RESEARCH CENTER

FIELD
Algorithmics, Programming, Software and Architecture

Activity Report 2017

Section Highlights of the Team

Edition: 2018-02-19

ARIC Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

H2020 project Prometheus (on privacy-preserving quantum-resistant cryptographic primitives, coordinated by Benoît Libert and hosted by ENS de Lyon). 4-year project (accepted in August 2017) starting from January 2018.

Publication of the book [48] “Algorithmes Efficaces en Calcul Formel.”

J.-M. Muller was elected Fellow member of the IEEE in Jan. 2017.

AROMATH Project-Team (section vide)

CARAMBA Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

The CARAMBA team organized the “Journées Codage et Cryptographie 2017”, whose objective is to regroup the French speaking community working on error-correcting codes and on cryptography. It is affiliated with the “Groupe de travail C2” of the GDR-IM.

CASCADE Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Conferences

- We organised the Eurocrypt '17 annual conference in Paris, from April 30 to May 4.

5.1.2. Awards

- Damien Vergnaud was nominated for a 5 year appointment as Junior Member of the Institut Universitaire de France
- Romain Gay received a Google PhD Fellowship.

DATASHAPE Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Chairs

Jean-Daniel Boissonnat was elected a professor at the Collège de France, on the Chair Informatics and Computational Sciences for the academic year 2016-2017.

GAMBLE Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

The project-team VEGAS terminated at the end of 2016. Our main highlight is actually the creation of the new project-team GAMBLE (Geometric Algorithms and Models Beyond the Linear and Euclidean realm) on July 1st.

Another highlight of this year is that after two failures, both ANR projects we are coordinating finally won at the ANR lottery with two projects that will start in 2018: ASPAG (ANR-17-CE40-0017) and SoS (ANR-17-CE40-0033).

GRACE Project-Team

4. Highlights of the Year

4.1. Highlights of the Year

4.1.1. Presentation at Inria@SiliconValley

D. Augot made a presentation at a one day workshop "Blockchain Technology for Cybersecurity and Social Impact" at Berkeley's CITRIS https://project.inria.fr/siliconvalley/bis2017-day1-conference-blockchain

4.1.2. Workshop on Coding theory and Cryptography (WCC)

D. Augot was co-chair of the Program Commitee of WCC 2017 (St Petersburg, Russia).

4.1.3. NIST Call for post quantum cryptography

In the context of NIST's call for post quantum cryptography:

https://csrc.nist.gov/Projects/Post-Quantum-Cryptography

members of the team participated to two sumbissions:

- A. Couvreur and E. Barelli participated to the submission of **BIG QUAKE** proposal [19]:
  https://bigquake.inria.fr/
- L. De Feo participated to the submission of **SIKE** proposal:
  https://rwc.iacr.org/2018//Slides/Longa.pdf

LFANT Project-Team

4. Highlights of the Year

4.1. Highlights of the Year

Aurel Page has been recruited as a Inria CR in the team.

Damien Robert organised a one-week workshop with the members of the associated team FAST with several African countries.

The book [17] by Henri Cohen on *Modular Forms: A Classical Approach* has been published.

4.1.1. Awards

The paper [] describing Arb in the IEEE Transactions on Computers was selected as the best paper of this journal's Special Issue on Computer Arithmetic.
BEST PAPERS AWARDS :
[] **IEEE Transactions on Computers**. F. JOHANSSON.

POLSYS Project-Team

4. Highlights of the Year

4.1. Highlights of the Year

Dongming Wang has been elected as a Member of the Academia Europaea.

Elias Tsigaridas was awarded an ANR “Jeune Chercheur Grant”. The title of the project is GALOP (Games through the lens of ALgebra and OPptimization)

SECRET Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. NIST post-quantum cryptography standardisation

The end of this year was the deadline to submit proposals to the NIST competition [0], whose purpose is to standardize quantum-safe public-key primitives. This call concerns all three major cryptographic primitives, namely public-key cryptosytems, key-exchange protocols and digital signature schemes. The most promising techniques today for addressing this issue are code-based cryptography, lattice-based cryptography, mutivariate cryptography, and hash-based cryptography.

