

# Contents

## Privacy and Identity Management

An Efficient Self-blindable Attribute-Based Credential Scheme . . . . .	3
<i>Sietse Ringers, Eric Verheul, and Jaap-Henk Hoepman</i>	
Real Hidden Identity-Based Signatures . . . . .	21
<i>Sherman S. M. Chow, Haibin Zhang, and Tao Zhang</i>	
BehavioCog: An Observation Resistant Authentication Scheme. . . . .	39
<i>Jagmohan Chauhan, Benjamin Zi Hao Zhao, Hassan Jameel Asghar, Jonathan Chan, and Mohamed Ali Kaafar</i>	
Updatable Tokenization: Formal Definitions and Provably Secure Constructions . . . . .	59
<i>Christian Cachin, Jan Camenisch, Eduarda Freire-Stögbuchner, and Anja Lehmann</i>	

## Privacy and Data Processing

SecGDB: Graph Encryption for Exact Shortest Distance Queries with Efficient Updates . . . . .	79
<i>Qian Wang, Kui Ren, Minxin Du, Qi Li, and Aziz Mohaisen</i>	
Outsourcing Medical Dataset Analysis: A Possible Solution . . . . .	98
<i>Gabriel Kaptchuk, Matthew Green, and Aviel Rubin</i>	
Homomorphic Proxy Re-Authenticators and Applications to Verifiable Multi-User Data Aggregation . . . . .	124
<i>David Derler, Sebastian Ramacher, and Daniel Slamanig</i>	

## Cryptographic Primitives and API's

A Provably Secure PKCS#11 Configuration Without Authenticated Attributes. . . . .	145
<i>Ryan Stanley-Oakes</i>	
A Post-quantum Digital Signature Scheme Based on Supersingular Isogenies . . . . .	163
<i>Youngho Yoo, Reza Azarderakhsh, Amir Jalali, David Jao, and Vladimir Soukharev</i>	

Optimally Sound Sigma Protocols Under DCRA. . . . .	182
<i>Helger Lipmaa</i>	

Economically Optimal Variable Tag Length Message Authentication. . . . .	204
<i>Reihaneh Safavi-Naini, Viliam Lisý, and Yvo Desmedt</i>	

**Vulnerabilities and Exploits**

PEEP: Passively Eavesdropping Private Input via Brainwave Signals. . . . .	227
<i>Ajaya Neupane, Md. Lutfor Rahman, and Nitesh Saxena</i>	

Fantastic Timers and Where to Find Them: High-Resolution Microarchitectural Attacks in JavaScript. . . . .	247
<i>Michael Schwarz, Clémentine Maurice, Daniel Gruss, and Stefan Mangard</i>	

Attacks on Secure Logging Schemes. . . . .	268
<i>Gunnar Hartung</i>	

Economy Class Crypto: Exploring Weak Cipher Usage in Avionic Communications via ACARS. . . . .	285
<i>Matthew Smith, Daniel Moser, Martin Strohmeier, Vincent Lenders, and Ivan Martinovic</i>	

Short Paper: A Longitudinal Study of Financial Apps in the Google Play Store. . . . .	302
<i>Vincent F. Taylor and Ivan Martinovic</i>	

Short Paper: Addressing Sophisticated Email Attacks. . . . .	310
<i>Markus Jakobsson</i>	

**Blockchain Technology**

Escrow Protocols for Cryptocurrencies: How to Buy Physical Goods Using Bitcoin. . . . .	321
<i>Steven Goldfeder, Joseph Bonneau, Rosario Gennaro, and Arvind Narayanan</i>	

Trust Is Risk: A Decentralized Financial Trust Platform. . . . .	340
<i>Orfeas Stefanos Thyfronitis Litos and Dionysis Zindros</i>	

A Smart Contract for Boardroom Voting with Maximum Voter Privacy. . . . .	357
<i>Patrick McCorry, Siamak F. Shahandashti, and Feng Hao</i>	

Improving Authenticated Dynamic Dictionaries, with Applications to Cryptocurrencies . . . . .	376
<i>Leonid Reyzin, Dmitry Meshkov, Alexander Chepurnoy, and Sasha Ivanov</i>	

