

1. Record Nr.	UNISA996587859403316
Autore	Pöpper Christina
Titolo	Applied Cryptography and Network Security : 22nd International Conference, ACNS 2024, Abu Dhabi, United Arab Emirates, March 5-8, 2024, Proceedings, Part III
Pubbl/distr/stampa	Cham : , : Springer, , 2024 ©2024
ISBN	3-031-54776-4
Edizione	[1st ed.]
Descrizione fisica	1 online resource (476 pages)
Collana	Lecture Notes in Computer Science Series ; ; v.14585
Altri autori (Persone)	BatinaLejla
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Preface -- Organization -- Abstracts of Keynote Talks -- Applying Machine Learning to Securing Cellular Networks -- Real-World Cryptanalysis -- CAPTCHAs: What Are They Good For? -- Contents - Part III -- Blockchain -- Mirrored Commitment: Fixing "Randomized Partial Checking" and Applications -- 1 Introduction -- 1.1 Notation -- 2 Chaumian Randomized Partial Checking (RPC) Mix Net -- 2.1 Protocol Description -- 2.2 RPC Audit -- 2.3 Attacks on RPC -- 3 Mirrored Randomized Partial Checking (mRPC) -- 3.1 Protocol Description -- 3.2 mRPC Audit -- 3.3 Attack Examples on mRPC -- 3.4 Security of mRPC -- 4 Privacy Guarantees of RPC and mRPC -- 4.1 Constant Number of Mix-Servers -- 4.2 Mixing Time -- 5 Application: Cryptocurrency Unlinkability -- 6 Conclusions -- A Proofs -- A.1 Proof of Lemma 4 -- A.2 Proof of Lemma 6 -- A.3 Proof of Lemma 7 -- References -- Bitcoin Clique: Channel-Free Off-Chain Payments Using Two-Shot Adaptor Signatures -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Related Work -- 2 Preliminaries -- 3 Model -- 3.1 Blockchain and Transaction Model -- 3.2 Commit-Chain Model -- 3.3 Communication and Adversarial Assumptions -- 3.4 Security and Performance Guarantees -- 4 Protocol Overview -- 5 Bitcoin Clique Protocol -- 6 Future Work -- A Bitcoin Clique Healing -- A.1 Healing Extension Details -- A.2 Discussion and Future Work -- References -- Programmable Payment Channels -- 1 Introduction -- 1.1 Our

