RESEARCH CENTER

FIELD
Algorithmics, Programming, Software and Architecture

Activity Report 2013

Section highlights of the Team

Edition: 2014-03-20

ALGORITHMICS, COMPUTER ALGEBRA AND CRYPTOLOGY

ARCHITECTURE, LANGUAGES AND COMPILATION

EMBEDDED AND REAL TIME SYSTEMS

EMBEDDED AND REAL-TIME SYSTEMS

PROGRAMS, VERIFICATION AND PROOFS

PROOFS AND VERIFICATION

SECURITY AND CONFIDENTIALITY

ARIC Project-Team

2.2. Highlights of the Year

- Jean-Michel Muller received the CNRS-INS2I silver medal.
- Damien Stehlé was awarded a “starting” ERC grant for his project “Euclidean lattices: algorithms and cryptography” (LattAC).
- Vincent Lefèvre, Nicolas Louvet, and Jean-Michel Muller received the “Prix La Recherche pour les Sciences de l’Information”.

CARAMEL Project-Team

2.2. Highlights of the Year

- A spectacular new result has been obtained in the context of the cryptanalysis of the discrete logarithm problem in certain types of fields [22]. The complexity for solving this hard problem has been reduced from « sub-exponential » complexity, roughly $\exp(O(n^{1/3}))$ for an input size n, to the much lower « quasi-polynomial » complexity written as $\exp(O((\log n)^2))$. As a result, a whole range of cryptographic proposals have lost momentum, notably proposals related to pairing-based cryptography over small characteristic fields.
- Still in the realm of the computation of discrete logarithm, a new record computation has been completed by the team for binary fields of *prime* extension degree [15], using the Function Field Sieve algorithm. This establishes a useful comparison point between the Function Field Sieve and the newly proposed algorithm discussed above.
- The 2.0 release of the CADO-NFS software package, developed by the team, was made available in november. This releases incorporates an important number of improvements over the previous release which was 2 years earlier. CADO-NFS is available from the project page http://cado-nfs.gforge.inria.fr/.

CASCADE Project-Team (section vide)

CRYPT Team

2.3. Highlights of the Year

Phong Nguyen and Xiaoyun Wang obtained a 973 grant from China's Ministry of Science and Technology (MOST): the so-called 973 grants are China's largest grants for fundamental research.

BEST PAPER AWARD :

[19] **ISSAC '13 - 38th international symposium on International symposium on symbolic and algebraic computation**. J. BI, Q. CHENG, M. ROJAS.

GEOMETRICA Project-Team

2.2. Highlights of the Year

Jean-Daniel Boissonnat has obtained an "advanced" grant from the ERC (European Research Council) for his project Gudhi : Geometry Understanding in Higher Dimensions.

GRACE Project-Team

2.2. Highlights of the Year

- *Number-Theoretic Algorithms for Asymmetric Cryptology* Workshop. On June 20 and 21, 2013, GRACE hosted an international workshop on number-theoretic algorithms for asymmetric cryptology (with the support of Digicosme). Our invited speakers included Steven Galbraith (Auckland), Florian Hess (Oldenburg), Razvan Barbulescu (LORIA), Andreas Enge (Inria Bordeaux), Antoine Joux (UVSQ and Cryptoexperts), and Vadim Lyubashevsky (Inria Paris–Rocquencourt). Forty researchers attended over the two days. This workshop saw the first public announcement and presentation of what is undoubtedly the most remarkable new result in algorithmic number theory in 2013, if not the last decade: Barbulescu, Gaudry, Joux, and Thomé's quasi-polynomial time algorithm for discrete logarithms in a large class of finite fields.
- ISN-Privacy. In year 2013, N. Boujemaa's proposal for an *Institut de la société du numérique* (Digital Society Institute) was accepted within IDEX Paris-Saclay. This proposal aims to foster interdisciplinary research involving both computer scientists and researchers in the humanities. Daniel Augot joined researchers from project-teams COMETE (Saclay) and SMIS (Paris–Rocquencourt) in regular monthly discussions with economists and lawyers; a seminar will be held in Summer 2014. Funding was allocated from the IDEX to the PAIP (*Pour une Approche Interdisciplinaire de la Privacy*) project for all the partners of the privacy group.
- A special issue of *Designs, Codes and Cryptography* co-edited by Daniel Augot, devoted to the WCC2011 conference proceedings, was published in January 2013 [16].

