More information about this series at http://www.springer.com/series/7410
Man-Ho Au · Atsuko Miyaji (Eds.)

Provable Security

9th International Conference, ProvSec 2015
Kanazawa, Japan, November 24–26, 2015
Proceedings

Springer
Preface

The 9th International Conference on Provable Security (ProvSec 2015) was held in Kanazawa, November 24–26, 2015. The previous ProvSec series were successfully held in Wollongong, Australia (2007), Shanghai, China (2008), Guangzhou, China (2009), Malacca, Malaysia (2010), Xi’an, China (2011), Chengdu, China (2012), Malacca, Malaysia (2013) and Hong Kong, China (2014). This was the first ProvSec held in Japan.

The main goal of ProvSec as a conference is to promote research on all aspects of provable security for cryptographic primitives or protocols, including but 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; and steganography and steganalysis. This year we received 60 submissions from 23 different countries. Each submission was reviewed by at least three, and on average four, Program Committee members. Papers submitted by Program Committee members received at least four, and on the average 4.4, reviews. The committee decided to accept 19 regular papers and seven short papers. The broad range of areas covered by the high-quality accepted papers in the current edition attests to the fulfillment of that goal.

The program included three invited talks, given by Prof. Sanjam Garg (University of California, Berkeley) titled “New Advances in Secure RAM Computation,” Prof. Phillip Rogaway (University of California, Davis) titled “Advances in Authenticated Encryption,” and Prof. Serge Vaudenay (École Polytechnique Fédérale de Lausanne) titled “On Privacy for RFID.”

The decision on the best paper award was based on a vote among the Program Committee members. The best paper award was conferred upon the paper “From Stateful Hardware to Resettable Hardware Using Symmetric Assumptions” authored by Nico Döttling, Daniel Krachewski, Jörn Müller-Quade, and Tobias Nilges. In addition, the Program Committee selected the best student paper. To be eligible for selection, the primary author of the paper has to be a full-time student who gives a presentation at the conference. The winner was Bei Liang from the University of Chinese Academy of Sciences, Beijing, China, for the paper “Constrained Verifiable Random Functions from Indistinguishability Obfuscation.”

We are very grateful to our supporters and sponsors. The conference was co-organized by the Information-technology Promotion Agency, Japan (IPA) and Japan Advanced Institute of Science and Technology (JAIST), it was supported by the Technical Committee on Information and Communication System Security (ICSS), IEICE, Japan, the Technical Committee on Information Security (ISEC), IEICE, Japan, and the Special Interest Group on Computer Security (CSEC) of IPSJ, Japan, and was co-sponsored by Mitsubishi Electric, National Institute of Information and
Communications Technology (NICT), Support Center for Advanced Telecommunications Technology Research (SCAT), and Nippon Telegraph and Telephone Corporation (NTT).

We would like to thank the authors for submitting their papers to the conference. The selection of the papers was a challenging and dedicated task, and we are deeply grateful to the 35 Program Committee members and the external reviewers for their reviews and discussions. We would also like to thank EasyChair for providing a user-friendly interface for us to manage all submissions and proceedings files. Finally, we would like to thank the general chair, Dr. Tatsuaki Okamoto, and we the members of the local Organizing Committee.

September 2015

Man-Ho Au
Atsuko Miyaji
Provsec 2015
The 9th International Conference
on Provable Security

Jointly organized by

Information-technology Promotion Agency, Japan (IPA)
and
Japan Advanced Institute of Science and Technology (JAIST).

General Chair

Tatsuaki Okamoto  NTT, Japan

Program Co-chairs

Man Ho Au  Hong Kong Polytechnic University, SAR China
Atsuko Miyaji  Osaka University/JAIST, Japan

Program Committee

Michel Abdalla  École normale supérieure, 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  Florida State University, USA
Liqun Chen  Hewlett-Packard Laboratories, UK
Chen-Mou Cheng  Kyushu University, Japan
Céline Chevalier  Université Panthéon-Assas, France
Yvo Desmedt  The University of Texas at Dallas, USA and UCL, UK
Alexandre Duc  École polytechnique fédérale de Lausanne, 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  Saarland University, Germany
Kwangjo Kim  KAIST, Korea
Mirosław  Wrocław University of Technology, Poland
Kutylowski  
Alptekin Küpçi  Koç University, Turkey
Joseph 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, USA
Jonghwan Park  Sangmyung University, Korea
Josef Pieprzyk  Queensland University of Technology, Australia
Willy Susilo  University of Wollongong, Australia
Mehdi Tibouchi  NTT, Japan
Damien Vergnaud  École normale supérieure, France
Cong Wang  City University of Hong Kong, Hong Kong, SAR China
Shouhuai Xu  University of Texas at San Antonio, USA
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

Organizing Committee

Local Arrangements Co-chairs
Kazumasa Omote  JAIST, Japan
Shoichi Hirose  University of Fukui, Japan
Kenji Yasunaga  Kanazawa University, Japan
Yuji Suga  IIJ, Japan
Jiageng Chen  JAIST, Japan

