)

Location: Prague (Virtual), Czechia, 9 Dec 2020 – 11 Dec 2020.

Participating Members:

- Réka MARKOVICH (Program Committee Member)

34th Conference on Artificial Intelligence AAAI-20

Location: New York, United States of America, 7 Feb 2020 – 12 Feb 2020.

Participating Members:

- Wojciech JAMROGA (Program Committee Member)

35th International Conference on Information Security and Privacy Protection IFIP SEC 2020

Location: Maribor (virtual), Slovenia, 26 May 2020 – 28 May 2020.

Participating Members:

- Wojciech JAMROGA (Program Committee Member)

3rd AAAI/ACM Conference on AI Ethics and Society

Location: New York, United States of America, 7 Feb 2020 – 8 Feb 2020.

Participating Members:

- Amro NAJJAR (Sub-reviewer)

3rd International Conference on Applied Informatics (ICAI 2020)

Location: Ota (virtual), Nigeria, 29 Oct 2020 – 31 Oct 2020.

Participating Members:

- Christian GREVISSE (Steering Committee Member, Program Committee Member)

4th International Workshop on Cryptocurrencies and Blockchain Technology (CBT 2020)

https://deic-web.uab.cat/cbt/cbt2020/

Location: Surrey, United Kingdom, 17 Sep 2020 – 18 Sep 2020.

Participating Members:

- Alexei BIRYUKOV (Program Committee Member)

5th Asian Workshop on Philosophical Logic (AWPL 2020)

Location: Hangzhou (Virtual), China, 26 Oct 2020 – 2 Nov 2020.

Participating Members:

- Emil WEYDERT (Program Committee Member)

5th International Conference on Cloud Computing and Artificial Intelligence: Technologies and Applications (CloudTEch 2020)

Location: Marrakesh, Morocco, 28 May 2020 – 30 May 2020.

Participating Members:

- Grégoire DANOY (PC Member)

5th Workshop on Advances in Secure Electronic Voting

Location: Kota Kinabalu, Malaysia, 14 Feb 2020.

Participating Members:

- Peter ROENNE (Co-Chair)

6th Global Conference on Artificial Intelligence (GCAI 2020)

http://www.gcai-2020.info/

Location: Zhejiang, China, 6 Apr 2020 – 9 Apr 2020.

Description: The 6th Global Conference on Artificial Intelligence (GCAI 2020) is part of the International Conferences on Logic and Artificial Intelligence at Zhejiang University (ZJULogAI). With its special focus theme on “Explainable AI and Responsible AIO´, the summit intends to promote the interplay between logical approaches and machine learning based approaches in order to make AI more transparent, responsible and accountable.

Participating Members:

- Grégoire DANOY (Program Committee Co-Chair)
- Jun PANG (Program Committee Co-Chair)

6th International Conference on Mathematics & Computing (ICMC 2020)

Location: Gangtok, India, 23 Sep 2020 – 25 Sep 2020.

Participating Members:

- Alfredo RIAL (Program Committee Member)

6th Workshop on ”Critical Automotive applications: Robustness & Safety” (CARS)

Location: Munich, Germany, 7 Sep 2020 – 10 Sep 2020.

Description: The CARS workshop is a forum focusing on architecture, methods and development techniques for safety-related automotive embedded systems and applications. The 6th edition of CARS is collocated with EDCC 2020.

Participating Members:

- Nicolas NAVET (Program Committee Member)

7th International Workshop on Self-Improving System Integration (SISSY 2020)

Location: Washington, DC (virtual), United States of America, 21 Aug 2020.

Participating Members:

- Jean BOTEV (Program Committee Member)

7th Workshop on Practical Aspects of Automated Reasoning PAAR2020

Location: Paris (virtual), France, 29 Jun 2020 – 30 Jun 2020.

Participating Members:

- Tomer LIBAL (Program Committee Member)
- Alexander STEEN (Program Committee Member)

8th International Conference on Computational Models of Argument (COMMA 2020)

Location: Perugia (Virtual), Italy, 8 Sep 2020 – 11 Sep 2020.

Participating Members:

- Emil WEYDERT (Program Committee Member)

AI4Health Lecture Series 2020

https://acc.uni.lu/ai4health/

Location: Luxembourg, Luxembourg, 1 Jan 2020 – 31 Dec 2020.

Description: University of Luxembourg organises lectures to exchange about Artificial Intelligence in the biomedical sector. These lectures are organised by Prof. Christoph Schommer and Dr. Jun Pang from the Department of Computer Science and by Prof. Thomas Sauter and Prof. Daniel Abankwa from the Department of Life Sciences and Medicine at the University of Luxembourg

Participating Members:

- Jun PANG (Workshop Organiser / Co-Organiser)

Anti-Covid: Informatics in Mitigation of Covid-19

Location: Online, Poland, 22 Jun 2020 – 23 Jun 2020.

Description: Keynote talk: Facilitating optimal containment and exit strategies with minimal disclosure access control and tracking.

Participating Members:

- Wojciech JAMROGA (Keynote speaker)

APF 2020

https://www.enisa.europa.eu/events/annual-privacy-forum-2020

Location: Athens, Greece, 17 Jun 2020 – 18 Jun 2020.

Description: The value of personal data in the online world has significantly increased over the last years as electronic products, services and processes have permeated every fold of everyday life. Limitations in the transparency, the functionality and interconnectivity of online and communication services increases the risk of having personal data processed out of control of any accountable person or organization or simply becoming exposed to all sorts of privacy threats.

The EU legal framework on personal data protection is key in an effort to better control the processing of personal data while ensuring an adequate level of protection. Even the best legislative efforts cannot keep up to speed with the pace of innovative technology and business models that challenge the way personal data is processed and privacy is protected across the EU and beyond; therefore, examining what is at stake and where threats thereto originate from becomes of paramount importance.

Against this background, ENISA, DG CONNECT and the Católica University of Portugal, Lisbon school of Law are organizing the Annual Privacy Forum (APF) 2020

Due to the COVID-19 situation, this years’ edition of APF will take place as a **webinar on 22nd and 23rd of October 2020**.

Participating Members:

- Stefan SCHIFFNER (PC Member)

Dutch-Belgian Database Day

https://soft.vub.ac.be/DBDBD2020/

Location: Brussels, Belgium, 11 Dec 2020.

Description: The Dutch-Belgian DataBase Day (DBDBD) is a yearly one-day workshop, organized in a Belgian or Dutch university, whose general topic is database research. DBDBD 2020 will be held online. Due to the cooperation between SIKS and the local organisation of DBDBD, registration for SIKS-members is free.

Participating Members:

- Vinu ELLAMPALLIL VENUGOPAL (Invited Speaker (Workshops))
- Martin THEOBALD (Attendant)

E-Vote-ID 2020

Location: Online, Austria, 6 Oct 2020 – 9 Oct 2020.

Participating Members:

- Johannes MUELLER (Program Committee Member)
- Peter ROENNE (Program Committee Member, Chair of Demos and communication)

EXTRAAMAS2020

Location: Auckland, New Zealand, 9 May 2020 – 13 May 2020.

Description: Human decisions are increasingly relying on Artificial Intelligence (AI) techniques implementing autonomous decision making and distributed problem-solving. However, reasoning and dynamics powering such systems are becoming increasingly opaque. This has raised ethical concerns related to the lack of transparency and the need for explainability. As a consequence, new legal constraints have been defined to enforce transparency and explainability in IT systems. Emphasizing the need for transparency in AI systems, recent studies pointed out that equipping intelligent systems with explanation abilities has a positive impact on users, (e.g., contributing to overcome discomfort, confusion, and self-deception due to the lack of understanding). Being able to comprehend AI systems, would produce a better mapping “expectation - understanding”, thereby increasing their trust in decisions and behaviors displayed by AI systems. On the contrary, the absence of explanation may lead the users to construct erroneous ToM of the users which causes confusion, misunderstanding, and uneasy collaboration.

