RESEARCH CENTER
Saclay - Île-de-France

FIELD

Activity Report 2015

Section Highlights of the Team

Edition: 2016-03-21

COMETE Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Awards

- SIGSAC Doctoral Dissertation Award 2015 for the thesis “Measuring Privacy with Distinguishability Metrics: Definitions, Mechanisms and Application to Location Privacy” [29] by Nicolás Bordenabe (Defended on Sep 12, 2014)
- Prix de thèse de l’Ecole Polytechnique 2015 for the thesis “Measuring Privacy with Distinguishability Metrics: Definitions, Mechanisms and Application to Location Privacy” [29] by Nicolás Bordenabe (Defended on Sep 12, 2014)

GEOMETRICA Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Awards

Clément Maria has been awarded the Prix de thèse Gilles Kahn - Académie des Sciences.

5.1.2. Books

Steve Oudot published a book on persistence theory in the AMS series *Mathematical Surveys and Monographs* [35].

GRACE Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

Freestart collision for the full SHA-1.

Together with M. Stevens and T. Peyrin, P. Karpman gave the first freestart collision for the full SHA-1 hash function [32]. Although theoretical attacks on this function were known since 2005, this work is an important milestone in SHA-1 cryptanalysis and it had a concrete impact on the use of SHA-1 in existing systems, such as TLS certificates. In particular, the CA/Browser forum (which regroups some of the major industries of the internet) withdrew an internal ballot proposing to extend the use of SHA-1 in new certificates through 2016. Major browser developers such as Mozilla are also encouraging the timely withdrawal of SHA-1 certificates by updating the in-browser security warnings when such certificates are used. This result was also vulgarised in technical press such as *Ars Technica* and more general newspapers such as *Le monde*.

Discrete logarithm record computation in finite fields

F. Morain and A. Guillevic together with P. Gaudry (CARAMEL team, Inria Nancy Grand Est) and R. Barbulescu (CNRS, IMJ) published a new discrete logarithm record in a finite field of 180 decimal digits (dd), i.e. 595 bits. This result was presented at the Eurocrypt 2015 conference [19]. The Discrete Logarithm Problem (DLP) is widely studied in prime fields GF(p) and was broken in small characteristic finite fields of the form GF(2^n) and GF(3^n) with smooth n very recently. It was not known whether the DLP is as hard in extensions of finite fields compared to prime fields, for the same global size. With this record of the same size as the most recent record in a prime field, F. Morain and A. Guillevic showed that DLP in GF(p^2) is much faster than in a prime field of the same size, and even faster than a factorization of an RSA modulus of the same size.

Table 1. Comparison of running time for integer factorization (NFS-IF), discrete logarithm in prime field (NFS-DL(p)) and in quadratic field (NFS-DL(p 2)) of same global size 180 dd.

Algorithm	relation collection	linear algebra	total
NFS-IF	5 years	5.5 months	5.5 years
NFS-DL(p)	50 years	80 years	130 years
NFS-DL(p^2)	157 days	18 days (GPU)	0.5 years

F. Morain and A. Guillevic contributed with P. Gaudry and E. Thomé to other DL computation records in finite fields GF(p^3) of 508 bits and 512 bits, and GF(p^4) of 392 bits. The practical difficulty is increasing with the extension degree.

CATREL conference

The 1st and 2nd of October 2015, F. Morain, B. Smith and A. Guillevic organized an international workshop to conclude the CATREL project. There were 14 invited speakers from all around the world, from Palaiseau with A. Guillevic to as far as Auckland in New Zealand with S. Galbraith. A. Joux presented an historical summary of DL computation from the 80's. P. Gaudry, E. Thomé and C. Bouvier from the Caramel Team (Inria Nancy), presented their contribution, and K. Bhargavan presented the Logjam attack. There were also members of abroad teams leader in discrete logarithm record breaking. G. Adj from Mexico and R. Granger and T. Kleinjung presented their recent records in small characteristic.

