RESEARCH CENTER

FIELD
Algorithmics, Programming, Software and Architecture

Activity Report 2017

Section Contracts and Grants with Industry

Edition: 2018-02-19

ARIC Project-Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

Bosch (Germany) ordered from us some support for implementing complex numerical algorithms.

8.2. Bilateral Grants with Industry

- Miruna Rosca and Radu Titiu are employees of BitDefender. Their PhD's are supervised by Damien Stehlé and Benoît Libert, respectively. Miruna Rosca works on the foundations of lattice-based cryptography, and Radu Titiu works on pseudo-random functions and functional encryption.
- Adel Hamdi is doing is PhD with Orange Labs and is supervised by Fabien Laguillaumie. He is working on advanced encryption protocols for the cloud.
- Within the program Nano 2017, we collaborate with the Compilation Expertise Center of STMicroelectronics on the theme of floating-point arithmetic for embedded processors.

AROMATH Project-Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Grants with Industry

MISSLER Software provided a grant to the team AROMATH, related to the collaboration on geometric modeling methods for toolpath generation and machining.

CARAMBA Project-Team

8. Bilateral Contracts and Grants with Industry

8.1. Training and Consulting with French Ministry of Defense

We have training and consulting activities with the French Ministry of Defense.

8.2. Consulting with Docapost

Together with the PESTO team, we have a contract with the Docapost company, the purpose of which is to impove their e-voting solution, adding some verifiability properties and switching to elliptic curve cryptography.

8.3. Consulting with Canton of Geneva

In this contract the goal is to audit and prove security properties of a new e-voting protocol to be used in a few cantons of Switzerland.

8.4. Research Contract with Orange

This contract with Orange Gardens at Chatillon-Montrouge is dedicated to the supervision of Sandra Rasoamiaramanana's PhD thesis about security in the white box context.

8.5. FUI Industrial Partnership on Lightweight Cryptography

This contract, called PACLIDO, is an FUI project with many companies dedicated to the definition of new lightweight cryptographic primitives for the IoT.

CASCADE Project-Team (section vide)

DATASHAPE Project-Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

- Collaboration with Sysnav, a French SME with world leading expertise in navigation and geopositioning in extreme environments, on TDA, geometric approaches and machine learning for the analysis of movements of pedestrians and patients equipped with inetial sensors (CIFRE PhD of Bertrand Beaufils).
- Collaboration with Fujitsu on TDA and Machine learning (started in Dec 2017).

8.2. Bilateral Grants with Industry

- DATASHAPE and Sysnav have been selected for the ANR/DGA Challenge MALIN (funding: 700 kEuros) in September 2017.

GAMBLE Project-Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

A two-years licence and cooperation agreement was signed on April 1st, 2016 between WATERLOO MAPLE INC., Ontario, Canada (represented by Laurent Bernardin, its Executive Vice President Products and Solutions) and Inria. On the Inria side, this contract involves the teams VEGAS and OURAGAN (Paris), and it is coordinated by Fabrice Rouillier (OURAGAN).

F. Rouillier and VEGAS are the developers of the ISOTOP software for the computation of topology of curves. One objective of the contract is to transfer a version of ISOTOP to WATERLOO MAPLE INC.

GRACE Project-Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

- **NOKIA BELL LABS**
  - New PhD student H. Khazaie is funded by ADR with NOKIA BELL LABS. The PhD topic is the security of distributed storage systems.
  - Post doctoral researcher N. Coxon is funded by ADR with NOKIA BELL LABS. The post doc topic is an information theoretically secure private information retrieval scheme.
- **SAFRAN Identity and Security (Ex Morpho and now Idemia)**
  - Post doctoral researcher W. George is funded by Idemia to design an identity management scheme based on Bitcoin's blockchain.

