

# Contents

## Invited Paper

On Privacy for RFID . . . . .	3
<i>Serge Vaudenay</i>	

## Fundamental

From Stateful Hardware to Resettable Hardware Using Symmetric Assumptions. . . . .	23
<i>Nico Döttling, Daniel Kraschewski, Jörn Müller-Quade, and Tobias Nilges</i>	
Constrained Verifiable Random Functions from Indistinguishability Obfuscation . . . . .	43
<i>Bei Liang, Hongda Li, and Jinyong Chang</i>	
An Improved Attack for Recovering Noisy RSA Secret Keys and Its Countermeasure . . . . .	61
<i>Noboru Kunihiro</i>	

## Protocol

Augmented Secure Channels and the Goal of the TLS 1.3 Record Layer . . . .	85
<i>Christian Badertscher, Christian Matt, Ueli Maurer, Phillip Rogaway, and Björn Tackmann</i>	
Sound Proof of Proximity of Knowledge . . . . .	105
<i>Serge Vaudenay</i>	
Multi-party Computation with Small Shuffle Complexity Using Regular Polygon Cards . . . . .	127
<i>Kazumasa Shinagawa, Takaaki Mizuki, Jacob C.N. Schuldt, Koji Nuida, Naoki Kanayama, Takashi Nishide, Goichiro Hanaoka, and Eiji Okamoto</i>	

## Authenticated Encryption and Key Exchange

Forward-Secure Authenticated Symmetric Key Exchange Protocol: New Security Model and Secure Construction . . . . .	149
<i>Suvradip Chakraborty, Goutam Paul, and C. Pandu Rangan</i>	

Full PRF-Secure Message Authentication Code Based on Tweakable Block Cipher . . . . .	167
<i>Yusuke Naito</i>	
Efficient Key Authentication Service for Secure End-to-End Communications . . . . .	183
<i>Mohammad Etemad and Alptekin Küpçü</i>	
PPAE: Practical Parazoa Authenticated Encryption Family . . . . .	198
<i>Donghoon Chang, Sumesh Manjunath R., and Somitra Kumar Sanadhya</i>	
<b>Encryption and Identification</b>	
Lightweight Anonymous Authentication for Ad Hoc Group: A Ring Signature Approach . . . . .	215
<i>Xu Yang, Wei Wu, Joseph K. Liu, and Xiaofeng Chen</i>	
Reset-Secure Identity-Based Identification Schemes Without Pairings . . . . .	227
<i>Ji-Jian Chin, Hiroaki Anada, and Syh-Yuan Tan</i>	
Attribute-Based Encryption for Finite Automata from LWE . . . . .	247
<i>Xavier Boyen and Qinyi Li</i>	
Functional Signcryption: Notion, Construction, and Applications. . . . .	268
<i>Pratish Datta, Ratna Dutta, and Sourav Mukhopadhyay</i>	
<b>Privacy and Cloud</b>	
BetterTimes: Privacy-Assured Outsourced Multiplications for Additively Homomorphic Encryption on Finite Fields . . . . .	291
<i>Per Hallgren, Martín Ochoa, and Andrei Sabelfeld</i>	
Provably Secure Identity Based Provable Data Possession . . . . .	310
<i>Yong Yu, Yafang Zhang, Yi Mu, Willy Susilo, and Hongyu Liu</i>	
Efficient Private Set Intersection Cardinality in the Presence of Malicious Adversaries . . . . .	326
<i>Sumit Kumar Debnath and Ratna Dutta</i>	
A Formal Dynamic Verification of Choreographed Web Services Conversations . . . . .	340
<i>Karim Dahmani, Mahjoub Langar, and Riadh Robbana</i>	
Efficient Unconditionally Secure Comparison and Privacy Preserving Machine Learning Classification Protocols . . . . .	354
<i>Bernardo David, Rafael Dowsley, Raj Katti, and Anderson C.A. Nascimento</i>	

## Leakage-Resilient Cryptography and Lattice Cryptography

Attribute-Based Encryption Resilient to Auxiliary Input . . . . .	371
<i>Zhiwei Wang and Siu Ming Yiu</i>	
On Provable Security of wPRF-Based Leakage-Resilient Stream Ciphers . . . .	391
<i>Maciej Skórski</i>	
Tighter Security for Efficient Lattice Cryptography via the Rényi	
Divergence of Optimized Orders . . . . .	412
<i>Katsuyuki Takashima and Atsushi Takayasu</i>	

## Signature and Broadcast Encryption

Black-Box Separations of Hash-and-Sign Signatures in the	
Non-Programmable Random Oracle Model. . . . .	435
<i>Zongyang Zhang, Yu Chen, Sherman S.M. Chow, Goichiro Hanaoka,</i>	
<i>Zhenfu Cao, and Yunlei Zhao</i>	
Rethinking Privacy for Extended Sanitizable Signatures	
and a Black-Box Construction of Strongly Private Schemes . . . . .	455
<i>David Derler and Daniel Slamanig</i>	
Unique Signature with Short Output from CDH Assumption . . . . .	475
<i>Shiuan-Tzuo Shen, Amir Rezapour, and Wen-Guey Tzeng</i>	
Constructions of Unconditionally Secure Broadcast Encryption from Key	
Predistribution Systems with Trade-Offs Between Communication	
and Storage . . . . .	489
<i>Yohei Watanabe and Junji Shikata</i>	
<b>Author Index</b> . . . . .	503

Provable Security

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

Au, M.-H.; Miyaji, A. (Eds.)

2015, XIX, 504 p. 65 illus. in color., Softcover

ISBN: 978-3-319-26058-7