We hosted more than 50 participants for the two intensive days of the workshop. The schedule of the workshop is available on the following link. http://www.lix.polytechnique.fr/cryptologie/CATREL-workshop

AGC^{2}T 15

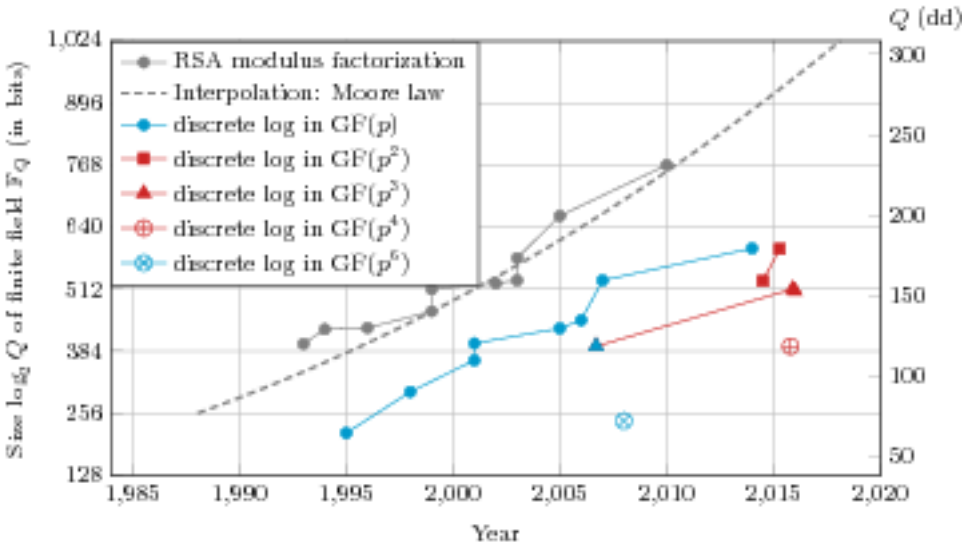

Figure 1. Records of DL computation in finite fields, and RSA modulus factorization. F. Morain and A. Guillevic contributed to the records in red in 2014–2015.

A. Couvreur was one of the organizers of the conference AGC^{2}T 15 (Arithmetic Geometry Cryptography and Coding Theory) at CIRM (Marseille).

MEXICO Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Major Results

5.1.1.1. Approaching the Coverability Problem Continuously

The coverability problem for Petri nets plays a central role in the verification of concurrent shared-memory programs. However, its high EXPSPACE-complete complexity poses a challenge when encountered in real-world instances. In [39], we develop a new approach to this problem which is primarily based on applying forward coverability in continuous Petri nets as a pruning criterion inside a backward coverability framework. A cornerstone of our approach is the efficient encoding of a recently developed polynomial-time algorithm for reachability in continuous Petri nets into SMT. We demonstrate the effectiveness of our approach on standard benchmarks from the literature, which shows that our approach decides significantly more instances than any existing tool and is in addition often much faster, in particular on large instances.

5.1.1.2. An Automata-Theoretic Approach to the Verification of Distributed Algorithms

In [21] we introduce an automata-theoretic method for the verification of distributed algorithms running on ring networks. In a distributed algorithm, an arbitrary number of processes cooperate to achieve a common goal (e.g., elect a leader). Processes have unique identifiers (pids) from an infinite, totally ordered domain. An algorithm proceeds in synchronous rounds, each round allowing a process to perform a bounded sequence of actions such as send or receive a pid, store it in some register, and compare register contents w.r.t. the associated total order. An algorithm is supposed to be correct independently of the number of processes. To specify correctness properties, we introduce a logic that can reason about processes and pids. Referring to leader election, it may say that, at the end of an execution, each process stores the maximum pid in some dedicated register. Since the verification of distributed algorithms is undecidable, we propose an underapproximation technique, which bounds the number of rounds. This is an appealing approach, as the number of rounds needed by a distributed algorithm to conclude is often exponentially smaller than the number of processes. We provide an automata-theoretic solution, reducing model checking to emptiness for alternating two-way automata on words. Overall, we show that round-bounded verification of distributed algorithms over rings is PSPACE-complete.

