1. Record Nr. UNISA996466185603316

Titolo	Financial Cryptography and Data Security [[electronic resource]] : FC 2015 International Workshops, BITCOIN, WAHC, and Wearable, San Juan, Puerto Rico, January 30, 2015, Revised Selected Papers / / edited by Michael Brenner, Nicolas Christin, Benjamin Johnson, Kurt Rohloff
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2015
ISBN	3-662-48051-4
Edizione	[1st ed. 2015.]
Descrizione fisica	1 online resource (XII, 309 p. 59 illus.)
Collana	Security and Cryptology ; ; 8976
Disciplina	332.10285
Soggetti	Computer security Data encryption (Computer science) E-commerce Application software Management information systems Computer science Systems and Data Security Cryptology e-Commerce/e-business Computer Appl. in Administrative Data Processing Management of Computing and Information Systems
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di contenuto	Intro -- BITCOIN 2015: Second Workshop on Bitcoin Research -- WAHC 2015: Third Workshop on Encrypted Computing and Applied Homomorphic Cryptography -- Wearable 2015: First Workshop on Wearable Security and Privacy -- Contents -- On the Malleability of Bitcoin Transactions -- 1 Introduction -- 1.1 Possible Fixes to the Bitcoin Malleability Problem -- 1.2 Our Contribution -- 1.3 Ethical Issues -- 2 Bitcoin Description -- 3 Experiments -- 4 Malleability in Bitcoin Contracts -- 4.1 The Deposit Protocol -- 4.2 Other Protocols Vulnerable to the Malleability Attack -- 5 Our Technique -- 5.1 Bitcoin-Based Timed Commitment Scheme -- 5.2 The Details of Our

Method -- References -- Trends, Tips, Tolls: A Longitudinal Study of Bitcoin Transaction Fees -- 1 Introduction -- 2 Background and Research Questions -- 3 Data and Method -- 4 Results -- 4.1 Trends: Descriptive Analysis -- 4.2 Tips: Explaining the Decision to Offer a Fee -- 4.3 Tolls: Mining Pools as Gatekeepers -- 5 Discussion -- 6 Concluding Remarks -- References -- ZombieCoin: Powering Next-Generation Botnets with Bitcoin -- 1 Introduction -- 2 Background -- 2.1 Botnet C&C Mechanisms -- 2.2 Bitcoin -- 3 ZombieCoin -- 3.1 Inserting C&C Instructions in Transactions -- 4 Proof of Concept -- 5 Discussion -- 6 Prior Work -- 7 Conclusion -- References -- Cuckoo Cycle: A Memory Bound Graph-Theoretic Proof-of-Work -- 1 Introduction -- 2 Motivation -- 3 Graph-Theoretic Proofs-of-work -- 4 Cuckoo Cycle -- 5 Cuckoo Hashing -- 6 Cycle Detection in Cuckoo Cycle -- 7 Union-Find -- 8 Cuckoo Cycle Basic Algorithm -- 9 Difficulty Control -- 10 Edge Trimming -- 11 Time-Memory Trade-Offs (TMTOs) -- 12 Choice of Cycle Length -- 13 Parallelization -- 14 Choice of Graph Size -- 15 Dynamic Sizing -- 16 Conclusion -- References -- When Bitcoin Mining Pools Run Dry -- 1 Introduction -- 2 Related Work -- 3 Model.
3.1 Overview -- 3.2 Players -- 3.3 Choices -- 3.4 Consequences -- 4 Model Analysis -- 4.1 Steady-State Pool Sizes -- 4.2 Steady-State Pool Utilities -- 4.3 Peaceful Equilibria -- 4.4 One-Sided Attack Equilibria -- 5 Numerical Illustrations -- 5.1 The Peaceful Equilibrium -- 5.2 One-Sided Attack Equilibria -- 6 Conclusion and Future Work -- References -- Issues in Designing a Bitcoin-like Community Currency -- Abstract -- 1 Background -- 1.1 Cryptocurrencies -- 2 Community Cryptocurrency Features -- 2.1 Mining -- 2.2 Geofencing -- 2.3 Privileged Transactions -- 2.4 Demurrage -- 2.5 The Community Loan Fund -- 2.5.1 Adding to the Community Fund -- 2.5.2 Disbursing from the Community Fund -- 3 Challenges with a Cryptocurrency Community Fund -- 3.1 Identity -- 3.2 Voting -- 3.3 Loan Regulation -- 4 Vulnerability Assessment -- 4.1 STRIDE Framework -- 4.2 The Vulnerability Matrix -- 4.3 Mitigations -- 5 Conclusion and Future Research -- References -- The Bitcoin Market Potential Index -- References -- Cryptographic Currencies from a Tech-Policy Perspective: Policy Issues and Technical Directions -- 1 Introduction -- 2 Our Process -- 3 Background: Bitcoin and Crypto Currencies -- 4 Analysis of Relevant Legal Contexts -- 5 Tech-Policy Issues for Crypto Currencies -- 5.1 Where Is the Money? -- 5.2 What About Anonymity and Pseudonymity? -- 5.3 What Happens as the World Evolves? -- 6 Conclusion -- References -- Blindcoin: Blinded, Accountable Mixes for Bitcoin -- 1 Introduction -- 1.1 Mixing Services -- 1.2 Current Bitcoin Mixing Services -- 1.3 Our Contribution -- 2 Background -- 2.1 Mixcoin Summary -- 2.2 Blind Signatures -- 3 Blindcoin Description -- 3.1 Model -- 3.2 Protocol -- 4 Analysis -- 4.1 Properties -- 4.2 Overheads -- 5 Conclusion -- References -- Privacy-Enhancing Overlays in Bitcoin -- 1 Introduction -- 2 Definitions and Notation.
2.1 Distributed Electronic Cash -- 2.2 Coinjoin -- 2.3 Taint Resistance -- 3 Achieving Taint Resistance -- 3.1 Using a Trusted Server -- 3.2 Reducing Trust in the Central Server -- 3.3 Removing the Central Server -- 4 Experimental Analysis -- 4.1 Auxiliary Information Based on Value -- 5 Related Work -- 6 Conclusions and Open Problems -- References -- Search-and-Compute on Encrypted Data -- 1 Introduction -- 1.1 Our Results -- 1.2 A High-Level Overview of Our Approach -- 1.3 Closely Related Work -- 2 Preliminaries -- 2.1 The BGV-Type SWHE Scheme -- 2.2 Security Model -- 3 Circuit Primitives -- 3.1 Equality Circuit -- 3.2 Greater-than Comparison Circuit -- 3.3 Integer Addition Circuit -- 4 Search-and-Compute on Encrypted Data

