RESEARCH CENTER

FIELD
Algorithmics, Programming, Software and Architecture

Activity Report 2017

Section Popularization

Edition: 2018-02-19

ARIC Project-Team

10.3. Popularization

Nathalie Revol is a member of the steering committee of the MMI: Maison des Mathématiques et de l'Informatique, and in particular she was involved in the creation of the *Magimatique 2* exhibition. She presented some magic tricks at Bibliothèque Municipale de la Part-Dieu and at MMI for 3 classes during the Science Fair. She gave talks for a large audience during "Forum Maths Vivantes" and for "La tournée de Pi" (mathematical musical, around 600 attendees) (March 2017). As an incentive for high-school pupils, and especially girls, to choose scientific careers, she gave talks at Lycée Ella Fitzgerald (Saint-Romain-en-Gal) and Mondial des Métiers (in February 2017) and during "Journée Filles et Sciences" in Musée des Confluences and "Journée Filles" by INSA Lyon (above 550 attendees in total, March 2017). She co-organized for two "Coding gouters" organized by MixTeen. She co-organized two days on "Info Sans Ordinateur" gathering researchers interested in unplugged activities. She is a member of the editorial committee of Interstices: https://interstices.info. She taught how to disseminate (computer) science for PhD students in a 20h module of *Insertion Professionnelle*.

Bruno Salvy will give a talk at the Collège de France in December 2017 on methods of analytic combinatorics in random generation.

Damien Stehlé hosted a visit at ENS de Lyon by the regional winners of the Alkindi competition (midde highschool and highschool).

AROMATH Project-Team (section vide)

CARAMBA Project-Team

10.3. Popularization

- Pierrick Gaudry organized and participated in a debate fed by excerpts from movies on the topic of cryptography and privacy in March 2017. He also gave a podcast interview about electronic voting for Interstices [15].
- Pierre-Jean Spaenlehauer did a short presentation of asymetric cryptography to middle school students who were award winners of the Alkindi competition.
- Paul Zimmermann co-animated a “Math-en-Jeans” atelier with lycée Vauban in Luxembourg city (Luxembourg).

CASCADE Project-Team (section vide)

DATASHAPE Project-Team

10.3. Popularization

10.3.1. Inria-Industry Meeting

Marc Glisse, Miro Kramar and Steve Oudot held a booth for half a day.

Marc Glisse played for a small video which is now on the InriaInnovation YouTube channel https://youtu.be/lKNjGk-Z6b4.

GAMBLE Project-Team

10.3. Popularization

L. Dupont participated to several days of popularization of computerscience: Open Bidouille Camp March, 26th 2017, popularization of programming, general audience ; ISN day March, 30th 2017, popularization of computerscience for high-school teachers ; Fête de la Science 14th October 2017 Inria event, general audience, and Google Day in Nancy 21st October 2017, general audience.

GRACE Project-Team

9.3. Popularization

- A. Couvreur gave the *Conférence inaugurale* of the *Semaine des mathématiques* in the accadémie de Créteil: *Cryptographie, le langage des secrets*.

LFANT Project-Team

8.3. Popularization

The book Guide to Pairing-Based Cryptography [26] has been published by CHAPMAN and HALL/CRC. D. Robert wrote with Sorina Ionica the chapter "Pairings" of this book. This book aims to help Engineers understand and implement pairing based cryptography; in the Chapter "Pairings", D. Robert give a self contained definition and proof of the Weil and Tate pairing; including how to handle divisors with non disjoint support (this is often skipped in scientific papers but is important for practical implementations).

A. Page gave a popularization talk "À la découverte de la cryptologie : la science du secret" during the Fête de la Science event. Two groups of high school students and one group of Inria agents participated in this activity. Following this talk, three high school students decided to work on the RSA cryptosystem for their TPE essay and came back to the IMB to meet A. Page and talk about this topic in greater detail.

POLSYS Project-Team

9.3. Popularization

The activity of POLSYS in post-quantum cryptography has been covered in several large audience magazines:

- "Enfin! La révolution quantique", L'Usine Nouvelle, November 2017.
- "QUANTIQUE : THE NEXT BIG THING(K)", L'Informaticien, November 2017.
- "L'ORDINATEUR QUANTIQUE VA-T-IL METTRE À MAL LA CYBERSÉCURITÉ MONDIALE?", Bouygues Blog, October 2017.

