RESEARCH CENTER
Paris

FIELD

Activity Report 2016

Section Highlights of the Team

Edition: 2017-08-25

ALPAGE Project-Team

4. Highlights of the Year

4.1. Highlights of the Year

In 2016, Alpage has obtained several new national fundings: the team is the leader of a new ANR project (Parsiti), and a partner of a new ANR project (Profiterole) and of a new ANR-NSF project (MCM-NL).

ALPINES Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Awards

5.1.1.1. SIAM Siag on Supercomputing Best Paper Prize 2016

for the most outstanding paper published in 2012-2015 in a journal in the field of high performance computing. Co-authors are J. Demmel, L. Grigori, M. Hoemmen, and J. Langou, for the paper Communication-Optimal Parallel and Sequential QR and LU Factorizations, published in SIAM Journal on Scientific Computing 2012. Citation of the jury: *This is a cornerstone paper in Numerical Linear Algebra and Parallel Processing that lays down both theoretical and practical algorithmic frameworks for communication-avoiding algorithms. The paper provides powerful insights and renews attention on communication reduction both of which will have long-lasting and practical impact in parallel and distributed computing.*

5.1.1.2. Bull-Joseph Fourier 1st Prize 2015 (15 000 euros)

for our work *Imaging of cerebrovascular accident through High Performance Computing* by V. Dolean, F. Hecht, P. Jolivet, F. Nataf and P-H. Tournier. This was the sixth edition of this competition which corresponds to the French "Gordon Bell Prize".

ANGE Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

While the theory and the numerics related to the nonlinear shallow water equations are extensively studied, the understanding of more complex models including dispersive ones is not achieved. Two PhD theses about these issues were defended in 2016 within the team (N. Aïssiouene and D. Kazerani). To go further, a collaboration with spanish collaborators from the university of Sevilla was launched with multiple trips in Spain and France resulting in a preprint [25]. The collaboration is expected to be made more formal in 2017.

Moreover, the team has been reinforced by two young engineers: J. Ledoux in the framework of the ANR project Hyflo-Eflu and F. Souillé. The latter recruitment has been allowed by the Inria ADT grant F2O ("Freshkiss to Others") and is aimed at easing the transfer of the Freshkiss code in cooperation with SciWorks Technologies.

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 2016, and among the applied results we underline the release of MemCad, the first analyzer that can handle the analysis of various data structures.

AOSTE Project-Team (section vide)

ARAMIS Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

- Stanley Durrleman’s ERC Starting Grant "LEASP" has started.
- H2020 project EuroPOND, under societal challenge "Personalizing Health and Care" has started.
- ANR-NIH project NETBCI, under the "Collaborative Research in Computational Neuroscience" program (CRCNS) has started.
- The team has been awarded the ANR-NIH project HIPLAY7, under the "Collaborative Research in Computational Neuroscience" program (CRCNS)
- The team has been awarded the ANR project BRANDY, under the generic call programme "Vie, Sante et Bien-etre", Project duration: 2017-2020
- ARAMIS participates to the Human Brain Project (European Flagship).
- Anne Bertrand was awarded a one year Inria-APHP interface contract (i.e., "poste d’accueil"), allowing her to work half-time in the ARAMIS project team, from november 2016 to november 2017.
- Pietro Gori and Barbara Gris successfully defended their PhD.
- S. Durrleman has been appointed associate editor of IEEE Transactions on Medical Imaging (TMI).

CASCADE Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Conferences

- Hoeteck Wee is one of the invited speakers at Asiacrypt 2016.
- Michel Abdalla is one of the invited speakers at ICISC 2016.

5.1.2. Awards

Romain Gay and Hoeteck Wee, together with Dennis Hofheinz and Eike Kiltz, received the Best Paper Award at Eurocrypt 2016 .

BEST PAPERS AWARDS :

[40] **Advances in Cryptology – EUROCRYPT 2016**. R. GAY, D. HOFHEINZ, E. KILTZ, H. WEE.

CLIME Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Awards

Inria and Paris City were awarded a Décibel d'Argent 2016 in research category for the mobile application Ambiciti. The award was attributed by the Conseil National du Bruit, which depends on the Ministry of Ecology, Sustainable Development and Energy, and is a national organization in charge of noise. The selection committee pointed out the Ambiciti articulation between research, citizen involvement, city or government actions and the operational development of a rich and perennial mobile application.

DYOGENE Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Awards

F. Baccelli received a Honorary Doctorate of Heriot-Watt University. The graduation took place on November 17, 2016, in Edinburgh, United Kingdom.