LFANT Project-Team (section vide)

POLSYS Project-Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Grants with Industry

Until the mid 2000's, multivariate cryptography was developing very rapidly, producing many interesting and versatile public-key schemes. However, many of them were soon successfully cryptanalysed (a lot have been done in this group). As a consequence, the confidence in multivariate cryptography cryptosystems declined. It seems that there have emerged new important reasons for renewal of the interest in a new generation of multivariate schemes. In the past two years, the algorithms for solving the Discrete Logarithm Problem over small characteristic fields underwent an extraordinary development. This clearly illustrates the risk to not consider alternatives to classical assumptions based on number theory. In parallel, two of the most important standardization bodies in the world, NIST and ETSI have recently started initiatives for developing cryptographic standards not based on number theory, with a particular focus on primitives resistant to quantum algorithms. An objective here is then to focus on the design of multivariate schemes.

The team is involved in the industrial transfer of post-quantum cryptography. The maturation project, called HFEBOOST, is supervised by SATT-LUTECH.

SATT-LUTECH specializes in the processing and transfer of technologies from research laboratories of its shareholders: Inria, CNRS, University of Technology of Compiègne, National Museum of Natural History, Institute Curie, Université Panthéon-Assas, Paris Sorbonne University and National School of Industrial Creation).

The team has recently developed, in partnership with a mobile application development company (WASSA), an Android app for smartphones (Samsung S5 type) that uses multivariate cryptography. The application has been tested mid-November in a series of experiments supervised by DGA and French Ministry of Defense. The experiment gathered a total of hundred participants from various operational units. This is a first milestone in the maturation project whose goal is to create a start-up.

7.2. Public Contracts

CEA LETI / DSYS / CESTI

In smart card domain, the emanations of a component during a cryptographic computation may compromise the information that is directly or not linked to the secret keys. The most part of the side channel attacks are based on statistical tools that exploit relations between the handled data and the signals. However these methods do not take advantage of all the signal information. The goal is to study the existing algorithms in pattern and speech recognition and to apply them to signals related to cryptographic computations. The objective will be to improve the attacks efficiency and resolve more complex problems.

SECRET Project-Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Grants with Industry

- **Thales** ($02/14 \rightarrow 01/17$)
  Funding for the supervision of Julia Chaulet's PhD.
  30 kEuros.

SPECFUN Project-Team (section vide)

CAIRN Project-Team (section vide)

CAMUS Team

8. Bilateral Contracts and Grants with Industry

8.1. NANO 2017/PSAIC

The CAMUS team is taking part of the NANO 2017 national research program and its sub-project PSAIC (Performance and Size Auto-tuning thru Iterative Compilation) with the company STMicroelectronics, which started in January 2015. Since the release of our automatic speculative parallelization framework Apollo, we have been working on an extension making Apollo usable as a advanced program profiling tool. We are currently working in extending Apollo to the memoization of the memory behavior for loops that are invoked several times.

8.2. Caldera

Vincent Loechner and Cédric Bastoul are involved in a collaboration with the French company Caldera (http://www.caldera.com), specialized in software development for wide image processing. The goal of this collaboration is the development of parallel and scalable image processing pipeline for industrial printing. The project started in September 2016 and involves a contract established between the ICube laboratory and the Caldera company. This contract includes the funding of the industrial thesis (CIFRE) of Paul Godard (started in September 2016) on the topic of the collaboration, under the supervision of Vincent Loechner and Cédric Bastoul.

CORSE Project-Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

- CORSE is involved in a contract with Kalray which objective is the automatic integration of neural networks into the manycore architecture developed by Kalray.

7.2. Bilateral Grants with Industry

- PSAIC Nano2017 is a bilateral Grant with STMicroelectronics. CORSE is involved in the development of trace analysis and hybrid compilation.
- DEMA Nano2017 is a bilateral Grant with STMicroelectronics. CORSE is involved in the development of debugging of multi-threaded applications.

PACAP Project-Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

7.1.1. Nano 2017 PSAIC

Participants: Arif Ali Ana-Pparakkal, Erven Rohou.

Nano 2017 PSAIC is a collaborative R&D program involving Inria and STMicroelectronics. The PSAIC (Performance and Size Auto-tuning through Iterative Compilation) project concerns the automation of program optimization through the combination of several tools and techniques such as: compiler optimization, profiling, trace analysis, iterative optimization and binary analysis/rewriting. For any given application, the objective is to devise through a fully automated process a compiler profile optimized for performance and code size. For this purpose, we are developing instrumentation techniques that can be focused and specialized to a specific part of the application aimed to be monitored.