For all these reasons, Explainable Artificial Intelligence (XAI) has recently re-emerged and is considered to be a crucial topic in AI, attracting research from domains such as machine learning, robot planning, and multi-agent systems.

Agents and Multi-Agent Systems (MAS) can have two core contributions for XAI. The first is in the context of personal intelligent systems providing tailored and personalized feedback (e.g., recommendations and coaching systems). Autonomous agent and multi-agent approaches have recently gained noticeable results and scientific relevance in different research domains (e.g., e-health, UAVs, smart environments). However, despite possibly being correct, the outcomes of such agent-based systems, as well as their impact and effect on users, can be negatively affected by the lack of clarity and explainability of their dynamics and rationality. Nevertheless, if explainable, their understanding, reliability, and acceptance can be enhanced. In particular, user personal features (e.g., user context, expertise, age, and cognitive abilities), which are already used to compute the outcome, can be employed in the explanation process providing a user-tailored solution.

The second axis is agent/robot teams or mixed human-agent teams. In this context, succeeding in collaboration necessitates a mutual understanding of the status of other agents/users/ their capacities and limitations. This ensures efficient teamwork and avoids potential dangers caused by misunderstandings. In such a scenario, explainability goes beyond single human-agent settings into agent-agent or even mixed agent-human team explainability.

Based on the evidence highlighted in the first edition of EXTRAAMAS, new objectives and domains demand attention. For example, there is an emerging need to address the synergy between XAI and ethics, pivoting on explorable cognitive agents (e.g., BDI agents).

Therefore, the purpose of this second "International workshop on Explainable Intelligence in Autonomous Agent and Multi-Agent Systems" (EXTRAAMAS) is seven-fold:

- to strengthen the common ground among the explainable agents and robots communities,
- to explore the ethical implication among XAI and non-XAI systems and within XAI itself,
- to investigate the potential of agent-based systems in personalized user-aware XAI, – to explore the generation of symbolic knowledge from subsymbolic representations
- to assess the impact of transparent and explained solutions on the user/agent behaviors,
- to discuss and motivate concrete applications and contributions overcoming the lack of explainability, and
- to assess and discuss the first solutions paving the way for the next generation systems.

Participating Members:

- Amro NAJJAR (Co-Chair)
- Jérémie DAUPHIN (Program Committee Member)
- Leon VAN DER TORRE (International Advisory Committee)

FISEE 2020 - Second international workshop on frontiers in software engineering education

Location: Villebrumier, France, 7 Dec 2020 – 9 Dec 2020.

Participating Members:

- Nicolas GUELFI (Programme Chair, Organizing Chair)

IEEE 3rd 5G World Forum (5GWF'20)

https://ieee-wf-5g.org/

Location: Bangalore, India, 10 Sep 2020 – 12 Sep 2020.

Description: The 2020 IEEE 3^{rd} 5G World Forum (5GWF'20) aims to bring experts from industry, academia and research to exchange their vision as well as their achieved advances towards 5G and encourage innovative cross-domain studies, research, early deployment and large-scale pilot showcases that address the challenges of 5G.

The 2020 IEEE 3^{rd} 5G World Forum (5GWF'20) in Bangalore, India, seeks contributions on how to nurture and cultivate 5G technologies and applications for the benefit of society. 5G systems should unveil a novel mobile network architecture that not only improves physical data rate, but also creates a new ecosystem allowing the deployment of novel services and applications. A key target is to build a novel network architecture that should support not only classical mobile broadband applications and services but also vertical industry (e.g. Intelligent Transport, Industrial IoT, eHealth, etc.) and other 5G-based services.

Participating Members:

- Abdelwahab BOUALOUACHE (Technical Program Committee Member)

IEEE 91st Vehicular Technology Conference

https://events.vtsociety.org/vtc2020-spring/

Location: Victoria, Canada, 4 Oct 2020 – 7 Oct 2020.

Participating Members:

- Ridha SOUA (Technical Program Committee Member)
- Abdelwahab BOUALOUACHE (Paper presentation)

IEEE CLOUDCOM 2019

http://2019.cloudcom.org/

Location: Sydney, Australia, 11 Dec 2019 – 13 Jan 2020.

Description: CloudCom is the premier conference on Cloud Computing worldwide, attracting researchers, developers, users, students and practitioners from the fields of big data, systems architecture, services research, virtualization, security and privacy, high performance computing, always with an emphasis on how to build cloud computing platforms with real impact. The conference is co-sponsored by the Institute of Electrical and Electronics Engineers (IEEE), is steered by the Cloud Computing Association, and draws on the excellence of its world-class Program Committee and its participants.

The 11th IEEE International Conference on Cloud Computing Technology and Science (CloudCom 2019) will be held in Sydney, Australia on 11-13 December 2019.

Participating Members:

- Valentin PLUGARU (Program Committee Member)

IEEE COMNETSAT 2020

https://ieeexplore.ieee.org/xpl/conhome/9328779/proceeding

Location: Batam, Indonesia, 17 Dec 2020 – 18 Dec 2020.

Participating Members:

- Abdelwahab BOUALOUACHE (PC Member)

IEEE Congress on Evolutionary Computation (CEC 2020)

Location: Glasgow, United Kingdom, 19 Jul 2020 – 24 Jul 2020.

Participating Members:

- Grégoire DANOY (Program Committee Member)

IEEE Consumer Communications & Networking Conference (CCNC)

https://ccnc2020.ieee-ccnc.org/

Location: Las Vegas, United States of America, 10 Jan 2020 – 13 Jan 2020.

Description: EEE Consumer Communications and Networking Conference, sponsored by IEEE Communications Society, is a major annual international conference organized with the objective of bringing together researchers, developers, and practitioners from academia and industry working in all areas of consumer communications and networking.

IEEE CCNC was organized specifically to help the consumer electronics industry drive the advancement of the numerous wireless and wireline communications technologies that will one day provide on-demand access to both entertainment and information anytime, anywhere, regardless of time or location. This includes a detailed analysis of nearly every technological area ranging from cognitive and peer-to-peer networking to the designer services and tools used to ensure ease-of-use, security and stunning interactivity.

IEEE CCNC 2020 will present the latest developments and technical solutions in the areas of home networking, consumer networking, enabling technologies (such as middleware) and novel applications and services. The conference will include a peer-reviewed program of technical sessions, special sessions, business application sessions, tutorials, and demonstration sessions.

Participating Members:

- Ion TURCANU (Technical Program Committee Member)

IEEE Global Communications Conference (IEEE GLOBECOM) 2020

https://globecom2020.ieee-globecom.org/

Location: Taipei, Taiwan, 7 Dec 2020 – 11 Dec 2020.

Description: IEEE GLOBECOM 2020 was held as a hybrid conference allowing registrants the choice to participate virtually or in-person in Taipei. The entire program was available on the virtual platform on 7-11 December 2020, while the presentations and exhibitions that could be made in-person was also taken place at the Taipei International Convention Center (TICC) on 8-10 December 2020

Participating Members:

- Abdelwahab BOUALOUACHE (PC Member)

IEEE International Conference on Communications

https://icc2020.ieee-icc.org/

Location: Dublin, Ireland, 7 Jun 2020 – 11 Jun 2020.

Participating Members:

- Abdelwahab BOUALOUACHE (Technical Program Committee Member)
- Ridha SOUA (Technical Program Committee Member)
- Abdelwahab BOUALOUACHE (Paper presentation)

IFIP Summer school on Privacy and Identity Management

https://ifip-summerschool.org/

Location: Maribor, Slovenia, 20 Sep 2020 – 23 Sep 2020.

Description: The 15th IFIP Summer School on Privacy and Identity Management is seeking papers for the conference, which will now be co-located with IFIP SEC from September 20-23, 2020, in Maribor, Slovenia.