EVA Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

Awards

- Prof. Steven Glaser (UC Berkeley) and **Thomas Watteyne** recipients of the France-Berkeley Fund award for the project "SHRIMP: Smart Harbor Implementation", August 2016.
- Keoma Brun-Laguna and **Thomas Watteyne**, together with Ana Laura Diedrichs, Javier Emilio Chaar, Diego Dujovne, Juan Carlos Taffernaberry, Gustavo Mercado. Runner up IEEE SECON 2016 Best Demo Award with "A Demo of the PEACH IoT-based Frost Event Prediction System for Precision Agriculture", London, UK, 28 June 2016.
- Remy Leone and **Thomas Watteyne**. Recipient Google IoT Technology Research Award on "6TiSCH and WiFi coexistence with OpenWSN", March 2016.
- Tengfei Chang and **Thomas Watteyne**, together with Pedro Henrique Gomes, Pradipta Gosh, Bhaskar Krishnamachari. EWSN dependability competition 4th place with project "Reliability through Time-Slotted Channel Hopping and Flooding-based Routing", 16 February 2016.

Meeting & Seminars

Organization of Workshops and Conferences

- ***PEMWN 2016*** international conference on Performance Evaluation and modeling in Wired and wireless Networks, co-chaired by Leila Saidane and **Pascale Minet** and Farouk Kamoun , held in Paris, France, November 2016. Pascale Minet was general co-chair with Leila Saidane from ENSI (Tunisia) of the PEMWN 2016 conference, the 5th IFIP international conference on Performance Evaluation and Modeling of Wired and Wireless Networks, technically co-sponsored by IFIP WG6.2 and IEEE ComSoc (see https://sites.google.com/site/pemwn2016/). This conference was held at CNAM in Paris, 22-24 November 2016. It was sponsored by Inria, CNAM and ENSI. The organization co-chairs were Samia Bouzefrane and Selma Boumerdassi. Three tutorials were given:
  - *Internet of Vehicles: From Intelligent Grid to Autonomous Cars and Vehicular Clouds* by Mario Gerla, Professor, University of California, Los Angeles.
  - *5G: Can we make it by 2020?* by Merouane Debbah, Mathematical and Algorithmic Sciences Lab, Huawei, France.
  - *Internet of Things, hyper-massive wireless networks, where are the theoretical limits?* by Philippe Jacquet, NOKIA, France.

  Sixteen papers have been selected by the technical program committee and presented during the three days of the PEMWN 2016 conference.
- ***InterIoT 2016*** The 2nd EAI International Conference on Interoperability in IoT was co-organized by Nathalie Mitton, Thomas Noël (general co-chairs) and Thomas Watteyne (TPC chair). It took place 26-27 October 2016 in Paris, France.

Tutorials

- Standards for the Industrial IoT: a Hands-on Tutorial with OpenWSN and OpenMote. Xavier Vilajosana, Pere Tuset-Peiro, Tengfei Chang, **Thomas Watteyne**. IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), Valencia, Spain, 4-8 September 2016.
- Introduction to the IETF 6TiSCH stack with OpenWSN & OpenMote. **Thomas Watteyne**, Xavier Vilajosana, Pere Tuset-Peiro, Tengfei Chang. International Conference on Telecommunications (ICT), Thessaloniki, Greece, 16-18 May 2016.

Standardization Activities

- ***Standardization*** *meeting co-chaired by Inria-EVA*
  6TiSCH working group meeting at IETF 97, 17 November 2016, Seoul, South Korea.
- ***Standardization*** *meeting co-chaired by Inria-EVA*
  6TiSCH working group meeting at IETF 96, 18 July 2016, Berlin, Germany.
- ***Interop event*** *organized by ETSI and Inria-EVA*
  ETSI 6TiSCH 3 plugtests, 15-16 July 2016, Berlin, Germany.
- ***Standardization*** *meeting co-chaired by Inria-EVA*
  6TiSCH working group meeting at IETF 95, 4 April 2016, Buenos Aires, Argentina.
- ***Standardization*** *meeting co-chaired by Inria-EVA*
  ETSI 6TiSCH 2 plugtests, 2-4 February 2016, Paris, France.