We have contributed to three proposals to the NIST call. In two of them, "BIKE" [67] and "Big Quake" [69], our action is central and we also have a marginal participation in another, "Classic McEliece". Those projects are of great importance for us because they are a means to demonstrate our long lasting expertise in code-based cryptography. They are the product of numerous research works, including several PhD theses, on the design, the implementation, and the cryptanalysis of code-based cryptographic primitives. There are 69 projects in that call, which will be evaluated by the NIST and the academic cryptographic community in the next three to five years and whose outcome will certainly influence cryptographic applications for one or several decades.

5.1.2. Quantum symmetric cryptanalysis and collision search

The resistance of symmetric primitives to quantum computers is a topic that has received recently a lot of attention from our community. The ERC starting grant QUASYModo on this subject, awarded to M. Naya-Plasencia, has started in September 2017. We have continued the work started last year obtaining new results, as cryptanalysis of concrete proposals [44], or analysis on attacks considering modular additions (preliminary described in [14]). In particular, we have proposed in [47] a new quantum algorithm for finding collisions. This new algorithm, based on BHT, exploits distinguished points as well as an improved optimization of the parameters, and allows to find for the first time, collisions on n bits with a better time complexity than $2^{n/2}$. Its time and query complexity are of about $2^{2n/5}$, needing $2^{n/5}$ classical memory and a polynomial amount of quantum memory. As collision search is a tool widely used in symmetric cryptanalysis, this algorithm, that also can be applied to multiple preimage search, considerably improves the best known previous attacks when having a relatively small quantum computer available.

5.1.3. Émergences grant on quantum money

André Chailloux was awarded an Émergences grant from the city of Paris for a project on quantum money. This project aims at providing a comprehensive theoretical and experimental study of unforgeable quantum money, one of the most powerful protocols in quantum information science, and historically the first. A quantum money scheme enables a secure transaction between a client, a vendor and a bank via the use of a credit card or banknotes, with maximal security guarantees, unreachable with classical technologies. This application is central in the context of the emerging quantum network infrastructures guaranteeing the long-term security of data and communications against all-powerful adversaries.

Quantum money has been largely considered difficult to bring to the experimental realm, but a demonstration became more accessible recently, thanks to the conception of new practical schemes. The goal of our project will be to perform a theoretical analysis of such schemes, both in the discrete and continuous-variable frameworks, to adapt them to realistic conditions, and to implement them using state-of-the-art photonic quantum technologies. The project, centered around Inria, is interdisciplinary at its core, bringing together young partners with world leading expertise in all aspects of the proposed work, including theoretical and experimental quantum cryptography.

[0] https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization

SPECFUN Project-Team

4. Highlights of the Year

4.1. Highlights of the Year

4.1.1. Awards

Pierre Lairez was awarded the SIAM/AAG (SIAM Activity Group on Algebraic Geometry) Early Career Prize.

CAIRN Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

Members of CAIRN published six papers accepted at IEEE/ACM Design Automation and Test in Europe for 2017, one of the major events in design automation.
[30] was among the few papers nominated for best paper at IEEE FPL.

CAMUS Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Awards

A team composed of four CAMUS members (Cédric Bastoul, Vincent Loechner, Harenome Ranaivoarivony-Razanajato and Maxime Schmitt) participated to the Google Hash Code contest. They were ranked 9 during the qualification round, over more than 26000 participants from Europe, Middle-East and Africa, and qualified for the final. They were 34th at the final hosted in the Google Paris office.

CORSE Project-Team (section vide)

PACAP Project-Team (section vide)

AOSTE2 Team

5. Highlights of the Year

5.1. Highlights of the Year

Our team has hosted for the first time in France the 38th Real-Time Systems Symposium (RTSS'17) which is the flag conference of our research domain. All the members of team jointly participated to the big effort of ensuring an excellent edition.

HYCOMES Project-Team (section vide)

KAIROS Team (section vide)

PARKAS Project-Team

4. Highlights of the Year

4.1. Highlights of the Year

4.1.1. Awards

- Francesco Zappa Nardelli received the *Most Influential ICFP Paper Award* for 2007 paper "Ott: Effective Tool Support for the Working Semanticist" (http://www.sigplan.org/Awards/ICFP/).

