

# Contents

## Encrypted Computing and Applied Homomorphic Cryptography

Simple Encrypted Arithmetic Library - SEAL v2.1 . . . . .	3
<i>Hao Chen, Kim Laine, and Rachel Player</i>	
Towards Privacy-Preserving Multi-party Bartering. . . . .	19
<i>Stefan Wüller, Ulrike Meyer, and Susanne Wetzl</i>	
Multi-level Access in Searchable Symmetric Encryption . . . . .	35
<i>James Alderman, Keith M. Martin, and Sarah Louise Renwick</i>	
Privacy-Preserving Computations of Predictive Medical Models with Minimax Approximation and Non-Adjacent Form . . . . .	53
<i>Jung Hee Cheon, Jinhyuck Jeong, Joohee Lee, and Keewoo Lee</i>	
Private Outsourced Kriging Interpolation . . . . .	75
<i>James Alderman, Benjamin R. Curtis, Oriol Farràs, Keith M. Martin, and Jordi Ribes-González</i>	
An Analysis of FV Parameters Impact Towards Its Hardware Acceleration. . .	91
<i>Joël Cathébras, Alexandre Carbon, Renaud Sirdey, and Nicolas Ventroux</i>	
Controlled Homomorphic Encryption: Definition and Construction . . . . .	107
<i>Yvo Desmedt, Vincenzo Iovino, Giuseppe Persiano, and Ivan Visconti</i>	

## Bitcoin and Blockchain Research

ValueShuffle: Mixing Confidential Transactions for Comprehensive Transaction Privacy in Bitcoin . . . . .	133
<i>Tim Ruffing and Pedro Moreno-Sanchez</i>	
Could Network Information Facilitate Address Clustering in Bitcoin? . . . . .	155
<i>Till Neudecker and Hannes Hartenstein</i>	
Switch Commitments: A Safety Switch for Confidential Transactions . . . . .	170
<i>Tim Ruffing and Giulio Malavolta</i>	
(Short Paper) PieceWork: Generalized Outsourcing Control for Proofs of Work . . . . .	182
<i>Philip Daian, Ittay Eyal, Ari Juels, and Emin Gün Sirer</i>	

Enhancing Bitcoin Transactions with Covenants . . . . .	191
<i>Russell O'Connor and Marta Piekarska</i>	
Decentralized Prediction Market Without Arbiters . . . . .	199
<i>Iddo Bentov, Alex Mizrahi, and Meni Rosenfeld</i>	
An Analysis of Bitcoin OP_RETURN Metadata . . . . .	218
<i>Massimo Bartoletti and Livio Pompianu</i>	
Constant-Deposit Multiparty Lotteries on Bitcoin . . . . .	231
<i>Massimo Bartoletti and Roberto Zunino</i>	
Exchange Pattern Mining in the Bitcoin Transaction Directed Hypergraph . . .	248
<i>Stephen Ranshous, Cliff A. Joslyn, Sean Kreyling, Kathleen Nowak, Nagiza F. Samatova, Curtis L. West, and Samuel Winters</i>	
Incentivizing Blockchain Forks via Whale Transactions . . . . .	264
<i>Kevin Liao and Jonathan Katz</i>	
Mixing Coins of Different Quality: A Game-Theoretic Approach . . . . .	280
<i>Svetlana Abramova, Pascal Schöttle, and Rainer Böhme</i>	
Smart Contracts Make Bitcoin Mining Pools Vulnerable . . . . .	298
<i>Yaron Velner, Jason Teutsch, and Loi Luu</i>	
BatchVote: Voting Rules Designed for Auditability . . . . .	317
<i>Ronald L. Rivest, Philip B. Stark, and Zara Perumal</i>	
<b>Advances in Secure Electronic Voting Schemes</b>	
Existential Assertions for Voting Protocols . . . . .	337
<i>R. Ramanujam, Vaishnavi Sundararajan, and S.P. Suresh</i>	
Marked Mix-Nets . . . . .	353
<i>Olivier Pereira and Ronald L. Rivest</i>	
Pseudo-Code Algorithms for Verifiable Re-encryption Mix-Nets . . . . .	370
<i>Rolf Haenni, Philipp Locher, Reto Koenig, and Eric Dubuis</i>	
Using Selene to Verify Your Vote in JCJ. . . . .	385
<i>Vincenzo Iovino, Alfredo Rial, Peter B. Rønne, and Peter Y.A. Ryan</i>	
A Roadmap to Fully Homomorphic Elections: Stronger Security, Better Verifiability . . . . .	404
<i>Kristian Gjøsteen and Martin Strand</i>	
Enabling Vote Delegation for Boardroom Voting . . . . .	419
<i>Oksana Kulyk, Stephan Neumann, Karola Marky, and Melanie Volkamer</i>	