LFANT Project-Team

2.2. Highlights of the Year

V. Verneuil's PhD thesis work, co-supervised by K. Belabas and carried out in the company Inside Secure, has been awarded the "Prix de thèse AMIES 2013" of AMIES, l'Agence pour les Mathématiques en Interaction avec l'Entreprise et la Société. The prize recognises outstanding work securing elliptic curve cryptographic systems against side-channel attacks on smartcards and an exceptional integration into the company, see http://www.agence-maths-entreprises.fr/a/?q=fr/node/292.

After two years of development, version 2.6.0 of the Pari/GP computer algebra system has been released, incorporating numerous improvements related to the programming language and the implementation of number fields, finite fields and elliptic curves. The new release maintains Pari/GP as the world leader for number theoretic computations.

POLSYS Project-Team

2.2. Highlights of the Year

- Mohab Safey El Din was invited speaker in the International Symposium on Symbolic and Algebraic Computation (ISSAC), held in Boston, June 26-29, 2013.
- In [6] we investigate the security of HFE and Multi-HFE schemes. Our attacks are based on solving the MinRank problem. We prove that they are polynomial in the degree of the extension field for all possible practical settings used in HFE and Multi-HFE.
- In [11] we consider an algorithm to solve the DLP problem on Edwards curves, which are a well-known family of elliptic curves. We exploit the symmetries and the structure of twisted Edwards and twisted Jacobi intersections curves to gain an exponential factor $2^{\omega(n-1)}$ in the complexity bound where ω is the exponent of matrix multiplication.
- In [17] we give an explicit upper bound for the algebraic degree and an explicit lower bound for the absolute value of the minimum of a polynomial function on a compact connected component of a basic closed semialgebraic set when this minimum is not zero and is attained.

SECRET Project-Team

2.2. Highlights of the Year

- *Cryptanalysis of several recently proposed lightweight block ciphers:* The area of lightweight primitives has drawn considerable attention over the last years, due to the need for low-cost cryptosystems for several emerging applications like RFID tags and sensor networks. The strong demand from industry has led to the design of a large number of lightweight block ciphers, with different implementation features. In this context, the need for a significant cryptanalysis effort is obvious. The demand from industry for clearly recommended lightweight ciphers requires that the large number of these potential candidates be narrowed down. In this context, the project-team has obtained cryptanalytic results on several recently proposed lightweight block ciphers, including an attack against the full cipher KLEIN-64, the best known attack against a round-reduced version of PRINCE, and some distinguishers on the internal permutation of LED.
- *Cryptanalysis of a variant of the McEliece public-key cryptosystem based on some wild Goppa codes:* The original McEliece cryptosystem proposed in 1978 uses the class of classical binary Goppa codes as private codes. Many other classes of codes have been suggested since the original proposal, but most of them have been cryptanalysed, while the class of Goppa codes still resists all structural attacks. Then, the use of a more general family of Goppa codes over $\mathbf{F}_q$, $q \geq 2$, named wild Goppa codes, has been proposed in 2010 by Bernstein *et al.* in order to reduce the key size of the system. Our recent work leads to an attack which allows to recover the private key in polynomial time when wild Goppa codes over a quadratic finite field extension are used. This is the very first structural attack of the McEliece cryptosystem when some Goppa codes are used. The key-point in the attack is the behaviour of these codes with respect to component-wise product of codes. A similar technique has also been exploited for breaking some other variants of the McEliece system, including one based on Reed-Solomon codes.
- *Experimental demonstration of long-distance continuous-variable quantum key distribution:* Distributing secret keys with information-theoretic security is arguably one of the most important achievements of the field of quantum information processing and communications. The rapid progress in this field has enabled quantum key distribution in real-world conditions and commercial devices are now readily available. Quantum key distribution systems based on continuous variables provide the major advantage that they only require standard telecommunication technology. However, to date, these systems have been considered unsuitable for long-distance communication. In collaboration with experimental groups, we have overcome all previous limitations and demonstrated for the first time continuous-variable quantum key distribution over 80 km of optical fibre. Our results correspond to an implementation guaranteeing the strongest level of security for quantum key distribution reported so far for such long distances and pave the way to practical applications of secure quantum communications.

