The Seventh International Conference on Provable Security (ProvSec 2013) will be held in Melaka, Malaysia on 23-25 October 2013. It will be organized by Universiti Teknikal Malaysia Melaka.

Provable security is an important research area in modern cryptography. Cryptographic primitives or protocols without a rigorous proof cannot be regarded as secure even 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 previous ProvSec conference series were successfully held in Wollongong, Australia (2007), Shanghai, China (2008), Guangzhou, China (2009), Malacca, Malaysia (2010), 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: Topics include all aspects of provable security for cryptographic primitives or protocols, and include but are not limited to the following areas:

- Cryptographic primitives
- Digital signatures
- Formal security model
- Lattice-based security reductions
- 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

Instructions for authors: Submissions must not substantially duplicate work that any of the authors has published elsewhere or has submitted in parallel for consideration of any other journal, conference/workshop with proceedings. The submission should begin with a title followed by a short abstract and keywords. Submissions should have at most 12 pages excluding the bibliography and appendices, and at most 20 pages in total, using at least 11-point fonts and with reasonable margins. All submissions should be anonymous. Authors of accepted papers must guarantee that at least one of the authors will attend the conference and present their paper. Submissions will be received electronically via EasyChair.

Important Dates:
- Paper submission deadline: 23 May 2013
- Notification of acceptance: 23 July 2013
- Proceedings version deadline: 12 August 2013

Conference Organization:

General Chairs:
Shekh Faisal Abdul-Latip (Universiti Teknikal Malaysia Melaka, Malaysia) shekhfaisal@utem.edu.my
Jennifer Seberry (University of Wollongong, Australia) jennie@uow.edu.au

Program Chairs:
Willy Susilo (University of Wollongong, Australia) wsusilo@uow.edu.au
Reza Reyhanitabar (EPFL, Switzerland) reza.reyhanitabar@epfl.ch
Program Committee:

Elena Andreeva (KU Leuven, Belgium)
Man Ho Au (University of Wollongong, Australia)
Joonsang Baek (Khalifa University of Science, Technology and Research, UAE)
Feng Bao (Institute for Infocomm Research, Singapore)
Ioana Boureanu (EPFL, Switzerland)
Xiaofeng Chen (Xidian University, China)
Sherman S.M. Chow (Chinese University of Hong Kong, Hong Kong)
Shoichi Hirose (University of Fukui, Japan)
Qiong Huang (South China Agricultural University, China)
Kauro Kurosawa (Ibaraki University, Japan)
Fabien Laguillaumie (UCBL, France)
Dong Hoon Lee (Korea University, Korea)
Jin Li (Guangzhou University, China)
Joseph K Liu (Institute for Infocomm Research, Singapore)
Masahiro Mambo (Kanazawa University, Japan)
Kazuhiko Minematsu (NEC Corporation, Japan)
Miyako Ohkubo (NICT, Japan)
Tatsuaki Okamoto (NTT, Japan)
Josef Pieprzyk (Macquarie University, Australia)
Rei Safavi-Naini (University of Calgary, Canada)
Tsuyoshi Takagi (Kyushu University, Japan)
Duncan S. Wong (City University of Hong Kong, China)
Guomin Yang (University of Wollongong, Australia)
Kan Yasuda (NTT, Japan)
Tsz Hon Yuen (University of Hong Kong, Hong Kong)