SPADES Project-Team (section vide)

TEA Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

Inria created a new International Chair and appointed American computer engineer Rajesh Gupta to the part-time position. Gupta is a professor and former chair of the Computer Science and Engineering (CSE) department in the Jacobs School of Engineering at the University of California San Diego. Rajesh Gupta will hold the International Chair for a period of five years. Starting this summer, he will engage with researchers in Inria's research center in Rennes. The position enables him to spend as much as a year spread out over the five years of his appointment.

ANTIQUE Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

The team obtained several strong results published in excellent international conferences, with high theoretical and applied impact (see detailed results). Among the theoretical results we underline those presented in conferences like Principles of programming languages POPL 2017, with the proposal of a novel and groundbreaking way to improve the precision and scalability of analyses performed with disjunctive abstract domains, using silhouette abstraction.

5.1.1. Awards

Patrick Cousot received the IEEE John Von Neumann Medal.

CELTIQUE Project-Team (section vide)

CONVECS Project-Team (section vide)

DEDUCTEAM Project-Team (section vide)

GALLIUM Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Awards

In 2017, Jacques-Henri Jourdan received the “prix du GDR GPL” (http://gdr-gpl.cnrs.fr/node/284) for his dissertation, entitled “Verasco: a Formally Verified C Static Analyzer”. Jacques-Henri was a Ph.D. student in the Gallium team, advised by Xavier Leroy.

MARELLE Project-Team

4. Highlights of the Year

4.1. Highlights of the Year

Our effort to setup a consortium around the Coq system has made significant progress this year as illustrated by two noticeable events: the first engineer was hired by InriaSoft for this consortium (Maxime Dénès) and the first funding was collected from academic partners (the first is Princeton University).

MEXICO Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

See the 'New results' section.

PARSIFAL Project-Team (section vide)

PI.R2 Project-Team

4. Highlights of the Year

4.1. Highlights of the Year

4.1.1. Awards

Amina Doumane was awarded the The Kleene Award for Best Student Paper at the LICS 2017 conference, for her work on “Constructive Completeness for the Linear-Time mu-Calculus”. She also received in January 2018 the prize of the Journal La Recherche for the same paper.

Amina Doumane was awarded the Gilles Kahn 2017 prize for her PhD thesis entitled “On the infinitary proof theory of logics with fixed points” supervised by Alexis Saurin, David Baelde and Pierre-Louis Curien.

Ludovic Patey was awarded the Prix Thiessé de Rosemont / Demassieux 2017 for his PhD thesis “Les mathématiques à rebours de théorèmes de type Ramsey”, supervised by Laurent Bienvenu and Hugo Herbelin.
BEST PAPERS AWARDS :
[37] **Conference on Logic in Computer Science 2017**. A. DOUMANE.
[] **On the infinitary proof theory of logics with fixed points**.

SUMO Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. New partnership

Several members of the team are involved in the joint research team "Softwarization of Everything", part of the joint research lab of Nokia Bell Labs France and Inria. This activity will finance two PhDs in the team, related to the management and control of software-defined networks.

5.1.2. Awards

- Engel Lefaucheux received the best young-researcher-paper award ("Prix Jeune Chercheur") at MSR 2017 for his paper titled *Diagnostic et contrôle de la dégradation des systèmes probabilistes* .
- Nicolas Markey was awarded an *Allocation d'Installation Scientifique* (at senior-researcher level) from Rennes Métropole.

BEST PAPERS AWARDS :
[42] **MSR 2017 - Modélisation des Systèmes Réactifs**. N. BERTRAND, S. HADDAD, E. LEFAUCHEUX.

TOCCATA Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

S. Conchon has co-organized POPL'2017 (January, Paris, http://conf.researchr.org/home/POPL-2017).

C. Marché has co-organized the first joint Frama-C/SPARK day (May, Paris, http://frama-c.com/FCSD17.html), in the context of the Open Source Innovation Spring (http://www.open-source-innovation-spring.org/).

S. Boldo and G. Melquiond have published a book: Computer Arithmetic and Formal Proofs, Verifying Floating-point Algorithms with the Coq System [32].

5.1.1. Awards

M. Pereira and R. Rieu-Helft received the "Best student team" award, and J.-C. Filliâtre the "Best overall team" award, at the *VerifyThis@ETAPS2017 verification competition*.

