1. Record Nr. UNISA996464531103316

| | |
|---|---|
| Titolo | Financial cryptography and data security : 25th international conference, FC 2021, virtual event, March 1-5, 2021, revised selected papers, part I / / edited by Nikita Borisov and Claudia Diaz |
| Pubbl/distr/stampa | Berlin, Germany ; ; New York, New York : , : Springer-Verlag, , [2021]<br>©2021 |
| ISBN | 3-662-64322-7 |
| Descrizione fisica | 1 online resource (529 pages) |
| Collana | Lecture Notes in Computer Science ; ; v.12674 |
| Disciplina | 005.824 |
| Soggetti | Computer networks<br>Data encryption (Computer science)<br>Computer security |
| Lingua di pubblicazione | Inglese |
| Formato | Materiale a stampa |
| Livello bibliografico | Monografia |
| Nota di bibliografia | Includes bibliographical references and index. |
| Nota di contenuto | Intro -- Preface -- Organization -- Contents - Part I -- Contents - Part II -- Smart Contracts -- Attacking the DeFi Ecosystem with Flash Loans for Fun and Profit -- 1 Introduction -- 2 Background -- 2.1 DeFi Platforms -- 2.2 Reverting EVM State Transitions -- 2.3 Flash Loan Usage in the Wild -- 2.4 Related Work -- 3 Flash Loan Post-Mortem -- 3.1 Pump Attack and Arbitrage (PA&amp -- A) -- 3.2 Oracle Manipulation Attack -- 4 Optimizing DeFi Attacks -- 4.1 System and Threat Model -- 4.2 Parametrized Optimization Framework -- 5 Evaluation -- 5.1 Optimizing the Pump Attack and Arbitrage -- 5.2 Optimizing the Oracle Manipulation Attack -- 6 Implications of Transaction Atomicity -- 7 Discussion -- 8 Conclusion -- A Classifying Flash Loan Use Cases -- B  Flash Loan Use Cases -- B.1 Wash Trading -- B.2  Collateral Swapping -- B.3  Flash Minting -- C DeFi Models -- D  Optimizing the Pump Attack and Arbitrage -- E Optimizing the Oracle Manipulation Attack -- F  Extended Discussion -- References -- The Eye of Horus: Spotting and Analyzing Attacks on Ethereum Smart Contracts -- 1 Introduction -- 2 Background -- 3 The Horus Framework -- 3.1 Extraction -- 3.2 Analysis -- 3.3 Tracing -- 4 Evaluation -- 4.1 Results -- 4.2 Validation -- 5 Analysis -- 5.1 Volume and Frequency of Attacks -- 5.2 Forensic Analysis on Uniswap and |

Lendf.me Incidents -- 6 Related Work -- 7 Conclusion -- References -- Timelocked Bribing -- 1 Introduction -- 1.1 HTLC -- 1.2 Bribing Attack -- 1.3 Payment Channels -- 1.4 Atomic Swaps -- 2 Analysis -- 2.1 Assumptions -- 2.2 Setting -- 2.3 All Miners Are Strong -- 2.4 One Miner is Weak -- 2.5 The Elimination of Dominated Strategies -- 2.6 The Elimination of Dominated Strategies of Strong Miners -- 3 Solutions -- 3.1 Mining Pools and Their Hashpower Shares -- 3.2 Lightning -- 3.3 Atomic Swaps -- 4 Related Work -- 4.1 Ignore Attacks.
