

Contents

Outsourcing Computations

- A Server-Assisted Hash-Based Signature Scheme 3
Ahto Buldas, Risto Laanoja, and Ahto Truu
- Outsourcing of Verifiable Attribute-Based Keyword Search 18
Go Ohtake, Reihaneh Safavi-Naini, and Liang Feng Zhang

Privacy Preservation

- Is RCB a Leakage Resilient Authenticated Encryption Scheme? 39
Farzaneh Abed, Francesco Berti, and Stefan Lucks
- Practical and Secure Searchable Symmetric Encryption
with a Small Index 53
*Ryuji Miyoshi, Hiroaki Yamamoto, Hiroshi Fujiwara,
and Takashi Miyazaki*
- Anonymous Certification for an e-Assessment Framework 70
*Christophe Kiennert, Nesrine Kaaniche, Maryline Laurent,
Pierre-Olivier Rocher, and Joaquin Garcia-Alfaro*
- PARTS – Privacy-Aware Routing with Transportation Subgraphs 86
Christian Roth, Lukas Hartmann, and Doğan Kesdoğan

Security and Privacy in Machine Learning

- Bayesian Network Models in Cyber Security: A Systematic Review 105
*Sabarathinam Chockalingam, Wolter Pieters, André Teixeira,
and Pieter van Gelder*
- Improving and Measuring Learning Effectiveness
at Cyber Defense Exercises 123
Kaie Maennel, Rain Ottis, and Olaf Maennel
- Privacy-Preserving Frequent Itemset Mining for Sparse and Dense Data 139
Peeter Laud and Alisa Pankova

Applications

Free Rides in Denmark: Lessons from Improperly Generated
 Mobile Transport Tickets 159
Rosario Giustolisi

Using the Estonian Electronic Identity Card for Authentication
 to a Machine 175
Danielle Morgan and Arnis Parsovs

Data Aware Defense (DaD): Towards a Generic and Practical
 Ransomware Countermeasure 192
*Aurélien Palisse, Antoine Durand, Hélène Le Bouder, Colas Le Guernic,
 and Jean-Louis Lanet*

A Large-Scale Analysis of Download Portals and Freeware Installers 209
Alberto Geniola, Markku Antikainen, and Tuomas Aura

Access Control

GPASS: A Password Manager with Group-Based Access Control 229
Thanh Bui and Tuomas Aura

Towards Accelerated Usage Control Based on Access Correlations 245
Richard Gay, Jinwei Hu, Heiko Mantel, and Johannes Schickel

Emerging Security Areas

Generating Functionally Equivalent Programs Having Non-isomorphic
 Control-Flow Graphs 265
*Rémi Géraud, Mirko Koscina, Paul Lenczner, David Naccache,
 and David Saupic*

Proof of a Shuffle for Lattice-Based Cryptography 280
Nuria Costa, Ramiro Martínez, and Paz Morillo

An Analysis of Bitcoin Laundry Services 297
Thibault de Balthasar and Julio Hernandez-Castro

Author Index 313



<http://www.springer.com/978-3-319-70289-6>

Secure IT Systems

22nd Nordic Conference, NordSec 2017, Tartu, Estonia,

November 8-10, 2017, Proceedings

Lipmaa, H.; Mitrokotsa, A.; Matulevičius, R. (Eds.)

2017, XVIII, 313 p. 77 illus., Softcover

ISBN: 978-3-319-70289-6