Ludovic Perret is member of the Cloud Security Alliance (CSA) quantum-safe security working group. In particular, he contributed to the following documents:

- B. Huttner, J. Melia, G. Carter, L. Perret and L. Wilson. "Applied Quantum-Safe Security", Feb. 2017.
- B. Huttner, J. Melia, G. Carter, L. Perret and L. Wilson. "Quantum Safe Security Glossary", January 2017.

Ludovic Perret is also member of the quantum-safe cryptography specification group of the European Telecommunications Standards Institute (ETSI) where is the referee for a document on quantum-safe signatures.

Since May 2010, Daniel Lazard is engaged in a strong edition work on the English Wikipedia (more than 6 000 contributions, including vandalism revert and talk pages). Initially focused on the themes of POLSYS, these contributions were later enlarged to general algebra and algebraic geometry, because many elementary articles require to be expanded to be useful as a background for computer algebra. Examples of articles that have been subject of major editing: "System of polynomial equations" (created), "Computer algebra", "Algebra", "Algebraic geometry", "Polynomial greatest common divisor", "Polynomial factorization", "Finite field", "Hilbert series and Hilbert polynomial",...

For the year 2017, this contribution amounts to about $2,000$ edits on the English Wikipedia.

Mohab Safey El Din was invited by FMJH to present and popularize symbolic and algebraic computation to Master students in Mathematics following the curricula proposed by Univ. Paris-Saclay.

SECRET Project-Team

10.3. Popularization

- **Alkindi cipher challenge:** Several members of the project-team are involved in the cipher challenge for high-school students "concours Alkindi" http://www.concours-alkindi.fr/. Matthieu Lequesne organized the challenge and created the scientific content of the competition. He also gave a talk during the final of the cipher challege Alkindi on May 17 at the "Cité des Sciences" in Paris. The 2018 edition of the competition has been launched in December 2017 at Lycée de la Vallée de Chevreuse, Gif-sur-Yvette. Matthieu Lequesne, Sébastien Duval and Yann Rotella gave talks on cryptography during the opening ceremony. The best teams from Académies de Dijon and Orléans-Tours have been visiting the SECRET project-team in June 2017 https://www.youtube.com/watch?v=EVLHEOWAORc.
- N. Sendrier, *Code-Based Cryptography: State of the Art and Perspectives*, IEEE Security & Privacy, Special Issue on Post-quantum Cryptography. July/August 2017.
- A. Chailloux *Cryptographie Quantique en théorie* - Journée Maths en Mouvement sur l'ordinateur quantique organized by the FSMP, Paris, France, May 2017
- Matthieu Lequesne co-organized the final of the French Tournament of Young Mathematicians at École polytechnique on May 26-28 and was chaired the jury sessions. He also participated to the elaboration of the problems for the 8th French Tournament of Young Mathematicians (TFJM^2) in December 2017.
- Matthieu Lequesne co-organized the International Tournament of Young Mathematicians (ITYM) in Iasi, Romania in July 2017 and was part of the international jury.
- Matthieu Lequesne taught for one week during a mathematical summer camp for high school students in Bethlehem, Palestine, organized by the Al Khwarizmi Noether Institute in August 2017.
- Matthieu Lequesne co-organized a weekend for female high-school students interested in mathematics (Rendez-vous des Jeunes Mathématiciennes) at ENS Ulm, November 25-26.
- Yann Rotella gave a talk on cryptography at Lycée Théophile Gautier, Tarbes, January 31, 2017.
- Yann Rotella gave a presentation for *Raconte-moi ta thèse !* during Fete de la Science, at IHP, Paris, October 2017.
- Several members of the team (C. Boura, A. Canteaut, M. Lequesne, A. Leverrier, Y. Rotella) have been involved in the *Cinquante ans d'Inria*, November 2017. They hold a stand to present a serious game on cryptography. A. Canteaut has participated on a panel on Cyber-security. A. Leverrier gave a short talk (pitch de science) on quantum computing.
- Matthieu Lequesne was auditioned by the committee in charge of proposing a reform of mathematical education (Mission Maths Villani-Torossian) on November 29.