Contributions -- 1.2 Related Work -- 2 Preliminaries -- 3  
Programmable Payment Channels -- 3.1 Defining FPPC -- 3.2 PPC  
Preliminaries -- 3.3 Ideal Functionality FPPC -- 3.4 Concrete  
Implementation of FPPC -- 3.5 Lightweight Applications of  
Programmable Payments -- 3.6 Implementation and Evaluation -- 4  
State Channels from FPPC -- 4.1 Modifying FPPC to Capture State  
Channels -- 4.2 Defining FSC.  
4.3 Implementing FSC in the FPPC-Hybrid World -- 5 Conclusions --  
References -- Fair Private Set Intersection Using Smart Contracts -- 1  
Introduction -- 1.1 Other Coin-Compensated PSI -- 2 Related Work --  
3 Preliminaries and Notations -- 4 Fair PSI Using Smart Contracts --  
4.1 Smart Contract as the TTP in Optimistic Mutual PSI -- 4.2 Security  
Model -- 4.3 Ideal Functionality for Coin-Compensated PSI -- 5 A  
Coin-Compensated Fair SC-Aided PSI -- 5.1 Security Analysis -- 6  
Improving the Efficiency of -- 6.1 Our Technique for Optimizing the  
Protocol -- 6.2 Overview of \* -- 6.3 Security Analysis -- 7 Complexity  
Analysis -- 8 Implementation -- 8.1 Evaluation -- 9 Concluding  
Remarks -- References -- Powers-of-Tau to the People: Decentralizing  
Setup Ceremonies -- 1 Introduction -- 2 Related Work -- 2.1  
Multiparty Setup Ceremonies -- 2.2 Setup Ceremonies in Practice --  
2.3 Proof Systems with Transparent Setup -- 3 A Powers-of-Tau  
System: Definitions -- 4 Powers-of-Tau Setup with Full Data On-Chain  
-- 4.1 Security -- 5 Powers-of-Tau Setup Protocol with Data Off-Chain  
-- 5.1 Off-Chain Setup Using a Transparent Succinct Proof -- 5.2 Off-  
Chain Setup Using AFGHO Commitments On-Chain -- 6  
Implementation and Evaluation on Ethereum -- 7 Concluding  
Discussion and Open Problems -- 7.1 Incentives for Participation --  
7.2 Verifying Participation -- 7.3 Sequential Participation and Denial-  
of-Service -- 7.4 Verification with General-Purpose Roll-Ups -- 7.5  
Protocol-Specific ZK Rollups via Proof Batching -- 7.6 Protocol-Specific  
Optimistic Verification and Checkpointing -- 7.7 Fully Off-Chain  
Verification via IVC/PCD -- 7.8 Forking/Re-starting -- A Proof of  
Theorem 2 -- B Inner-Pairing Product Arguments for Sect.5.2 -- C Off-  
Chain Setup from IPP Arguments with a Smaller Setup -- D Powers-of-  
Tau with a Punctured Point -- References.  
Smart Infrastructures, Systems and Software -- Self-sovereign Identity  
for Electric Vehicle Charging -- 1 Introduction -- 2 Background -- 2.1  
E-mobility -- 2.2 Self-Sovereign Identity (SSI) -- 3 Related Work -- 4  
System Model and Requirement Analysis -- 4.1 Scope -- 4.2 Attacker  
Model -- 4.3 Functional Requirements -- 4.4 Security and Privacy  
Requirements -- 5 SSI Concept -- 5.1 Concept Overview -- 5.2  
Provisioning DID Creation -- 5.3 Contract Credential Installation -- 5.4  
Charging Process and Credential Validation -- 5.5 Integration into ISO  
15118-20 -- 6 Implementation -- 7 Evaluation -- 7.1 Performance  
Measurements -- 7.2 Security and Privacy Analysis with Tamarin -- 7.3  
Discussion of Requirements -- 8 Conclusion -- References -- "Hello?  
Is There Anybody in There?" Leakage Assessment of Differential Privacy  
Mechanisms in Smart Metering Infrastructure -- 1 Introduction -- 2  
Preliminaries -- 2.1 Differential Privacy -- 2.2 Statistical t-test Analysis  
-- 3 System and Threat Model -- 3.1 Threat Surfaces -- 3.2  
Capabilities of the Adversary -- 3.3 Goal of the Adversary -- 4 Formal  
Analysis of Leakage Due to Privacy-Utility Trade-Off in Smart Metering  
Systems -- 5 Proposed Attack Methodology -- 5.1 Precomputation  
Phase -- 5.2 t-test Based Attack Methodology -- 6 Evaluation of the  
Proposed Attack Methodology -- 6.1 Experimental Setup -- 6.2  
Experimental Evaluation -- 7 Discussion -- 8 Conclusion and Future  
Work -- References -- Security Analysis of BigBlueButton and eduMEET  
-- 1 Introduction -- 2 Background -- 2.1 WebRTC -- 2.2 WebRTC

Architectures in Conferencing Systems -- 3 Analysis Method -- 3.1 High-Level Analysis -- 3.2 Source Code Supported Security Analysis -- 4 Architectures of the Analyzed Open-Source Conferencing Systems (RQ1) -- 4.1 Shared Architecture -- 4.2 Implementation of BigBlueButton -- 4.3 Implementation of eduMEET.

5 Features and User Roles (RQ2) -- 5.1 Comparison of Features -- 5.2 User Roles -- 6 Attacker Model -- 7 Evaluation (RQ3) -- 7.1 BigBlueButton -- 7.2 eduMEET -- 7.3 Responsible Disclosure -- 8 Discussion -- 8.1 BigBlueButton -- 8.2 eduMEET -- 8.3 Limitations -- 9 Related Work -- 10 Conclusions and Future Work -- A Appendix -- A.1 eduMEET -- A.2 Status of Fixes in BigBlueButton -- References --

An In-Depth Analysis of the Code-Reuse Gadgets Introduced by Software Obfuscation -- 1 Introduction -- 2 Background -- 2.1 Code Obfuscation -- 2.2 Code-Reuse Attack -- 3 Code-Reuse Gadgets Introduced by Obfuscation -- 3.1 Benchmark and Obfuscation Selection -- 3.2 Gadget Measurement -- 4 Study Results -- 4.1 Gadget Quantity -- 4.2 Gadget Exploitability -- 4.3 Gadget Quality -- 4.4 Code-Reuse Attack Risk -- 5 The Anatomy of the Obfuscations and Gadgets -- 5.1 Instructions Substitution -- 5.2 Control Flow Flattening -- 5.3 Bogus Control Flow -- 5.4 Virtualization -- 5.5 Just-In-Time Dynamic -- 5.6 Self-modification -- 5.7 Encode Components -- 6 Mitigation -- 6.1 Strategy -- 6.2 Evaluation -- 7 Related Work -- 8 Conclusion -- References --