Finance Co-chairs
Takato Hirano  Mitsubishi Electric, Japan
Masaki Fujikawa  ALSOK, Japan
Yuichi Futa  JAIST, Japan

Publicity Co-chairs
Takeshi Chikazawa  IPA, Japan
Ryo Kikuchi  NTT, Japan
Tsuyoshi Takagi  Kyushu University, Japan
Naoto Yanai  Osaka University, Japan
Liaison Co-chairs
Toru Nakamura KDDI Labs, Japan
Toru Nakanishi Hiroshima University, Japan
Seonghan Shin AIST, Japan

System Co-chairs
Atsuo Inomata NAIST, Japan
Akira Kanaoka Toho University, Japan
Toshihiro Yamauchi Okayama University, Japan
Masaaki Shirase Future University Hakodate, Japan

Publication Co-chairs
Isao Echizen NII, Japan
Keita Emura NICT, Japan
Satoru Tanaka JAIST, Japan

Registration Co-chairs
Hideyuki Miyake Toshiba, Japan
Dai Watanabe Hitachi, Japan
Chunhua Su JAIST, Japan

External Reviewers
Aminanto, Muhamad Erza Kakvi, Saqib A.
Arriaga, Afonso Kawai, Yutaka
Azzurra Marson, Giorgia Kim, Hakju
Behnia, Rouzbeh Kim, Hyoseung
Blasco Moreno, Pol Kim, Jong Hyun
Bogos, Sonia Kiyoshima, Susumu
Chen, Rongmao Kluczniak, Kamil
Choi, Rakyong Kuchta, Veronika
Ciampi, Michele Kuo, Po-Chun
Condition, Merge Lai, Junzuo
De Caro, Angelo Langlois, Adeline
Eom, Ji Eun Lauks-Dutka, Anna
Etemad, Mohammad Li, Huige
Faust, Sebastian Liang, Kaitai
Fuchsbauer, Georg Liu, Jianghua
Golebiewski, Zbigniew Matsuo, Shinichiro
Han, Jinguang Naito, Yusuke
Hanzlik, Lucjan Nakasho, Kazuhisa
Hassanzadeh, Yahya Onete, Cristina
Hirano, Takato Park, Seung Hwan
Iovino, Vincenzo Peters, Thomas
Poettering, Bertram
Rafols, Carla
Siniscalchi, Luisa
Slowik, Marcin
Sugawara, Takeshi
Sung, Jaechul
Taheri, Sanaz
Takashima, Katsuyuki
Tan, Syhyuan
Tang, Jiayong
Vaudenay, Serge

Vivek, Srinivas
Vizár, Damian
Wang, Ding
Wodo, Wojciech
Wu, Wei
Xagawa, Keita
Xie, Shaohao
Yau, Wei-Chuan
Yu, Yu
Zhang, Huang
Zhang, Yuexin
Invited Talks
Advances in Authenticated Encryption

Phillip Rogaway
Department of Computer Science, University of California, Davis, USA
rogaway@cs.ucdavis.edu

Abstract. Authenticated encryption (AE) is a rare topic for so effectively bringing provable-security to cryptographic practice. I’ll describe some recent advances in the AE, placing the ideas in their historical context. In particular, I’ll look at robust AE and why it was developed, and I’ll describe a recent notion for online AE, and why it was developed. I’ll give a modern account of generic composition. Finally, I’ll talk a bit about the CAESAR competition, which drew 57 AE submissions.
New Advances in Secure RAM Computation

Sanjam Garg
University of California, Berkeley, USA
sanjamg@berkeley.edu

Abstract. Customarily secure computation techniques are devised for circuits. Securing random access machine (RAM) programs using these approaches requires the conversion of the RAM program to a circuit, which can be prohibitive for various applications. For example, this conversion implies an exponential slowdown for binary search. State-of-the-art direct constructions for securing RAM programs suffer from inefficiencies such as large round-complexity or non-black-box use of underlying cryptographic primitives. In this talk we describe techniques for overcoming these barriers.

(Based on joint works with Steve Lu, Peihan Miao, Payman Mohassel, Omkant Pandey, Charalampos Papamanthou, Antigoni Polychroniadou, Rafail Ostrovsky, and Alessandra Scafuro.)
On Privacy for RFID

Serge Vaudenay

EPFL
CH-1015 Lausanne, Switzerland
http://lasec.epfl.ch

Abstract. Many wearable devices identify themselves in a pervasive way. But at the same time, people want to remain anonymous. Modeling anonymity and unlinkability in identification protocols is a delicate issue. In this paper, we revisit the privacy model from Asiacrypt 2007. We show how to achieve forward-privacy (in the V07 sense) using an IND-CCA secure cryptosystem with the PKC protocol. We review the impossibility result of strong privacy and the model extension from CANS 2012 to reach strong privacy (in the OV12 sense) using the PKC protocol with plaintext awareness. We also discuss on the simplified model from ESORICS 2011 and achieve strong-privacy (in the HPVP11 sense) using IND-CCA security only. Finally, we apply these results to add privacy protection in distance bounding protocols.
Contents