Real-World Deployments

The networking technology developed at Inria-EVA has reached the level of maturity for it to be used in real-world deployment. We have worked on 3 main sets of deployments in 2016:

- **Save the Peaches** (http://www.savethepeaches.com/), a 23-node network in Western Argentina which monitors temperature and humidity to be predict frost events in peach orchards.
- **SnowHow** (http://www.snowhow.io/), a set of 18 low-power wireless networks (945 sensors total) deployed throughout the Californian Sierra Nevada to monitor the snowpack.
- *(current work)* A Smart Building deployment in the Inria-Paris research center.

From a networking point of view, these deployments SolSystem (see Section 6.8) as a back-end solution. Sensor data and network statistics are available at our Inria-Paris servers (https://sol.paris.inria.fr/) seconds after they were measured in the field.

Distinguished Visitors

- ***Invited Professor Mario Gerla***, from UCLA, USA. He stayed in the EVA team during 2 1-week stays (31 August-23 September, 10-20 December) to work with the EVA team on shock-wave mitigation using vehicular ad hoc networks.
- ***Invited Professor Leila Saidane***, from ENSI, Tunisia. She stayed in the EVA team from 28 November to 2 December 2016 to prepare common publications and identify further research directions.
- ***Invited Professor Diego Dujovne***, from Universidad Diego Portales, Chile. He stayed in the EVA team for a 1-week visit (22-31 July 2016) to integrate sensors in the low-power wireless platforms, to be deployed in Argantina as part of the PEACH project.
- ***Invited Professor Steven Glaser***, from UC Berkeley, USA. He stayed in the EVA team for a 1-week visit (21-25 June 2016) to explore funding opportunities beyond the REALMS associate team.
- ***Invited Professor Branko Kerkez***, from U. Michigan, USA. He stayed in the EVA team for a 1-week visit (17-22 June 2016) to work on the Internet of Water (2 papers submitted). This visit was part of the REALMS associate team.

GALLIUM Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

Xavier Leroy received the 2016 Royal Society Milner Award “in recognition of his exceptional achievements in computer programming which includes the design and implementation of the OCaml programming language”.

Xavier Leroy received one of the two 2016 Van Wijngaarden Awards from Centrum Wiskunde & Informatica (Amsterdam).

Xavier Leroy received the ACM SIGPLAN Most Influential POPL Paper Award for his POPL 2006 paper, *Formal certification of a compiler back-end or: programming a compiler with a proof assistant* [51].

GANG Project-Team (section vide)

MAMBA Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Personnel

Marie Doumic has moved in September 2015 for a 1-year sabbatical to the Wolfgang Pauli Institute in Vienna. Stefan Hoehme left in July 2015 to start a prestigious “Emmy Noether” junior research group at University of Leipzig, faculty for computer sciences. Of note, this is the first Emmy Noether research group in Leipzig, and he was the only one accepted this year (out of 20 presented).

Nicolas Vauchelet left the team in September 2015, becoming a full professor at University Paris XIII.

5.1.2. THE ITMO Cancer national call.

The team has been successful in simultaneously participating in 2 different funded projects of the ITMO Cancer THE (“Tumour Heterogeneity in its Ecosystem”, a programme managed by INSERM) national call for 2016: one, EcoAML (4 teams), on early leukaemogenesis in Acute Myelogenous Leukaemia (AML), headed by François Delhommeau (CDR St Antoine, Paris), with whom we have a long-lasting collaboration, and the other, MoGlImaging (8 teams), on treatment-induced treatment resistance and heterogeneity in glioblastoma, headed by Elizabeth Moyal (INSERM, Toulouse), a project inside which we have recently developed a work collaboration with the team of François Vallette (INSERM, Nantes) on the in-vitro resistance of glioblastoma to temozolomide. In both these collaborative projects, begun in November 2016 and to be integrated in 2017 in the future THE consortium (gathering the 6 projects laureates to the national call), we propose to develop our phenotype-structured models for both the cancer and the supporting stromal cell populations, with representation of mutualistic interactions between them.

MATHERIALS Project-Team (section vide)

MATHRISK Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

- Creation of a joint seminar on Numerical probability and Mathematical Finance with the LPMA laboratory, University Paris-Diderot.
- Organization by B. Jourdain with B. Bouchard (Université Paris-Dauphine) and E. Gobet (Ecole Polytechnique) of the 2015-2016 thematic semester on Monte Carlo methods (financed by the Institute Louis Bachelier) at Institut Henri Poincaré, Paris https://www.ceremade.dauphine.fr/montecarlo/MonteCarlo.html, and the international closing conference in July 2016. https://montecarlo16.sciencesconf.org