A joint activity of IFIP Working Groups 9.2, 9.6/11.7, 11.6 and Special Interest Group 9.2.2, the Summer School will be held as a virtual event if a physical conference is not feasible.

The IFIP Summer School takes a holistic approach to society and technology, and supports interdisciplinary exchange through keynote and plenary lectures, tutorials, workshops, and research paper presentations. In particular, the conference welcomes contributions that combine technical, legal, regulatory, socio-economic, social or societal, political, ethical, anthropological, philosophical or psychological perspectives. The interdisciplinary character of the work is fundamental to the School.

The research paper presentations and the workshops have a particular focus on involving students, and on encouraging the publication of high-quality, thorough research papers from students/young researchers.

Participating Members:

- Stefan SCHIFFNER (Co-Chair, Invited Speaker)

International Conference in Optimization and Learning (OLA2020)

Location: Cadiz, Spain, 17 Feb 2020 – 19 Feb 2020.

Description: The International Conference in Optimization and Learning (OLA2020) focuses on the future challenges of optimization and learning methods and their applications.

Participating Members:

- Pascal BOUVRY (Co-Chair)
- Matthias R. BRUST (Program Committee Member)
- Grégoire DANOY (Program Committee Member)

International Conference on Mobile Secure and Programmable Networking (MSPN’2020)

Location: Paris, France, 1 Jul 2020 – 2 Jul 2020.

Participating Members:

- Christian FRANCK (Technical Program Committee Member)

International Conferences on Logic and Artificial Intelligence at Zhejiang University (ZJULogAI 2020)

Location: Hangzhou (Virtual), China, 26 Oct 2020 – 2 Nov 2020.

Participating Members:

- Alexander STEEN (Workshop Organiser / Co-Organiser)

International Workshop on the Implementation of Logics (IWIL 2020) [Postponed]

Location: Alicante (postponed), Spain, 22 May 2020.

Participating Members:

- Alexander STEEN (Program Committee Member)

Lifelike Computing Systems Workshop (LIFELIKE 2020)

Location: Montréal (virtual), Canada, 13 Jul 2020 – 18 Jul 2020.

Participating Members:

- Jean BOTEV (Co-Chair)

SecITC 2020 : International Conference on Information Technology and Communications

Location: Online, Romania, 19 Nov 2020 – 20 Nov 2020.

Participating Members:

- Peter ROENNE (Program Committee Member)

SMILE - Spring Workshop on Mining and Learning 2020

https://dtai.cs.kuleuven.be/sml/registration.php?hash=329cd5

Location: Lenzkirch-Saig, Germany, 3 Feb 2020 – 5 Feb 2020.

Description: The goal of the SMiLe workshop series, which has been organised bi-annually since 2006, is to bring together leading machine learning, data mining and artificial intelligence researchers in Europe in an informal and stimulating atmosphere, where they can report on interesting recent research results, share their vision on future developments, have stimulating discussions with peers, and start new collaborations. SMiLe aims at broad, high-level, and visionary talks rather than very specialised technical contributions. The talks in the program will be selected on the basis of an informal abstract. A poster session will be open to all participants.

Participating Members:

- Maciej SKORSKI (Invited Speaker (Workshops))
- Martin THEOBALD (Attendant)

Software Verification and Testing track at ACM Symposium on Applied Computing (SAC-SVT 2020)

http://guedemann.org/svt2020/

Location: Brno, Czechia, 30 Mar 2020 – 3 Apr 2020.

Participating Members:

- Jun PANG (Program Committee Member)

The 12th Asia-Pacific Symposium on Internetware Methods (InternetWare 2020)

https://internetware2020.github.io/

Location: Singapore, Singapore, 1 Nov 2020 – 3 Nov 2020.

Participating Members:

- Jun PANG (Program Committee Member)

The 14th International Symposium on Theoretical Aspects of Software Engi- neering (TASE 2020)

https://sei.ecnu.edu.cn/tase2020/

Location: Hangzhou, China, 15 Jul 2020 – 17 Jul 2020.

Participating Members:

- Jun PANG (Program Committee Member)

The 17th International Colloquium on Theoretical Aspects of Computing (ICTAC 2020)

https://ictac2020.github.io/

Location: Macau S.A.R., China, 30 Nov 2020 – 4 Dec 2020.

Participating Members:

- Ross James HORNE (Program Committee Member)

The 2020 IEEE International Conference on Computational Intelligence in Bioinformatics and Computational Biology (CIBCB 2020)

Location: Santiago, Chile, 27 Oct 2020 – 29 Oct 2020.

Participating Members:

- Andrzej MIZERA (Program Committee Member)

The 22nd International Conference on Formal Engineering Methods (ICFEM 2020)

https://formal-analysis.com/icfem/2020/

Location: Singapore, Singapore, 2 Nov 2020 – 6 Nov 2020.

Participating Members:

- Jun PANG (Program Committee Member)

The 25th International Conference on Engineering of Complex Computer Systems (ICECCS 2020)

http://formal-analysis.com/iceccs/2020/

Location: Singapore, Singapore, 28 Oct 2020 – 31 Oct 2020.

Participating Members:

- Jun PANG (Program Committee Member)

The 2th International Conference on Social Informatics (SocInfo 2020)

https://kdd.isti.cnr.it/socinfo2020/

Location: Pisa, Italy, 6 Oct 2020 – 9 Oct 2020.

Participating Members:

- Zhiqiang ZHONG (Program Committee Member)

The 46th Annual Conference of the IEEE Industrial Electronics Society

Location: Singapore, Singapore, 18 Oct 2020 – 21 Oct 2020.

Participating Members:

- Tingting HU (Reviewer)

The 4th International Workshop on the Synergy between Parallel Comuting Optimization and Simulation

Location: Barcelona, Spain, 10 Dec 2020 – 14 Dec 2020.

Participating Members:

- Grégoire DANOY (Workshop Organiser / Co-Organiser)

The 6th Global Conference on Artificial Intelligence (GCAI 2020)

http://www.gcai-2020.info/

Location: Zhejiang, China, 6 Apr 2020 – 9 Apr 2020.

Description: The 6th Global Conference on Artificial Intelligence (GCAI 2020) is part of the International Conferences on Logic and Artificial Intelligence at Zhejiang University (ZJULogAI). With its special focus theme on “Explainable AI and Responsible AIO´, the summit intends to promote the interplay between logical approaches and machine learning based approaches in order to make AI more transparent, responsible and accountable.

Participating Members:

- Jun PANG (Program Committee Co-Chair)

The 6th International Symposium on Dependable Software Engineering Theories Tools and Applications (SETTA 2020)

http://lcs.ios.ac.cn/setta2020/index.html

Location: Guangzhou, China, 24 Nov 2020 – 28 Nov 2020.

Description: The purpose of the SETTA is to bring international researchers together to exchange research results and ideas on bridging the gap between formal methods and software engineering. The interaction with the Chinese computer science and software engineering community is a central focus point. The aim is to show research interests and results from different groups so as to initiate interest-driven research collaboration. The SETTA is aiming at academic excellence and its objective is to become a flagship conference on formal software engineering in China.

Participating Members:

- Jun PANG (Program Committee Co-Chair)

The 7th International Workshop on Graphical Models for Security (GraMSec 2020)

https://gramsec.uni.lu/organization.php

Location: Boston, United States of America, 22 Jun 2020.

Participating Members:

- Sjouke MAUW (Steering Committee Member)
- Ross James HORNE (Program Committee Member)

The 9th International Conference on Complex Networks and their Applications (Complex Networks 2020)

https://complexnetworks.org/

Location: Madrid, Spain, 1 Dec 2020 – 3 Dec 2020.

Participating Members:

- Xihui CHEN (Program Committee Member)
- Andrzej MIZERA (Program Committee Member)

The European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases 2020 (ECML-PKDD 2020)

https://ecmlpkdd2020.net/

Location: Ghent, Belgium, 14 Sep 2020 – 18 Sep 2020.