Invited Paper

On Privacy for RFID. .............................................. 3
Serge Vaudenay

Fundamental

From Stateful Hardware to Resettable Hardware Using Symmetric Assumptions. ........................................ 23
Nico Döttling, Daniel Kraschewski, Jörn Müller-Quade,
and Tobias Nilges

Constrained Verifiable Random Functions from Indistinguishability Obfuscation ........................................ 43
Bei Liang, Hongda Li, and Jinyong Chang

An Improved Attack for Recovering Noisy RSA Secret Keys and Its Countermeasure .................................... 61
Noboru Kunihiro

Protocol

Augmented Secure Channels and the Goal of the TLS 1.3 Record Layer . . . 85
Christian Badertscher, Christian Matt, Ueli Maurer, Phillip Rogaway,
and Björn Tackmann

Sound Proof of Proximity of Knowledge ......................... 105
Serge Vaudenay

Multi-party Computation with Small Shuffle Complexity Using Regular Polygon Cards ................................ 127
Kazumasa Shinagawa, Takaaki Mizuki, Jacob C.N. Schuldt, Koji Nuida,
Naoki Kanayama, Takashi Nishide, Goichiro Hanaoka,
and Eiji Okamoto

Authenticated Encryption and Key Exchange

Forward-Secure Authenticated Symmetric Key Exchange Protocol:
New Security Model and Secure Construction .................... 149
Suvradip Chakraborty, Goutam Paul, and C. Pandu Rangan
Full PRF-Secure Message Authentication Code Based on Tweakable Block Cipher ................................. 167
  Yusuke Naito

Efficient Key Authentication Service for Secure End-to-End Communications .................................. 183
  Mohammad Etemad and Alptekin Küçü

PPAE: Practical Parazoa Authenticated Encryption Family ................................. 198
  Donghoon Chang, Sumesh Manjunath R., and Somitra Kumar Sanadhya

Encryption and Identification

Lightweight Anonymous Authentication for Ad Hoc Group:
A Ring Signature Approach ........................................ 215
  Xu Yang, Wei Wu, Joseph K. Liu, and Xiaofeng Chen

Reset-Secure Identity-Based Identification Schemes Without Pairings ............ 227
  Ji-Jian Chin, Hiroaki Anada, and Syh-Yuan Tan

Attribute-Based Encryption for Finite Automata from LWE ...................... 247
  Xavier Boyen and Qinyi Li

Functional Signcryption: Notion, Construction, and Applications. ............ 268
  Pratish Datta, Ratna Dutta, and Sourav Mukhopadhyay

Privacy and Cloud

BetterTimes: Privacy-Assured Outsourced Multiplications for Additively Homomorphic Encryption on Finite Fields .................... 291
  Per Hallgren, Martín Ochoa, and Andrei Sabelfeld

Provably Secure Identity Based Provable Data Possession ....................... 310
  Yong Yu, Yafang Zhang, Yi Mu, Willy Susilo, and Hongyu Liu

Efficient Private Set Intersection Cardinality in the Presence of Malicious Adversaries ........................................ 326
  Sumit Kumar Debnath and Ratna Dutta

A Formal Dynamic Verification of Choreographed Web Services
Conversations ................................................................ 340
  Karim Dahmani, Mahjoub Langar, and Riadh Robbana

Efficient Unconditionally Secure Comparison and Privacy Preserving Machine Learning Classification Protocols .................... 354
  Bernardo David, Rafael Dowsley, Raj Katti,
  and Anderson C.A. Nascimento
Leakage-Resilient Cryptography and Lattice Cryptography

Attribute-Based Encryption Resilient to Auxiliary Input .......................... 371
  Zhiwei Wang and Siu Ming Yiu

On Provable Security of wPRF-Based Leakage-Resilient Stream Ciphers ......... 391
  Maciej Skórski

Tighter Security for Efficient Lattice Cryptography via the Rényi
Divergence of Optimized Orders ........................................... 412
  Katsuyuki Takashima and Atsushi Takayasu

Signature and Broadcast Encryption

Black-Box Separations of Hash-and-Sign Signatures in the
Non-Programmable Random Oracle Model ..................................... 435
  Zongyang Zhang, Yu Chen, Sherman S.M. Chow, Goichiro Hanaoka,
  Zhenfu Cao, and Yunlei Zhao

Rethinking Privacy for Extended Sanitizable Signatures
and a Black-Box Construction of Strongly Private Schemes ................. 455
  David Derler and Daniel Slamanig

Unique Signature with Short Output from CDH Assumption .................... 475
  Shiuan-Tzuo Shen, Amir Rezapour, and Wen-Guey Tzeng

Constructions of Unconditionally Secure Broadcast Encryption from Key
Predistribution Systems with Trade-Offs Between Communication
and Storage ................................................................. 489
  Yohei Watanabe and Junji Shikata

Author Index ........................................................................... 503