MIMOVE Team

5. Highlights of the Year

5.1. Highlights of the Year

Members of MiMove are co-founders of the Ambiciti start-up (http://ambiciti.io) together with the Inria team CLIME, and the NUMTECH and the Civic Engine SMEs. Ambiciti's technology is a single platform delivering real-time data on street-by-street exposure and risks on multiple environmental pollutants. The platform's technology leverages open data along with cloud, IoT, mobile and data analytics technologies. Ambiciti collects real-time, street-by-street pollution data and provides urban citizens with a means to personalize their decisions with regard to environmental hazards. The aim is to enable citizens to make more informed choices about their activities, personal behavior and location, and to protect their own health. Ambiciti also supplies businesses with crucial data that allows to better inform consumers and to increase the valuation of services (e.g., real estate). Eventually, Ambiciti supports governments in protecting citizens' health and in growing cities more sustainably in providing the necessary urban pollution data. Key elements of the Ambiciti platform include the Ambiciti mobile app that leverages mobile phone sensing middleware solutions to monitor the individual and collective exposure of citizens to environmental pollutions in a resource-efficient way (more at https://www.inria.fr/en/centre/paris/news/ambiciti-an-application-a-start-up). The first version of the Ambiciti App (successor of SoundCity) deals with noise and air pollution. In particular, Inria and the Paris city council were awarded a *Décibel d'Argent* prize for the App (more at https://www.inria.fr/en/centre/paris/news/2016-decibel-d-or-golden-decibel-competition-ambiciti-receives-the-decibel-d-argent-silver-decibel-prize-in-the-research-category).

MOKAPLAN Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

New ERC Grant for G. Peyré

Gabriel Peyré is the recipient of a second ERC grand (consolidator), project NORIA (http://www.gpeyre.com/noria/) on Numerical Optimal tRansport for ImAging, that will start on Oct. 2017.

Pisa

Four members of Mokaplan : G. Peyré, G. Carlier, J-D. Benamou, Simone di Marino (starting 2017) have been invited speakers at the Pisa Scuola Normale Bi-Annual Optimal Transport Conference (November 7-11). This is considered as the most prestigious conference in the field.

MUSE Team (section vide)

MUTANT Project-Team

4. Highlights of the Year

4.1. Highlights of the Year

Startup Creation

Arshia Cont with José Echeveste and Philippe Cuvillier (former PhD students) are creating a Startup around Antescofo to bring the product to greater public starting March 2016 http://antescofo.com. The project is hosted by the French Incubator AgoraNov.

It was awarded the “Emergence Award” in 2015 that help emerging new technology companies to study the project, and an i-LAB prize in 2016, supported by the French Ministry of Culture and Bpifrance, and it has been a finalist of the Midemlab 2016.

MYCENAE Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

- PhD defense of Lucile Megret. Explosion of limit cycles : qualitative analysis, numerical simulations and models. Université Pierre & Marie Curie – Sorbonne Universités, November 25th 2016.
- PhD defense of Elif Köksal Ersöz. A mathematical study on coupled multiple timescale systems, synchronization of populations of endocrine neurons. Université Pierre & Marie Curie – Sorbonne Universités, December 13th 2016.
- PhD defense of Tanguy Cabana. Limits of randomly connected networks and their dynamics. Université Pierre & Marie Curie – Sorbonne Universités, December 14th 2016.
- Invited plenary conference at ICAR2016 http://www.icar2016.org 18th International Congress on Animal Reproduction. Multiscale mathematical modeling of the hypothalamo-pituitary-gonadal axis. Tours (France), June 26-30th 2016.

PARKAS Project-Team

4. Highlights of the Year

4.1. Highlights of the Year

4.1.1. Awards

Marc Pouzet won the Inria/French Académie des Sciences/Dassault Systèmes Innovation award.

PI.R2 Project-Team (section vide)

POLSYS Project-Team

4. Highlights of the Year

4.1. Highlights of the Year

The goal of the RISQ project is to prepare the security industry to the upcoming shift of classical cryptography to quantum-safe cryptography. The RISQ project is a massive effort at the French level to embrace the quantum-safe revolution. The project gather 15 partners : ANSSI, C&S, CEA, Crypto Experts, EADS, ENS Lyon, ENS Paris, Gemalto, Orange, PCQC, POLSYS (Inria de Paris), Université de Rennes, Secure IC, Thales CS, and Université de Versailles.

The RISQ project is certainly the biggest (in term of number of partners, as well as funding) industrial project ever organized in quantum-safe cryptography. RISQ is one of few projects accepted in the “Grands Défis du Numérique” which is managed by BPI France, and will be funded thanks to the PIA.