-- 4.1 General-Purpose Search-and-Compute -- 4.2 Applications to Encrypted Databases -- 5 Performance Improvements -- 5.1 Larger Message Spaces with Lazy Carry Processing -- 5.2 Calibrating Circuit Primitives -- 6 Experimental Results -- 6.1 Adjusting the Parameters -- 6.2 Experiments for Search -- 6.3 Experiments for Search-and-Sum -- References -- Accelerating SWHE Based PIRs Using GPUs -- 1 Introduction -- 2 Background -- 3 GPU Implementation -- 4 Performance -- References -- Combining Secret Sharing and Garbled Circuits for Efficient Private IEEE 754 Floating-Point Computations -- 1 Introduction -- 2 Preliminaries -- 3 Combining Garbled Circuits with Secret Sharing -- 3.1 An Implementation of the Hybrid Protocol -- 3.2 Security of the Hybrid Protocol -- 4 Using the Hybrid Protocol for Efficient Computations -- 4.1 Circuits for IEEE 754 Primitives -- 4.2 Performance Analysis -- 5 Conclusion -- References -- Cryptanalysis of a (Somewhat) Additively Homomorphic Encryption Scheme Used in PIR -- 1 Introduction -- 2 Preliminaries -- 2.1 Trostle and Parrish's SHE Scheme -- 2.2 Applications to PIR -- 2.3 The Orthogonal Lattice.
3 Breaking the One-Wayness of the Scheme -- 3.1 Overview -- 3.2 Applying Orthogonal Lattice Techniques -- 3.3 Larger Message Space -- 4 Implementation of the Attack -- 4.1 Attack Summary -- 4.2 Experimental Results -- References -- Homomorphic Computation of Edit Distance -- 1 Introduction -- 2 Preliminaries -- 2.1 Homomorphic Encryption -- 2.2 Edit Distance -- 3 Circuit Building Blocks -- 3.1 Equality Circuit -- 3.2 Comparison Circuit -- 3.3 Addition Circuits -- 4 Encrypted Edit Distance Algorithm -- 4.1 Encrypted Edit Distance Algorithm -- 4.2 Performance Analysis of Encrypted Edit Distance Algorithm -- 4.3 Optimization of Encrypted Edit Distance Algorithm -- 5 Implementation and Discussions -- 5.1 Estimates -- 5.2 Experimental Result -- 6 Conclusion -- References -- HEtest: A Homomorphic Encryption Testing Framework -- 1 Introduction -- 2 Overview of Homomorphic Encryption and HElib -- 3 Test Data -- 3.1 Generation Parameters -- 3.2 Circuit and Input Generation -- 3.3 Test Suite Representation -- 3.4 SQLite Database -- 4 The Test Framework -- 4.1 The Test Harness -- 4.2 The Baseline -- 5 Report Generation -- 6 Experimental Results -- 6.1 Experimental Setup -- 6.2 Real-World Applicability -- 6.3 Parameters Tested -- 6.4 Overview of Results -- 6.5 Key Generation -- 6.6 Circuit Ingestion -- 6.7 Encryption and Decryption -- 6.8 Homomorphic Evaluation -- 6.9 Evaluation Time by Gate Type -- 7 Conclusion -- References -- Users' Privacy Concerns About Wearables -- Abstract -- 1 Introduction -- 2 Related Work -- 2.1 Privacy in Ubiquitous Computing -- 2.2 Privacy in Mobile Devices -- 2.3 Privacy in Wearable Devices -- 2.4 Users' Perspectives on Privacy -- 3 Methods -- 3.1 IRB Approval -- 3.2 Data Selection, Extraction and Analysis -- 3.3 Devices, Online Data Sources and Figures -- 4 Identifying User Privacy Concerns for Wearable Technologies.
4.1 Privacy Concerns for Wrist-Mounted Devices -- 4.1.1 General Social Implications: Unawareness -- 4.1.2 Right to Forget -- 4.1.3 Implications of Location Disclosure -- 4.1.4 Discrete Display of Confidential Information: Non-Disclosure -- 4.1.5 Lack of Access Control -- 4.1.6 Users' Fears: Surveillance and Sousveillance -- 4.2 Privacy Concerns for Head-Mounted Devices -- 4.2.1 Speech Disclosure -- 4.2.2 Surveillance, Sousveillance and Criminal Abuse -- 4.2.3 Surreptitious Audio and Video Recording: Unawareness -- 4.2.4 Surveillance, Sousveillance and Social Implications: Unawareness -- 4.2.5 Facial Recognition: Identifiability -- 4.2.6 Automatic Synchronization with Social Media: Linkability -- 4.2.7 Visual Occlusion: Non-Disclosure -- 4.3 Privacy Concerns Across Form Factors -- 5 Discussion -- 5.1 Limitations -- 6 Conclusion -- Acknowledgments --

