Contents

Privacy, Logics, and Computational Models

A Proof Calculus for Attack Trees in Isabelle . . . . . . . . . . . . . . . . . . . . . . . . 3
  Florian Kammüller

Confidentiality of Interactions in Concurrent Object-Oriented Systems . . . . 19
  Olaf Owe and Toktam Ramezanifarkhani

Using Oblivious RAM in Genomic Studies . . . . . . . . . . . . . . . . . . . . . . . . . 35
  Nikolaos P. Karvelas, Andreas Peter, and Stefan Katzenbeisser

Privacy and Encrypted Search

Towards Efficient and Secure Encrypted Databases: Extending
Message-Locked Encryption in Three-Party Model . . . . . . . . . . . . . . . . . . . . . . 55
  Yuuji Furuta, Naoto Yanai, Masashi Karasaki, Katsuhioko Eguchi,
  Yasunori Ishihara, and Toru Fujiwara

Searchable Encrypted Relational Databases: Risks and Countermeasures . . 70
  Mohamed Ahmed Abdelraheem, Tobias Andersson,
  and Christian Gehrmann

Private Verification of Access on Medical Data: An Initial Study . . . . 86
  Thais Bardini Idalino, Dayana Spagnuelo, and Jean Everson Martina

Data Privacy, Data Mining, and Applications

Default Privacy Setting Prediction by Grouping User’s Attributes
and Settings Preferences . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 107
  Toru Nakamura, Welderufael B. Tesfay, Shinsaku Kiyomoto,
  and Jetzabel Serna

δ-privacy: Bounding Privacy Leaks in Privacy Preserving Data Mining . . 124
  Zhizhou Li and Ten H. Lai

Threshold Single Password Authentication . . . . . . . . . . . . . . . . . . . . . . . . . . 143
  Devriş İşler and Alptekin Küpçü

Towards a Toolkit for Utility and Privacy-Preserving Transformation
of Semi-structured Data Using Data Pseudonymization . . . . . . . . . . . . . . . . . . 163
  Saffija Kasem-Madani, Michael Meier, and Martin Wehner
User Privacy

Privacy Dashcam – Towards Lawful Use of Dashcams
Through Enforcement of External Anonymization .................................................. 183
  Paul Wagner, Pascal Birnstill, Erik Krempel, Sebastian Bretthauer,
  and Jürgen Beyerer

DLoc: Distributed Auditing for Data Location Compliance in Cloud .............. 202
  Mojtaba Eskandari, Bruno Crispo, and Anderson Santana de Oliveira

Inonomous: Anonymous Invitation-Based System .............................................. 219
  Sanaz Taheri Boshrooyeh and Alptekin Küpçü

Applied Cryptography and Privacy

PCS, A Privacy-Preserving Certification Scheme .............................................. 239
  Nesrine Kaaniche, Maryline Laurent, Pierre-Olivier Rocher,
  Christophe Kiennert, and Joaquín García-Alfaro

Order-Preserving Encryption Using Approximate Integer
Common Divisors .................................................................................................. 257
  James Dyer, Martin Dyer, and Jie Xu

Privacy-Preserving Deterministic Automata Evaluation
with Encrypted Data Blocks ................................................................................ 275
  Giovanni Di Crescenzo, Brian Coan, and Jonathan Kirsch

Consensus and Smart Contracts

Securing Proof-of-Stake Blockchain Protocols .................................................. 297
  Wenting Li, Sébastien Andreina, Jens-Matthias Bohl, and Ghassan Karame

Merged Mining: Curse or Cure? ........................................................................ 316
  Aljosha Judmayer, Alexei Zamyatin, Nicholas Stifter,
  Artemios G. Voyiatzis, and Edgar Weippl

Atomically Trading with Roger: Gambling on the Success of a Hardfork ........ 334
  Patrick McCorry, Ethan Heilman, and Andrew Miller

Smart Contracts and Blockchain Identity

In Code We Trust? Measuring the Control Flow Immutability
of All Smart Contracts Deployed on Ethereum ............................................. 357
  Michael Fröwis and Rainer Böhme
**Who Am I? Secure Identity Registration on Distributed Ledgers**
Sarah Azouvi, Mustafa Al-Bassam, and Sarah Meiklejohn

373

**A User-Centric System for Verified Identities on the Bitcoin Blockchain**
Daniel Augot, Hervé Chabanne, Thomas Chenevier, William George, and Laurent Lambert

390

**Short Papers**

**Towards a Concurrent and Distributed Route Selection for Payment Channel Networks**
Elias Rohrer, Jann-Frederik Laß, and Florian Tschorsch

411

**Graphene: A New Protocol for Block Propagation Using Set Reconciliation**
A. Pinar Ozisik, Gavin Andresen, George Bissias, Amir Houmansadr, and Brian Levine

420

**Short Paper: Revisiting Difficulty Control for Blockchain Systems**
Dmitry Meshkov, Alexander Chepurnoy, and Marc Jansen

429

**Secure Event Tickets on a Blockchain**
Björn Tackmann

437

**Author Index**

445
Data Privacy Management, Cryptocurrencies and Blockchain Technology
2017, XIII, 446 p. 68 illus., Softcover
ISBN: 978-3-319-67815-3