POLSYS actively participated to gather the partners of RISQ, and in defining the proposal. POLSYS will lead the academic effort in RISQ.

Jointly with LAAS (D. Henrion, S. Naldi), we have released a new MAPLE library SPECTRA for finding a real point $x = (x_1, ..., x_n)$ such that the symmetric matrix $A(x) = A_0 + A_1\, x_1 + \cdots + A_n\, x_n$ is positive semidefinite using exact arithmetic (see http://homepages.laas.fr/henrion/software/spectra/).

Our open source C library SLV has been officially released this year with a presentation at ISSAC. It aims at solating and approximating the real roots of univariate polynomials with integer coefficients (see http://www-polsys.lip6.fr/~elias/soft.html)

4.1.1. Awards

Matías Bender received the Distinguished Student Author Award of ISSAC2016 for his paper [22] written with J.-Ch. FAUGÈRE, L. PERRET and E. TSIGARIDAS.
BEST PAPERS AWARDS :
[22] **ISSAC ’16 - 41st International Symposium on Symbolic and Algebraic Computation**. M. R. BENDER, J.-C. FAUGÈRE, L. PERRET, E. TSIGARIDAS.

PROSECCO Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

This year, we published 18 articles in international peer-reviewed journals and conferences, including papers in prestigious conferences such as POPL, IEEE S&P Oakland, ACM CCS, NDSS, CSF, and WPES. Notably, Bruno Blanchet published a book surveying the use of ProVerif, his state-of-the-art protocol verification tool. We also won several research awards for our work, detailed below. Our work also exposed two new attacks, SLOTH and SWEET32, on Transport Layer Security, resulting in security updates and CVEs in popular web browsers and VPN software.

5.1.1. Awards

- Catalin Hritcu was awarded an ERC Starting Grant
- Catalin Hritcu was awarded an ANR Jeune Chercheur/Jeune Chercheuse Grant
- Karthikeyan Bhargavan was awarded an ERC Consolidator Grant
- Karthikeyan Bhargavan and Gaëtan Leurent won a Best Paper award at NDSS 2016
- Karthikeyan Bhargavan, Cedric Fournet, Markulf Kohlweiss, and Alfredo Pironti were awarded the Levchin prize for contributions to Real-World Cryptography
- Karthikeyan Bhargavan was awarded a Microsoft Outstanding Collaborator Award
- Karthikeyan Bhargavan was awarded the Prix Inria – Académie des sciences du Jeune chercheur

QUANTIC Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

- Pierre Rouchon was a plenary speaker at 55th IEEE Conference on Decision and Control.
- First demonstration of a quantum error correcting code extending the lifetime of a quantum bit: this experiment performed at Yale in collaboration with the team of Robert J. Schoelkopf realizes the hardware-efficient quantum error correction protocol that we had proposed a few years ago. This is the first experiment where a redundant encoding of quantum information, together with continuous measurements of an error syndrome and real-time closed-loop error corrections, extend the lifetime of the encoded information beyond the best physical part. This result was published in Nature [22].
- An experimental marriage of two central concepts of mechanics, the Schrödinger cat states and the entanglement, was realized in collaboration with the team of Robert J. Schoelkopf at Yale. Following our earlier theoretical proposals, an entangled Schrödinger cat state of light shared between two boxes (two high-Q cavities) were successfully achieved and measured. Experimental realization of such states of light were proposed more than 20 years ago and have important applications in quantum information processing. This result was published in Science [28] and has attracted important press converge around the world.
- First experimental demonstration of the quantum-state diffusion associated with spontaneous emission that triggered the field of quantum trajectories in the 1990s. This result was published in Phys. Rev. X [16]. This also led us to implement a first experimental demonstration of multi-input multi-output (MIMO) feedback in the quantum regime. This result was published in Phys. Rev. Lett. [15].

RAP Project-Team (section vide)

REGAL Project-Team

4. Highlights of the Year

4.1. Highlights of the Year

- We initiate a collaboration with ICL Lab (University of Tennessee) to study failure detection in Exascale computing. We designed and evaluated a new robust failure detector. This result is published at SC 2016 [26].

REO Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

An important industrial partnership has been signed with the start-up companies Kephalios and Epygon, for the mathematical modeling of implantable cardiac devices.