Short Paper: Service-Oriented Sharding for Blockchains. . . . .	393
<i>Adem Efe Gencer, Robbert van Renesse, and Emin Gün Sirer</i>	

## Security of Internet Protocols

The Security of NTP's Datagram Protocol . . . . .	405
<i>Aanchal Malhotra, Matthew Van Gundy, Mayank Varia, Haydn Kennedy, Jonathan Gardner, and Sharon Goldberg</i>	

Short Paper: On Deployment of DNS-Based Security Enhancements . . . . .	424
<i>Pawel Szalachowski and Adrian Perrig</i>	

## Blind Signatures

A Practical Multivariate Blind Signature Scheme . . . . .	437
<i>Albrecht Petzoldt, Alan Szepieniec, and Mohamed Saied Emam Mohamed</i>	

Efficient Round-Optimal Blind Signatures in the Standard Model . . . . .	455
<i>Essam Ghadafi</i>	

## Searching and Processing Private Data

Secure Multiparty Computation from SGX. . . . .	477
<i>Raad Bahmani, Manuel Barbosa, Ferdinand Brasser, Bernardo Portela, Ahmad-Reza Sadeghi, Guillaume Scerri, and Bogdan Warinschi</i>	

Efficient No-dictionary Verifiable Searchable Symmetric Encryption . . . . .	498
<i>Wakaha Ogata and Kaoru Kurosawa</i>	

Faster Homomorphic Evaluation of Discrete Fourier Transforms . . . . .	517
<i>Anamaria Costache, Nigel P. Smart, and Srinivas Vivek</i>	

## Secure Channel Protocols

Short Paper: TLS Ecosystems in Networked Devices vs. Web Servers. . . . .	533
<i>Nayanamana Samarasinghe and Mohammad Mannan</i>	

Unilaterally-Authenticated Key Exchange. . . . .	542
<i>Yevgeniy Dodis and Dario Fiore</i>	

Formal Modeling and Verification for Domain Validation and ACME . . . . .	561
<i>Karthikeyan Bhargavan, Antoine Delignat-Lavaud, and Nadim Kobeissi</i>	

Why Banker Bob (Still) Can't Get TLS Right: A Security Analysis of TLS in Leading UK Banking Apps . . . . .	579
<i>Tom Chothia, Flavio D. Garcia, Chris Heppel, and Chris McMahon Stone</i>	

**Privacy in Data Storage and Retrieval**

Lavinia: An Audit-Payment Protocol for Censorship-Resistant Storage . . . . .	601
<i>Cecylia Bocovich, John A. Doucette, and Ian Goldberg</i>	

A Simpler Rate-Optimal CPIR Protocol . . . . .	621
<i>Helger Lipmaa and Kateryna Pavlyk</i>	

**Poster Papers**

Accountability and Integrity for Data Management Using Blockchains . . . . .	641
<i>Anirban Basu, Joshua Jeesson Daniel, Sushmita Ruj, Mohammad Shahriar Rahman, Theo Dimitrakos, and Shinsaku Kiyomoto</i>	

The Amount as a Predictor of Transaction Fraud . . . . .	643
<i>Niek J. Bouman and Martha E. Nikolaou</i>	

$\Sigma$ -State Authentication Language, an Alternative to Bitcoin Script . . . . .	644
<i>Alexander Chepurnoy</i>	

Broker-Mediated Trade Finance with Blockchains . . . . .	646
<i>Mohammad Shahriar Rahman, Anirban Basu, and Shinsaku Kiyomoto</i>	

OpenTimestamps: Securing Software Updates Using the Bitcoin Blockchain . . . . .	647
<i>Peter Todd and Harry Halpin</i>	

<b>Author Index</b> . . . . .	649
-------------------------------	-----

Financial Cryptography and Data Security  
21st International Conference, FC 2017, Sliema, Malta,  
April 3-7, 2017, Revised Selected Papers  
Kiayias, A. (Ed.)  
2017, XIV, 650 p. 132 illus., Softcover  
ISBN: 978-3-319-70971-0