Specfun Team

2.3. Highlights of the Year

This year, we complete a first work emblematic of the interdisciplinary activity of the team: a computer-algebra based formal proof of irrationality of the mathematical constant $\zeta(3)$, that is, the evaluation at 3 of the Riemann zeta function of number theory. This motivated collateral enhancements of libraries for the interactive theorem prover Coq. This is described in more details in the new results.

VEGAS Project-Team (section vide)

ALF Project-Team (section vide)

ATEAMS Project-Team

2.2. Highlights of the Year

- Paul Klint was Knighted Officer in the order of Oranje Nassau based on his contributions to science and education.
- Paul Klint was appointed Research Fellow, Centrum Wiskunde & Informatica

CAIRN Project-Team

2.2. Highlights of the Year

The paper has been nominated for the best paper award at IEEE/ACM ICCAD, one of the major event in Design Automation.

BEST PAPERS AWARDS :

[56] **IEEE/ACM International Conference on Computer-Aided Design (ICCAD)**. K. PARASHAR, D. MENARD, O. SENTIEYS.

CAMUS Team

2.2. Highlights of the Year

- Sept. 2013, Cédric Bastoul joined the CAMUS team as a Professor of the University of Strasbourg.

COMPSYS Project-Team

2.5. Highlights of the Year

For 2013, from the point of view of organization, funding, collaborations, the main points to highlight are:

- The Zettice startup project, initiated by Alexandru Plesco and Christophe Alias, won the *concours OSEO 2013* grant (Banque Publique d'Investissement, 40 Keuros) and the *"most promising start-up award"* at SAME 2013. See more details in Section 7.3 .
- Laure Gonnord was hired as assistant professor at ENS-Lyon, she is now a permanent member of Compsys. Fabrice Rastello has left Compsys and will continue his research in Grenoble.
- The collaborations with Colorado State University (S. Rajopadhye) and Ohio State University (Sadayappan) were very successful. New topics of collaboration with the Inria Parkas and Camus teams have started.
- From April 2013 to July 2013, Compsys organized 4 scientific events on compilation, regrouped in a larger and coherent *thematic quarter on compilation* [2], with international audience and visibility. It was mainly funded by the Labex MILYON, see details in Section 9.1 .

From a scientific point of view, the shift, in Compsys III, towards the analysis of parallel programs, the extensions of the polyhedral model, both in terms of techniques and applications, and the code optimizations based on trace analysis has been already fruitful, see the section "New Results", in particular:

- Innovative contributions on parametric tiling [8], [5] as extensions of the polyhedral model.
- A groundbreaking introduction of polyhedral techniques for the analysis of parallel programs, in particular X10 [10], [7].
- Several important contributions (e.g., [2]) that demonstrate the interest of mixing trace analysis and static analysis for code (in particular locality) improvements.