References -- On Vulnerabilities of the Security Association in the IEEE 802.15.6 Standard -- 1 Introduction -- 2 Security Structure of the IEEE 802.15.6 Standard -- 3 Key Agreement Protocols in the IEEE 802.15.6 Standard -- 4 Security Problems -- 4.1 Protocol I -- 4.2 Protocol II -- 4.3 Protocol III -- 4.4 Protocol IV -- 5 Conclusion -- References -- Visual Cryptography and Obfuscation: A Use-Case for Decrypting and Deobfuscating Information Using Augmented Reality -- 1 Introduction -- 2 Related Work -- 3 Visual Cryptography -- 3.1 Original Version -- 3.2 Modified Version -- 3.3 Using a Seven-Segment Display -- 4 Visual Obfuscation -- 4.1 Digit Representation -- 4.2 Analysis of 2-Way Partitioning -- 4.3 Optimizing the Partitioning -- 4.4 Analysis of 4-Bar Shape -- 4.5 Analysis of 3-Way Partitioning -- 5 Results -- 6 Discussion -- 7 Conclusion -- References -- Ok Glass, Leave Me Alone: Towards a Systematization of Privacy Enhancing Technologies for Wearable Computing -- 1 Introduction -- 2 Properties.
3 Systematization of Privacy Enhancing Technologies.

Sommario/riassunto

This book constitutes the refereed proceedings of three workshops held at the 19th International Conference on Financial Cryptography and Data Security, FC 2015, in San Juan, Puerto Rico, in January 2015. The 22 full papers presented were carefully reviewed and selected from 39 submissions. They feature the outcome of the Second Workshop on Bitcoin Research, BITCOIN 2015, the Third Workshop on Encrypted Computing and Applied Homomorphic Cryptography, WAHC 2015, and the First Workshop on Wearable Security and Privacy, Wearable 2015.