Participating Members:

- Zhiqiang ZHONG (Program Committee Member)

The Genetic and Evolutionary Computation Conference (GECCO 2020)

Location: Cancun, Mexico, 8 Jul 2020 – 12 Jul 2020.

Participating Members:

- Grégoire DANOY (Program Committee Member)
- Daniel STOLFI ROSSO (Program Committee Member)

Third International Conference on Logic and Argumentation (CLAR 2020)

Location: Hangzhou (Virtual), China, 26 Oct 2020 – 2 Nov 2020.

Participating Members:

- Réka MARKOVICH (Program Committee Member)

Twenty-Fourth International Conference on Financial Cryptography and Data Security

Location: Kota Kinabalu, Malaysia, 10 Feb 2020 – 14 Feb 2020.

Participating Members:

- Alfredo RIAL (Program Committee Member)

Workshop on Automated Reasoning in Quantified Non-Classical Logics (ARQNL 2020) [Postponed]

Location: Paris (postponed), France, 29 Jun 2020.

Participating Members:

- Alexander STEEN (Program Committee Member)

Workshop on Privacy Security and Trust in Artificial Intelligence (PSTrustAI)

https://aciids.pwr.edu.pl/2020/download/ACIIDS_2020_Special_Session_(PSTrustAI_2020)_CFP_v.5.0.pdf

Location: Phuket, Thailand, 23 Mar 2020 – 26 Mar 2020.

Description: Workshop on Privacy, Security, and Trust in Artificial Intelligence (PSTrustAI), co-hosted with *12th Asian Conference on Intelligent Information and Database Systems,*

Participating Members:

- Pascal BOUVRY (Workshop Organiser / Co-Organiser)
- Matthias R. BRUST (Workshop Organiser / Co-Organiser)
- Grégoire DANOY (Workshop Organiser / Co-Organiser)

C.2 Doctoral Thesis Defense Committee Memberships

Jeremie Dauphin, University of Luxembourg

Date: 9 Nov 2020
Location: Esch-sur-Alzette, Luxembourg

PhD Defense Jury Members:

- Sjouke MAUW (Chairman)
- Leon VAN DER TORRE (Supervisor)

PhD Defense Jury External Partners:

- Beishui Liao (Vice-chairman)
- Ken Satoh (Member)
- Matthias Thimm (Member)

Jérémie Dauphin, University of Luxembourg

Date: 9 Nov 2020
Location: Esch-sur-Alzette, Luxembourg

PhD Defense Jury Members:

- Sjouke MAUW (Chairman)
- Leon VAN DER TORRE (Supervisor)

PhD Defense Jury External Partners:

- Beishui Liao (Vice-chairman)
- Ken Satoh (Member)
- Matthias Thimm (Member)

PhD Advisory Board External Partners:

- Marcos Cramer (Advisor)

Denis de Montigny, UC London

Date: 3 Jul 2020
Location: London, United Kingdom

PhD Defense Jury Members:

- Christoph SCHOMMER (Chairman)
- Christoph SCHOMMER (Chairman)

PhD Defense Jury External Partners:

- Philip Treleaven (Supervisor)

Antonio Di Maio, University of Luxembourg

Date: 3 Jun 2020
Location: Luxembourg, Luxembourg

PhD Defense Jury Members:

- Ulrich SORGER (Vice-chairman)
- Thomas ENGEL (Supervisor)

PhD Defense Jury External Partners:

- Torsten Braun (Member)
- Maria Rita Palattella (Member)

Junior Dongo, Universite Paris Est

Date: 22 May 2020
Location: Paris, France

PhD Defense Jury Members:

- Martin THEOBALD (Examiner)

Dániel FEHÉR, University of Luxembourg

Date: 24 Sep 2020
Location: Belval, Luxembourg

PhD Defense Jury Members:

- Paulo ESTEVES-VERISSIMO (Chairman)
- Volker MÜLLER (Vice-chairman)
- Alexei BIRYUKOV (Supervisor)

PhD Defense Jury External Partners:

- Rainer BÖHME (Examiner)
- Ghassan KARAME (Examiner)

Ziya Alper Genc, University of Luxembourg

Date: 14 Oct 2020
Location: Esch/Alzette, Luxembourg

PhD Defense Jury Members:

- Peter Y A RYAN (Chairman)
- Sjouke MAUW (Vice-chairman)

PhD Defense Jury External Partners:

- Jean-Louis Lanet (Member)

- Gianluca Stringhini (Member)

Christian Grévisse, University of Luxembourg

Date: 8 Jan 2020
Location: Esch-sur-Alzette, Luxembourg

PhD Defense Jury Members:

- Denis ZAMPUNIERIS (Chairman)
- Steffen ROTHKUGEL (Supervisor)

PhD Defense Jury External Partners:

- Olga Mariño (Vice-chairman)
- Seungoh Paek (Member)

Xiaojie GUO, Université Grenoble Alpes

Date: 18 Dec 2020
Location: Grenoble, France

PhD Defense Jury Members:

- Nicolas NAVET (Member)

Sven Hammann, Eidgenössische Technische Hochschule Zürich

Date: 3 Dec 2020
Location: Zürich, Switzerland

PhD Defense Jury Members:

- Sjouke MAUW (Member)

Abdallah IBRAHIM, University of Luxembourg

Date: 10 Jan 2020
Location: Belval, Luxembourg

PhD Defense Jury Members:

- Ulrich SORGER (Chairman)
- Pascal BOUVRY (Supervisor)
- Sébastien VARRETTE (Advisor)

PhD Defense Jury External Partners:

- El-Ghazali Talbi (Vice-chairman)

Sasan Jafarnejad, University of Luxembourg

Date: 9 Jan 2020
Location: Luxembourg, Luxembourg

PhD Defense Jury Members:

- Thomas ENGEL (Supervisor)

PhD Defense Jury External Partners:

- Marco Fiore (External Expert)
- Fabian Lanze (Advisor)
- Johan Wahlström (External Expert)

Robert Mebenga Mbala, University of Luxembourg

Date: 10 Sep 2020
Location: University Luxembourg + U Louvain (co-tutuelle), Luxembourg

PhD Defense Jury Members:

- Christoph SCHOMMER (Chairman)
- Christoph SCHOMMER (Chairman)

Thanh Dat Nguyen, École Nationale Supérieure de Mécanique et d'Aérotechnique

Date: 10 Jul 2020
Location: Poitiers, France

PhD Defense Jury Members:

- Nicolas NAVET (Member)

Maryam Pahlevan, University of Siegen

Date: 29 Jan 2020
Location: Siegen, Germany

PhD Defense Jury Members:

- Nicolas NAVET (Examiner)
- Nicolas NAVET (Examiner)

Tahereh Pazouki, University of Luxembourg

Date: 22 Jan 2020
Location: Luxembourg, Luxembourg

PhD Defense Jury Members:

- Christoph SCHOMMER (Vice-chairman)

Vitor Pereira, University of Luxembourg

Date: 20 Oct 2020
Location: Esch-sur-Alzette, Luxembourg

PhD Defense Jury Members:

- Alexei BIRYUKOV (Chairman)
- Volker MÜLLER (Vice-chairman)
- Jean-Sébastien CORON (Supervisor)

PhD Defense Jury External Partners:

- Diego F. Aranha (Member)
- Frederik Vercauteren (Member)

Aleksandr Pilgun, University of Luxembourg

Date: 6 Nov 2020
Location: Esch-sur-Alzette, Luxembourg

PhD Defense Jury Members:

- Yves LE TRAON (Chairman)
- Sjouke MAUW (Supervisor)
- Pascal BOUVRY (Member)

PhD Defense Jury External Partners:

- Olga Gadyatskaya (Vice-chairman)
- Yang Liu (Member)

