International View of the State-of-the-Art of Cryptography and Security and its Use in Practice (VII)

May 1 2015

Venue: Sofia Hotel Balkan, Royal II

Participation:

Please contact Claire Vishik (claire.vishik@intel.com) if interested in participation and/or presenting. There is no registration or attendance fee.

Workshop Description

The goal of the workshop series is to provide a forum for an informal discussion in order to exchange opinions or provide updates on issues associated with the design, implementation, and use of commercial cryptography and secure computation.

Building on the ***International View of the State-of-the-Art of Cryptography and Security and its Use in Practice*** workshops in Dagstuhl in 2011, Beijing in 2012 Athens and Bangalore in 2013 and Copenhagen and Kaosiung in 2014, we will meet again in Sofia following EuroCrypt 2014 to bring together researchers from Europe, Asia, and North America from industry, academia, and government.

The one day workshop in Sofia will discuss directions and developments in theoretical and applied cryptography and surrounding societal and regulatory issues.

Based on suggestions of the workshop community, we will be covering several broad topics including (but not limited to):

- Real-life cryptography and implementation issues
- Areas of interest: lightweight cryptography, homomorphic encryption, secure computation
- Policy, regulatory, and cryptography usage environment
- Innovative use cases and ideas for cryptography
- Updates on cryptography-related research projects

We invite the attendees to send topics of interest to them and proposals for talks and/or discussions prior to the workshop. On May 1st, we will follow the format we used for the last four workshops: the focus areas will be anchored by an invited talk and/or panel of short talks, and the emphasis will be on discussion and exchange of opinions.

The program will be posted here as it firms up; updates will be also distributed by email to the workshop email list.

Workshop Program

9:00-9:20am	20 min	Opening statements, introductions – organizers
9:20-10:40am	80 min	Session 1 Secure computation and applications Christian Rechberger (DTU) – “Ciphers for MPC and FHE” Yvo Desmedt (University of Dallas), “ From Cryptology to Cryptonomy, or Are we putting all our Crypto Eggs in a Single Basket?” Discussion
10:40-11:00am	20 min	Break
11:00-12:30pm	90 min	Session 2: Post-quantum and homoorphic cryptography Tanja Lange (Eindhoven), Dan Bernstein (UIC, Eindhoven) – “Project PQCRYPTO” Bo-Yin Yang (NTU) –“ Recent Work on Post-Quantum Information Security Infrastructure” Andreas Hulsing (Eindhoven), “Standardization of hash-based signatures". Discussion
12:30-1:30pm	60 min	Lunch
1:30-3:00pm	90 min	Session 3. Novel applications Aggelos Kiyiaias (University of Athens), “Analyzing the bitcoin backbone : proving the security of blockchain protocols” Jens Groth (UCL), “Square Span Programs with Applications to Succinct NIZK Arguments” Discussion
3:00-3:15pm	15 min	Break
3:15-4:30pm	75 min	Session 4. Encryption & privacy and regulatory space Luis Brandao (CMU), “An analysis of two nation-scale brokered identification systems” Rene Peralta (NIST) – NIST work on privacy enhancing cryptography

		Claire Vishik (Intel) – Trends in the perceptions of the role of encryption around the world Discussion
4:30pm-5pm	20 min	Post workshop: Future topics, suggested format. Adjourn