The Eighth International Conference on Provable Security (ProvSec 2014)
9-10 October 2014, University of Hong Kong, Hong Kong

Provable security is an important research area in modern cryptography. Cryptographic primitives or protocols without a rigorous proof cannot be regarded as secure in practice. In fact, there are many schemes that were originally thought as secure but eventually broken, which clearly indicates the need of formal security assurance. With provable security, we are confident in using cryptographic schemes and protocols in various real-world applications. Meanwhile, schemes with provable security sometimes give only theoretical feasibility rather than a practical construction, and correctness of the proofs may be difficult to verify. ProvSec conference thus provides a platform for researchers, scholars and practitioners to exchange new ideas for solving these problems in the provable security area.

The conference time and place puts it before **ISC 2014** in the same venue. This is a wonderful opportunity to attend two excellent security conferences in one trip!

The previous ProvSec conferences were successfully held in Wollongong, Australia (2007), Shanghai, China (2008), Guangzhou, China (2009), Malacca, Malaysia (2010 and 13), Xi'an, China (2011), and Chengdu, China (2012). The conference proceedings will be published by Springer-Verlag in the Lecture Notes in Computer Science series.

Conference Topics: All aspects of **provable security** for cryptographic primitives or protocols, include but are not limited to the following areas:

- Asymmetric provably secure cryptography
- Cryptographic primitives
- Lattice-based cryptography and security reductions
- Leakage-resilient cryptography
- Pairing-based provably secure cryptography
- Privacy and anonymity technologies
- Provable secure block ciphers and hash functions
- Secure cryptographic protocols and applications
- Security notions, approaches, and paradigms
- Steganography and steganalysis

Special issues:

Journal: Security and Communication Networks (SCN)
Topic: Provably Secure Cryptographic Solutions for Wireless Networks

Journal: Pervasive and Mobile Computing (PMC)
Topic: Security and Privacy in Mobile Clouds

Important Dates:

Conference date: **9-10 October 2014**
Paper submission deadline: ~~20~~ **30 June 2014**
Notification of acceptance: ~~23 July~~ **2 Aug 2014**
Proceedings version deadline: **12 August 2014**

General Co-Chairs:

Lucas C.K. Hui (University of Hong Kong, Hong Kong) hui@cs.hku.hk
S.M. Yiu (University of Hong Kong, Hong Kong) smyiu@cs.hku.hk

Program Co-Chairs:

Sherman S. M. Chow	(Chinese University of Hong Kong, Hong Kong)
Joseph K. Liu	(Institute for Infocomm Research, Singapore)

Program Committee:

Elena Andreeva	(KU Leuven, Belgium)
Man-Ho Au	(University of Wollongong, Australia)
Reza Azarderakhsh	(Rochester Institute of Technology, US)
Joonsang Baek	(Khalifa University of Science Technology & Research, UAE)
Paulo S. L. M. Barreto	(University of São Paulo, Brazil)
Olivier Blazy	(RUHR, Germany)
Andrej Bogdanov	(Chinese University of Hong Kong, Hong Kong)
Zhenfu Cao	(Shanghai Jiao Tong University, China)
Sanjit Chatterjee	(IISC, India)
Liqun Chen	(HP Labs, UK)
Xiaofeng Chen	(Xidian University, China)
Seung Geol Choi	(United States Naval Academy, US)
Nico Döttling	(Aarhus University, Denmark)
Georg Fuchsbauer	(IST, Austria)
David Galindo	(LORIA-CNRS, France)
Sanjam Garg	(IBM Research, US)
Matt Henricksen	(Institute for Infocomm Research, Singapore)
Xinyi Huang	(Fujian Normal University, China)
Stanislaw Jarecki	(University of California at Irvine, US)
Aniket Kate	(Sarrland University, Germany)
Miroslaw Kutylowski	(Wroclaw University of Technology, Poland)
Jin Li	(Guangzhou University, China)
Shengli Liu	(Shanghai Jiao Tong University, China)
Mark Manulis	(University of Surrey, UK)
Sarah Meiklejohn	(University of California at San Diego, US)
Kazuhiko Minematsu	(NEC, Japan)
Atsuko Miyaji	(JAIST, Japan)
Alptekin Küpçü	(Koç University, Turkey)
Reza Reyhanitabar	(EPFL, Switzerland)
Reihaneh Safavi-Naini	(University of Calgary, Canada)
Jacob C.N. Schuldt	(Royal Holloway University of London, UK)
Alice Silverberg	(University of California at Irvine, US)
Willy Susilo	(University of Wollongong, Australia)
Koutarou Suzuki	(NTT, Japan)
Tsuyoshi Takagi	(Kyushu University, Japan)
Berkant Ustaoğlu	(İzmir Institute of Technology, Turkey)
Cong Wang	(City University of Hong Kong, Hong Kong)
Duncan Wong	(City University of Hong Kong, Hong Kong)
Wun-She Yap	(Universiti Tunku Abdul Rahman, Malaysia)
Rui Zhang	(Chinese Academy of Sciences, China)
Zongyang Zhang	(AIST, Japan)