4.2 Fork Attacks -- 5 Conclusion -- Appendix A  Transactions in Pseudo Bitcoin Script -- Appendix B  Iterated Removal of Dominated Strategies -- Appendix C  Risk Free Atomic Swaps -- References -- Shielded Computations in Smart Contracts Overcoming Forks -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Related Work -- 2 Threat Model -- 3 Parallel Coin Tossing -- 3.1 Our PCT Protocol -- 3.2 Experimental Evaluation -- 4 Our Generic Compiler -- 5 Conclusions -- References -- A Formal Model of Algorand Smart Contracts -- 1 Introduction -- 2 The Algorand State Machine -- 2.1 Accounts and Transactions -- 2.2 Blockchain States -- 2.3 Executing Single Transactions -- 2.4 Executing Atomic Groups of Transactions -- 2.5 Executing Smart Contracts -- 2.6 Authorizing Transactions, and User-Blockchain Interaction -- 2.7 Fundamental Properties of ASC1 -- 3 Designing Secure Smart Contracts in Algorand -- 3.1 Attacker Model -- 3.2 Smart Contracts -- 4 From the Formal Model to Concrete Algorand -- 5 Conclusions -- References -- Anonymity and Privacy in Cryptocurrencies -- Everything You Ever Wanted to Know About Bitcoin Mixers (But Were Afraid to Ask) -- 1 Introduction -- 2 Background -- 3 Bitcoin Mixers -- 4 Academic Mixing Techniques -- 4.1 Decentralized Mixing Protocols -- 4.2 Centralized Mixing Protocols -- 5 Public Mixing Services -- 6 Evaluation -- 6.1 Methodology -- 7 Analysis -- 7.1 Implementation Analysis -- 7.2 Security Analysis -- 7.3 Additional Interesting Behavior -- 8 Discussion and Limitations -- 9 Conclusion -- A  Appendix 1 -- A.1  Public Mixer Characteristics -- B Appendix 2 -- B.1  ChipMixer Results -- B.2  MixTum Results -- B.3 Bitcoin Mixer Results -- B.4  CryptoMixer Results -- B.5  Sudoku Wallet Results -- C  Appendix 3 -- C.1  Chip Generation Transactions -- References -- Perimeter: A Network-Layer Attack on the Anonymity of Cryptocurrencies.
1 Introduction -- 2 Background -- 2.1 Bitcoin Workings -- 2.2 Ethereum Workings -- 2.3 Internet Routing -- 3 Overview -- 3.1 Perimeter at a High-Level -- 3.2 Perimeter in Action -- 3.3 Generalizing Perimeter to Ethereum -- 4 Perimeter Workings -- 4.1 Recognizing Bitcoin Traffic -- 4.2 Creating the Initial Anonymity Set -- 4.3 Analyzing Data -- 4.4 Feature Selection -- 5 Perimeter's Practicality -- 5.1 Methodology -- 5.2 Findings -- 6 Perimeter's Effectiveness -- 6.1 Perimeter in Simulation -- 6.2 Perimeter in the Wild -- 7 Countermeasures -- 8 Related Work -- 9 Conclusion -- References -- An Empirical Analysis of Privacy in the Lightning Network -- 1 Introduction -- 1.1 Ethical Considerations -- 1.2 Related Work -- 2 Background -- 3 Blockchain Analysis -- 3.1 Data and Measurements -- 3.2 Private Channels -- 4 Balance Discovery -- 5 Path Discovery -- 5.1 Lightning Network Simulator -- 5.2 Simulation Results -- 6 Payment Discovery -- 6.1 Payment Discovery Algorithm -- 6.2 Attack Simulation -- 6.3 Simulated Attack Results -- 7 Conclusions -- References -- Cross-Layer Deanonymization Methods in the Lightning Protocol -- 1 Introduction -- 2 Background and Problem Statement -- 2.1 BTC Blockchain (Layer 1) -- 2.2 Nodes and Payment Channels in the LN (Layer 2) -- 2.3 Cross-Layer Interaction -- 2.4 The Cross-Layer Linking