The project involves the Inria teams PACAP, AriC, CAMUS and CORSE. PACAP contributes program analyses at the binary level, as well as binary transformations. We will also study the synergy between static (compiler-level) and dynamic (run-time) analyses.

7.2. Bilateral Grants with Industry

7.2.1. Intel research grant INTEL2014-8957

Participants: André Seznec, Biswabandan Panda, Fernando Endo.

Intel is supporting the research of the PACAP project-team on “Mixing branch and value prediction to enable high sequential performance”.

7.2.2. Intel research grant INTEL2016-11174

Participants: André Seznec, Pierre Michaud, Kleovoulos Kalaitzidis, Niloofar Charmchi.

Intel is supporting the research of the PACAP project-team on “Design tradeoffs for extreme cores”.

AOSTE2 Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Grants with Industry

The Airbus CIFRE grant which started on March 2014, provides full support for the PhD thesis of Cristian Maxim. The thesis concerns the statistical timing analysis while different variability factors are taken into account. The proposed methods are built on top of existing statistical approaches while proving appropriate programs for training these methods and thus learning from the history of the execution.

8.2. Bilateral Grants with Industry

The IFPEN grant which started on December 2014, provides full support for the PhD thesis of Salah-Eddine Saidi. The thesis concerns the automatic parallelization and scheduling approaches for co-simulation of numerical models on multi-core processors. The goal of the first research topic is to propose multi-core scheduling solutions for the co-simulation in order to accelerate its execution. The second research topic aims at proposing multi-core scheduling solutions in order to enable the execution of co-simulation under real-time constraints in the context of Hardware-in-the-Loop validation.

HYCOMES Project-Team

6. Bilateral Contracts and Grants with Industry

6.1. GLOSE

The simulation of system-level models requires synchronizing, at simulation-time, physical models with software models. These models are developed and maintained by different stakeholders: physics engineers, control engineers and software engineers. Models designed by physics engineers are either detailed 3D finite-elements models, with partial differential equations (PDEs), or finite-dimension 0D models (obtained by model reduction techniques, or by empirical knowledge) expressed in modeling languages such as Simulink (with ordinary differential equations, or ODEs), Modelica (with differential algebraic equations, or DAEs), or directly as a C code embedding both the differential equations and its discretization scheme. Control engineers favor Matlab/Simulink, mainly because of its toolboxes and ease of use. Computer scientists program or model real-time reactive software, either with a dedicated language, for instance SCADE, hierarchical state machines or sequence/activity diagrams (as in UML/SysML) or directly in C. Coupling together heterogeneous models and programs, so that they can be co-simulated, is not only a technological challenge, but more importantly raises several deep and difficult questions: Can we trust simulations? What about their reproducibility? Will it be possible to simulate large systems with hundreds to thousands of component models?

The objective of the GLOSE project is to address these objectives, and propose both sound foundations and practical technological solutions to system level modeling and simulation. The GLOSE project has started in December 2017 and is funded by Safran, in the realm of the DESIR joint Safran-Academia research network. The academic teams contributing to GLOSE are the Hycomes, Diverse and Kairos Inria teams, and IRIT/CNRS in Toulouse.

KAIROS Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

7.1.1. IRT Saint-Exupery ATIPPIC project

Participants: Robert de Simone, Julien Deantoni, Amin Oueslati.

We are collaborating here with Thales Alenia Space and some of their partners, with engineering forces put in secondment to the direct governance of IRT Saint-Exupery, on the topic of introducing COTS processor usage for satellite mission systems, with the corresponding methodological needs (sharing software tasks on a single (multi)processor, with safety-critical constraints against cosmic radiations). We attempt to make this a show-case study for our formal model-based design approach.

7.1.2. GLoSE project of the SAFRAN DESIR research programme

Participants: Robert de Simone, Julien Deantoni, Giovanni Liboni, Frédéric Mallet.

