

**The Institute of Electronics, Information and Communication Engineers (IEICE)
Invited Talk 2016**

TOWARDS USER-FRIENDLY CRYPTOGRAPHY

Date: 2 December 2016 (Friday)

Time: 2.30 to 4.30 pm

Venue: Pullman Kuala Lumpur City Centre

Abstract

In this talk, we discuss user friendliness in cryptography and its importance. Especially, we reconsider the significance of generic constructions of cryptographic tools, using the case of proxy re-encryption as an example. We then suggest that enjoyable aspects of cryptographic tools may also be important for technology diffusion. We illustrate this using the case of card-based protocols as an example.

Dr. Goichiro Hanaoka



- Bachelor's degree, Department of Engineering, University of Tokyo (1997).
- Ph.D. degree, University of Tokyo (2002)
- Leader of the Advanced Cryptosystems Research Group, Information Technology Research Institute, National Institute of Advanced Industrial Science and Technology (AIST)

Honors:

- DoCoMo Mobile Science Award, Mobile Communication Fund (2016)
- Wilkes Award (2007), British Computer Society
- Best Paper Award (2008), The Institute of Electronics, Information and Communication Engineers (IEICE)
- Innovative Paper Awards (2012, 2014), Symposium on Cryptography & Information Security (SCIS), IEICE

Research Interests:

Dr. Goichiro Hanaoka engages in the R&D for encryption and information security technologies including the efficient design and security evaluation of public key cryptosystems.

Organized by IEICE Malaysia Section

Co-hosted by