5.1.1.3. Unfolding-Based Process Discovery

In [33] we presents a novel technique for process discovery. In contrast to the current trend, which only considers an event log for discovering a process model, we assume two additional inputs: an independence relation on the set of logged activities, and a collection of negative traces. After deriving an intermediate net unfolding from them, we perform a controlled folding giving rise to a Petri net which contains both the input log and all independence-equivalent traces arising from it. Remarkably, the derived Petri net cannot execute any trace from the negative collection. The entire chain of transformations is fully automated. A tool has been developed and experimental results are provided.

PARSIFAL Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

Accattoli's paper with Ugo Dal Lago titled "Beta Reduction is Invariant, Indeed" that appeared in CSL-LICS 2014 was invited to a special issue of LMCS of selected papers from that meeting.

Miller ended his second and final term as the Editor-in-Chief of the ACM Transactions on Computational Logic. He remains as an Area Editor for Proof Theory.

Miller was a plenary speaker at the joint meeting of LOPSTR 2015 and PPDP 2015 (Siena, Italy) and was an invited speaker at LSFA 2015 (Natal Brazil) and in the Session on History and Philosophy of Computing at the 15th Congress of Logic, Methodology and Philosophy of Science, Helsinki.

Miller spoke at the ETH Zurich Department of Computer Science Distinguished Colloquium Series on April 20.

Graham-Lengrand gave an invited talk at the IFIP Working Group 1.6 on Term Rewriting, on the occasion of its 2015 annual meeting in Warsaw, Poland.

Accattoli was an invited speaker at the 16th International Workshop on Logic and Computational Complexity (Kyoto, Japan, 5th of July).

POSTALE Team

4. Highlights of the Year

4.1. Highlights of the Year

Marc Baboulin was invited plenary speaker at the HPCSE conference, Solan, Czech Republic, May 25-28, 2015.

The Random Butterfly Transformations developed by Postale are now available in the MAGMA library for GPU (release 1.6) and Intel Xeon Phi (release 1.3).

Marc Baboulin is general vice-chair of the HPC Symposium to be held in April 2016, Pasadena, CA.

SPECFUN Project-Team

4. Highlights of the Year

4.1. Highlights of the Year

4.1.1. Awards

Pierre Lairez has been awarded this year the “Ecole Polytechnique thesis prize”, for his PhD thesis defended in 2014 [53].

TOCCATA Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Awards

- C. Paulin-Mohring received the award "Michel Monpetit – Institut National de Recherche en Informatique et en Automatique" of the French Academy of Sciences (http://www.academie-sciences.fr/fr/Laureats/laureats-2015-prix-thematiques.html).
- J.-C. Filliâtre and G. Melquiond received the "Best team" award of the VerifyThis@ETAPS2015 verification competition (http://verifythis2015.cost-ic0701.org/results). The Why3 tool also received the "Distinguished user-assistance tool feature" award.
- The *Concours Castor informatique* (http://castor-informatique.fr/) had an even larger success than in the previous years. In November 2015, more than 345,000 teenagers from over 2280 schools participated and solved the interactive tasks of the contest. Arthur Charguéraud and Sylvie Boldo, from the Toccata team, significantly contributed to the prepation of the tasks and to the organization of the contest.

COMMANDS Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Awards

- B. Heymann received a Siebel Scholar fellowship from the Siebel foundation. These fellowships are given to top graduate students of partner institutions, namely here the Ecole Polytechnique. See the List of Siebel Scholars

DEFI Project-Team (section vide)

DISCO Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

Dec. 2015 - Frédéric Mazenc is President of the "Commission Scientifique" Inria Saclay-Ile-de-France.

GECO Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

- GECO is one of one of the partners of the ANR SRGI, which has been funded in 2015. SRGI deals with sub-Riemannian geometry, hypoelliptic diffusion and geometric control.
- In the recent preprint [23] we answer an open problem proposed by J.P. Hespanha in 2003 in the volume "Unsolved Problems in Mathematical Systems & Control Theory". The problem deals with the characterization of the finiteness of the L_2-gain of a switched linear control systems, in dependence of the value of the minimal dwell-time of its switching laws.

Maxplus Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Awards

- Pascal Benchimol obtained in June 2015 a prize of Ecole polytechnique for his PhD thesis [70].
- Best paper award for the paper presented by Nikolas Stott of EMSOFT'15.