Problem -- 2.5 Related Work -- 3 Dataset -- 3.1 Off-Chain Data: LN -- 3.2 On-Chain Data: BTC Blockchain -- 3.3 Ground Truth Data: LN Payments -- 4 Clustering Heuristics -- 4.1 On-Chain BTC Entity Clustering (Layer 1) -- 4.2 Off-Chain LN Nodes Clustering (Layer 2) -- 5 Linking LN Nodes and BTC Entities -- 5.1 Linking Algorithm 1: Coin Reuse -- 5.2 Linking Algorithm 2: Entity Reuse -- 5.3 Validation -- 6 Assessing Security and Privacy Impact -- 6.1 Privacy Impact on BTC Entities (Layer 1) -- 6.2 Security and Privacy Impact on the LN (Layer 2). 7 Conclusion and Future Work -- References -- The Complex Shape of Anonymity in Cryptocurrencies: Case Studies from a Systematic Approach -- 1 Introduction -- 1.1 Our Contribution -- 1.2 Other Related Work -- 2 Anonymity Framework -- 2.1 A Generic Cryptocurrency Scheme -- 2.2 A Comprehensive Adversarial Capability Model -- 2.3 All-in-one Generic Flexible Anonymity Game -- 2.4 Notions of Anonymity -- 3 Analysis -- 3.1 A Trusted Third Party (TTP) Scheme -- 3.2 Bitcoin -- 3.3 Zcash -- 3.4 Monero -- 3.5 Mimblewimble -- 4 Discussion -- 5 Conclusion -- A  Anonymity framework -- A.1  Anonymity Game -- A.2  Anonymity Notions -- References -- Secure Multi-party Computation -- Improving the Efficiency of AES Protocols in Multi-Party Computation -- 1 Introduction -- 1.1 Our Contributions -- 2 Preliminaries -- 3 Analysis of Previous MPC AES Implementations -- 3.1 Complexity of Available SPDZ Modules for AES -- 3.2  AES-BD Arithmetic Circuits ch11AESActiveCovertSecureDKLMS2012 -- 4 AES Decryption in MPC -- 4.1 Optimized  AES-BD for Inverse AES -- 4.2 Performance Optimization of Protocol 2 -- 4.3 Optimizations with Offline Phase -- 4.4 Offline Phase Tuples -- 4.5 Comparison with Other AES MPC Implementations -- 5 Conclusion -- 6  Appendix -- 6.1  AES-LT with Masked Table ch11AESTableLookUpKORSSV2017 -- 6.2  Details of BDEmbed -- 6.3  Regarding The Embedding from  GF(28) to  GF(240) -- References -- Rabbit: Efficient Comparison for Secure Multi-Party Computation -- 1 Introduction -- 1.1 Our Contribution -- 1.2 Technical Overview -- 2 Comparison Protocols -- 2.1 Comparison with Bitwise Shared Input - LTBits Protocol -- 2.2 Comparison with a Constant - LTC Protocol -- 2.3 ReLU - Special Case of LTC for R = 2k-1,  M = 2k -- 2.4 Comparison with Secret - LTS Protocol -- 3 Evaluation -- 3.1 Throughput of Rabbit comparisons -- 3.2 Neural Network Evaluation.
4 Discussion -- 4.1 Elimination of ``Slack'' in Comparisons -- 4.2 Applications to Machine Learning and Beyond -- 4.3 Statistical Security -- 5 Comparison with Related Work -- 6 Conclusion -- References -- Efficient Noise Generation to Achieve Differential Privacy with Applications to Secure Multiparty Computation -- 1 Introduction -- 1.1 Our Results -- 1.2 Related Work -- 2 Preliminaries -- 2.1 Notations -- 2.2 Secure Multiparty Computation -- 2.3 Differential Privacy -- 3 A General Framework for Distributed Noise Generation -- 4 A Novel Protocol for Discrete Laplace Noise Generation -- 4.1 The Bernoulli Distribution -- 4.2 The Discrete Laplace Distribution -- 5 A Novel Protocol for Binomial Noise Generation -- 6 Comparison -- 6.1 The Discrete Laplace Distribution -- 6.2 The Binomial Distribution -- A Appendix -- A.1  The Protocol for Discrete Laplace Noise Generation ch13DKMMN06 -- A.2  The Protocol for Binomial Noise Generation ch13DKMMN06 -- References -- System and Application Security -- Specfuscator: Evaluating Branch Removal as a Spectre Mitigation -- 1 Introduction -- 2 Background -- 2.1 Speculative Execution Attacks -- 2.2 M/o/Vfuscator -- 3 Blank Spots in the Spectre Defense Landscape -- 4 Specfuscator -- 4.1 Design of Specfuscator -- 4.2 Security of Specfuscator -- 4.3 Implementation of Specfuscator -- 5 Evaluation --

5.1 Security Evaluation -- 5.2 Performance Evaluation -- 6 Discussion -- 7 Conclusion -- References -- Speculative Dereferencing: Reviving Foreshadow -- 1 Introduction -- 2 Background and Related Work -- 3 From Address-Translation Attack to Foreshadow-L3 -- 3.1 H1: Prefetch Instruction Required -- 3.2 H2: Values in Registers Required -- 3.3 H3: sched_yield Required -- 3.4 H4: userspace_accessible Bit Required -- 3.5 H5: Effect only on Intel CPUs -- 3.6 Speculative Execution in the Kernel -- 3.7 Meltdown-L3 and Foreshadow-L3. 4 Improving the Leakage Rate.