SAFRAN tech set up a collaborative research programme with the major French academic partners in the field of Embedded Systems and Data Analytics, named DESIR. Robert de Simone is Prime Investigator for the Embedded System side. Julien DeAntoni heads a specific research project of this programme, named GloSE (Globalization in Systems Engineering), on co-modeling and co-design to enable co-simulation using enhanced FMU/FMI interfaces. A new PhD thesis should start early next year under a related CIFRE grant, with Giovanni Liboni as PhD candidate (he was with us already as intern last Spring).

PARKAS Project-Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

Polly Labs contract with ARM, 2015-2019, with the participation of Qualcomm, Xilinx and Facebook (human resources, consulting services and and hiring former PARKAS members).

SPADES Project-Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

- INRIA and Orange Labs have established in 2015 a joint virtual research laboratory, called I/O LAB. We have been heavily involved in the creation of the laboratory and are actively involved in its operation (Jean-Bernard Stefani is one of the two co-directors of the lab). I/O LAB focuses on the network virtualization and cloudification. As part of the work of I/O LAB, we have cooperated with Orange Lab, as part of a cooperative research contract funded by Orange, on defining architectural principles and frameworks for network cloud infrastructures encompassing control and management of computing, storage and network resources.
- With Daimler (subcontracting via iUTBS): We have bridged the gap between LET as it was originally proposed [59] and its current use in the automotive industry.

7.2. Bilateral Grants with Industry

With Thales: Early Performance assessment for evolving and variable Cyber-Physical Systems. This CIFRE grant funds the PhD of Christophe Prévot.

With Orange: Programming IoT and sofware defined radio with dynamic dataflow models of computation. This CIFRE grant funds the PhD of Arash Shafiei.

TEA Project-Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Grants with Industry

8.1.1. Mitsubishi Electric R&D Europe (2015-2018)

Title: Analysis and verification for correct by construction orchestration in automated factories

Inria principal investigator: Jean-Pierre Talpin, Simon Lunel

International Partner: Mitsubishi Electric R&D Europe

Duration: 2015 - 2018

Abstract: The primary goal of our project is to ensure correctness-by-design in cyber-physical systems, i.e., systems that mix software and hardware in a physical environment, e.g., Mitsubishi factory automation lines. We develop a component-based approach in Differential Dynamic Logic allowing to reason about a wide variety of heterogeneous cyber-physical systems. Our work provides tools and methodology to design and prove a system modularly.

ANTIQUE Project-Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Grants with Industry

Xavier Rival received a Facebook Faculty Award (2017).

CELTIQUE Project-Team (section vide)

CONVECS Project-Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Grants with Industry

7.1.1. Orange Labs

Participants: Umar Ozeer, Gwen Salaün.

Umar Ozeer is supported by a PhD grant (from November 2016 to November 2019) from Orange Labs (Grenoble) on detecting and repairing failures of data-centric applications distributed in the cloud and the IoT (see § 6.5.1), under the supervision of Xavier Etchevers (Orange Labs), Gwen Salaün (CONVECS), François Gaël Ottogalli (Orange Labs), and Jean-Marc Vincent (POLARIS project-team).

7.1.2. Nokia Bell Labs

Participants: Radu Mateescu, Ajay Muroor Nadumane, Gwen Salaün.

Ajay Muroor Nadumane is supported by a PhD grant (from October 2017 to October 2020) from Nokia Bell Labs (Nozay) on IoT service composition supported by formal methods, under the supervision of Gwen Salaün (CONVECS), Radu Mateescu (CONVECS), Ludovic Noirie, and Michel Le Pallec (Nokia Bell Labs).

DEDUCTEAM Project-Team (section vide)

GALLIUM Project-Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

8.1.1. The Caml Consortium

Participants: Xavier Leroy [**contact**], Damien Doligez, Michel Mauny, Didier Rémy.

The Caml Consortium is a formal structure where industrial and academic users of OCaml can support the development of the language and associated tools, express their specific needs, and contribute to the long-term stability of Caml. Membership fees are used to fund specific developments targeted towards industrial users. Members of the Consortium automatically benefit from very liberal licensing conditions on the OCaml system, allowing for instance the OCaml compiler to be embedded within proprietary applications.

