



Second Workshop on Communication Security WCS2017

affiliated with EUROCRYPT 2017
Paris (France), April 30, 2017

- 8:00-9:00 WELCOME COFFEE
- 9:00-10:30 SESSION I
 - **A Study of Injection and Jamming Attacks in Wireless Secret Sharing Systems**
Arsenia Chorti
 - **Robust Secret Sharing for End-to-End Key Establishment with Physical Layer Keys under Active Attacks**
Stefan Pfennig, Sabrina Engelmann, Elke Franz and Anne Wolf
 - **Semantically-Secured Message-Key Trade-off over Wiretap Channels with Random Parameters**
Alexander Bunin, Ziv Goldfeld, Haim Permuter, Shlomo Shamai, Paul Cuff and Pablo Piantanida
 - **Hash-then-Encode: A Modular Semantically Secure Wiretap Code**
Setareh Sharifian, Fuchun Lin and Rei Safavi-Naini
- 10:30-11:00 COFFEE BREAK
- 11:00-12:00 INVITED TALK I
Prof. Jean Claude Belfiore, *Finite-Length Lattice Coding for Gaussian Wiretap Channels: A theta series perspective*
- 12:00-14:00 LUNCH BREAK
- 14:00-15:00 INVITED TALK II
Dr. Stefano Tessaro, *A Cryptographic Perspective on Information-theoretic Secrecy*
- 15:00-15:30 SESSION II
 - **A CCA-Secure Cryptosystem Using Massive MIMO Channels**
Thomas Dean and Andrea Goldsmith
- 15:30-16:00 COFFEE BREAK
- 16:00-17:30 SESSION III
 - **You are how you play: authenticating mobile users via game playing**
Marco Baesso, Pasquale Capuozzo, Mauro Conti, Luciano Gamberini, Merylin Monaro, Giuseppe Sartori and Riccardo Spolaor
 - **Fuzzy Authentication using Rank Distance**
Alessandro Neri, Joachim Rosenthal and Davide Schipani
 - **A McEliece-based Key Exchange Protocol for Optical Communication Systems**
Joo Yeon Cho, Helmut Griesser and Danish Rafique
 - **An ICN-based Authentication Protocol for a Simplified LTE Architecture**
Alberto Compagno, Mauro Conti and Muhammad Hassan Khan