Man-Ho Au · Atsuko Miyaji (Eds.)

Provable Security

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

Springer
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

Suvradip Chakraborty, Goutam Paul, and C. Pandu Rangan
Contents

Full PRF-Secure Message Authentication Code Based on Tweakeable Block Cipher ................................................................. 167  
Yusuke Naito

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

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, Martin 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