Cybersecurity Institute
Univ. Grenoble Alpes

Subscribe to our newsletter

# Newsletter #4 – April 2019

## Editorial

The Grenoble Alpes Cybersecurity Institute held the first edition of its Partners'Day on April 5th in the Auditorium of the IMAG building. All presentations are now available here.

We also co-sponsored the first edition of the Workshop on Randomness and Arithmetics for Cryptography on Hardware (WRAC-H) in Roscoff (France, April 15-19). With 8 talks by members of the Institute, Univ. Grenoble Alpes was one of the largest community present during the event. Congratulations to Eleonora Cagli (CEA-LETI), Titouan Coladon (Institut Fourier), Marie-Angela Cornélie (CEA-LETI), Cécile Dumas (CEA-LETI), Cyril Hugounenq (Institut Fourier), Etienne Marcatel (ATOS/Institut Fourier), Ramtine Tofighi-Shirazi (Trusted Labs/Institut Fourier) and Mohamed Traoré (Institut Fourier) for the quality of their presentations (all presentations will be available soon).

Finally, this edition's monthly column focuses on the activities of the Institut Fourier in the field of cybersecurity.

Univ. Grenoble Alpes
Editorial executive: philippe.elbaz-vincent@univ-grenoble-alpes.fr
Editor: romain.xu@univ-grenoble-alpes.fr

Cybersecurity Institute
Univ. Grenoble Alpes

Subscribe to our newsletter

# Events

RESSI'19 – May 15-17th 2019
Cyber@Alps will be present at RESSI'19 with two teaching papers (Cédric Lauradoux (Inria), Marie-Laure Potet and Laurent Mounier (Verimag)), a presentation of the project ASTRID SACADE (Scénarios d'Attaque Contre Automates avec Distribution et Encapsulation) by Stéphane Mocanu (LIG) and a presentation entitled "Les défis posés par la sécurisation de l'IoT industriel" by Maxime Puys et Pierre-Henri Thevenon (CEA-LETI).

JAIF'19 – May 23rd 2019
Following the 2018 edition held in Jussieu (May 29 2018), the Cybersecurity Institute is co-sponsoring a workshop on Fault Injection that will take place on May 23 2019 on the Minatec campus. Registration is now opened here.

Global Challenges Science Week – June 3-6th 2019
During the Global Challenges Science Week, the Grenoble Alpes Cybersecurity Institute will organize a workshop entitled "*Cybersecurity and society: on the necessity of an interdisciplinary approach*". The full program and registration form is available here.

# Accepted papers and conferences

- Cécile Dumas, **TRNG - Evaluation & certification**,
Workshop on Randomness and Arithmetics for Cryptography on Hardware (WRAC'H), Roscoff, France, April 15-19 2019
- Marie-Angéla Cornélie, **VHDL design of a crypto-processor for elliptic curves**,
Workshop on Randomness and Arithmetics for Cryptography on Hardware (WRAC'H), Roscoff, France, April 15-19 2019
- Eleonora Cagli, **Classifying Side-Channel desynchronized signals with convolutional neural networks**,
Workshop on Randomness and Arithmetics for Cryptography on Hardware (WRAC'H), Roscoff, France, April 15-19 2019
- Ramtine Tofighi, **Using Machine Learning to defeat software protection**,
Workshop on Randomness and Arithmetics for Cryptography on Hardware (WRAC'H), Roscoff, France, April 15-19 2019
- Titouan Coladon, Ph. Elbaz-Vincent, Etienne Marcatel, Cyril Hugounenq, **Hermitian fplll and applications**,
Workshop on Randomness and Arithmetics for Cryptography on Hardware (WRAC'H), Roscoff, France, April 15-19 2019
- Titouan Coladon, Ph. Elbaz-Vincent and Cyril Hugounenq, **MPHELL: a fast and robust library with unified arithmetic for elliptic curves cryptography**,
Workshop on Randomness and Arithmetics for Cryptography on Hardware (WRAC'H), Roscoff, France, April 15-19 2019
- Ph. Elbaz-Vincent, Cyril Hugounenq and Sebastien Riou, **SPAE: An authenticated encryption algorithms for low-cost embedded systems**,
Workshop on Randomness and Arithmetics for Cryptography on Hardware (WRAC'H), Roscoff, France, April 15-19 2019
- Ph. Elbaz-Vincent and Mohamed Traoré, **Generating RSA keys the wrong way!**,
Workshop on Randomness and Arithmetics for Cryptography on Hardware (WRAC'H), Roscoff, France, April 15-19 2019

# Internship opportunities

Several internship opportunities are still opened.

- Administration système et développement d'applications web
- Etat de l'art scientifique sur l'intégration des nouveaux risques de cyberattaque par les entreprises industrielles
- Vulnérabilités et évaluation des générateurs de nombres aléatoires des composants sécurisés
- Implementation of Post Quantum Cryptographic algorithms using High Level Synthesis tools on FPGAs

Univ. Grenoble Alpes
Editorial executive: philippe.elbaz-vincent@univ-grenoble-alpes.fr
Editor: romain.xu@univ-grenoble-alpes.fr

Cybersecurity Institute
Univ. Grenoble Alpes

Subscribe to our newsletter

# PhD positions

- Vulnerability search in Industrial Control Systems; a reverse engineering approach
- Hardware/Software co-design of countermeasures against fault injection
- Tools and methods for securing a memory hierarchy against software side-channel attacks
- Study of new solutions for the security of embedded systems
- Protecting binary elliptic curve cryptography against Template atttacks and Horizontal attacks
- Securing integrated circuits against deep learning based attacks
- Resistant and resilient processor to fault attacks and side-channel attacks
- Sécurisation matérielle de cryptographie post-quantique basée sur les isogénies entre courbes elliptiques

Univ. Grenoble Alpes
Editorial executive: philippe.elbaz-vincent@univ-grenoble-alpes.fr
Editor: romain.xu@univ-grenoble-alpes.fr

# Monthly column

## Focus on: Institut Fourier

*Philippe Elbaz-Vincent (Institut Fourier)*

Research activities of the CRYPTO Team of Institut Fourier
are focused on:

- cryptology of asymmetric ciphers (including post-quantum cryptography)
- design and security models of cryptographic mechanisms
- analysis of random number generators (in particular hardware RNGs)
- secure implementations and arithmetics of cryptographic mechanisms
- tools for software protections and whitebox cryptography (e.g., code obfuscation)
- analysis of security/cryptographic architectures
- mathematical foundations for cryptography

Most of our research projects are in partnership with small and large companies, in which we provide cryptographic specifications, and help in the generation of cryptographic parameters or the design of security/cryptographic architectures. **Read more**

Univ. Grenoble Alpes
Editorial executive: philippe.elbaz-vincent@univ-grenoble-alpes.fr
Editor: romain.xu@univ-grenoble-alpes.fr