BEST PAPERS AWARDS :
[29] **International Conference on Embedded Software (EMSOFT'2015)**. X. ALLAMIGEON, S. GAUBERT, E. GOUBAULT, S. PUTOT, N. STOTT.

POEMS Project-Team (section vide)

SELECT Project-Team (section vide)

TAO Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

- **DataScienc@LHC** First of a series of workshops officially organized at CERN - TAO leader on the ML side.

5.1.1. Awards

- Best Paper Award in the Genetic Programming track at GECCO 2015 (Madrid, July 2015) for the paper [39].
- First place in the Taxonomy Induction task of SemEval 2015 (Denver, June 2015) [55].

BEST PAPERS AWARDS :

[39] **Genetic and Evolutionary Computation COnference (GECCO 2015)**. R. FFRANCON, M. SCHOENAUER.

AMIB Project-Team

4. Highlights of the Year

4.1. Highlights of the Year

4.1.1. Keynote addresses

Y. Ponty delivered one of the 8 plenary addresses at the 5th biennial Canadian Discrete and Algorithmic Mathematics Conference (CanaDAM) in University of Saskatchewan (Saskatoon, Canada). Held every two-years, with $\sim$300 participants and $\sim$150 contributed and invited talks, CanaDAM is the foremost event in Discrete Mathematics in Canada.

4.1.2. Awards

Alice Héliou received "Prix Poster École Doctorale Interfaces,Pôle : Science Du Vivant"

GALEN Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Awards

- Pr. Iasonas Kokkinos was appointed associate editor for the Computer Vision and Image Understandin Journal.
- Pr. Pawan Kumar was appointed associate editor for the Computer Vision and Image Understandin Journal.
- Pr. Nikos Paragios was admitted as a senior fellow at the Insitut Universitaire de France in the section of Mathematics.

M3DISIM Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Awards

A. Collin (who did her PhD in the team) received the SMAI-GAMNI award 2015 for Best PhD thesis and the ECCOMAS PhD award 2015.

A. Aalto received the award for the best doctoral thesis in Aalto University School of Science during 2014.

PARIETAL Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

Michael Eickenberg got an oral presentation at the OHBM 2015 conference(success rate < 1%). Elvis Dohmatob got an oral presentation at the OHBM 2015 conference(success rate < 1%).

POPIX Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Awards

Marc Lavielle received the 2015 ISoP (International Society of Pharmacometrics) Innovation award

Marc Lavielle received the 2015 Inria – French Académie des Sciences – Dassault Systèmes Innovation Award

INFINE Team

4. Highlights of the Year

4.1. Highlights of the Year

1. In collaboration with Charles Bordenave (CNRS, Toulouse) and Marc Lelarge (Inria) we proved the so-called « spectral redemption conjecture » formulated by physicists in 2013, suggesting that a novel spectral method for community detection would perform non-trivial detection under optimal conditions. This has been presented in the IEEE FOCS conference, one of the top two theoretical computer science conferences.
2. In collaboration with Freie Universitaet Berlin we have further developed RIOT, which now aggregates open source contributions from 120+ people (and counting) from all over the world, coming both from academia and from industry.

4.1.1. Awards

Aline Viana was awarded the PEDR in 2015, the Inria award for research excellence.

AVIZ Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

We had a number of highlights this year:

- Aviz researchers contributed 29 publications this year. Amongst these seven papers were presented at IEEE VIS, the largest international Visualizations and Visual Analytics conference. Four full papers were presented at CHI, the largest international conference on human computer interaction;
- Aviz researchers organized two workshops and one tutorial at international conferences (ACM ITS, and IEEE VIS);
- Eight awards were won by Aviz researchers for papers, service contributions, and PhD theses (see below);
- We welcomed three international researchers and students to our lab for research visits;
- Aviz researchers taught four lectures at various French and international universities.