SPECFUN Project-Team

8.3. Popularization

- Assia Mahboubi has written an article for the MathExpress journal, at the occasion of the *salon Culture & Jeux Mathématiques*. See the Maths Language express volume at http://www.cijm.org/accueil/productions-cijm/90-maths-express.

CAIRN Project-Team (section vide)

CAMUS Team

10.3. Popularization

A. Charguéraud is one of the three organizers of the *Concours Castor informatique*http://castor-informatique.fr/. The purpose of the Concours Castor in to introduce pupils (from *CM1* to *Terminale*) to computer sciences. More than 500,000 teenagers played with the interactive exercises in November 2017.

Jens Gustedt is blogging about efficient programming, in particular about the C programming language. He also is an active member of the stackoverflow community a technical Q&A site for programming and related subjects.

Cédric Bastoul prepared activities and participated to *Fête de la Science* at University of Strasbourg in October 2017.

CORSE Project-Team (section vide)

PACAP Project-Team

9.3. Popularization

Nicolas Kiss, Damien Hardy and Erven Rohou presented a poster at the “European Cyber Week”, organized by the “Pôle d’Excellence Cyber”.

Erven Rohou presented a poster at the Teratec Café, describing the ANTAREX H2020 project.

AOSTE2 Team

10.3. Popularization

Popularization video of the probabilistic notions for mixed-criticality systems https://www.youtube.com/watch?v=sSJT4eGhS_A

HYCOMES Project-Team (section vide)

KAIROS Team (section vide)

PARKAS Project-Team (section vide)

SPADES Project-Team (section vide)

TEA Project-Team (section vide)

ANTIQUE Project-Team (section vide)

CELTIQUE Project-Team

6.3. Popularization

Article “JavaScript, un langage à la croissance organique”, Alan Schmitt, blog Binaire Le Monde. http://binaire.blog.lemonde.fr/2017/05/12/javascript-un-langage-a-la-croissance-organique/

Article “L’assistant de preuve Coq”, Sandrine Blazy, Pierre Castéran, Hugo Herbelin, Techniques et Sciences de l’ingénieur, août 2017. https://www.techniques-ingenieur.fr/base-documentaire/technologies-de-l-information-th9/programmation-42304210/coq-assistant-de-preuve-h3310/

Talk “Bug, Virus, Intrusion, Pirates... So many threats and no defense? Yes... maths.”, Thomas Genet, given three times in high schools close to Rennes.

CONVECS Project-Team

9.3. Popularization

H. Garavel participates to the program committee and organization committee of FMF (*Formal Methods Forum*) [0], a series of industrial conferences on formal methods set up by the competitivity clusters Aerospace Valley and Minalogic, with the support of Inria and many other partners. The 7th FMF conference, devoted to formal methods and cybersecurity, was held on January 31, 2017. The 8th FMF conference, devoted to formal methods and autonomous vehicles, was held on October 10, 2017. Both events gathered a large audience.

L. Marsso, R. Mateescu, and Olivier Clozeau (Innovista Sensors) participated to the "*Forum 5i*" held on June 1st, 2017 at Grenoble (World Trade Center), where they held a stand dedicated to the results of the Bluesky project [0].

R. Mateescu gave a lecture entitled "*Validation d'applications embarquées par des jumeaux numériques formels*" at the *Journée thématique Minalogic sur la modélisation des systèmes cyber-physiques* held in Grenoble on November 16, 2017.

[0] http://projects.laas.fr/IFSE/FMF
[0] http://www.minalogic.com/en/project/bluesky

DEDUCTEAM Project-Team (section vide)

GALLIUM Project-Team

10.3. Popularization

Xavier Leroy wrote a popularization article describing the hunt for a hardware bug in Intel processors, which was published by the Web news site *The Next Web* [32].

MARELLE Project-Team

8.3. Popularization

Laurent Théry gave a talk in high-school (Centre International de Valbonne) in the context of the annual "Fête de la Science".

Damien Rouhling and Cécile Baritel-Ruet participated to the event "My thesis in 180 seconds" at the regional level.

MEXICO Project-Team (section vide)

PARSIFAL Project-Team (section vide)

PI.R2 Project-Team

8.3. Popularization

Hugo Herbelin wrote with Sandrine Blazy and Pierre Castéran an introduction to Coq for engineers edited by Techniques de l'Ingénieur.