VERIDIS Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

Jasmin Blanchette, Mathias Fleury, and Christoph Weidenbach were invited to submit a short version of their IJCAR 2016 paper "A Verified SAT Solver Framework with Learn, Forget, Restart, and Incrementality" (which had received the Best Paper Award) to the Sister Conference Best Paper Track of IJCAI 2017 [25]. The paper was also invited to a special issue of *Logical Methods in Computer Science*.

The paper "A Formal Proof of the Expressiveness of Deep Learning" [22] by Jasmin Blanchette et al., presented at ITP 2017, has been invited to a special issue of the *Journal of Automated Reasoning*.

The paper "Decidability of the Monadic Shallow Linear First-Order Fragment with Straight Dismatching Constraints" [39] by Andreas Teucke and Christoph Weidenbach presented at CADE 26 has been invited to a special issue of the *Journal of Automated Reasoning*.

Two systems developed in the context of the SMArT project were submitted to the SMT competition SMT-COMP 2017. Redlog won the non-linear real arithmetic (NRA) category, and veriT+Redlog performed nicely on the quantifier-free non-linear real arithmetic (QF_NRA) category.

CARTE Team

5. Highlights of the Year

5.1. Highlights of the Year

We worked on the computable aspects of an elementary problem in real analysis: extending a continuous function on a larger domain. More precisely, if a real-valued function f is defined on an interval $[0, a)$ (with $0 < a < 1$) and is computable there, under which conditions can it be extended to a computable function on $[0, 1]$? Our results show how the answer depends on a and on the way f converges at a. This provides new characterizations of already existing classes of real numbers previously defined in computability theory. Our work was presented at LICS 2017 [19].

CIDRE Project-Team

5. Highlights of the Year

5.1. Highlights

This year, the CIDRE team would like to emphasize the following publications that appeared in major academic venues:

- Formal verification of an information flow monitor, presented at SEFM'17 [11]. See below (5.1.1) for a more complete description of this work.
- Automated quantitative information flow analysis for imperative deterministic programs, presented at POPL'17 [8].
- Reconstruction of connectivity graph for cloud infrastructures, presented at NCA'2017 [17]
- Co-processor-based Behavior Monitoring: Application to the Detection of Attacks Against the SMM, presented at ACSAC'17 [10]

5.1.1. Awards

Laurent Georget, Mathieu Jaume (LIP6), Guillaume Piolle, Frédéric Tronel and Valérie Viet Triem Tong received the best paper award at the SEFM'17 conference , which is a well established conference focused on the link between software development and formal methods. This publication is based on the work realized by Laurent Georget during his PhD. It focuses on the automated verification of the correctness of an information flow monitor that operates at the kernel level (Linux kernel). This information flow monitor relies on the Linux Security Module (LSM hereafter) framework. This framework has been designed for mandatory access control. This work tries to answer the question of its correctness when used for information flow monitoring. The verification is operated by a GCC plugin during the compilation phase of a full Linux kernel. Based on an ad-hoc static analysis, it can determine if the LSM hooks are correctly placed with respect to a property of complete mediation of systems calls. Each system call that is known to generate an information flow during its execution (34 system calls on a grand total of 340) is analyzed to determine if the LSM framework through the hooks it provides can intercept each execution that potentially generates an information flow. We have demonstrated that for 4 system calls, the hooks are not well placed, and discovered that 4 systems calls are simply lacking LSM hooks. A patch has been produced to improve this situation.
BEST PAPERS AWARDS :
[11] **15th International Conference on Software Engineering and Formal Methods (SEFM 2017)**. L. GEORGET, M. JAUME, G. PIOLLE, F. TRONEL, V. VIET TRIEM TONG.

COMETE Project-Team (section vide)

DATASPHERE Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Awards

Kavé Salamatian has been awarded in 2018 a President's International Fellowship of the Chinese Academy of Sciences.

PESTO Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

The paper [3] is listed in ACM Computing Reviews' 21st Annual Best of Computing list of notable books and articles [0] for 2016.

The voting system Belenios, developed in the Pesto and Caramba teams, has served as a basis of the development of two industrial systems (Docapost and Orange).

A 4-year ANR project on *Protocol Analysis — Combining Existing Tools* (TECAP) has been accepted. It will start in 2018 with Vincent Cheval as project leader.