Practical Governmental Voting with Unconditional Integrity and Privacy . . . .	434
<i>Nan Yang and Jeremy Clark</i>	

### **Trusted Smart Contracts**

Findel: Secure Derivative Contracts for Ethereum . . . . .	453
<i>Alex Biryukov, Dmitry Khovratovich, and Sergei Tikhomirov</i>	
Decentralized Execution of Smart Contracts: Agent Model Perspective and Its Implications . . . . .	468
<i>Lin Chen, Lei Xu, Nolan Shah, Zhimin Gao, Yang Lu, and Weidong Shi</i>	
A Concurrent Perspective on Smart Contracts . . . . .	478
<i>Ilya Sergey and Aquinas Hobor</i>	
An Empirical Analysis of Smart Contracts: Platforms, Applications, and Design Patterns . . . . .	494
<i>Massimo Bartoletti and Livio Pompianu</i>	
Trust in Smart Contracts is a Process, As Well . . . . .	510
<i>Firas Al Khalil, Tom Butler, Leona O'Brien, and Marcello Ceci</i>	
Defining the Ethereum Virtual Machine for Interactive Theorem Provers . . . .	520
<i>Yoichi Hirai</i>	
SmartCast: An Incentive Compatible Consensus Protocol Using Smart Contracts . . . . .	536
<i>Abhiram Kothapalli, Andrew Miller, and Nikita Borisov</i>	
On the Feasibility of Decentralized Derivatives Markets . . . . .	553
<i>Shayan Eskandari, Jeremy Clark, Vignesh Sundaresan, and Moe Adham</i>	
A Proof-of-Stake Protocol for Consensus on Bitcoin Subchains . . . . .	568
<i>Massimo Bartoletti, Stefano Lande, and Alessandro Sebastian Podda</i>	

### **Targeted Attacks**

X-Platform Phishing: Abusing Trust for Targeted Attacks Short Paper . . . . .	587
<i>Hossein Siadati, Toan Nguyen, and Nasir Memon</i>	
What to Phish in a Subject? . . . . .	597
<i>Ana Ferreira and Rui Chilro</i>	
Unpacking Spear Phishing Susceptibility . . . . .	610
<i>Zinaida Benenson, Freya Gassmann, and Robert Landwirth</i>	

**Poster Papers**

Scripting Smart Contracts for Distributed Ledger Technology . . . . .	631
<i>Pablo Lamela Seijas, Simon Thompson, and Darryl McAdams</i>	
ZeroTrade: Privacy Respecting Assets Trading System Based on Public Ledger . . . . .	633
<i>Lei Xu, Lin Chen, Nolan Shah, Zhimin Gao, Yang Lu, and Weidong Shi</i>	
<b>Author Index</b> . . . . .	635

Financial Cryptography and Data Security

FC 2017 International Workshops, WAHC, BITCOIN,  
VOTING, WTSC, and TA, Sliema, Malta, April 7, 2017,

Revised Selected Papers

Brenner, M.; Rohloff, K.; Bonneau, J.; Miller, A.; Ryan,  
P.Y.A.; Teague, V.; Bracciali, A.; Sala, M.; Pintore, F.;  
Jakobsson, M. (Eds.)

2017, XXII, 636 p. 97 illus., Softcover

ISBN: 978-3-319-70277-3