The Consortium currently has 16 member companies:

- Aesthetic Integration
- Ahrefs
- Be Sport
- Bloomberg
- CEA
- Citrix
- Dassault Aviation
- Docker
- Esterel Technologies
- Facebook
- Jane Street
- Kernelyze LLC
- LexiFi
- Microsoft
- OCamlPro
- SimCorp

For a complete description of this structure, refer to http://caml.inria.fr/consortium/. Xavier Leroy chairs the scientific committee of the Consortium.

8.1.2. The OCaml Foundation

Participant: Michel Mauny.

Throughout 2017, Michel Mauny has been preparing the project of an OCaml Foundation, which should support OCaml in a more efficient way than the existing Caml Consortium could do, thanks to the facilities and flexibility provided by the recently created Inria Foundation. The goal is to raise enough funds to effectively support the development and evolution of OCaml, and to animate and grow its user and teaching communities.

8.1.3. Scientific Advisory for OCamlPro

Participant: Fabrice Le Fessant.

OCamlPro is a startup company founded in 2011 by Fabrice Le Fessant to promote the use of OCaml in the industry, by providing support, services and tools for OCaml to software companies. OCamlPro performs a lot of research and development, in close partnership with academic institutions such as IRILL, Inria and Univ. Paris Sud, and is involved in several collaborative projects with Gallium, such as the Bware ANR, the Vocal ANR and the Secur-OCaml FUI.

Since 2011, Fabrice Le Fessant has been a scientific advisor at OCamlPro, as part of a collaboration contract for Inria, to transfer his knowledge on the internals of the OCaml runtime and the OCaml compilers. Fabrice has left Inria in October 2017 to join OCamlPro on a full-time position.

MARELLE Project-Team (section vide)

MEXICO Project-Team (section vide)

PARSIFAL Project-Team (section vide)

PI.R2 Project-Team (section vide)

SUMO Project-Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

8.1.1. ADR Softwarization of Everything

Joint Nokia-Inria research lab: Several researchers of SUMO are involved in the joint research lab of Nokia Bell Labs France and Inria, in a common research team called "Softwarization of Everything". The objective of this joint team is to design programming and management methods for software defined networks. Several other Inria teams take part to this group: Convecs, Diverse, Spades. Within this team, SUMO focuses on the management of reconfigurable systems, both at the edge (IoT based applications) and in the core (e.g. virtualized IMS systems). In particular, we focus on control and diagnosis issues for such systems.

8.1.2. Alstom P22

Joint Alstom-Inria research lab: Several researchers of SUMO are involved in the joint research lab of Alstom and Inria, in a common research team called P22. On Alstom side, this joint research team involves researchers of the ATS division (Automatic Train Supervision). The objective of this joint team is to evaluate regulation policies of urban train systems, to assess their robustness to perturbations and failures, to design more efficient regulation policies and finally to provide decision support for human regulators. The project started in march 2014. A second phase of the project started in 2016, for a duration of three years. This covers in particular the CIFRE PhD of Karim Kecir.

TOCCATA Project-Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

8.1.1. ProofInUse Joint Laboratory

Participants: Claude Marché [contact], Jean-Christophe Filliâtre, Andrei Paskevich.

ProofInUse is a joint project between the Toccata team and the SME AdaCore. It was selected and funded by the ANR programme "Laboratoires communs", starting from April 2014, for 3 years http://www.spark-2014.org/proofinuse.

The SME AdaCore is a software publisher specializing in providing software development tools for critical systems. A previous successful collaboration between Toccata and AdaCore enabled *Why3* technology to be put into the heart of the AdaCore-developed SPARK technology.

The goal is now to promote and transfer the use of deduction-based verification tools to industry users, who develop critical software using the programming language Ada. The proof tools are aimed at replacing or complementing the existing test activities, whilst reducing costs.

VERIDIS Project-Team

8. Bilateral Contracts and Grants with Industry

8.1. Modeling a Distributed File System

Participant: Stephan Merz.

