

# Contents

## Secure Computation I: Primitives and New Models

Universally Verifiable Multiparty Computation from Threshold Homomorphic Cryptosystems . . . . .	3
<i>Berry Schoenmakers and Meelof Veeningen</i>	
Communication-Optimal Proactive Secret Sharing for Dynamic Groups . . . . .	23
<i>Joshua Baron, Karim El Defrawy, Joshua Lampkins, and Rafail Ostrovsky</i>	
Round-Optimal Password-Based Group Key Exchange Protocols in the Standard Model . . . . .	42
<i>Jing Xu, Xue-Xian Hu, and Zhen-Feng Zhang</i>	

## Public Key Cryptographic Primitives

Generic Construction of UC-Secure Oblivious Transfer . . . . .	65
<i>Olivier Blazy and Céline Chevalier</i>	
Non-malleability Under Selective Opening Attacks: Implication and Separation . . . . .	87
<i>Zhengan Huang, Shengli Liu, Xianping Mao, and Ke-Wei Chen</i>	
A Signature Scheme with a Fuzzy Private Key . . . . .	105
<i>Kenta Takahashi, Takahiro Matsuda, Takao Murakami, Goichiro Hanaoka, and Masakatsu Nishigaki</i>	
Practical Ciphertext-Policy Attribute-Based Encryption: Traitor Tracing, Revocation, and Large Universe . . . . .	127
<i>Zhen Liu and Duncan S. Wong</i>	

## Secure Computation II: Applications

Zero-Knowledge Authenticated Order Queries and Order Statistics on a List . . .	149
<i>Esha Ghosh, Olga Ohrimenko, and Roberto Tamassia</i>	
Private Database Access with HE-over-ORAM Architecture . . . . .	172
<i>Craig Gentry, Shai Halevi, Charanjit Jutla, and Mariana Raykova</i>	
Accumulable Optimistic Fair Exchange from Verifiably Encrypted Homomorphic Signatures . . . . .	192
<i>Jae Hong Seo, Keita Emura, Keita Xagawa, and Kazuki Yoneyama</i>	

LightCore: Lightweight Collaborative Editing Cloud Services for Sensitive Data . . . . .	215
<i>Weiyu Jiang, Jingqiang Lin, Zhan Wang, Huorong Li, and Lei Wang</i>	

**Anonymity and Related Applications**

Violating Consumer Anonymity: Geo-Locating Nodes in Named Data Networking . . . . .	243
<i>Alberto Compagno, Mauro Conti, Paolo Gasti, Luigi Vincenzo Mancini, and Gene Tsudik</i>	
Post-Quantum Forward-Secure Onion Routing: (Future Anonymity in Today’s Budget) . . . . .	263
<i>Satrajit Ghosh and Aniket Kate</i>	
Scalable Divisible E-cash . . . . .	287
<i>Sébastien Canard, David Pointcheval, Olivier Sanders, and Jacques Traoré</i>	
Recovering Lost Device-Bound Credentials . . . . .	307
<i>Foteini Baldimtsi, Jan Camenisch, Lucjan Hanzlik, Stephan Krenn, Anja Lehmann, and Gregory Neven</i>	

**Cryptanalysis and Attacks (Symmetric Crypto)**

Analysis of Boomerang Differential Trails via a SAT-Based Constraint Solver URSA . . . . .	331
<i>Aleksandar Kircanski</i>	
Time–Memory Trade-Off Attack on the GSM A5/1 Stream Cipher Using Commodity GPGPU (Extended Abstract) . . . . .	350
<i>Jiqiang Lu, Zhen Li, and Matt Henricksen</i>	
Evaluation and Cryptanalysis of the Pandaka Lightweight Cipher . . . . .	370
<i>Yuval Yarom, Gefei Li, and Damith C. Ranasinghe</i>	

**Privacy and Policy Enforcement**

Cryptographic Enforcement of Information Flow Policies Without Public Information . . . . .	389
<i>Jason Crampton, Naomi Farley, Gregory Gutin, Mark Jones, and Bertram Poettering</i>	
A Fully Decentralized Data Usage Control Enforcement Infrastructure . . . . .	409
<i>Florian Kelbert and Alexander Pretschner</i>	

Oblivion: Mitigating Privacy Leaks by Controlling the Discoverability of Online Information . . . . .	431
<i>Milivoj Simeonovski, Fabian Bendun, Muhammad Rizwan Asghar, Michael Backes, Ninja Marnau, and Peter Druschel</i>	

### **Authentication via Eye Tracking and Proofs of Proximity**

Exploiting Eye Tracking for Smartphone Authentication . . . . .	457
<i>Dachuan Liu, Bo Dong, Xing Gao, and Haining Wang</i>	
Optimal Proximity Proofs Revisited. . . . .	478
<i>Handan Kılınç and Serge Vaudenay</i>	

### **Malware Analysis and Side Channel Attacks**

Replacement Attacks: Automatically Impeding Behavior-Based Malware Specifications . . . . .	497
<i>Jiang Ming, Zhi Xin, Pengwei Lan, Dinghao Wu, Peng Liu, and Bing Mao</i>	
Partial Key Exposure Attacks on CRT-RSA: Better Cryptanalysis to Full Size Encryption Exponents. . . . .	518
<i>Atsushi Takayasu and Noboru Kunihiro</i>	
Differential Power Analysis of a McEliece Cryptosystem. . . . .	538
<i>Cong Chen, Thomas Eisenbarth, Ingo von Maurich, and Rainer Steinwandt</i>	

### **Side Channel Countermeasures and Tamper Resistance/PUFs**

Arithmetic Addition over Boolean Masking: Towards First- and Second-Order Resistance in Hardware . . . . .	559
<i>Tobias Schneider, Amir Moradi, and Tim Güneysu</i>	
Foundations of Reconfigurable PUFs. . . . .	579
<i>Jonas Schneider and Dominique Schröder</i>	
mrPUF: A Novel Memristive Device Based Physical Unclonable Function. . .	595
<i>Yansong Gao, Damith C. Ranasinghe, Said F. Al-Sarawi, Omid Kavehei, and Derek Abbott</i>	

### **Leakage Resilience and Pseudorandomness**

On the XOR of Multiple Random Permutations . . . . .	619
<i>Bart Mennink and Bart Preneel</i>	

Robust Pseudo-Random Number Generators with Input Secure Against  
Side-Channel Attacks . . . . . 635  
*Michel Abdalla, Sonia Belaïd, David Pointcheval, Sylvain Ruhault,  
and Damien Vergnaud*

Leakage-Resilient Cryptography over Large Finite Fields: Theory  
and Practice . . . . . 655  
*Marcin Andrychowicz, Daniel Masny, and Edoardo Persichetti*

Secrecy Without Perfect Randomness: Cryptography with (Bounded) Weak  
Sources . . . . . 675  
*Michael Backes, Aniket Kate, Sebastian Meiser, and Tim Ruffing*

**Author Index** . . . . . 697

Applied Cryptography and Network Security

13th International Conference, ACNS 2015, New York,

NY, USA, June 2-5, 2015, Revised Selected Papers

Malkin, T.; Kolesnikov, V.; Lewko, A.B.; Polychronakis, M.

(Eds.)

2015, XVIII, 698 p. 152 illus. in color., Softcover

ISBN: 978-3-319-28165-0