Zach Smith, University of Luxembourg

Date: 10 Sep 2020
Location: Esch-sur-Alzette, Luxembourg

PhD Defense Jury Members:

- Peter Y A RYAN (Chairman)
- Sjouke MAUW (Supervisor)

PhD Defense Jury External Partners:

- Cas Cremers (Member)
- Steve Kremer (Member)
- Rolando Trujillo Rasua (Vice-chairman)

Cui Su, University of Luxembourg

Date: 3 Nov 2020
Location: Esch-sur-Alzette, Luxembourg

PhD Defense Jury Members:

- Sjouke MAUW (Chairman)
- Jun PANG (Supervisor)

PhD Defense Jury External Partners:

- Loic Pauleve (Member)
- Jaco van de Pol (Member)

PhD Advisory Board Members:

- Andrzej MIZERA (Advisor)

Sergei Tikhomirov, University of Luxembourg

Date: 17 Sep 2020
Location: Belval, Luxembourg

PhD Defense Jury Members:

- Volker MÜLLER (Chairman)
- Alexei BIRYUKOV (Supervisor)

PhD Defense Jury External Partners:

- Matteo MAFFEI (Examiner)
- Patrick Mc Corry (Examiner)
- Andrew MILLER (Vice-chairman)

Itzel Vazquez Sandoval, University of Luxembourg

Date: 3 Nov 2020
Location: Esch/Alzette, Luxembourg

PhD Defense Jury Members:

- Peter Y A RYAN (Chairman)

PhD Defense Jury External Partners:

- Volker Birk (Expert)
- Pascal Lafourcade (Member)
- Fabio Martinelli (Member)
- Luca Vigano (Vice-chairman)

Haoyang Wang, Nanyang Technological University

Date: 9 Dec 2020
Location: Singapore, Singapore

PhD Defense Jury Members:

- Alexei BIRYUKOV (Member)

Marie-Laure Zollinger, University of Luxembourg

Date: 25 Sep 2020
Location: Esch/Alzette, Luxembourg

PhD Defense Jury Members:

- Yves LE TRAON (Chairman)
- Peter ROENNE (Vice-chairman)
- Peter Y A RYAN (Supervisor)

PhD Defense Jury External Partners:

- Olivier Pereira (Member)
- Angela Sasse (Member)

C.3 Awards

7th International Olympiad in Cryptography (NUSCRYPTO 2020), 10 Dec 2020

Recipient: Giuseppe VITTO
Giuseppe Vitto won a silver medal at the 7th International Olympiad in Cryptography (NUSCRYPTO 2020) in the ”Professional” category. NSUCRYPTO is a unique Cryptographic Olympiad containing scientific mathematical problems for professionals, school and university students from any country. Its aim is to involve young researchers in solving curious and tough scientific problems of modern cryptography. http://nsucrypto.nsu.ru/archive/2020/total_results/#data

Best Demo/Poster Award at the 17th GI VR/AR Workshop, 24 Sep 2020

Recipient: Jean BOTEV
The demonstration ”Forest SaVR – A Virtual-Reality Application to Raise Awareness of Deforestation” received the best demo/poster award at the 2020 GI VR/AR Workshop in Trier, Germany. The 17th edition of the main event of the VR/AR special interest group of the German Informatics Society was held virtually/online due to the coronavirus pandemic.

Best Student Paper at COMMA 2020, 11 Sep 2020

Recipients: Jérémie DAUPHIN, Leon VAN DER TORRE, Tjitze Rienstra

Excellent Doctoral Thesis Award, 25 Sep 2020

Recipient: Marie-Laure ZOLLINGER

LexisNexis Best Paper Award of the International Legal Informatics Symposium (IRIS 2020), 29 Feb 2020

Recipients: Tomer LIBAL, Alexander STEEN
For the paper: ”NAI - Towards Transparent and Usable Semi-Automated Legal Analysis”

PhD Colloquium presentation award at E-Vote-ID 2020, 6 Oct 2020

Recipient: Ehsan ESTAJI

Teaching Award delivered by the University of Luxembourg, 27 Oct 2020

Recipient: Alfredo CAPOZUCCA

Teaching Award of the University of Luxembourg, 17 Oct 2020

Recipients: Alfredo CAPOZUCCA, Martin THEOBALD
The Teaching Award honours outstanding teachers committed to quality teaching and contributing significantly to the academic success of their students. Students and faculty staff members nominate their candidate for the teaching award selection committee who picks the final recipient of the award.

C.4 Media Appearances

An open letter on End-to-End-Encryption in response to the EU resolution draft (Scientists4Crypto)

https://sites.google.com/view/scientists4crypto/

Interview (Internet), 22 Dec 2020
Members: Stefan SCHIFFNER
Stefan Schiffner was one of the main contributors to an open letter on End-to-End-Encryption in response to the EU resolution draft “Security through encryption and security despite encryption”: https://sites.google.com/view/scie

ntists4crypto/. This letter was signed by 452 co-signers from 27 countries. In this context he was interviewed by ORF (Österreichischer Rundfunk): https://fm4.orf.at/stories/3010176/

Is it time Luxembourg adopted a contact tracing app? (Delano)

https://delano.lu/d/detail/news/it-time-luxembourg-adopted-contact-tracing-app/212118

Article (Internet), 26 Oct 2020
Members: Peter Y A RYAN

Internet der Dinge: Wenn der Kühlschrank gehackt wird (Luxemburger Wort)

https://www.wort.lu/de/business/internet-der-dinge-wenn-der-kuehlschrank-gehackt-wird-5f60c61fde135b9236fa0201

Article (Newspaper), 16 Sep 2020
Members: Johann GROSZSCHÄDL

Video Podcast / RTL Today (RTL)

Article (Internet), 9 Jul 2020
Members: Christoph SCHOMMER
9 July 2020. Insightful video on DeepFakes technology.

https://today.rtl.lu/news/science-and-environment/a/1545337.html

Radio Podcast (100,7)

https://www.100komma7.lu/podcast/304408

Interview (Radio), 12 Jun 2020
Members: Christoph SCHOMMER
Christoph Schommer was part of a radio podcast in Radio 100,7 (in German): Kënne Roboteren an Zukunft Mënschen ersetzen

Kunst, künstliche Intelligenz – und ganz viel Pathos: Uni stellt Projekt zu ”Esch2022“ vor (Tageblatt)

https://www.tageblatt.lu/headlines/kunst-kuenstliche-intelligenz-und-ganz-viel-pathos-uni-stellt-projekt-zu-esch2022-vor/

Article (Newspaper), 11 Jun 2020
Members: Christoph SCHOMMER
Kunst, künstliche Intelligenz – und ganz viel Pathos: Uni stellt Projekt zu ”Esch2022“ vor. Tageblatt, 11 Juni 2020.

Luxembourg becomes a participating member of ISO / TC 20 / SC 16 [Expert Testimony] (Portail Qualité - Luxembourg)

https://portail-qualite.public.lu/fr/actualites/normes-normalisation/2020/le-luxembourg-devient-membre-participant-du-sous-comite-technique-de-normalisation-iso-tc-20-sc-16-sur-les-aeronefs-sans-pilot

Article (Internet), 28 Apr 2020
Members: Nader SAMIR LABIB

Researchers Surface Privacy Vulnerabilities in Bitcoin Lightning Network Payments (CoinDesk.com)

https://www.coindesk.com/researchers-surface-privacy-vulnerabilities-in-bitcoin-lightning-network-payments

Article (Internet), 21 Apr 2020
Members: Alexei BIRYUKOV, Sergei TIKHOMIROV

Researchers Highlight Privacy Issues With Lightning Network (CoinTelegraph.com)

https://cointelegraph.com/news/researchers-highlight-privacy-issues-with-lightning-network

Article (Internet), 17 Apr 2020

Members: Alexei BIRYUKOV, Sergei TIKHOMIROV

Wallet balances on Bitcoin’s Lightning Network aren’t private, new report says (Decrypt.co)

https://decrypt.co/25800/wallet-balances-on-bitcoins-lightning-network-arent-private-new-report-says

Article (Internet), 16 Apr 2020
Members: Alexei BIRYUKOV, Sergei TIKHOMIROV

Eine Doktorarbeit zu beginnen ist (relativ) leicht” (Luxemburger Wort)

https://www.pressreader.com/luxembourg/luxemburger-wort/20200328/page/10

Article (Newspaper), 28 Mar 2020
Members: Christoph SCHOMMER
Christoph Schommer, Luxemburger Wort (28/29 March 2020): ”Eine Doktorarbeit zu beginnen ist (relativ) leicht”, page 10. 28 March 2020.