[2] http://labexcompilation.ens-lyon.fr

CONTRAINTES Project-Team (section vide)

DREAMPAL Team (section vide)

INDES Project-Team (section vide)

PAREO Project-Team (section vide)

TASC Project-Team

2.2. Highlights of the Year

1. Best young researcher paper for Jean-Guillaume Fages and Tanguy Lapègue at the 19th International Conference on Principles and Practice of Constraint Programming.
2. Silver medal for the library Choco at the MiniZinc International Challenge 2013 in the *open class* category.
3. Silver medal for the library Choco at the MiniZinc International Challenge 2013 in the *parallel search* category.
4. Bronze medal for Florian Richoux at the AI competitions organized at the conferences AIIDE 2013 and CIG 2013 for developing an artificial intelligence, AIUR, to play the real time strategy game $StarCraft^{tm}$, using both machine learning and constraint-based techniques.

BEST PAPERS AWARDS :

[30] **19th International Conference on Principles and Practice of Constraint Programming (CP'13)**. J.-G. FAGES, T. LAPÈGUE.

ESPRESSO Project-Team

2.4. Highlights of the Year

Polarsys is an Eclipse Industry Working Group focusing on open source tools for the development of embedded systems. After previous years experimentation, POP, A Polychronous Modeling Environment on Polarsys, has been approved as open source project under the Polarsys Top-Level Project, which is operating under the auspices of the Polarsys Industry Working Group.

S4 Project-Team

2.2. Highlights of the Year

TRIO Team

2.2. Highlights of the Year

This is the last activity report of TRIO team, as the team ends in 2013. TRIO has been, originally, created in 2002 under the guidance of Françoise Simonot-Lion. In 2010, when Françoise became director of Laboratoire Lorrain de Recherche en Informatique et ses Applications (LORIA), Nicolas Navet became the leader of the team. In 2012, when Nicolas Navet became Professor at University of Luxembourg, Liliana Cucu-Grosjean became the last leader of TRIO team. The team ends on an excellent Inria evaluation in 2012 that underlines the important contribution of its members within their scientific communities. Following the natural life process of an Inria team, the end of TRIO indicates the evolution of its members to new exciting research problems.

Liliana Cucu-Grosjean gave the keynote talk of the 21st International Conference on Real-Time Networks and Systems. Her talk concerned the probabilistic real-time systems.

Dorin Maxim and Liliana Cucu-Grosjean published a paper entitled "Response Time Analysis for Fixed-Priority Tasks with Multiple Probabilistic Parameters" at the IEEE Real-Time Systems Symposium (RTSS), the flag conference on real-time systems.

The FP7 STREP PROARTIS has been successfully completed in July 2013. TRIO was leader of the work package on the probabilistic approaches and tools within this project.

AOSTE Project-Team

2.2. Highlights of the Year

The 2013 edition of the RTNs conference was organized in Sophia-Antipolis, with Robert de Simone as General Chair and Liliana Cucu-Grosjean as keynote speaker. Rob Davis, from the University of York, was granted a five-year Inria International Chair position in our team at Rocquencourt.

CONVECS Project-Team (section vide)

Hycomes Team

2.1. Highlights of the Year

Albert Benveniste has been elected IFAC Fellow [1] for his fundamental contributions to stochastic systems theory, and for connecting control, signal processing, and real-time software development.

[1] http://www.ifac-control.org/awards/ifac-fellows

MUTANT Project-Team

2.2. Highlights of the Year

Figure 2. Antescofo presentation and demo in Bercy, Ministry of Industry.

Antescofo has been awarded the Industry prize by the French Minister of Industry, for its R&D and upcoming industrial applications.

Antescofo has been presented at the MIF Show (salon Made In France) invited by the ministère du redressement productif (November 2013).

Invited Demonstration at the 10th anniversary of La Recherche Prize.

PARKAS Project-Team

2.2. Highlights of the Year

Robin Morisset was Awarded a Google Doctoral Fellowship.

Louis Mandel and Marc Pouzet received a reward for the paper introducing the ReactiveML language for the first time and presented at the French conference JFLA 2005 (“On the occasion of this quarter century, the program committees and steering selected four outstanding contributions from the articles published in JFLA past decade.")

Louis Mandel has been hired in Sept. 2014 at Collège de France, as an Assistant Professor.