SUMO Project-Team

10.3. Popularization

- Éric Badouel gave a talk at TEDx Lorient on digital democracy (coordination of citizen debates).

TOCCATA Project-Team

10.3. Popularization

S. Boldo, scientific head for Saclay for the MECSI group for networking about computer science popularization inside Inria.

S. Boldo gave a talk at the Inria Saclay about how to popularize programming.

During the “Fête de la science” on October 13th, S. Boldo demonstrated unplugged computer science to teenagers and F. Faissole run a stand about an introduction to programming with robots. S. Boldo also did this activity to kids from 7 to 17 at the Massy opera on November, 17th.

S. Boldo gave a talk during at a *Girls can code* weekend on August 23rd in Paris.

S. Boldo went to the Arpajon high-school for presenting Women in Science on December 19th.

S. Boldo gave a popularization talk to the administrative staff of Inria at Rocquencourt for the Inria birthday on November 16th.

VERIDIS Project-Team (section vide)

CARTE Team

10.3. Popularization

- Nazim Fatès contributed to a booklet on the theme "Mathématiques et langages" edited by the Commission française pour l'enseignement des mathématiques (CFEM) for the forum "Mathématiques vivantes" (see http://forum-maths-vivantes.fr/-Panorama).
- This text appeared in a revised version on the CNRS website "images des mathématiques" [27].
- Nazim Fatès participated to a meeting ("projection-debat") at the Réseau et transport de l'électricité (RTE) at Villers-lès-Nancy on the these "Visages de la robotique", organised by "Sciences en lumière" (formerly Festival du film de chercheur).
- Nazim Fatès participated to a workshop on ethics in the "Forum des Sciences cognitives" organised by the "UFR mathématiques et informatique".
- Simon Perdrix gave an invited talk on quantum algorithms at the event "Mathématiques en mouvement sur l'Ordinateur quantique" organised by the Fondation Sciences Mathématiques de Paris at IHP.

CIDRE Project-Team

10.3. Popularization

Valérie Viet Triem Tong has participated to the scientific television show *l'Esprit Sorcier* recorded at *Musée des Sciences et de l'Industrie* during the *Fête de la Science*. She has also participated to the scientific promotion movie about *High Security Laboratory* recorded at Nancy.

Damien Crémilleux has participated to the event "Ma thèse en 180s" and the "RCC challenge: my thesis 3.0" for the popularization of his work's thesis on security visualization.

COMETE Project-Team (section vide)

DATASPHERE Team (section vide)

PESTO Project-Team

10.3. Popularization

- How to Explain Modern Security Concepts to your Children [11] (J. Dreier)
- Vote par Internet [41] (V. Cortier and S. Kremer)
- 2 days of debate on privacy at *Moments d'invention 2016*, organized by Grand Nancy (V. Cortier)
- booth at the *Open Government Summit* organized at Sénat (V. Cortier)
- Conference and debate at the *ISN day*, conference for teachers in computer science (V. Cortier)
- Interview for *silicon.fr* on weakening cryptosystems to allow limited access by authorities (S. Kremer)
- France 3 Lorraine radio interview on computer security (S. Kremer)
- Interview for *AFP* on electronic voting (S. Kremer)
- Interview for *AFP* and *Huffington Post* on electronic voting (V. Cortier)

PRIVATICS Project-Team

9.3. Popularization

9.3.1. Hearings

D. Le Métayer at the French National Assembly about the implementation of the General Data Protection Regulation (Jan. 2017).

D. Le Métayer at the Conseil national du numérique (CNNum) about the regulation of algorithms (Jul. 2017).

M. Cunche at le Comité Consultatif National d'Ethique (CCNE)[0] (Mar. 2017).

9.3.2. Interviews

M. Cunche by Valentine Faure in Glamour, Donner ses données, juin-juillet 2017.

M. Cunche by Martin Untersinger in lemonde.fr, Apple donne à nouveau des gages en matière de vie privée, 27/09/2017, http://www.lemonde.fr/pixels/article/2017/09/27/apple-donne-a-nouveau-des-gages-en-matiere-de-vie-privee_5192469_4408996.html