RTL TV Kloertext (RTL)

Interview (TV), 31 Jan 2020
Members: Christoph SCHOMMER
see https://www.rtl.lu/tele/kloertext/a/1463380.html

Getting animated about science (Delano)

https://delano.lu/d/detail/news/getting-animated-about-science/209208

Article (Internet), 25 Jan 2020
Members: Jim Jean-Pierre BARTHEL

Zweischneidiges Schwert (Revue Luxembourg)

http://www.revue.lu/zweischneidiges-schwert/

Article (Magazine), 20 Jan 2020 , p. 42-44
Members: Christoph SCHOMMER
Article, based on an interview with the journalist Cheryl Cadamuro. Photography by the photographer Philippe Reuter.

Luxemburg will im Kampf der Superrechner mitmischen (Wort)

https://www.wort.lu/de/business/luxemburg-will-im-kampf-der-superrechner-mitmischen-5e20023cda2cc1784e3541c0

Article (Newspaper), 16 Jan 2020
Members: Pascal BOUVRY, Sébastien VARRETTE
Updates in wort_lu (in german) on HPC developments in Luxembourg, in particular within the University of Luxembourg to offer a cutting-edge research infrastructure to Luxembourg public research while serving as edge access to the upcoming EuroHPC-JU Luxembourg supercomputer Meluxina.

Atos empowers researchers at the University of Luxembourg with its BullSequana XH2000 supercomputer (Atos)

https://atos.net/en/2020/press-release_2020_01_07/atos-empowers-researchers-at-the-university-of-luxembourg-with-its-bullsequana-xh2000-supercomputer?utm_campaign=G+-+PR+-+BullSequana+XH2000+Uni+of+Lu

Article (Internet), 7 Jan 2020
Members: Pascal BOUVRY, Hyacinthe CARTIAUX, Emmanuel KIEFFER, Frederic PINEL, Valentin PLUGARU, Sébastien VARRETTE

C.5 Guest Researchers

The following guest researchers were invited to the DCS:

Ruba Abu-Salma

Period: 4 Mar 2020 – 5 Mar 2020
Hosted by: Peter Y A RYAN

Guillaume Aucher
Period: 2 Jun 2020 – 6 Jun 2020
Hosted by: Leon VAN DER TORRE

Prof Dr Christoph Benzmüller (Freie University Berlin)
Period: 1 Jan 2019 – 30 Jun 2020
Hosted by: Leon VAN DER TORRE

Mohamed Bourennane
Period: 24 Jan 2020 – 25 Jan 2020
Hosted by: Peter Y A RYAN

Sofia Celi
Period: 31 Jan 2020 – 1 Feb 2020
Hosted by: Peter Y A RYAN

David Fuenmayor
Period: 9 Dec 2020
Hosted by: Alexander STEEN, Leon VAN DER TORRE

Thomas Haines
Period: 5 Mar 2020 – 6 Mar 2020
Hosted by: Peter Y A RYAN

Thomas Haines (NTNU Trondheim)
Period: 4 Mar 2020 – 6 Mar 2020
Hosted by: Johannes MUELLER

Georges-Axel Jaloyan
Period: 4 Feb 2020 – 5 Feb 2020
Hosted by: Peter Y A RYAN

Tim Kampik
Period: 6 Jan 2020 – 19 Jan 2020
Hosted by: Amro NAJJAR

Damian Kurpiewski
Period: 4 Feb 2020 – 8 Feb 2020
Hosted by: Wojciech JAMROGA

Cheng-Te Li (National Cheng Kung University)
Period: 17 Jan 2020 – 20 Jan 2020
Hosted by: Jun PANG

Chonghui Li (Zhejiang University)
Period: 11 Nov 2019 – 20 Jan 2020
Hosted by: Leon VAN DER TORRE

Alessandra Marra (MCMP Munich)
Period: 4 Dec 2020
Hosted by: Réka MARKOVICH, Leon VAN DER TORRE

David Naccache
Period: 8 Jul 2020 – 9 Jul 2020
Hosted by: Peter Y A RYAN

David Naccache
Period: 11 Mar 2020 – 12 Mar 2020
Hosted by: Peter Y A RYAN

Sana Nouzri (Cadi Ayyad University)
Period: 10 Feb 2020 – 14 Feb 2020
Hosted by: Leon VAN DER TORRE

Tjitze Rienstra
Period: 23 Mar 2020 – 27 Mar 2020
Hosted by: Leon VAN DER TORRE

Siavash Shahrjedi (Sorbonne)
Period: 6 May 2020
Hosted by: Leon VAN DER TORRE

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.**

Srdjan Vesic

Period: 6 Jan 2020 – 10 Jan 2020
Hosted by: Leon VAN DER TORRE

Yi N. Wang (Hangzhou)

Period: 20 Jan 2020 – 24 Jan 2020
Hosted by: Leon VAN DER TORRE

C.6 Visits

The following visits by DCS members to external organisations took place:

Alfredo CAPOZUCCA

Institution: Innopolis University
Location: Kazan, Tatarstan, Russia
Period: 26 Feb 2020 – 1 Mar 2020.

Jérémie DAUPHIN

Institution: Technische Universität Dresden
Location: Dresden, Germany
Period: 17 Feb 2020 – 28 Feb 2020.
Reason: Collaboration with Dr. Marcos Cramer

Ross James HORNE

Institution: ANU Canberra
Location: Canberra, Australia
Period: 3 Feb 2020 – 14 Feb 2020.

Asya MITSEVA

Institution: Brandenburg University of Technology (BTU)
Location: Cottbus, Germany
Period: 6 Jan 2020 – 17 Jan 2020.
Reason: Erasmus+ staff mobility

Overall objective of the mobility: sharing of teaching and other scientific knowledge between UL and BTU.

Yunior RAMIREZ CRUZ

Institution: Deakin University
Location: Melbourne, Australia
Period: 17 Feb 2020 – 28 Feb 2020.

Peter ROENNE

Institution: Surrey University
Location: Guildford, United Kingdom
Period: 20 Jan 2020 – 22 Jan 2020.

Andy RUPP

Institution: University of Wuppertal
Location: Wuppertal, Germany
Period: 22 Jan 2020 – 24 Jan 2020.
Reason: Discussion of topics for joint research and grant proposals with Professor Tibor Jager.

Jeroen VAN WIER

Institution: Sorbonne Université - LIP6 Quantum Information Group
Location: Paris, France
Period: 24 Feb 2020 – 1 Mar 2020.

Denis ZAMPUNIERIS

Institution: University of Namur
Location: Namur, Belgium
Period: 16 Feb 2020 – 18 Jun 2020.
Reason: Prof. Zampuniéris has been welcomed as visiting professor at the Faculty of CS of the University of Namur (B) by prof. Colin.

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: Many small improvements and bug fixes have been applied to Accord in 2020.

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), Cui SU (Developer)

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), Jiaqi TIAN (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), Stanislav KONCHENKO (Designer), Benoit RIES (Analyst)

Description: Development of the BiCS Management Tool, a web application for managing the BiCS Semester Projects.