[0] http://www.computingreviews.com

PRIVATICS Project-Team

4. Highlights of the Year

4.1. An Privacy Risk Analysis of the TES system

The decree of 28 October 2016 authorising the creation of a centralised file of "secure electronic documents" (TES) has raised a certain number of questions and concerns. The main aim put forward by the French government is the fight against identity fraud. However, the text of the decree also authorises certain accesses to the database by officers of the national police, national Gendarmerie and intelligence. Many voices have been raised to highlight the risks that such a centralised file could represent with regard to individual freedom, and particularly the invasion of citizens' privacy. The strengthening of the means to fight fraud (and, more generally, criminality) and the requirement to protect privacy are not necessarily in contradiction. However, in order to be able to reach a decision on the advantages and disadvantages of a management system for electronic documents, it seemed necessary to: (1) Clearly define the desired functionalities and the advantages that can be expected from them, in particular with respect to the current situation and other solutions. (2) Describe the technical solution chosen in a sufficiently precise way to enable its analysis. (3) Rigorously analyse the risks of an invasion of privacy with regard to the expected benefits.

As a contribution to this debate, we have analyzed several architectures and alternative solutions which are described in an Inria Analysis Note [15]. This note received a lot of attention, and was partially covered by several high-audience media.

4.2. A Novel Authentication Scheme based on Implicit Memory

Selecting and remembering secure passwords puts a high cognitive burden on the user, which has adverse effects on usability and security. Authentication schemes based on implicit memory can relieve the user of the burden of actively remembering a secure password. In [8], we propose a new authentication scheme (MooneyAuth) that relies on implicitly remembering the content of previously seen Mooney images. These images are thresholded two-tone images derived from images containing single objects. Our scheme has two phases: In the enrollment phase, a user is presented with Mooney images, their corresponding original images, and labels. This creates an implicit link between the Mooney image and the object in the user's memory that serves as the authentication secret. In the authentication phase, the user has to label a set of Mooney images, a task that gets performed with substantially fewer mistakes if the images have been seen in the enrollment phase. We applied an information-theoretical approach to compute the eligibility of the user, based on which images were labeled correctly. This new dynamic scoring is substantially better than previously proposed static scoring by considering the surprisal of the observed events. We built a prototype and performed three experiments with 230 and 70 participants over the course of 264 and 21 days, respectively. We show that MooneyAuth outperforms current implicit memory-based schemes, and demonstrates a promising new approach for fallback authentication procedures on the Web. This work was published at ISOC NDSS'17, one of top conferences in security and privacy.

PROSECCO Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

- We published 20 papers at top-tier conferences such as POPL (2), IEEE S&P (2), ACM CCS (1), IEEE CSF (1), ICFP (1), PETS (1), and IEEE Euro S&P (2).
- Bruno Blanchet published a paper on the applied pi calculus in the prestigious Journal of the ACM.
- The HACL* verified cryptographic library developed in our group was integrated into Mozilla Firefox 57 and is being actively used by hundreds of millions of users around the world.
- We organized the second edition of the IEEE Euro S&P Conference in Paris, which was attended by over 200 security researchers from around the world.

5.1.1. Awards

- Karthikeyan Bhargavan, Bruno Blanchet, and Nadim Kobeissi won a Distinguished Paper award at IEEE S&P 2017 .
- Catalin Hritcu was awarded a new DARPA SSITH grant called HOPE with DRAPER Labs.
- Antoine Delignat-Lavaud received an “accessit” for the prix de thèse GDR GPL 2016.

BEST PAPERS AWARDS :
[24] **38th IEEE Symposium on Security and Privacy**. K. BHARGAVAN, B. BLANCHET, N. KOBEISSI.

TAMIS Team

5. Highlights of the Year

5.1. Highlights of the Year

"Chaire Analyse de Menaces" (Threat Analysis)

Participants: Axel Legay, Fabrizio Biondi

Creation of the "Chaire Analyse de Menaces" (Threat Analysis), that has been assigned to Fabrizio Biondi.

Thales Air Operations partnership

Participants: Axel Legay, Louis-Marie Traonouez

Creation of a partnership with Thales Air Operations for machine learning algorithms to detect anomalies in ground-to-air communications.