- Call for papers -

The Ninth International Conference on Provable Security (ProvSec 2015)
November 24-26, 2015 Kanazawa, Japan

Web Page: https://security-lab.jaist.ac.jp/provsec2015/ Contact: provsec2015-info@aqua.jaist.ac.jp

---

The Ninth International Conference on Provable Security (ProvSec 2015) will be held at Kanazawa Tokyu Hotel in Kanazawa, Japan on November 24-26, 2015. 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.

Publication and Awards:

The conference proceedings will be published by Springer-Verlag in the Lecture Notes in Computer Science series. The best paper(s) and best student paper(s) will be selected and awarded a prize.

Special Issues:

International Journal of Applied Cryptography (IJACT): Special Issue on "Provable Security for Information and Communications"
Journal of Mathematical Cryptology (JMC): Special Issue on "Recent Progress in Provable Security"
Computer Standards & Interfaces (CSI): Special Issue on "Cloud Computing Security and Privacy: Standards and Regulations"
Journal of Information Security and Applications (JISA): Special Issue on "Provable Security"

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 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

Important Dates:

Conference date:	**November 24-26, 2015**
Paper submission deadline:	~~June 17, 2015~~ ~~extended to June 29~~ **re-extended to July 4 at 23:59 (JST)**
Notification of acceptance:	~~August 17, 2015~~ **August 24, 2015**
Camera ready deadline:	~~August 24, 2015~~ **August 31, 2015**

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 conference or workshop with proceedings. Submissions should be anonymous, with no author names, affiliations, acknowledgement or obvious references. Submissions should have at most 16 pages excluding the bibliography and appendices, and at most 20 pages in total, using at least 11-point fonts and with reasonable margins. Please number the pages in submissions. The total length of the final versions for Springer's LNCS will be at most 20 pages. Committee members are not required to read appendices; the paper should be intelligible without them. At least one author of each accepted paper must register with the conference and present the paper. Submissions must be submitted electronically in PDF format, and the submission procedure and the submission link are announced at the web page. Submissions not meeting the submission guidelines risk rejection without consideration of their merits. It is strongly encouraged that submissions be processed in LaTeX.

Conference Venue:
Kanazawa is the prefectural capital of Ishikawa Prefecture and located in the central part of the mainland of Japan. It takes 45 min by airplane and 2 hours 28 min by bullet train from Tokyo. In Kanazawa, there are one of Japan's three most beautiful gardens called Kenrokuen, and Kanazawa Castle. For more information, visit http://www.kanazawa-tourism.com/.

Stipends:
The ProvSec 2015 student grant program provides a limited number of stipends to help partially cover travel and accommodation expenses for full-time students whose paper is accepted and present the paper at ProvSec 2015. More information about stipends, including instructions about how to apply, will appear on the web page.

Invited Lectures: *(tentative)*
Sanjam Garg (University of California, Berkeley): *Garbled Random-Access Machines.*
Phillip Rogaway (University of California, Davis): *Advances in Authenticated Encryption.*
Serge Vaudenay (EPFL): *On Privacy for RFID.*

Conference Organization:
Supported by:
Technical Committee on Information and Communication System Security (ICSS), IEICE, Japan
Technical Committee on Information Security (ISEC), IEICE, Japan
Special interest group on Computer SECurity (CSEC) of IPSJ, Japan

Jointly Organized by:
Information-technology Promotion Agency, Japan (IPA)
Japan Advanced Institute of Science and Technology (JAIST)

Sponsored by:
Mitsubishi Electric
National Institute of Information and Communications Technology (NICT)
Support Center for Advanced Telecommunications Technology Research (SCAT)
Nippon Telegraph and Telephone (NTT)

General Chair:
Tatsuaki Okamoto (NTT, Japan)

Program Co-Chairs:
Man-Ho Au (The Hong Kong Polytechnic University, Hong Kong)
Atsuko Miyaji (JAIST, Japan)

Program Committee:
Michel Abdalla (Ecole Normale Superieure, France)
Elena Andreeva (KU Leuven, Belgium)
Joonsang Baek (Khalifa University of Science Technology and Research, UAE)
Olivier Blazy (Université de Limoges, France)
Carlo Blundo (University of Salerno, Italy)
Colin Boyd (Norwegian University of Science and Technology, Norway)
Mike Burmester (FSU, US)
Liqun Chen (HP Labs, UK)
Chen-Mou Cheng (Kyushu University, Japan)
Céline Chevalier (Université Panthéon-Assas, France)
Yvo Desmedt (University of Texas at Dallas, US, and UCL, UK)
Alexandre Duc (École polytechnique fédérale de Lausanne EPFL, Switzerland)
Eiichiro Fujisaki (NTT, Japan)
David Galindo (Scytl Secure Electronic Voting, Spain)
Swee-Huay Heng (Multimedia University, Malaysia)
Xinyi Huang (Fujian Normal University, China)
Aniket Kate (Sarrland University, Germany)
Kwangjo Kim (KAIST, Korea)
Mirosław Kutyłowski (Wrocław University of Technology, Poland)
Alptekin Küpçü (Koç University, Turkey)
Joseph K.Liu (Monash University, Australia)
Subhamoy Maitra (Indian Statistical Institute, India)
Mark Manulis (University of Surrey, UK)
Mitsuru Matsui (Mitsubishi Electric Corporation, Japan)
Ali Miri (Ryerson University, Canada)
Tarik Moataz (Colorado State University, US)
Jong Hwan Park (Sangmyung University, Korea)
Josef Pieprzyk (Queensland University of Technology, Australia)
Willy Susilo (University of Wollongong, Australia)
Mehdi Tibouchi (NTT, Japan)
Damien Vergnaud (Écolenormale supérieure, France)
Cong Wang (City University of Hong Kong, Hong Kong)
Shouhuai Xu (University of Texas at San Antonio, US)
Bo-Yin Yang (Academia Sinica, Taiwan)
Fangguo Zhang (Sun Yat-sen University, China)

Steering Committee:
Feng Bao (Huawei, Singapore)
Xavier Boyen (Queensland University of Technology, Australia)
Joseph K. Liu (Monash University, Australia)
Yi Mu (University of Wollongong, Australia)
Josef Pieprzyk (Queensland University of Technology, Australia)
Willy Susilo (University of Wollongong, Australia