Advances in Cryptology: from theory to practice

Scope and topics:

Due to the fast pace evolution of the Internet of Things and the highly increasing number of interconnected devices, cryptography, and more precisely public key cryptography became one of the most widespread solutions for Internet security. Various aspects related to this topic, such as new security models, highly technical and optimized implementations, ingenious side-channel attacks and new methods for cryptanalysis, were developed in the last decade. The scope of this session is to discuss several of these aspects with leading experts in the field.

Interested authors are encouraged to submit original contributions from a broad range of topics related to cryptology, including but not limited to the following areas:

- Foundations of cryptology
- New primitives in cryptography
- Security models
- Protocols
- Software and hardware implementations
- Side-channel attacks
- Applications

Special session organizers:

- **Assist. Prof. Vlad-Florin Drăgoi**

  V.F. Drăgoi was born in Arad, Romania in 1984. He received the B.Sc. degree in mathematics and the M.Sc. degree in applied mathematics, both from the Claude Bernard University Lyon 1, Lyon, France, in 2011 and respectively 2013, and the Ph.D. degree in computer science from the University of Rouen Normandy, Rouen, France, in 2017.

  Since 2018, he is a Research Fellow with the "Aurel Vlaicu" University of Arad (UAV), Arad, Romania. In 2020 he obtained a national research grant where he carries his research in code-based cryptography. He has published 24 journal/conference articles, and gave 14 talks to international conferences/workshops.

His research interests include post-quantum cryptography (with a focus on code-based cryptography), discrete mathematics applied to error correcting codes, and network reliability.

Dr. Drăgoi received a doctoral scholarship from the University of Rouen-Normandy from 2013 to 2016, and is the recipient of two IEEE best paper awards.

Invited talks:

- **Prof. Laureţiu Ferucio Ţiplea**

- **Assoc. Prof. Pierre-Louis Cayrel**
  After a bachelor degree in mathematics at the University of Avignon, a master in cryptography in Montpellier and a research master in Limoges, I did my PhD at the University of Limoges under the direction of Philippe Gaborit. I defended my PhD in October 2008. My PhD thesis was entitled "Design and optimization of cryptosystems based on error correcting codes". One year at the University Paris 8 as ATER helped me to progress in my research and get a two years' post-doc in Darmstadt CASED research center. Since September 2011, I am an associate professor at the University Jean Monnet Saint Etienne where I teach mathematics, computer science and electronics.

  Presentation: **Code-based identification and signature schemes**

- **Assoc. Prof. Brice Colombier**
  Brice Colombier received an Engineering degree in Electronics and Photonics from Télécom Saint-Étienne, France and an M.Sc. degree in Electronics and Embedded Systems from INSA Lyon, France, both in 2014. He then obtained a PhD in Microelectronics from Université de Lyon, France, in 2017. His PhD thesis subject was "Methods for protecting intellectual property of IP cores designers". After a one-year postdoc with CEA-Tech DPACA, Gardanne, France, and a two-year postdoc in Laboratoire Hubert Curien, Saint-Étienne, France, he joined Grenoble INP and the TIMA laboratory in Grenoble, France, as an Associate Professor in 2020. His research interests are in hardware security, applied cryptography and physical attacks. He teaches computer science and hardware security in Phelma Engineering School, Grenoble INP, France.

  Presentation: **Template attacks on implementations of symmetric cryptography algorithms**