

# Contents

## Applied Cryptography

Sampling from Arbitrary Centered Discrete Gaussians for Lattice-Based Cryptography. . . . .	3
<i>Carlos Aguilar-Melchor, Martin R. Albrecht, and Thomas Ricosset</i>	
Simple Security Definitions for and Constructions of 0-RTT Key Exchange . . . . .	20
<i>Britta Hale, Tibor Jager, Sebastian Lauer, and Jörg Schwenk</i>	
TOPSS: Cost-Minimal Password-Protected Secret Sharing Based on Threshold OPRF . . . . .	39
<i>Stanisław Jarecki, Aggelos Kiayias, Hugo Krawczyk, and Jiayu Xu</i>	
Secure and Efficient Pairing at 256-Bit Security Level. . . . .	59
<i>Yutaro Kiyomura, Akiko Inoue, Yuto Kawahara, Masaya Yasuda, Tsuayoshi Takagi, and Tetsutaro Kobayashi</i>	

## Data Protection and Mobile Security

No Free Charge Theorem: A Covert Channel via USB Charging Cable on Mobile Devices . . . . .	83
<i>Riccardo Spolaor, Laila Abudahi, Veelasha Moonsamy, Mauro Conti, and Radha Poovendran</i>	
Are You Lying: Validating the Time-Location of Outdoor Images . . . . .	103
<i>Xiaopeng Li, Wenyan Xu, Song Wang, and Xianshan Qu</i>	
Lights, Camera, Action! Exploring Effects of Visual Distractions on Completion of Security Tasks . . . . .	124
<i>Bruce Berg, Tyler Kaczmarek, Alfred Kobsa, and Gene Tsudik</i>	
A Pilot Study of Multiple Password Interference Between Text and Map-Based Passwords . . . . .	145
<i>Weizhi Meng, Wenjuan Li, Wang Hao Lee, Lijun Jiang, and Jianying Zhou</i>	

## Security Analysis

Hierarchical Key Assignment with Dynamic Read-Write Privilege Enforcement and Extended KI-Security . . . . .	165
<i>Yi-Ruei Chen and Wen-Guey Tzeng</i>	

A Novel GPU-Based Implementation of the Cube Attack: Preliminary Results Against Trivium. . . . . 184  
*Marco Cianfriglia, Stefano Guarino, Massimo Bernaschi, Flavio Lombardi, and Marco Pedicini*

Related-Key Impossible-Differential Attack on Reduced-Round SKINNY . . . . . 208  
*Ralph Ankele, Subhadeep Banik, Avik Chakraborti, Eik List, Florian Mendel, Siang Meng Sim, and Gaoli Wang*

Faster Secure Multi-party Computation of AES and DES Using Lookup Tables . . . . . 229  
*Marcel Keller, Emanuela Orsini, Dragos Rotaru, Peter Scholl, Eduardo Soria-Vazquez, and Srinivas Vivek*

**Cryptographic Primitives**

An Experimental Study of the BDD Approach for the Search LWE Problem . . . . . 253  
*Rui Xu, Sze Ling Yeo, Kazuhide Fukushima, Tsuyoshi Takagi, Hwajung Seo, Shinsaku Kiyomoto, and Matt Henricksen*

Efficiently Obfuscating Re-Encryption Program Under DDH Assumption . . . . . 273  
*Akshayaram Srinivasan and Chandrasekaran Pandu Rangan*

Lattice-Based Group Signatures: Achieving Full Dynamicity with Ease . . . . . 293  
*San Ling, Khoa Nguyen, Huaxiong Wang, and Yanhong Xu*

Breaking and Fixing Mobile App Authentication with OAuth2.0-based Protocols. . . . . 313  
*Ronghai Yang, Wing Cheong Lau, and Shangcheng Shi*

Adaptive Proofs Have Straightline Extractors (in the Random Oracle Model) . . . . . 336  
*David Bernhard, Ngoc Khanh Nguyen, and Bogdan Warinschi*

More Efficient Construction of Bounded KDM Secure Encryption . . . . . 354  
*Kaoru Kurosawa and Rie Habuka*

Signature Schemes with Randomized Verification . . . . . 373  
*Cody Freitag, Rishab Goyal, Susan Hohenberger, Venkata Koppula, Eysa Lee, Tatsuki Okamoto, Jordan Tran, and Brent Waters*

**Side Channel Attack**

Trade-Offs for S-Boxes: Cryptographic Properties and Side-Channel Resilience. . . . . 393  
*Claude Carlet, Annelie Heuser, and Stjepan Picek*

A Practical Chosen Message Power Analysis Approach Against Ciphers with the Key Whitening Layers . . . . . 415  
*Chenyang Tu, Lingchen Zhang, Zeyi Liu, Neng Gao, and Yuan Ma*

Side-Channel Attacks Meet Secure Network Protocols . . . . . 435  
*Alex Biryukov, Daniel Dinu, and Yann Le Corre*

**Cryptographic Protocol**

Lattice-Based DAPS and Generalizations: Self-enforcement in Signature Schemes . . . . . 457  
*Dan Boneh, Sam Kim, and Valeria Nikolaenko*

Forward-Secure Searchable Encryption on Labeled Bipartite Graphs . . . . . 478  
*Russell W.F. Lai and Sherman S.M. Chow*

Bounds in Various Generalized Settings of the Discrete Logarithm Problem . . . . . 498  
*Jason H.M. Ying and Noboru Kunihiro*

An Enhanced Binary Characteristic Set Algorithm and Its Applications to Algebraic Cryptanalysis . . . . . 518  
*Sze Ling Yeo, Zhen Li, Khoongming Khoo, and Yu Bin Low*

SCRAPE: Scalable Randomness Attested by Public Entities . . . . . 537  
*Ignacio Cascudo and Bernardo David*

cMix: Mixing with Minimal Real-Time Asymmetric Cryptographic Operations . . . . . 557  
*David Chaum, Debajyoti Das, Farid Javani, Aniket Kate, Anna Krasnova, Joeri De Ruiter, and Alan T. Sherman*

Almost Optimal Oblivious Transfer from QA-NIZK . . . . . 579  
*Olivier Blazy, Céline Chevalier, and Paul Germouty*

OnionPIR: Effective Protection of Sensitive Metadata in Online Communication Networks . . . . . 599  
*Daniel Demmler, Marco Holz, and Thomas Schneider*

**Data and Server Security**

Accountable Storage . . . . . 623  
*Giuseppe Ateniese, Michael T. Goodrich, Vassilios Lekakis, Charalampos Papamanthou, Evripidis Paraskevas, and Roberto Tamassia*

Maliciously Secure Multi-Client ORAM . . . . . 645  
*Matteo Maffei, Giulio Malavolta, Manuel Reinert,  
and Dominique Schröder*

Legacy-Compliant Data Authentication for Industrial  
Control System Traffic . . . . . 665  
*John Henry Castellanos, Daniele Antonioli, Nils Ole Tippenhauer,  
and Martín Ochoa*

Multi-client Oblivious RAM Secure Against Malicious Servers. . . . . 686  
*Erik-Oliver Blass, Travis Mayberry, and Guevara Noubir*

**Author Index** . . . . . 709



<http://www.springer.com/978-3-319-61203-4>

Applied Cryptography and Network Security  
15th International Conference, ACNS 2017, Kanazawa,  
Japan, July 10-12, 2017, Proceedings  
Gollmann, D.; Miyaji, A.; Kikuchi, H. (Eds.)  
2017, XVI, 710 p. 167 illus., Softcover  
ISBN: 978-3-319-61203-4