Awards

- Samuel Huron won the best thesis award at the IEEE VGTC Vis Pioneer Group Best PhD Dissertation Award for his thesis "Constructive Visualization: A Token-based Paradigm Allowing to Assemble Dynamic Visual Representation for Non-experts" []
- Jeremy Boy got an honorable mention award at the IEEE VGTC Vis Pioneer Group Best PhD Dissertation Award for his thesis "Engaging the People to Look Beyond the Surface of Online Information Visualizations" [10]
- Jean-Daniel Fekete received an IEEE TVCG service award for organizing VIS'14 in Paris
- Petra Isenberg and Tobias Isenberg received a IEEE Computer Society Certificate of Appreciation for co-chairing the http://beliv-2014.cs.univie.ac.at/index.php2014 BELIV Workshop on "Beyond Time And Errors: Novel Evaluation Methods For Visualization"
- Wesley Willet, Tobias Isenberg, and Pierre Dragicevic received a best paper award from the ACM Conference on Human Factors in Computing Systems (CHI) for their paper "Lightweight Relief Shearing for Enhanced Terrain Perception on Interactive Maps" [33].
- Charles Perin, Jeremy Boy and Frédéric Vernier received an honorable Mention (2nd prize) for "Le Tour de France at a Glance" visualiation in the IEEE VGTC/VPG International Data Visualization Contest.
- Jeremy Boy won the World Statistics Day 2015 Data Visualization Contest with his "Is the World a Better Place Today" online visualization platform.

BEST PAPERS AWARDS :

[] **Constructive Visualization**.

[33] **Proceedings of the Conference on Human Factors in Computing Systems (CHI)**. W. WILLETT, B. JENNY, T. ISENBERG, P. DRAGICEVIC.

DAHU Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Awards

Best student paper award for Nadime Francis [22] at the conference ICDT'15.

Luc Segoufin and Victor Vianu obtained the ACM Alberto O. Mendelzon PODS Test of Time Award in 2015.

EX-SITU Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Awards

Michel Beaudouin-Lafon received the ACM SIGCHI Lifetime Service Award, which "goes to individuals who have contributed to the growth and success of SIGCHI in a variety of capacities. This award is for extended services to the community at large over a number of years" (http://www.sigchi.org/about/awards/2015-sigchi-awards).

Jérémie Garcia received the "Prix Jeune Chercheur Science et Musique", a best thesis award organized by IRISA (Rennes) and sponsored by the Association Française d'Informatique Musicale for his thesis *""Le papier interactif pour la composition musicale"*, supervised by Wendy Mackay, Theophannis Tsandilas and Carlos Agon (IRCAM) (http://jsm.irisa.fr/index.php/prix-jc.

Nolwenn Maudet received the "Prix Spécial du Jury du premier concours EDUCNUM Opération Vie privée", organized by CNIL (national commission for informatics and freedom), for her project *Data Fiction* with Thomas Thibault. This online game is designed to help teenagers better understand how their personal data can be exposed online and how to protect it.

ExSitu received three paper awards. One paper, *Webstrates* [18] received a best paper award at UIST 2015. Two other papers, *Color Portraits* [17] and *SketchSliders* [20], received Honorable Mention awards at CHI 2015 (at most 5% of CHI submissions receive an Honorable Mention).
BEST PAPERS AWARDS :
[18] **28th Annual ACM Symposium on User Interface Software and Technology (UIST'15)**. C. KLOKMOSE, J. EAGAN, S. BAADER, W. MACKAY, M. BEAUDOUIN-LAFON.

ILDA Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Awards

- ACM CHI Honorable mention for **An Evaluation of Interactive Map Comparison Techniques** [4], awarded to the top 5% of all 2150 paper submissions.
- ACM CHI Honorable mention for **SketchSliders: Sketching Widgets for Visual Exploration on Wall Displays** [9], awarded to the top 5% of all 2150 paper submissions.

OAK Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Awards

I. Manolescu and X. Tannier (LIMSI) have obtained a Google Computational Research Journalism Award on "Event Thread Extraction for Viewpoint Analysis". The team has also secured an ANR contract on content management techniques applied to computational fact-checking (coordonated by I. Manolescu, to start in 2016) and an ADT engineer has joined the team to work on the same topic.

The best publications of the year appeared in SIGMOD citecamachorodriguez:hal-01178490, PODS [16], PVLDB [29], [8], [26], ICDE [15], [14], and IEEE TKDE [3]. Other highly visible publications appeared in CIDR [9] and CIKM [28], [7].

5.1.2. Inria researcher recruited

M. Thomazo has joined the team as a junior researcher (Inria CR2).