SPADES Team (section vide)

FORMES Team

2.3. Highlights of the Year

The project has released a new version of its **SimSoC** simulation software, as an open source software release 0.8, available from http://gforge.inria.fr/projects/simsoc/

SECSI Project-Team (section vide)

ABSTRACTION Project-Team

2.2. Highlights of the Year

Patrick and Radhia Cousot have received in 2013 the SIGPLAN Achievement award, for the invention, development, and application of abstract interpretation http://www.sigplan.org/Awards/Achievement/Main.

CELTIQUE Project-Team

2.2. Highlights of the Year

The European Association for Programming Languages and Systems (EAPLS) Best PhD Dissertation Award 2012 has been won by Delphine Demange (ENS Cachan - Brittany Extension and the Celtique team at IRISA / Inria Rennes, advisors Thomas Jensen and David Pichardie), for her dissertation on "Semantic Foundations of Intermediate Program Representations".

The thesis prize Gilles Kahn 2013, awarded by the Société Informatique de France (SiF) and sponsored by Academy of Sciences, was awarded to Delphine Demange for her dissertation "Semantic Foundations of Intermediate Program Representations" (ENS Cachan - Brittany Extension and the Celtique team at IRISA / Inria Rennes, advisors Thomas Jensen and David Pichardie).

DEDUCTEAM Exploratory Action

2.3. Highlights of the Year

The Version 2 of Dedukti has been released. Gilles Dowek has been invited speaker to CSR, Hapoc, and to the Colloquium of the University Pierre et Marie Curie. David Delahaye has been an invited speaker of PSATTT.

GALLIUM Project-Team

2.2. Highlights of the Year

Didier Le Botlan (INSA Toulouse) and Didier Rémy received the ACM SIGPLAN Most Influential ICFP Paper Award for their ICFP 2003 paper, *MLF: Raising ML to the power of System F* [44].

MARELLE Project-Team (section vide)

MEXICO Project-Team

2.2. Highlights of the Year

- We have made two major progresses in diagnosis this year:
  - For non-diagnosable discrete event systems, *active* diagnosis aims at synthesizing a partial-observabion based control for the system in order to make it diagnosable. While some solutions had already been proposed for the active diagnosis problem, their complexity remained to be improved. In [40], we solved both the active diagnosability decision problem and the active diagnoser synthesis problem, proving that (1) our procedures are optimal w.r.t. to computational complexity, and (2) the memory required for the active diagnoser produced by the synthesis is minimal. Furthermore, focusing on the minimal delay before detection, we establish that the memory required for any active diagnoser achieving this delay may be highly greater than the previous one. So we refine our construction to build with the same complexity and memory requirement an active diagnoser that realizes a delay bounded by twice the minimal delay. An extension to *probabilistic* systems has been accepted to *FoSSaCS 2014.*
  - In [41], we present a methodology for fault diagnosis in concurrent, partially observable systems with additional fairness constraints. In this *weak* diagnosis, one asks whether a concurrent chronicle of observed events allows to determine that a non-observable fault will inevitably occur, sooner or later, on any maximal system run compatible with the observation. The approach builds on strengths and techniques of unfoldings of safe Petri nets, striving to compute a compact prefix of the unfolding that carries sufficient information for the diagnosis algorithm. Our work extends and generalizes the unfolding-based diagnosis approaches by Benveniste et al. as well as Esparza and Kern. Both of these focused mostly on the use of sequential observations, in particular did not exploit the capacity of unfoldings to reveal inevitable occurrences of concurrent or future events studied by Balaguer et al. [19]. Our diagnosis method captures such indirect, revealed dependencies. We develop theoretical foundations and an algorithmic solution to the diagnosis problem, and present a SAT solving method for practical diagnosis with our approach.
- The article *Complexity Analysis of Continuous Petri Nets* by Estébaliz Fraca and Serge Haddad [39] received the *outstanding paper award* at the *International Conference on Application and Theory of Petri Nets and Concurrency, June 24-28, 2013, Milano, Italy.*

BEST PAPER AWARD :

[39] **34th International Conference on Applications and Theory of Petri Nets (ICATPN'13)**. E. FRACA, S. HADDAD.

