

Contents

Privacy, Logics, and Computational Models

A Proof Calculus for Attack Trees in Isabelle	3
<i>Florian Kammüller</i>	
Confidentiality of Interactions in Concurrent Object-Oriented Systems	19
<i>Olaf Owe and Toktam Ramezanifarkhani</i>	
Using Oblivious RAM in Genomic Studies	35
<i>Nikolaos P. Karvelas, Andreas Peter, and Stefan Katzenbeisser</i>	

Privacy and Encrypted Search

Towards Efficient and Secure Encrypted Databases: Extending Message-Locked Encryption in Three-Party Model	55
<i>Yuuji Furuta, Naoto Yanai, Masashi Karasaki, Katsuhiko Eguchi, Yasunori Ishihara, and Toru Fujiwara</i>	
Searchable Encrypted Relational Databases: Risks and Countermeasures	70
<i>Mohamed Ahmed Abdelraheem, Tobias Andersson, and Christian Gehrman</i>	
Private Verification of Access on Medical Data: An Initial Study	86
<i>Thais Bardini Idalino, Dayana Spagnuolo, and Jean Everson Martina</i>	

Data Privacy, Data Mining, and Applications

Default Privacy Setting Prediction by Grouping User's Attributes and Settings Preferences.	107
<i>Toru Nakamura, Welderufael B. Tesfay, Shinsaku Kiyomoto, and Jetzabel Serna</i>	
δ -privacy: Bounding Privacy Leaks in Privacy Preserving Data Mining	124
<i>Zhizhou Li and Ten H. Lai</i>	
Threshold Single Password Authentication	143
<i>Devriş İşler and Alptekin Küpçü</i>	
Towards a Toolkit for Utility and Privacy-Preserving Transformation of Semi-structured Data Using Data Pseudonymization	163
<i>Saffija Kasem-Madani, Michael Meier, and Martin Wehner</i>	

User Privacy

Privacy Dashcam – Towards Lawful Use of Dashcams Through Enforcement of External Anonymization	183
<i>Paul Wagner, Pascal Birnstill, Erik Krempel, Sebastian Brethauer, and Jürgen Beyerer</i>	
DLoc: Distributed Auditing for Data Location Compliance in Cloud	202
<i>Mojtaba Eskandari, Bruno Crispo, and Anderson Santana de Oliveira</i>	
Inonymous: Anonymous Invitation-Based System	219
<i>Sanaz Taheri Boshrooyeh and Alptekin Küpçü</i>	

Applied Cryptography and Privacy

PCS, A Privacy-Preserving Certification Scheme.	239
<i>Nesrine Kaaniche, Maryline Laurent, Pierre-Olivier Rocher, Christophe Kiennert, and Joaquin Garcia-Alfaro</i>	
Order-Preserving Encryption Using Approximate Integer Common Divisors	257
<i>James Dyer, Martin Dyer, and Jie Xu</i>	
Privacy-Preserving Deterministic Automata Evaluation with Encrypted Data Blocks	275
<i>Giovanni Di Crescenzo, Brian Coan, and Jonathan Kirsch</i>	

Consensus and Smart Contracts

Securing Proof-of-Stake Blockchain Protocols.	297
<i>Wenting Li, Sébastien Andreina, Jens-Matthias Bohli, and Ghassan Karame</i>	
Merged Mining: Curse or Cure?	316
<i>Aljosha Judmayer, Alexei Zamyatin, Nicholas Stifter, Artemios G. Voyiatzis, and Edgar Weippl</i>	
Atomically Trading with Roger: Gambling on the Success of a Hardfork	334
<i>Patrick McCorry, Ethan Heilman, and Andrew Miller</i>	

Smart Contracts and Blockchain Identity

In Code We Trust? Measuring the Control Flow Immutability of All Smart Contracts Deployed on Ethereum	357
<i>Michael Fröwis and Rainer Böhme</i>	

Who Am I? Secure Identity Registration on Distributed Ledgers	373
<i>Sarah Azouvi, Mustafa Al-Bassam, and Sarah Meiklejohn</i>	
A User-Centric System for Verified Identities on the Bitcoin Blockchain	390
<i>Daniel Augot, Hervé Chabanne, Thomas Chenevier, William George, and Laurent Lambert</i>	

Short Papers

Towards a Concurrent and Distributed Route Selection for Payment Channel Networks	411
<i>Elias Rohrer, Jann-Frederik Laß, and Florian Tschorsch</i>	
Graphene: A New Protocol for Block Propagation Using Set Reconciliation . . .	420
<i>A. Pinar Ozisik, Gavin Andresen, George Bissias, Amir Houmansadr, and Brian Levine</i>	
Short Paper: Revisiting Difficulty Control for Blockchain Systems	429
<i>Dmitry Meshkov, Alexander Chepurnoy, and Marc Jansen</i>	
Secure Event Tickets on a Blockchain	437
<i>Björn Tackmann</i>	
Author Index	445

Data Privacy Management, Cryptocurrencies and
Blockchain Technology
ESORICS 2017 International Workshops, DPM 2017 and
CBT 2017, Oslo, Norway, September 14-15, 2017,
Proceedings
Garcia-Alfaro, J.; Navarro-Arribas, G.; Hartenstein, H.;
Herrera-Joancomartí, J. (Eds.)
2017, XIII, 446 p. 68 illus., Softcover
ISBN: 978-3-319-67815-3