

Contents

Authentication and Key Establishment

On the Security of the Algebraic Eraser Tag Authentication Protocol	3
<i>Simon R. Blackburn and M.J.B. Robshaw</i>	
A Cryptographic Analysis of UMTS/LTE AKA	18
<i>Stephanie Alt, Pierre-Alain Fouque, Gilles Macario-rat, Cristina Onete, and Benjamin Richard</i>	
Low-Cost Mitigation Against Cold Boot Attacks for an Authentication Token	36
<i>Ian Goldberg, Graeme Jenkinson, and Frank Stajano</i>	
Two More Efficient Variants of the J-PAKE Protocol	58
<i>Jean Lancrenon, Marjan Škrobot, and Qiang Tang</i>	
Hash-Based TPM Signatures for the Quantum World	77
<i>Megumi Ando, Joshua D. Guttman, Alberto R. Papaleo, and John Scire</i>	

Signatures with Advanced Properties

Fuzzy Signatures: Relaxing Requirements and a New Construction	97
<i>Takahiro Matsuda, Kenta Takahashi, Takao Murakami, and Goichiro Hanaoka</i>	
Foundations of Fully Dynamic Group Signatures	117
<i>Jonathan Bootle, Andrea Cerulli, Pyrros Chaidos, Essam Ghadafi, and Jens Groth</i>	
A Lattice-Based Group Signature Scheme with Message-Dependent Opening	137
<i>Benoît Libert, Fabrice Mouhartem, and Khoa Nguyen</i>	
Threshold-Optimal DSA/ECDSA Signatures and an Application to Bitcoin Wallet Security	156
<i>Rosario Gennaro, Steven Goldfeder, and Arvind Narayanan</i>	
Legally Fair Contract Signing Without Keystones	175
<i>Houda Ferradi, Rémi Géraud, Diana Maimuț, David Naccache, and David Pointcheval</i>	

DoS Attacks and Network Anomaly Detection

Why Software DoS Is Hard to Fix: Denying Access in Embedded Android Platforms 193
Ryan Johnson, Mohamed Elsabagh, and Angelos Stavrou

Network Anomaly Detection Using Unsupervised Feature Selection and Density Peak Clustering. 212
Xiejun Ni, Daojing He, Sammy Chan, and Farooq Ahmad

Deterministic and Functional Encryption

More Efficient Constructions for Inner-Product Encryption. 231
Somindu C. Ramanna

Attribute Based Encryption with Direct Efficiency Tradeoff 249
Nuttapong Attrapadung, Goichiro Hanaoka, Tsutomu Matsumoto, Tadanori Teruya, and Shota Yamada

Turing Machines with Shortcuts: Efficient Attribute-Based Encryption for Bounded Functions 267
Xavier Boyen and Qinyi Li

Offline Witness Encryption 285
Hamza Abusalah, Georg Fuchsbauer, and Krzysztof Pietrzak

Deterministic Public-Key Encryption Under Continual Leakage 304
Venkata Koppula, Omkant Pandey, Yannis Rouselakis, and Brent Waters

Computing on Encrypted Data

Better Preprocessing for Secure Multiparty Computation 327
Carsten Baum, Ivan Damgård, Tomas Toft, and Rasmus Zakarias

Trinocchio: Privacy-Preserving Outsourcing by Distributed Verifiable Computation. 346
Berry Schoenmakers, Meilof Veeningen, and Niels de Vreede

Verifiable Multi-party Computation with Perfectly Private Audit Trail 367
Édouard Cuvelier and Olivier Pereira

Practical Fault-Tolerant Data Aggregation 386
Krzysztof Grining, Marek Klonowski, and Piotr Syga

Accelerating Homomorphic Computations on Rational Numbers 405
Angela Jäschke and Frederik Armknecht

Non-Interactive Proofs and PRFs

New Techniques for Non-interactive Shuffle and Range Arguments 427
Alonso González and Carla Ráfols

Constrained PRFs for Unbounded Inputs with Short Keys 445
Hamza Abusalah and Georg Fuchsbauer

Symmetric Ciphers

Wide Trail Design Strategy for Binary MixColumns: Enhancing Lower Bound of Number of Active S-boxes. 467
Yosuke Todo and Kazumaro Aoki

Automatic Search of Linear Trails in ARX with Applications to SPECK and Chaskey. 485
Yunwen Liu, Qingju Wang, and Vincent Rijmen

Square Attack on 7-Round Kiasu-BC 500
Christoph Dobraunig, Maria Eichlseder, and Florian Mendel

On the Design Rationale of SIMON Block Cipher: Integral Attacks and Impossible Differential Attacks against SIMON Variants 518
Kota Kondo, Yu Sasaki, and Tetsu Iwata

Correlation Power Analysis of Lightweight Block Ciphers: From Theory to Practice 537
Alex Biryukov, Daniel Dinu, and Johann Großschädl

Cryptography in Software

Assisted Identification of Mode of Operation in Binary Code with Dynamic Data Flow Slicing 561
Pierre Lestrinant, Frédéric Guihéry, and Pierre-Alain Fouque

Parallel Implementation of BDD Enumeration for LWE. 580
Elena Kirshanova, Alexander May, and Friedrich Wiemer

Memory Carving in Embedded Devices: Separate the Wheat from the Chaff. . . 592
Thomas Gougeon, Morgan Barbier, Patrick Lacharme, Gildas Avoine, and Christophe Rosenberger

Security for Human Use

CAPTCHaStar! A Novel CAPTCHA Based on Interactive Shape Discovery . . . 611
Mauro Conti, Claudio Guarisco, and Riccardo Spolaor

TMGuard: A Touch Movement-Based Security Mechanism for Screen
Unlock Patterns on Smartphones 629
Weizhi Meng, Wenjuan Li, Duncan S. Wong, and Jianying Zhou

Gesture-Based Continuous Authentication for Wearable Devices:
The Smart Glasses Use Case 648
*Jagmohan Chauhan, Hassan Jameel Asghar, Anirban Mahanti,
and Mohamed Ali Kaafar*

Author Index 667



<http://www.springer.com/978-3-319-39554-8>

Applied Cryptography and Network Security
14th International Conference, ACNS 2016, Guildford,
UK, June 19-22, 2016. Proceedings
Manulis, M.; Sadeghi, A.-R.; Schneider, S. (Eds.)
2016, XIV, 668 p. 110 illus., Softcover
ISBN: 978-3-319-39554-8