ProvIoT: Detecting Stealthy Attacks in IoT through Federated Edge-Cloud Security -- 1 Introduction -- 2 Background -- 2.1 Fileless Attacks on IoT Devices -- 2.2 System Provenance and Graph Learning -- 3 Threat Model -- 4 System Overview -- 4.1 Local Brain -- 4.2 Cloud Brain -- 5 Federated Detection -- 5.1 Graph Building and Path Selection -- 5.2 Document Embedding Model -- 5.3 Federated Autoencoder -- 6 Implementation -- 7 Evaluation -- 7.1 Dataset -- 7.2 Experimental Protocol -- 7.3 IoT Malware Detection -- 7.4 APT Detection -- 7.5 Federated Learning Benefits -- 7.6 ProvIoT Overhead -- 8 Limitations -- 9 Related Work -- 10 Discussion and Future Work -- 11 Conclusion -- A Appendix -- A.1 IoT Workload. -- A.2 Dataset Statistics.

A.3 APT Scenarios -- References --

Attacks -- A Practical Key-Recovery Attack on LWE-Based Key-Encapsulation Mechanism Schemes Using Rowhammer -- 1 Introduction -- 1.1 Paper Organization -- 2 Preliminaries -- 2.1 Learning with Errors (LWE) Problem and Its Variants -- 2.2 LPR Public-Key Encryption -- 2.3 Kyber -- 2.4 Saber -- 2.5 Related Works -- 3 Our Attack Using Binary Decision Tree on the LPR-Based Schemes -- 3.1 Implementing a Parallel Plaintext Checking (PC) Oracle -- 3.2 Generic Attack Model Using PC Oracle -- 3.3 Model for Kyber and Saber -- 3.4 Comparing Our Attack with the State-of-the-Art -- 4 Realization of the Fault Model -- 4.1 Nature of the Fault in the Attack -- 4.2 Our Target Devices -- 4.3 Probabilities of Incorporating Precise Fault Using Random Rowhammer -- 5 Discussion and Future Direction -- 5.1 Shuffling and Masking: -- 5.2 Extension of Our Attack on Other PQC Schemes -- 5.3 Combining of Lattice Reduction Techniques with Our Attack -- 5.4 Possible Countermeasures -- References --

A Side-Channel Attack on a Higher-Order Masked CRYSTALS-Kyber Implementation -- 1 Introduction -- 2 Previous Work -- 3 Background -- 3.1 Notation -- 3.2 Kyber Algorithm -- 4 Adversary Model -- 5 Attack Description -- 5.1 Profiling Stage -- 5.2 Attack Stage -- 6 Experimental Setup -- 7 Leakage Analysis -- 7.1 Unprotected Message Encoding -- 7.2 Masked Message Encoding -- 7.3 Finding New Leakage Points -- 8 Neural Network Training -- 8.1 Trace Acquisition and Pre-processing -- 8.2 Network Architecture and Training Parameters -- 9 New Chosen Ciphertext Construction Method

-- 9.1 Constructing Chosen Ciphertexts -- 9.2 Selecting Optimal Mapping -- 10 Experimental Results -- 10.1 Message Recovery Attack -- 10.2 Secret Key Recovery Attack -- 11 Countermeasures -- 12 Conclusion -- References.  
Time Is Money, Friend! Timing Side-Channel Attack Against Garbled Circuit Constructions.

2. Record Nr.	UNINA9910955511403321
Autore	Khan Azizur Rahman
Titolo	Inequality and poverty in China in the age of globalization // Azizur Rahman Khan, Carl Riskin
Pubbl/distr/stampa	Oxford : , : Oxford University Press, , 2023
ISBN	0-19-771030-1 1-280-83447-1 0-19-535041-3
Edizione	[1st ed.]
Descrizione fisica	1 online resource (197 p.)
Collana	Oxford scholarship online
Disciplina	339.5/0951
Soggetti	Equality - China Poverty - China Globalization
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Previously issued in print: 2001.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Contents; 1 Introduction; 2 Household Income: Its Composition and Growth; 3 The Distribution of Income: Evolution of Inequality 1988-1995; 4 Trends in the Incidence of Poverty; 5 Gender, Health and Education: Human Development Dimensions of Inequality; 6 Explaining the Increase in Inequality and the Decline in Poverty Reduction; 7 Policies for the Reduction of Inequality and Poverty; 8 Summary and Conclusions; Notes; Bibliography; Index
Sommario/riassunto	This text analyses the growing inequality in income in China since the era of reform began in 1979. The economic growth policies adopted by China are just one of the issues discussed through the course of this book.

