

Contents – Part I

Smart Contracts

Attacking the DeFi Ecosystem with Flash Loans for Fun and Profit	3
<i>Kaihua Qin, Liyi Zhou, Benjamin Livshits, and Arthur Gervais</i>	
The Eye of Horus: Spotting and Analyzing Attacks on Ethereum Smart Contracts	33
<i>Christof Ferreira Torres, Antonio Ken Iannillo, Arthur Gervais, and Radu State</i>	
Timelocked Bribing	53
<i>Tejaswi Nadahalli, Majid Khabbazzian, and Roger Wattenhofer</i>	
Shielded Computations in Smart Contracts Overcoming Forks	73
<i>Vincenzo Botta, Daniele Friolo, Daniele Venturi, and Ivan Visconti</i>	
A Formal Model of Algorand Smart Contracts	93
<i>Massimo Bartoletti, Andrea Bracciali, Cristian Lepore, Alceste Scalas, and Roberto Zunino</i>	

Anonymity and Privacy in Cryptocurrencies

Everything You Ever Wanted to Know About Bitcoin Mixers (But Were Afraid to Ask)	117
<i>Jaswant Pakki, Yan Shoshitaishvili, Ruoyu Wang, Tiffany Bao, and Adam Doupé</i>	
PERIMETER: A Network-Layer Attack on the Anonymity of Cryptocurrencies	147
<i>Maria Apostolaki, Cedric Maire, and Laurent Vanbever</i>	
An Empirical Analysis of Privacy in the Lightning Network	167
<i>George Kappos, Haaroon Yousaf, Ania Piotrowska, Sanket Kanjalkar, Sergi Delgado-Segura, Andrew Miller, and Sarah Meiklejohn</i>	
Cross-Layer Deanonymization Methods in the Lightning Protocol	187
<i>Matteo Romiti, Friedhelm Victor, Pedro Moreno-Sanchez, Peter Sebastian Nordholt, Bernhard Haslhofer, and Matteo Maffei</i>	

The Complex Shape of Anonymity in Cryptocurrencies: Case Studies from a Systematic Approach	205
<i>Niluka Amarasinghe, Xavier Boyen, and Matthew McKague</i>	

Secure Multi-party Computation

Improving the Efficiency of AES Protocols in Multi-Party Computation	229
<i>F. Betül Durak and Jorge Guajardo</i>	
Rabbit: Efficient Comparison for Secure Multi-Party Computation	249
<i>Eleftheria Makri, Dragos Rotaru, Frederik Vercauteren, and Sameer Wagh</i>	
Efficient Noise Generation to Achieve Differential Privacy with Applications to Secure Multiparty Computation	271
<i>Reo Eriguchi, Atsunori Ichikawa, Noboru Kunihiro, and Koji Nuida</i>	

System and Application Security

Specfusator: Evaluating Branch Removal as a Spectre Mitigation	293
<i>Martin Schwarzl, Claudio Canella, Daniel Gruss, and Michael Schwarz</i>	
Speculative Dereferencing: Reviving Foreshadow	311
<i>Martin Schwarzl, Thomas Schuster, Michael Schwarz, and Daniel Gruss</i>	
Sigforgery: Breaking and Fixing Data Authenticity in Sigfox	331
<i>Loïc Ferreira</i>	
Short Paper: Terrorist Fraud in Distance Bounding: Getting Around the Models	351
<i>David Gerault</i>	
SoK: Securing Email—A Stakeholder-Based Analysis	360
<i>Jeremy Clark, P. C. van Oorschot, Scott Ruoti, Kent Seamons, and Daniel Zappala</i>	

Zero-Knowledge Proofs

Zero-Knowledge Proofs for Set Membership: Efficient, Succinct, Modular	393
<i>Daniel Benarroch, Matteo Campanelli, Dario Fiore, Kobi Gurkan, and Dimitris Kolonelos</i>	
Generic Plaintext Equality and Inequality Proofs	415
<i>Olivier Blazy, Xavier Bultel, Pascal Lafourcade, and Octavio Perez Kempner</i>	

Somewhere Statistically Binding Commitment Schemes with Applications	436
<i>Prastudy Fauzi, Helger Lipmaa, Zaira Pindado, and Janno Siim</i>	
Another Look at Extraction and Randomization of Groth’s zk-SNARK	457
<i>Karim Baghery, Markulf Kohlweiss, Janno Siim, and Mikhail Volkhov</i>	
BooLigero: Improved Sublinear Zero Knowledge Proofs for Boolean Circuits	476
<i>Yaron Gvili, Sarah Scheffler, and Mayank Varia</i>	
Mining for Privacy: How to Bootstrap a Snarky Blockchain	497
<i>Thomas Kerber, Aggelos Kiayias, and Markulf Kohlweiss</i>	
Author Index	515