M. Cunche by Arnaud Devillard in Sciences et Avenir, Même coupé, le Wi-Fi sous Android peut suivre le téléphone, Oct. 2017, https://www.sciencesetavenir.fr/high-tech/meme-coupe-le-wi-fi-sous-android-peut-suivre-le-telephone_116061

M. Cunche by Camille Gruhier in Que-choisir, Smartphones Android Même une fois le Wi-Fi désactivé, vous êtes pisté, Oct. 2017 https://www.quechoisir.org/actualite-smartphones-android-meme-une-fois-le-wi-fi-desactive-vous-etes-piste-n46076/

M. Cunche by Emilie Brouze in Rue89 - L'Obs, Tu es resté 22 minutes chez l'opticien jeudi. Le centre commercial le sait, le 12 juillet 2017, http://tempsreel.nouvelobs.com/rue89/rue89-nos-vies-connectees/20170711.OBS1939/vous-etes-reste-22-minutes-chez-l-opticien-jeudi-et-le-centre-commercial-le-sait.html

M. Cunche by ZDnet.fr, http://www.zdnet.fr/actualites/android-desactiver-le-wi-fi-n-empeche-pas-d-etre-espionne-39856640.htm

M. Cunche by 01Net, http://www.01net.com/actualites/sur-android-le-wi-fi-peut-vous-tracer-meme-s-il-est-desactive-1245292.html

M. Cunche by l'informaticien, https://www.linformaticien.com/actualites/id/44894/desactiver-le-wifi-pour-eviter-le-flicage-une-protection-illusoire.aspx

M. Cunche by Nextinpact, https://m.nextinpact.com/news/105038-suivi-clients-dans-magasins-question-wi-fi-nest-pas-seule-a-se-poser.htm

C. Lauradoux by Sophie Eremian in Inriality, Quand l'énergie devient intelligente, Oct. 2017, https://www.inriality.fr/environnement/quand-lenergie-devient-intelligente/.

9.3.3. Press articles

D. Le Métayer in Slate, *Designing, explaining and controling algorithms*, in Presidential election, 100 proposals from the research community (Mar. 2017).

D. Le Métayer in Le Monde, *Gouverner les algorithmes pour éviter qu'ils nous gouvernent*, (Nov. 2017).

C. Castelluccia and D. Le Métayer in Inria Analysis note, *Secure electronic documents: is the centralisation of biometric data really inevitable?*, (Feb. 2017).

9.3.4. Conferences

[0] http://www.ccne-ethique.fr/fr

M. Cunche and C. Matte, *le traçage cyberphysique via Wi-Fi*, Exposition Terra Data at Cité des Sciences et de l'Industrie, Apr. 2017.

M. Cunche and C. Matte, *le traçage cyberphysique via Wi-Fi*, Fête de la science at Cité des Sciences et de l'Industrie, Oct. 2017 (broadcasted by Science et Vie TV and animated by l'Esprit Sorcier).

C. Lauradoux, *Email et vie privée: pourquoi utiliser GPG ?*, Cours Master 2, Nov. 2017.

C. Lauradoux, *Mathématiques et la protection de la vie privée*, Olympiades académiques de Mathématiques, May 2017.

C. Lauradoux, *Cryptographie visuelle*, Collège/Lycée Jean Prévost, 01/06/2016.

C. Lauradoux, *Cryptanalyse*, stage MathC2+, 06/2017.

PROSECCO Project-Team

9.3. Popularization

- Karthikeyan Bhargavan, Benjamin Beurdouche, Jean Karim Zinzindohoue published a paper in the Communications of the ACM.

TAMIS Team

10.3. Popularization

- Axel Legay participated to the "Forum Cyberstrategia" organized by the ministry of defense, September 2017
- Axel Legay participated to the "Inria Industry days" organized by Inria, October 2017
- Axel Legay participated to the "table ronde sur l'intelligence économique", Rennes November 2017
- Fabrizio Biondi participated to the "Forum International de la Cybersécurité", January 2017
- Fabrizio Biondi participated to the "Forum Cyberstrategia" organized by the ministry of defense, September 2017
- Fabrizio Biondi participated to the "Inria Industry days" organized by Inria, October 2017
- Fabrizio Biondi participated to the "European Cyber Week" organized by IRISA and Bretagne Development Innovation, November 2017