- Call for participation -

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 Copnference 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.

Program:
2015/11/24 (Tue)

09:30 - 10:15 Registration
10:15 - 10:25 Welcoming Remarks

Session: Fundamental
10:25 – 10:50 *From Stateful Hardware to Resettable Hardware Using Symmetric Assumptions*, Nico Döttling, Daniel Kraschewski, Jörn Müller-Quade and Tobias Nilges
10:50 – 11:15 *Constrained Verifiable Random Functions from Indistinguishability Obfuscation*, Bei Liang, Hongda Li and Jinyong Chang
11:15 – 11:40 *An Improved Attack for Recovering Noisy RSA Secret Keys and its Countermeasure*, Noboru Kunihiro

---

Invited Talk I
11:40 – 12:40 *Advances in Authenticated Encryption*, Philip Rogaway

---

13:00 - 22:00 Excursion (Including Lunch and Dinner)

2015/11/25 (Wed)

Session: Protocol
08:45 – 09:10 *Augmented Secure Channels and the Goal of the TLS 1.3 Record Layer*, Christian Badertscher, Christian Matt, Ueli Maurer, Phillip Rogaway and Björn Tackmann
09:10 – 09:35 *Sound Proof of Proximity of Knowledge*, Serge Vaudenay
09:35 – 10:00 *Multi-Party Computation with Small Shuffle Complexity Using Regular Polygon Cards*, Kazumasa Shinagawa, Takaaki Mizuki, Jacob Schuldt, Koji Nuida, Naoki Kanayama, Takashi Nishide, Goichiro Hanaoka and Eiji Okamoto

---

10:00 - 10:20 Coffee Break

Session: Authenticated Encryption & Key Exchange
10:20 – 10:45 *Forward-Secure Authenticated Symmetric Key Exchange Protocols: New Security Models and Some Constructions*, Suvradip Chakraborty, Goutam Paul and Chandrasekaran Pandu Rangan
10:45 – 11:10 *Full PRF-Secure Message Authentication Code based on Tweakable Block Cipher*, Yusuke Naito
11:10 – 11:25 *Efficient Key Authentication Service for Secure End-to-end Communications*, Mohammad Etemad and Alptekin Küpçü
11:25 – 11:40 *PPAE : Practical Parazoa Authenticated Encryption family*, Donghoon Chang, Sumesh Manjunath R and Somitra Kumar Sanadhya

---

Invited Talk II
11:40 – 12:40 *New Advances in Secure RAM Computation*, Sanjam Garg

---

12:40 - 13:50 Lunch

Session: Encryption & Identification
13:50 – 14:15 *Lightweight Anonymous Authentication for Ad Hoc Group: A Ring Signature Approach*, Xu Yang, Wei Wu, Joseph Liu and Xiaofeng Chen
14:15 – 14:40 *Reset-Secure Identity-Based Identification Schemes without Pairings*, Ji-Jian Chin, Hiroaki Anada and Syh-Yuan Tan
14:40 – 15:05 *Attribute-Based Encryption for Finite Automata from LWE*, Xavier Boyen and Qinyi Li
15:05 – 15:30 *Functional Signcryption: Notion, Construction, and Applications*, Pratish Datta, Ratna Dutta and Sourav Mukhopadhyay

15:30 - 15:50 Coffee Break

Session: Privacy and Cloud
15:50 – 16:15 *BetterTimes: Privacy-assured Outsourced Multiplications for Additively Homomorphic Encryption on Finite Fields*, Per Hallgren, Martín Ochoa and Andrei Sabelfeld
16:15 – 16:40 *Provably Secure Identity based Provable Data Possession*, Yong Yu, Yafang Zhang, Yi Mu, Willy Susilo and Hongyu Liu
16:40 – 16:55 *Efficient Private Set Intersection Cardinality in the Presence of Malicious Adversaries*, Sumit Kumar Debnath and Ratna Dutta
16:55 – 17:10 *A Formal Dynamic Verification of Choreographed Web Services Conversations*, Karim Dahmani, Mahjoub Langar and Riadh Robbana
17:10 – 17:25 *Efficient Unconditionally Secure Comparison and Private Preserving Machine Learning Classification Protocols*, Bernardo David, Rafael Dowsley, Raj Katti and Anderson Nascimento

18:30 - 20:30 Banquet

2015/11/26 (Thu)

Session: Leakage-Resilient Cryptography & Lattice Cryptography
08:45 – 09:10 *Attribute-based Encryption Leakage Resilient to Auxiliary Input*, Zhiwei Wang and Siu Ming Yiu
09:10 – 09:35 *On Provable Security of wPRF-based Leakage-Resilient Stream Ciphers*, Maciej Skórski
09:35 – 10:00 *Tighter Security for Efficient Lattice Cryptography via the Rényi Divergence of Optimized Orders*, Katsuyuki Takashima and Atsushi Takayasu

10:00 - 10:20 Coffee Break

Session: Signature & Broadcast Encryption
10:20 – 10:45 *Black-Box Separations of Hash-and-Sign Signatures in the Non-Programmable Random Oracle Model*, Zongyang Zhang, Yu Chen, Sherman S. M. Chow, Goichiro Hanaoka, Zhenfu Cao and Yunlei Zhao
10:45 – 11:10 *Rethinking Privacy for Extended Sanitizable Signatures and a Black-Box Construction of Strongly Private Schemes*, David Derler and Daniel Slamanig
11:10 – 11:25 *Unique Signature with Short Output from CDH Assumption*, Shiuan-Tzuo Shen, Amir Rezapour and Wen-Guey Tzeng
11:25 – 11:40 *Constructions of Unconditionally Secure Broadcast Encryption from Key Predistribution Systems with Trade-offs between Communication and Storage*, Yohei Watanabe and Junji Shikata

Invited Talk III
11:40 – 12:40 *On Privacy for RFID*, Serge Vaudenay

12:40 - Closing

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 (Osaka Univ/JAIST, Japan)