PARSIFAL Project-Team

2.2. Highlights of the Year

- The team organized the LIX Colloquium 2013: The Theory and Application of Formal Proofs, November 5–7. Webpage: http://www.lix.polytechnique.fr/colloquium2013/

PI.R2 Project-Team

2.2. Highlights of the Year

The Coq team received the 2013 ACM SIGPLAN Programming Language Software Award, which was presented at POPL'14 in San Diego. To quote: "The Programming Languages Software Award is given by ACM SIGPLAN to an individual or an institution to recognize the development a software system that has had a signicant impact on programming language research, implementations, and tools. The impact may be reflected in the wide-spread adoption of the system or its underlying concepts by the wider programming language community either in research projects, in the open-source community, or commercially."

SUMO Team

2.2. Highlights of the Year

- Loïc Hélouët and Hervé Marchand were co-chairs of the conference MSR 2013 (Modélisation des Systèmes Réactifs), located in Rennes this year and organized by SUMO (Laurence Dinh, Loïc Hélouët, Hervé Marchand and Paulin Fournier).
- ANR Stoch-MC has been accepted in 2013, led by SUMO (Blaise Genest (PI), Nathalie Bertrand and Éric Fabre). Its aim is to provide scalable algorithms to analyse stochastic systems.

TOCCATA Team

2.2. Highlights of the Year

- The *Castor informatique*http://castor-informatique.fr/, is an international competition to present computer science to pupils (from *6ème* to *terminale*). More than 170,000 teenagers played on more than 30 proposed exercises in November 2013. Two members of the Toccata team (S. Boldo and A. Charguéraud) belong to the organization committee (5 people).
- The full formalization of the JavaScript language specification (ECMAScript 5) was recently completed by the *JsCert* team [24], which includes A. Charguéraud and 7 collaborators from Imperial College and Inria Rennes (http://jscert.org). The formalization, which involves more than 10,000 lines of code and an inductive semantics with over 600 reduction rules, is the result of 2 years of effort. It lead to the discovery of bugs in the official standard, in the official test suites, and in all major browsers. In particular, it has raised the interest of several members of the ECMAScript standardization committee, and that of the developers of secure subsets for JavaScript.
- J.-C. Filliâtre was invited as keynote speaker (“One Logic To Use Them All” [19]) at the International Conference on Automated Deduction in 2013. It is the main conference of the year in the domain of Automated Reasoning. In this talk he presented the *Why3* approach for interacting with dozens of provers on the same theories and goals. This invited talk is a recognition by the community of this unique feature of *Why3*.
- Most 18-year old French students pass an exam called Baccalaureate which ends the high school and is required for attending the university. The idea was to try our Coq library Coquelicot on the 2013 mathematics test of the scientific Baccalaureate. C. Lelay went to the “Parc de Vilgénis” high school in Massy, France and took the 2013 test at the same time as the students, but had to formally prove the answers [45] (see also https://www.lri.fr/~lelay/).
- The Coq proof assistant received the ACM *Programming Languages Software Award* in 2013 http://www.sigplan.org/Awards/Software/Main. The development of Coq was initiated by Thierry Coquand and Gérard Huet in 1984. The current environment is the result of the work of more than 40 direct contributors, including major contributions by Christine Paulin-Mohring and Jean-Christophe Filliâtre from our team.

VERIDIS Project-Team

2.2. Highlights of the Year

Uwe Waldmann received a LICS Test of Time Award for the paper “Set constraints are the monadic class” published at LICS 1993 together with Leo Bachmair and Harald Ganzinger. He also won the TFA category (typed first-order logic with arithmetic) of the CADE ATP System Competition 2013 using the prover SPASS+T.