In a bilateral contract with Huawei R&D, we continued our work on modeling and verifying protocols underlying the Ceph distributed file system [66] in TLA$^+$. We also provided email support to Huawei engineers who use TLA$^+$ for modeling the systems they develop.

8.2. Modeling a Distributed Development Process

Participant: Christoph Weidenbach.

On the basis of a bilateral contract with L4B (Logic 4 Business), we studied models for a distributed development process of a leading German car manufacturer.

CARTE Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Grants with Industry

- PRCE ANR SoftQPro has Atos-Bull as a partner.
- ITEA 3 Quantex involves several industrial partners: Siemens, KPN, Atos-Bull.

CIDRE Project-Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

- **HP (2013-2019): Embedded Systems Security** We aim at researching and prototyping low-level intrusion detection mechanisms in embedded system software. This involves mechanisms in continuation of previous work realized by our team as well as investigating new techniques more directly tied to specific HP device architectures. Our main objective is to monitor low-level software (firmware, OS kernels, hypervisors) thanks to a dedicated external co-processor. Ronny Chevalier is doing is PhD in the context of this project. Being under NDA, details about this research program cannot be provided.

8.2. Bilateral Grants with Industry

- **Orange Labs: Privacy-preserving location-based services** Solenn Brunet has completed her PhD thesis in November 2017 within the context of a CIFRE contract with Orange Labs Caen. Her PhD subject was about privacy-preserving services that are able to provide the service to the user while preserving his privacy. In particular, Solenn Brunet has designed new cryptographic primitives to build anonymous accreditation and she has used these primitives to provide data anonymization mechanisms in the context of e-voting and e-cash.
- **DGA: BGP-like Inter Domain routing protocol for tactical mobile ad hoc networks: feasibility, performances and quality of service** Florian Grandhomme has completed his PhD thesis in September 2017 in cooperation with DGA-MI. The subject of the PhD was to propose new secure and efficient algorithms and protocols to provide inter-domain routing in the context of tactical mobile ad hoc network. The proposed protocol handles context modification due to the mobility of MANET, that is to say split of a MANET, merge of two or more MANET, and also handles heterogeneity of technology and infrastructure. The solution is independent from the underlying intra-domain routing protocol and from the infrastructure: wired or wireles, fixed or mobile.
- **DGA: Visualization for security events monitoring** Damien Crémilleux has started his PhD thesis in October 2015 in the context of a cooperation with DGA-MI. The subject of the PhD is to define relevant representations to allow front-line security operators to monitors systems from a security perspective. A first proposal was made that led to a tool, VEGAS, that allows to monitor large quantities of alerts in real time and to dispatch these alerts in a relevant way to security analysts.
- **DGA: Intrusion Detection in Distributed Applications** David Lanoé has started his PhD thesis in October 2016 in the context of a cooperation with DGA-MI. His work is focussing on the construction of behavioral models (during a learning phase) and their use to detect intrusions during an execution of the modelled distributed application.
- **Nokia: Risk-aware security policies adaptation in modern communication infrastructures** Pernelle Mensah was hired in January 2016 on this CIFRE funding in order to work on unexplored aspects of information security, and in particular response strategies to complex attacks, in the context of cloud computing architectures. The use case proposed by our industrial partner is a multi-tenant cloud computing platform involving software-defined networking in order to provide further flexibility and responsiveness in architecture management. The topic of the thesis is to adapt and improve the current risk-aware reactive response tools, based on attack graphs and adaptive security policies, to this specific environment, taking into account the heterogeneity of actors, platforms, policies and remediation options.