RITS Project-Team (section vide)

SECRET Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Post-quantum symmetric cryptanalysis

We have been considering the problem of symmetric cryptography in the future environment that will see the arrival of quantum computers. Indeed, this environment will pose a real problem for the majority of asymmetric primitives, but little is known about the implications for the security of symmetric primitives. Confidence in our symmetric primitives is entirely based on our knowledge within the field of cryptanalysis, but in reality, we do not know much about the symmetric post-quantum attacks. If we want post-quantum systems to be reliable and efficient, we need to understand how adversaries might exploit this new computing power. This year, two preliminary results have been obtained within the team and published at CRYPTO 2016 [51] and in the *IACR Transactions on Symmetric Cryptology* [23]. They include surprising results demonstrating that, in some scenarios, some symmetric systems can also become vulnerable to the quantum computer. Recently María Naya-Plasencia has been awarded an ERC starting grant, QUASYModo, to work on this subject. This grant will enable us to continue this work in more depth.

5.1.2. Real-word impact of some theoretical cryptanalytic works

Weak cryptography can be used long after weaknesses have been found by the academic community. For instance, Rogaway warned that the predictable IV used in TLS was a problem in 2002, but it took a public demonstration with a practical exploit in 2011 (the BEAST attack) for servers and clients to implement countermeasures. The same happened with the use of compression (CRIME), unsecure version fallback (POODLE), and known biases in RC4 (RC4NOMORE), to name a few examples. In joint works at NDSS and ACM CCS, K. Bhargavan from the PROSECCO project-team and G. Leurent showed two almost practical attacks against deprecated cryptographic primitives that are still used in real-world applications. The SLOTH attack targeted the use of MD5 in TLS for in-protocol signatures, and the Sweet32 attack targeted the use of 64-bit block ciphers: Blowfish in OpenVPN, and 3DES in TLS. Moreover, the SLOTH attack received a distinguished paper award at NDSS.

5.1.3. Symmetric ciphers for homomorphic encryption schemes

In order to avoid the (extremely) high expansion rate of homomorphic encryption, a solution consists in transmitting to the server the ciphertext c obtained by encrypting m with a symmetric scheme (the corresponding secret key encrypted by the homomorphic cipher is also transmitted). The server then needs to compute m encrypted with the homomorphic scheme from c, i.e. the server needs to homomorphically evaluate the decryption circuit of the symmetric cipher. Hybrid encryption schemes dedicated to this application then require the use of symmetric ciphers with very specific features. Our team has two important contributions on this topic: the design of new appropriate solutions based on stream ciphers [44], and the attack of a cipher proposed by Méaux et al. in this context [48], [32].

5.1.4. Awards

BEST PAPERS AWARDS :

[58] **Post-Quantum Cryptography - 7th International Workshop, PQCrypto 2016**. A. PHESSO, J.-P. TILLICH.

[41] **Network and Distributed System Security Symposium – NDSS 2016**. K. BHARGAVAN, G. LEURENT.

SERENA Team (section vide)

SIERRA Project-Team (section vide)

TAPDANCE Team

4. Highlights of the Year

4.1. Highlights of the Year

TAPDANCE Team created in June 2016.

A Starting Research Fellow, Pierre-Étiene Meunier, was hired by Inria to begin work with TAPDANCE in January 2017.

WHISPER Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

The main highlight of the year is the continuous spreading of Coccinelle within the developer community of the Linux kernel. We submitted the first patches to the Linux kernel based on Coccinelle in 2007. Since then, over 4500 patches have been accepted into the Linux kernel based on the use of Coccinelle, including around 3000 by over 500 developers from outside our research group. Another testimonial of the impact of our work is the signature of a Memorendum Of Understanding (MOU) with the Linux Foundation. As part of the MOU, Greg Kroah-Hartman will spend a year with Whisper starting in October 2016. Kroah-Hartman is one of the leading developers of the Linux kernel, and is one of only a few developers employed by the Linux Foundation, with another being Linus Torvalds. Greg participated in the activities of the Whisper team around the use of Coccinelle and research projects related to the Linux kernel, and he is a convinced ambassador of our research work.

Our work on Remote Core Locking (RCL) [10] was accepted in ACM Transaction in Computer Systems (TOCS) which is the most prestigious journal in systems. RCL is currently one of the most efficient locks for multicore architectures.

WILLOW Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Awards

- Jean Ponce (together with Svetlana Lazebnik and Cordelia Schmid) received the Longuet-Higgins Prize for “Fundamental contributions in Computer Vision", awarded at the IEEE Conference on Computer Vision and Pattern Recognition, 2016.