Pascal Fontaine was the main organizer and program committee chair (with Christophe Ringeissen and Renate Schmidt) of FroCos 2013 in September in Nancy.

CARTE Project-Team

2.2. Highlights of the Year

Our team made remarkable progress into the difference between “real world” systems and artefacts due to exact (infinite) precision computations. Olivier Bournez, Daniel Graça and Emmanuel Hainry succeeded in proving an equivalence between robustness and computability: Robust dynamical systems have computable dynamical properties [12], a strong evidence that “real world” systems will not exhibit undecidability properties.

Another highlight of the year is a paper by Hugo Férée, Mathieu Hoyrup and Walid Gomaa, accepted in LICS 2013 [19] that provides a systematic approach to define and analyse the complexity of algorithms acting on infinite precision numbers (infinite words).

CASSIS Project-Team

2.4. Highlights of the Year

- We have released the first version of *Belenios*, an electronic voting protocol based on a previous system, Helios. *Belenios* is an open-source voting system that offers transparent and verifiable elections. We have also signed a contract with a French company on electronic voting, Voxaly, to discuss their solution and a possible adaptation to *Belenios*' concepts.
- We have found a weakness in the biometric passports: under certain circumstances, it is possible to trace a passport holder, despite the existing security measures. Our flaw has been reported in the journals “Pour la Science” and “Journal du CNRS”.

COMETE Project-Team (section vide)

DICE Team

2.2. Highlights of the Year

The team has been launched this year and has gained some visibility after a tribune in the French daily Le Monde which obtained more than 1500 "like" on the day of its publication.

"Les données, puissance du futur", S. Grumbach, S. Frénot, Le Grand Débat, Le Monde, 8 janvier 2013

PRIVATICS Team

2.2. Highlights of the Year

The project Mobilitics has made significant advances in the context the Inria-CNIL convention in 2013. Major improvements have been made in the software, which include new capabilities and improved analysis (even for encrypted streams) for the two major systems that are iOS 6.2 and Android 4.1. A first phase of experiments for iOS took place in early 2013 with volunteers from the CNIL. It resulted in a press conference (April 2013) and a large media exposure. A second phase of experiments will take place in 2014 for Android. More targeted work on the our side also led to advances in understanding the ecosystem of mobile applications and the flows of personal information.

We have published at CODASPY 2013 [33] a new formal framework for the analysis of architectural choices. The privacy by design approach has already been put into practice in different application areas. We believe that the next challenge today is to go beyond individual cases and to provide methodologies to explore the design space in a systematic way. As a first step in this direction, we focus on the data minimization principle and consider different options using decentralized architectures in which actors do not necessarily trust each other. We propose a framework to express the parameters to be taken into account (the service to be performed, the actors involved, their respective requirements, etc.) and an inference system to derive properties such as the possibility for an actor to detect potential errors (or frauds) in the computation of a variable. This inference system can be used in the design phase to check if an architecture meets the requirements of the parties or to point out conflicting requirements.

PROSECCO Project-Team

2.2. Highlights of the Year

This year, we published 6 articles in international journals and 11 articles in peer-reviewed international conferences, including presitigious conferences such as IEEE S&P (1), ACM CCS (2), Usenix Security (1), ESORICS (2), and POST (3). In addition to these, we published 1 PhD thesis and several technical reports. We also have 3 articles already accepted for publication in international conferences in 2013: POPL (2), NDSS (1).

We released updates to several verification tools and software packages. We discovered and reported major security vulnerabilites in dozens of commercial software packages, hardware devices, and websites. The work of our group also spun-off a new startup company created by Graham Steel, and we continue to collaborate with this startup.

Of our work published in 2013, we would like to highlight the following:

- Our paper in IEEE S&P 2013 [21] presents the first cryptographically verified implementation of TLS.
- Our work on the computational analysis of cryptographic protocols yielded new results and major publications [19], [26].
- Our work on formally analyzing web application security uncovered major attacks on browsers and websites and proposed novel language-based verified solutions [20], [29], [25].