- **Thales: Privacy and Secure Multi-party Computation** Aurélien Dupin has started his PhD thesis in January 2016 within the context of a CIFRE contract with Thales. His PhD subject concerns secure multi-party computation. Secure two-party computation provides a way for two parties to compute a function, that depends on the two parties' inputs, while keeping them private. Known since the 1980s, Yao's garbled circuits appear to be a general solution to this problem, in the semi-honest model. Decades of optimizations have made this tool a very practical solution. However, it is well known that a malicious adversary could modify a garbled circuit before submitting it. Many protocols, mostly based on cut-&-choose, have been proposed to secure Yao's garbled circuits in the presence of malicious adversaries. Nevertheless, how much an adversary can modify a circuit and make it still executable have not been studied. In the context of his PhD, Aurélien Dupin is interested by such a question.
- **Thales: Combining Attack Specification and Dynamic Learning from traces for correlation rule generation** Charles Xosanavongsa has started his PhD thesis in December 2016 in the context of a CIFRE with Thales. His work will focus on the construction of correlation rules. In previous work on correlation rule generation, the usual approach is static. It always relies on the description of the supervised system using a knowledge base of the system. The use of correlation trees is an appealing solution because it allows to have a precise description of the attacks and can handle any kind of IDS. But in practice, the behavior of each IDS is quite difficult to predict, in particular for anomaly based IDS. To manage automatically the correlation rules (and adapt them if necessary), we plan to analyze synthetic traces containing both anomaly based and misused based IDS alerts resulting from an attack.
- **Ministry of Defence: Visualisation for the characterization of security events** Laetitia Leichtnam has started his PhD thesis in November 2016 in the context of a contract between CentraleSupelec and the French Ministry of Defence. His work consists in presenting events appearing in heterogeneous logs as a dependency graph between the lines of logs. This permits to the administrator to investigate easily the logs to discover the different steps that has performed an attack in the supervised system.
- **ANSSI: Security of Low-level Components** Thomas Letan has started his PhD thesis in the context of a contract between CentraleSupelec and the French National Computer Security Agency (ANSSI). His work consists in using formal methods to specify hardware/software security mechanisms and to verify that they correctly enforce some security policies.

COMETE Project-Team (section vide)

DATASPHERE Team (section vide)

PESTO Project-Team

8. Bilateral Contracts and Grants with Industry

8.1. Scytl - Electronic Voting Systems

Participants: Véronique Cortier, Mathieu Turuani.

Since 2014, a collaboration agreement has been signed between Loria and Scytl, a Spanish company who is proposing solutions for the organization of on-line elections, including legally binding elections, in several countries. In this context, Scytl has signed a contract in 2016 with the Pesto team as well as the University of Birmingham (David Galindo) to design a formal proof of both verifiability and privacy of the protocol developed by Scytl, for a deployment in Switzerland. The result of the analysis will be presented at the conference EuroS&P'18 [23].

8.2. Canton of Geneva - Electronic Voting Systems

Participants: Véronique Cortier, Mathieu Turuani.

The canton of Geneva has signed a contract in October 2017 with Pesto and Caramba, as well as Manifold Security (Bogdan Warinschi and David Bernhard) to design a formal and cryptographic proof of individual and universal verifiability of the protocol developed by the canton of Geneva, for a deployment in Switzerland.

8.3. Docapost - Electronic Voting Systems

Participant: Véronique Cortier.

Docapost has signed a 18-month contract in September 2017, with Pesto and Caramba, to enhance the voting solution of Docapost, in particular with respect to verifiability.

PRIVATICS Project-Team

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

7.1.1. IPSec with pre-shared key for MISTIC security

Title: IPSec with pre-shared key for MISTIC security.

Type: CIFRE.

Duration: Juillet 2014 - Juillet 2017.

Coordinator: Inria

Others partners: Privatics, Moais and Incas-ITSec.

PROSECCO Project-Team (section vide)

TAMIS Team

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

- CISCO (http://www.cisco.com) contract (2017–2022) to work on graph analysis of malware

8.2. Bilateral Grants with Industry

- CISCO (http://www.cisco.com) one grant (2016–2019) to work on semantical analysis of malware
- Thales (https://www.thalesgroup.com) one CIFRE (2016–2019) to work on verification of communication protocols, one grant (2018–2019) to work on learning algorithms
- Oberthur Technologies (http://www.oberthur.com/) one grant (2016–2020) to work on fuzzing and fault injection
- Secure IC (http://www.secure-ic.com/), one CIFRE (2017–2020) to work on post-quantum cryptography