



Dr. Goichiro Hanaoka

Cyber Physical Security Research Center, AIST, Japan

Promoting Social Implementation of Advanced Cryptography Using Visible Cryptography

Advanced cryptography is a generic term for technologies that provide both advanced functionality and security, such as data processing and access control while keeping data secret. In today's increasingly complex information society, these technologies are expected to be widely used as technologies that enable utilization of data while protecting it. However, since there are a vast number of different types of advanced cryptographic schemes according to their specific use cases, it is difficult for non-experts to properly select the appropriate technique for their application. Therefore, in order to promote social implementation of advanced cryptography, the research and development of explanatory techniques to convince non-experts of the functionalities and security of various advanced cryptography without difficulty is itself considered extremely important. In this talk, we introduce the results of such work.

Speaker bio

Dr. Goichiro HANAOKA graduated from the Department of Engineering, the University of Tokyo in 1997. He received the Ph.D. degree from the University of Tokyo in 2002. He joined the National Institute of Advanced Industrial Science and Technology (AIST) in 2005, and currently, is a Prime Senior Researcher at Cyber Physical Security Research Center, AIST. He engages in the R&D for advanced cryptography including the efficient design and security evaluation of secure computation. He received numerous awards including the Commendation for Science and Technology by the Minister of Education, Culture, Sports, Science and Technology (2018); the DoCoMo Mobile Science Award (2016), Mobile Communication Fund; the Wilkes Award (2007), British Computer Society; Best Paper Award (2008, 2019), The Institute of Electronics, Information and Communication Engineers (IEICE); and Innovative Paper Awards (2012, 2014), Symposium on Cryptography & Information Security (SCIS), IEICE.