## Contents

Efficient, Reusable Fuzzy Extractors from LWE ........................................... 1  
*Daniel Apon, Chongwon Cho, Karim Eldefrawy, and Jonathan Katz*

**GENFACE:** Improving Cyber Security Using Realistic Synthetic Face  
Generation ........................................................................................................ 19  
*Margarita Osadchy, Yan Wang, Orr Dunkelman, Stuart Gibson,  
Julio Hernandez-Castro, and Christopher Solomon*

Supervised Detection of Infected Machines Using Anti-virus  
Induced Labels (Extended Abstract) ............................................................... 34  
*Tomer Cohen, Danny Hendler, and Dennis Potashnik*

Building Regular Registers with Rational Malicious Servers and  
Anonymous Clients ....................................................................................... 50  
*Antonella Del Pozzo, Silvia Bonomi, Riccardo Lazzeretti,  
and Roberto Baldoni*

On the Optimality of the Exponential Mechanism ....................................... 68  
*Francesco Aldà and Hans Ulrich Simon*

On Pairing Inversion of the Self-bilinear Map on Unknown  
Order Groups .................................................................................................. 86  
*Hyang-Sook Lee, Seongan Lim, and Ikkwon Yie*

Brief Announcement: Anonymous Credentials Secure to  
Ephemeral Leakage ....................................................................................... 96  
*Łukasz Krzywiecki, Marta Wszoła, and Mirosław Kutyłowski*

The Combinatorics of Product Scanning Multiplication and Squaring ........ 99  
*Adam L. Young and Moti Yung*

Stylometric Authorship Attribution of Collaborative Documents ............. 115  
*Edwin Dauber, Rebekah Overdorf, and Rachel Greenstadt*

A Distributed Investment Encryption Scheme: Investcoin ............................ 136  
*Filipp Valovich*

Physical Layer Security over Wiretap Channels  
with Random Parameters ............................................................................... 155  
*Ziv Goldfeld, Paul Cuff, and Haim H. Permuter*
Assisting Malware Analysis with Symbolic Execution: A Case Study 171
Roberto Baldoni, Emilio Coppa, Daniele Cono D’Elia, and Camil Demetrescu

Brief Announcement: A Consent Management Solution for Enterprises 189
Abigail Goldsteen, Shelly Garion, Sima Nadler, Natalia Razinkov, Yosef Moatti, and Paula Ta-Shma

Brief Announcement: Privacy Preserving Mining of Distributed Data Using a Trusted and Partitioned Third Party 193
Nir Maoz and Ehud Gudes

Brief Announcement: A Technique for Software Robustness Analysis in Systems Exposed to Transient Faults and Attacks 196
Sergey Frenkel and Victor Zakharov

Symmetric-Key Broadcast Encryption: The Multi-sender Case 200
Cody Freitag, Jonathan Katz, and Nathan Klein

A Supervised Auto-Tuning Approach for a Banking Fraud Detection System 215
Michele Carminati, Luca Valentini, and Stefano Zanero

Scalable Attack Path Finding for Increased Security 234
Tom Gonda, Rami Puzis, and Bracha Shapira

Learning Representations for Log Data in Cybersecurity 250
Ignacio Arnaldo, Alfredo Cuesta-Infante, Ankit Arun, Mei Lam, Costas Bassias, and Kalyan Veeramachaneni

Attack Graph Obfuscation 269
Hadar Polad, Rami Puzis, and Bracha Shapira

Malware Triage Based on Static Features and Public APT Reports 288
Giuseppe Laurenza, Leonardo Aniello, Riccardo Lazzeretti, and Roberto Baldoni

Author Index 307
Cyber Security Cryptography and Machine Learning
First International Conference, CSCML 2017,
Beer-Sheva, Israel, June 29-30, 2017, Proceedings
Dolev, S.; Lodha, S. (Eds.)
2017, XII, 307 p. 59 illus., Softcover
ISBN: 978-3-319-60079-6