

Contents

Efficient, Reusable Fuzzy Extractors from LWE	1
<i>Daniel Apon, Chongwon Cho, Karim Eldefrawy, and Jonathan Katz</i>	
GENFACE: Improving Cyber Security Using Realistic Synthetic Face Generation	19
<i>Margarita Osadchy, Yan Wang, Orr Dunkelman, Stuart Gibson, Julio Hernandez-Castro, and Christopher Solomon</i>	
Supervised Detection of Infected Machines Using Anti-virus Induced Labels (Extended Abstract)	34
<i>Tomer Cohen, Danny Hendler, and Dennis Potashnik</i>	
Building Regular Registers with Rational Malicious Servers and Anonymous Clients	50
<i>Antonella Del Pozzo, Silvia Bonomi, Riccardo Lazzeretti, and Roberto Baldoni</i>	
On the Optimality of the Exponential Mechanism	68
<i>Francesco Aldà and Hans Ulrich Simon</i>	
On Pairing Inversion of the Self-bilinear Map on Unknown Order Groups	86
<i>Hyang-Sook Lee, Seongan Lim, and Ikkwon Yie</i>	
Brief Announcement: Anonymous Credentials Secure to Ephemeral Leakage	96
<i>Lukasz Krzywiecki, Marta Wszola, and Mirosław Kutylowski</i>	
The Combinatorics of Product Scanning Multiplication and Squaring	99
<i>Adam L. Young and Moti Yung</i>	
Stylometric Authorship Attribution of Collaborative Documents	115
<i>Edwin Dauber, Rebekah Overdorf, and Rachel Greenstadt</i>	
A Distributed Investment Encryption Scheme: Investcoin	136
<i>Filipp Valovich</i>	
Physical Layer Security over Wiretap Channels with Random Parameters	155
<i>Ziv Goldfeld, Paul Cuff, and Haim H. Permuter</i>	

Assisting Malware Analysis with Symbolic Execution: A Case Study	171
<i>Roberto Baldoni, Emilio Coppa, Daniele Cono D'Elia, and Camil Demetrescu</i>	
Brief Announcement: A Consent Management Solution for Enterprises	189
<i>Abigail Goldsteen, Shelly Garion, Sima Nadler, Natalia Razinkov, Yosef Moatti, and Paula Ta-Shma</i>	
Brief Announcement: Privacy Preserving Mining of Distributed Data Using a Trusted and Partitioned Third Party	193
<i>Nir Maoz and Ehud Gudes</i>	
Brief Announcement: A Technique for Software Robustness Analysis in Systems Exposed to Transient Faults and Attacks.	196
<i>Sergey Frenkel and Victor Zakharov</i>	
Symmetric-Key Broadcast Encryption: The Multi-sender Case	200
<i>Cody Freitag, Jonathan Katz, and Nathan Klein</i>	
A Supervised Auto-Tuning Approach for a Banking Fraud Detection System	215
<i>Michele Carminati, Luca Valentini, and Stefano Zanero</i>	
Scalable Attack Path Finding for Increased Security	234
<i>Tom Gonda, Rami Puzis, and Bracha Shapira</i>	
Learning Representations for Log Data in Cybersecurity	250
<i>Ignacio Arnaldo, Alfredo Cuesta-Infante, Ankit Arun, Mei Lam, Costas Bassias, and Kalyan Veeramachaneni</i>	
Attack Graph Obfuscation	269
<i>Hadar Polad, Rami Puzis, and Bracha Shapira</i>	
Malware Triage Based on Static Features and Public APT Reports	288
<i>Giuseppe Laurenza, Leonardo Aniello, Riccardo Lazzaretti, and Roberto Baldoni</i>	
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