10th International View of the State-of-the-Art of Cryptography and Security and its Use in Practice

Friday, December 9th, 2016 9am-5pm

Venue: Intercontinental Hanoi Westlake. Please follow signs to the meeting room.

Registration: If you are interested in participation, please contact Claire Vishik (claire.vishik@intel.com) for registration.

Workshop Description

The goal of the workshop is to create an informal discussion forum in order to exchange opinions on issues associated with the design, implementation, and use of commercial cryptography.

Following the workshops in Dagstuhl, Beijing, Athens, Bangalore, Copenhagen, Kaosiang, Sofia, and Auckland, and Vienna, the workshop in Hanoi will again bring together researchers & practitioners from different countries to discuss developments in theoretical and applied cryptography and surrounding societal and policy issues.

Each focus area will be anchored by an invited talk and/or panel of short talks, and the emphasis will be on discussion and exchange of opinions. Approaches and projects in different countries will be discussed, in order to continue to build a community of research and practice and in order to generate new ideas in this field.

Program will be distributed later. Proposed topics below are tentative.

9:00-9:20am	**Opening statements, introductions**
9:20-10:30am	**Session I. Blockchain: technology, economics, policy, etc.** **Speakers**: Juan Garay, Yahoo! Labs. ***Bootstrapping the Blockchain – Directly*** Claire Vishik, Intel. ***Industry Views on blockchain*** Others: TBD Discussion
10:30-10:50am	Break
10:50-12:00pm	**Session II. Emerging Standards and Technologies** Speakers: Bertram Pottering, Ruhr University Bochum. ***Standardized Signatures with Non-Standard Security Arguments.*** Jung He Cheon, Seoul National University***. Light-weight post-quantum public key encryption*** Others TBD Discussion
12:00-1:00pm	Lunch
1:00-2:30pm	**Session III: Innovation in Cryptography: Technology and Standards** **Speakers**: Rene Peralta, NIST. ***NIST Post-Quantum cryptography***

	Huy Vu Quoc, Hanoi University of Science and Technology. ***CONIKS: Bringing key transparency to end users with publicly verifiable Keystore*** **Discussion**
2:30-3:00pm	Break
3:00-4:30pm	**Session IV. New Ideas: Technology, Policy** **Speakers**: Qiang Tang, NJIT. ***Kleptographically IND-CPA Secure Public Key Encryption*** Rene Peralta, NIST. ***NIST Randomness Beacon*** **Discussion topics: regional differences in research; privacy; key policy issues. Moderator: Claire Vishik. Intel**
4:30pm-5pm	Closing, future workshops, adjourn