

Contents

On the Malleability of Bitcoin Transactions	1
<i>Marcin Andrychowicz, Stefan Dziembowski, Daniel Malinowski, and Łukasz Mazurek</i>	
Trends, Tips, Tolls: A Longitudinal Study of Bitcoin Transaction Fees.	19
<i>Malte Möser and Rainer Böhme</i>	
ZombieCoin: Powering Next-Generation Botnets with Bitcoin	34
<i>Syed Taha Ali, Patrick McCorry, Peter Hyun-Jeen Lee, and Feng Hao</i>	
Cuckoo Cycle: A Memory Bound Graph-Theoretic Proof-of-Work	49
<i>John Tromp</i>	
When Bitcoin Mining Pools Run Dry	63
<i>Aron Laszka, Benjamin Johnson, and Jens Grossklags</i>	
Issues in Designing a Bitcoin-like Community Currency	78
<i>David Vandervort, Dale Gaucas, and Robert St Jacques</i>	
The Bitcoin Market Potential Index	92
<i>Garrick Hileman</i>	
Cryptographic Currencies from a Tech-Policy Perspective: Policy Issues and Technical Directions	94
<i>Emily McReynolds, Adam Lerner, Will Scott, Franziska Roesner, and Tadayoshi Kohno</i>	
Blindcoin: Blinded, Accountable Mixes for Bitcoin	112
<i>Luke Valenta and Brendan Rowan</i>	
Privacy-Enhancing Overlays in Bitcoin	127
<i>Sarah Meiklejohn and Claudio Orlandi</i>	
Search-and-Compute on Encrypted Data	142
<i>Jung Hee Cheon, Miran Kim, and Myungsun Kim</i>	
Accelerating SWHE Based PIRs Using GPUs.	160
<i>Wei Dai, Yarkin Doröz, and Berk Sunar</i>	
Combining Secret Sharing and Garbled Circuits for Efficient Private IEEE 754 Floating-Point Computations	172
<i>Pille Pullonen and Sander Siim</i>	

Cryptanalysis of a (Somewhat) Additively Homomorphic Encryption Scheme Used in PIR	184
<i>Tancrede Lepoint and Mehdi Tibouchi</i>	
Homomorphic Computation of Edit Distance	194
<i>Jung Hee Cheon, Miran Kim, and Kristin Lauter</i>	
HEtest: A Homomorphic Encryption Testing Framework	213
<i>Mayank Varia, Sophia Yakubov, and Yang Yang</i>	
Users' Privacy Concerns About Wearables	231
<i>Vivian Genaro Motti and Kelly Caine</i>	
On Vulnerabilities of the Security Association in the IEEE 802.15.6 Standard	245
<i>Mohsen Toorani</i>	
Visual Cryptography and Obfuscation: A Use-Case for Decrypting and Deobfuscating Information Using Augmented Reality	261
<i>Patrik Lantz, Bjorn Johansson, Martin Hell, and Ben Smeets</i>	
Ok Glass, Leave Me Alone: Towards a Systematization of Privacy Enhancing Technologies for Wearable Computing.	274
<i>Katharina Krombholz, Adrian Dabrowski, Matthew Smith, and Edgar Weippl</i>	
Design and Analysis of Shoulder Surfing Resistant PIN Based Authentication Mechanisms on Google Glass	281
<i>Dhruv Kumar Yadav, Beatrice Ionascu, Sai Vamsi Krishna Ongole, Aditi Roy, and Nasir Memon</i>	
Glass OTP: Secure and Convenient User Authentication on Google Glass	298
<i>Pan Chan, Tzipora Halevi, and Nasir Memon</i>	
Author Index	309

Financial Cryptography and Data Security
FC 2015 International Workshops, BITCOIN, WAHC, and
Wearable, San Juan, Puerto Rico, January 30, 2015,
Revised Selected Papers
Brenner, M.; Christin, N.; Johnson, B.; Rohloff, K. (Eds.)
2015, XII, 309 p. 59 illus., Softcover
ISBN: 978-3-662-48050-2