Changes: The maintenance and development of the BiCS Management Tool have been continued. The focus is in improvement of the tool, adding new functionality and finding/fixing bugs as well as refactoring the current code to make it stable and decrease the manual administration work as much as possible. Also proposed a new architecture for future releases based on SPA, microservices, DevOps and Cloud approaches.

BiCS Website

License: to be defined

Members: Nicolas GUELFI (Analyst), Stanislav KONCHENKO (Architect), Gilles MAGALHAES (Developer), 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.

Changes: New website was developed and deployed to production. The newer version has been deployed in the middle of February 2020. It includes changes in the website architecture, uses new CMS (Wagtail), and it is based on deploying as a serverless app by using automated continuous delivery pipeline.

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), Cui SU (Developer)

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), Zachary Daniel SMITH (Developer)

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 verification methodology proposed in our paper ”Distance-Bounding Protocols: Verification 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), Romain ROLAND (Developer), Venkateshwaran THAMILSELVAN (Developer), Vanitha VARADHARAJAN (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).

Changes: Improvements on the GUI, added Admin mode, and support to run seminars. Multiple bug fixes and improvements in the deployment and testing process. Two new participants helped in the development of the application. They were: Vanitha VARADHARAJAN and Venkateshwaran THAMILSELVAN

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 Vulnterbaility 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.

Changes: Developed and available sicne 2020.

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://atom.io/packages/language-fudomo

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 plugin for the Atom text editor as well as command-line tools and libraries.

Changes: The user interface for the Fudomo tool was redone as a try-fudomo, a web application that can be used from any browser and does not require any further software to be installed on the user’s system.

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

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 1.5.

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: Small changes and bug fixes were applied to the MICS management system in 2020, including a new export function for student profile selections.

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.

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.

NHC

https://github.com/minimap-xl/nhc

License: AGPL-3.0 license (Affero GPL)

Members: Tingting HU (Developer), Nicolas NAVET (Architect)

Description: NHC is an automated tool that can be used to augment models written in the CPAL Domain-Specific Language, with non-functional features such as dependability. Model-to-model transformation is achieved by first constructing an Abstract Syntax Tree corresponding to the initial model and then manipulating the AST tree to add non-functional features and last dump it back as CPAL source file.

The goal of the software is to allow automate the "augmentation" of CPAL models with dependability mechanisms (e.g., process and data redundancy, voting). The software takes a model as input and transform it into a functionally equivalent model that meets additional dependability properties. Currently, the software is able to augment a model with the N-Version Programming fault-tolerance pattern, which is a central pattern in the field of critical systems.

This is the first MT framework dedicated to the CPAL language. Because it operates within the boundaries of the CPAL language it allows to retain the ability to accomplish non-functional analyses on both the original and the transformed model, be it in a simulation environment or on the actual target. For example, both scheduling and code coverage analysis, are still applicable to the transformed model, in order to properly assess MT suitability, overhead and performance in a specific application scenario. The MT framework is thread-safe and features a plugin based infrastructure and internal caches for speed. The MT framework has been designed according to a modular four-layer architecture depicted in the figure below and implemented as about 9500 lines of C code.

Copyright (C) 2018-2019 University of Luxembourg, National Research Council of Italy, and RealTime-at-Work.

Authors: Tingting Hu, Nicolas Navet, Ivan Cibrario Bertolotti, Loïc Fejoz, and Lionel Havet

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”.

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)

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 2020, highly-optimized Assembler implementations of the SPARKLE permutation for 8-bit AVR as well as 32-bit ARM Cortex-M0 and Cortex-M3 microcontrollers were added to the repository.

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.

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

ULHPC-credits

https://gitlab.uni.lu/vplugaru/ulhpc-tools

License: GPLv3

Members: Valentin PLUGARU (Designer)

ULHPC-platform-usage

License: GPLv3

Members: Valentin PLUGARU (Designer)

Description: Tool used on the UL HPC platform (Gaia/Chaos clusters: ‘ulhpc_platform_usage‘) to monitor per-user resource utilization, with configurable email alerting.

Combined with the ULHPC-credits tool, it allows for a more comprehensive understanding of platform utilization.

WFP toolbox

License: TBA

Members: Asya MITSEVA (Developer)

Description: The website fingerprinting toolbox consists of multiple scripts and binaries that allow a user to carry out research related to the website fingerprinting attack. The toolbox enables a user to automate the visit of websites, record the traffic traces, clean the traffic traces from wrong instances, extract features from the traffic traces and finally train a machine learning classifier.

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.

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.

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	56.53
Postdoctoral Researcher	27.06
Professor	20.92
Research Scientist	20.11
Research Associate	14.68
Scientific / Technical Support Staff	10.11
Student / Intern	7.99
Administrative Staff	4
Project Coordinator	1.11
Chief Scientist	1
Research Facilitator	0.09
Total	*163.58*

Table E.1: Number of Staff by Category

E.2 Distribution of Staff by Category

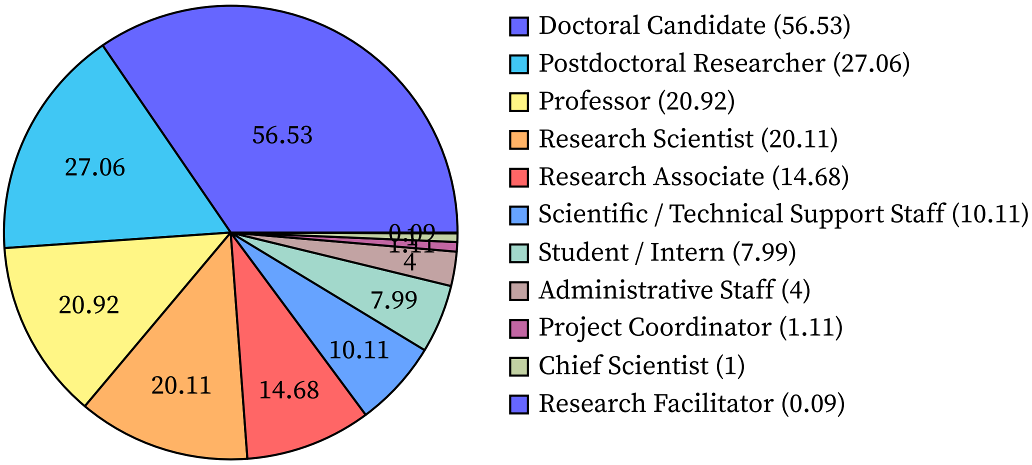


Figure E.1: Staff Distribution

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 (0.71 FTE)
	CORON	Jean-Sébastien
	ENGEL	Thomas
	ESTEVES-VERISSIMO	Paulo (0.83 FTE)
	GUELFI	Nicolas
	KELSEN	Pierre
	LE TRAON	Yves
	LEPREVOST	Franck
	MAUW	Sjouke
	MÜLLER	Volker
	NAVET	Nicolas
	PAPADAKIS	Mike (0.38 FTE)
	ROTHKUGEL	Steffen
	RYAN	Peter Y A
	SACHAU	Juergen
	SCHOMMER	Christoph
	SORGER	Ulrich
	STEENIS	Bernard
	THEOBALD	Martin
	VAN DER TORRE	Leon

Category	Last Name	First Name
	ZAMPUNIERIS	Denis
Chief Scientist	KLEIN	Jacques
Research Scientist	BISSYANDE	Tegawendé François d Assise
	BOTEV	Jean
	BRUST	Matthias R.
	CAPOZUCCA	Alfredo
	CORDY	Maxime
	DANOY	Grégoire
	DECOUCHANT	Jérémie
	FRANCK	Christian
	HU	Tingting
	JAMROGA	Wojciech (0.58 FTE)
	KIEFFER	Emmanuel
	MA	Qin
	PANG	Jun
	PAPADAKIS	Mike (0.62 FTE)
	PINEL	Frederic
	RIAL	Alfredo (0.92 FTE)
	RIES	Benoit
	ROENNE	Peter
	RUPP	Andy
	VARRETTE	Sébastien
	WEYDERT	Emil
Postdoctoral Researcher	ALEKSANDROVA	Marharyta
	ALLIX	Kevin
	BOYTSOV	Andrey (0.70 FTE)
	BURSUC	Sergiu
	CHANGAIVAL	Boonyarit (0.92 FTE)
	DESPOTOVIC	Vladimir
	DI MAIO	Antonio (0.38 FTE)
	ELLAMPALLIL VENUGOPAL	Vinu
	FEHER	Daniel (0.21 FTE)
	GREVISSE	Christian (0.96 FTE)
	GUI	Yujuan (0.46 FTE)
	GUO	Siwen (0.16 FTE)
	HASAN	Cengis
	HOEHN	Sviatlana
	HORNE	Ross James
	HURIER	Médéric (0.04 FTE)
	LIBAL	Tomer
	LOPEZ BECERRA	Jose Miguel (0.33 FTE)
	MARKOVICH	Réka
	MIZERA	Andrzej
	MOULINE	Ludovic (0.87 FTE)

Category	Last Name	First Name
	MUELLER	Johannes
	NAJJAR	Amro
	RAMPARISON	Mathias (0.75 FTE)
	RIAL	Alfredo (0.08 FTE)
	ROSSI	Arianna
	SAHU	Rajeev Anand
	SIRAJZADE	Joshgun (0.73 FTE)
	STEEN	Alexander
	STOLFI ROSSO	Daniel
	TIKHOMIROV	Sergei (0.25 FTE)
	TITCHEU CHEKAM	Thierry
	WANG	Qingju (0.99 FTE)
	WASIM	Muhammad Umer
	ZOLLINGER	Marie-Laure (0.25 FTE)
Research Associate	ATASHPENDAR	Arash (0.08 FTE)
	BARTEL	Alexandre (0.75 FTE)
	BOUALOUACHE	Abdelwahab
	CHEN	Xihui
	FOTIADIS	Georgios
	JAMROGA	Wojciech (0.41 FTE)
	KAISER	Daniel
	KRISHNASAMY	Ezhilmathi
	MESTEL	David
	OSTREV	Dimiter
	OSVIK	Dag Arne (0.20 FTE)
	RAMIREZ CRUZ	Yunior
	ROBALDO	Livio (0.41 FTE)
	ROBERT	Jérémy (0.92 FTE)
	SCHIFFNER	Stefan
	SOUA	Ridha (0.25 FTE)
	SYMEONIDIS	Iraklis (0.67 FTE)
	TALBOT	Pierre
	TURCANU	Ion
Project Coordinator	OCHSENBEIN	Anne (0.50 FTE)
	OESTLUND	Stefanie (0.61 FTE)
Research Facilitator	OESTLUND	Stefanie (0.09 FTE)
Scientific / Technical Support Staff	CARTIAUX	Hyacinthe
	DAUPHIN	Jérémie (0.08 FTE)
	GLODT	Christian
	GROSZSCHÄDL	Johann
	HOUITTE	Pierre-Yves
	KONCHENKO	Stanislav (0.75 FTE)
	LADID	Latif
	MACHALEK	Aurel
	PLUGARU	Valentin (0.28 FTE)

Category	Last Name	First Name
	REIS	Sandro
	SKORSKI	Maciej
	STEMPER	André
Doctoral Candidate	AL-JAWAHERI	Husam (0.16 FTE)
	ANTONIADIS	Nikolaos
	BALOGLU	Sevdenur
	BARTHEL	Jim Jean-Pierre
	BENEDICK	Paul-Lou
	BUSCEMI	Alessio
	CAPPONI	Andrea (0.67 FTE)
	CARDOSO DOS SANTOS	Luan
	CHANGAIVAL	Boonyarit (0.04 FTE)
	CHAYCHI	Samira
	CHEN	Ninghan
	CHENG	Hao
	CHITIC	Ioana Raluca
	DAMODARAN	Aditya Shyam Shankar
	DAUPHIN	Jérémie (0.92 FTE)
	DE LA CADENA RAMOS	Augusto Wladimir
	DI MAIO	Antonio (0.28 FTE)
	DUFLO	Gabriel
	EL ORCHE	Fatima Ezzahra
	ESMAEILZADEH DILMAGHANI	Saharnaz
	ESTAJI	Ehsan
	FARJAMI	Ali (0.92 FTE)
	FEHER	Daniel (0.79 FTE)
	FISCARELLI	Antonio Maria
	GAO	Jun
	GARG	Aayush
	GHAMIZI	Salah
	GREVISSE	Christian (0.04 FTE)
	GUI	Yujuan (0.53 FTE)
	GUO	Siwen (0.04 FTE)
	HADDADAN	Shohreh
	HU	Hailong
	IBRAHIM	Abdallah Ali Zainelabden Abdallah (0.12 FTE)
	JAFARNEJAD	Sasan (0.16 FTE)
	JAHIC	Benjamin
	KAMLOVSKAYA	Ekaterina
	KELLER	Patrick
	KIM	Kisub
	KOLBE	Niklas (0.70 FTE)

Category	Last Name	First Name
	KONG	Pingfan
	LIMA PEREIRA	Hilder Vitor
	LIU	Chao
	LIU	Kui (0.41 FTE)
	MA	Wei
	MAHYA	Parisa (0.28 FTE)
	MAI	TIEU LONG
	MEDER	Jeff Alphonse Antoine (0.70 FTE)
	MEDER	Paul Joseph Yves (0.67 FTE)
	MITSEVA	Asya (0.25 FTE)
	QIAO	Lisha (0.96 FTE)
	RIDA	Ahmad
	RIOM	Timothée
	RWEMALIKA	Renaud
	SALA	Petra
	SAMIR LABIB	Nader
	SIMONETTO	Thibault Jean Angel (0.16 FTE)
	SMITH	Zachary Daniel (0.45 FTE)
	SOROUSH	Najmeh
	SU	Cui (0.87 FTE)
	SUN	Ningyuan
	TAWAKULI	Amal
	TEMPERONI	Alessandro
	TIKHOMIROV	Sergei (0.75 FTE)
	TORCHYAN	Khachatur
	VAN WIER	Jeroen
	VITTO	Giuseppe
	YURKOV	Semen
	ZHONG	Zhiqiang
	ZOLLINGER	Marie-Laure (0.75 FTE)
Administrative Staff	EDWARDSDOTTIR FINNSSON	Helga Fanney
	KARPATI	Daniel (0.70 FTE)
	PUECH	Andrea (0.80 FTE)
	SCHMITZ	Fabienne
	SCHROEDER	Isabelle (0.50 FTE)
Student / Intern	AAMIR	Farah (0.37 FTE)
	ALSAHLI	Malik Ruzayq M (0.58 FTE)
	ANTROPOVA	Daria (0.96 FTE)
	ATASHPENDAR	Aryobarzan (0.97 FTE)
	BONTE	Eliott Cyril Michel (0.43 FTE)

Category	Last Name	First Name
	CARBOGNANI	Enrico Alarico (0.08 FTE)
	DUPONT	Briag Gerard Benjamin (0.71 FTE)
	ELZUBAIR	Ayman (0.20 FTE)
	FILIMONOV	Ihor (0.58 FTE)
	GAREEV	Daniel (0.08 FTE)
	KALF	Patrick (0.05 FTE)
	KIHN	Pol (0.04 FTE)
	KULAMANOVA	Enejan (0.50 FTE)
	MAGALHAES	Gilles (0.35 FTE)
	MEJRI	Nesryne (0.48 FTE)
	SIMONETTO	Thibault Jean Angel (0.57 FTE)
	THAMILSELVAN	Venkateshwaran (0.99 FTE)
	XU	Jingjing (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