1.

Record Nr.	UNISA996587860703316
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 II
Pubbl/distr/stampa	Cham : , : Springer, , 2024 ©2024
ISBN	3-031-54773-X
Edizione	[1st ed.]
Descrizione fisica	1 online resource (523 pages)
Collana	Lecture Notes in Computer Science Series ; ; v.14584
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 II -- Post-quantum -- Automated Issuance of Post-Quantum Certificates: A New Challenge -- 1 Introduction -- 2 Background -- 2.1 TLS Version 1.3 -- 2.2 ACMEv2 Characteristics -- 2.3 Post-Quantum Cryptography -- 3 Quantum Threat and PQC Adoption -- 3.1 Quantum Threats in ACME -- 3.2 Integrating PQC Algorithms -- 3.3 Impacts of PQC in ACME -- 4 Proposed ACME Challenge -- 4.1 Design Details -- 4.2 Issuance and Renewal Timings -- 4.3 Discussion -- 5 Final Remarks and Future Work -- A ACME's HTTP-01 Challenge -- B POST Request Example -- References -- Algorithmic Views of Vectorized Polynomial Multipliers - NTRU Prime -- 1 Introduction -- 1.1 Contributions -- 1.2 Code -- 1.3 Structure of This Paper -- 2 Preliminaries -- 2.1 Polynomials in NTRU Prime -- 2.2 Cortex-A72 -- 2.3 Modular Arithmetic -- 3 Fast Fourier Transforms -- 3.1 The Chinese Remainder Theorem (CRT) for Polynomial Rings -- 3.2 Cooley-Tukey FFT -- 3.3 Bruun-Like FFTs -- 3.4 Good-Thomas FFTs -- 3.5 Rader's FFT for Odd Prime p -- 3.6 Schönhage's and Nussbaumer's FFTs -- 4 Implementations -- 4.1 The Needs of Vectorization -- 4.2 Good-Thomas FFT in ``BigSmall'' Polynomial Multiplications -- 4.3 Good-Thomas, Schönhage's, and Bruun's FFT --

Aggregation -- 3.1 Our Construction -- 3.2 Aggregator Obliviousness -- 3.3 Parameters -- 3.4 Decentralized Setup -- 3.5 Client Failures -- 3.6 Optimizing Peer-to-Peer Communication -- 3.7 Dynamic Join and Leave -- 4 DPSA in the Standard Model -- 5 Conclusion -- A Private Stream Aggregation -- B Games for the Proof of Theorem 1 -- References -- Wireless and Networks.

A Security Analysis of WPA3-PK: Implementation and Precomputation Attacks -- 1 Introduction -- 2 Background -- 2.1 Simultaneous Authentication of Equals (SAE) -- 2.2 WPA3 Public Key (WPA3-PK) -- 2.3 Generation of the WPA3-PK Password -- 2.4 Security Guarantees Provided by WPA3-PK -- 3 Implementation and Network-Based Attacks -- 3.1 Bad Randomness Leaks the Password -- 3.2 Network-Based Attacks -- 4 Precomputation Attacks and Rainbow Tables -- 4.1 Background on Time-Memory Trade-Off Attacks -- 4.2 Motivation: SSID Reuse -- 4.3 Baseline Precomputation Attack Against WPA3-PK -- 4.4 Improved Analysis of the Baseline Precomputation Attack -- 4.5 Rainbow Tables for WPA3-PK -- 4.6 Rainbow Table: Performance Experiments -- 5 Multi-network Password Collisions -- 5.1 Constructing Password Collisions -- 5.2 Public Key Embedding and Trailing Data -- 5.3 Accepting Trailing Data Inside the Public Key -- 5.4 Multi-network Password Collisions -- 6 Defenses and Discussion -- 6.1 Handling Bad Randomness: Encrypting the Public Key -- 6.2 Preventing Network-Layer Attacks -- 6.3 Mitigating Time-Memory Trade-Off Attacks -- 6.4 Preventing Password Collisions: Committing to an SSID Length -- 7 Related Work -- 8 Conclusion -- References -- When and How to Aggregate Message Authentication Codes on Lossy Channels? -- 1 Introduction -- 2 MAC Aggregation on Lossy Channels -- 2.1 Message Authentication Codes -- 2.2 MAC Aggregation to Combat Bandwidth Scarcity -- 2.3 Introducing Existing MAC Aggregation Schemes -- 2.4 Interplay of Lossy Channels and MAC Aggregation -- 3 Synthetic Measurements -- 3.1 Simulation Setup -- 3.2 Influence of Channel Quality on Goodput -- 3.3 Influence of Payload Length on Goodput -- 3.4 Optimal Packet Lengths for Authenticated Data -- 4 MAC Aggregation in Real-World Scenarios -- 4.1 Description of the Scenarios.

4.2 Evaluating MAC Aggregation in Realistic Scenarios -- 5 Beyond Goodput as Evaluation Metric -- 5.1 Average Delay Until Authentication -- 5.2 Performance and Memory Overhead -- 5.3 Resilience to Adversarial Interference -- 6 Guidelines on Employing MAC Aggregation -- 6.1 When to Use MAC Aggregation on Lossy Channels? -- 6.2 How to Employ MAC Aggregation on Lossy Channels? -- 6.3 Selecting an MAC Aggregation Scheme -- 7 Conclusion -- References -- DoSat: A DDoS Attack on the Vulnerable Time-Varying Topology of LEO Satellite Networks -- 1 Introduction -- 2 Background and Related Work -- 2.1 LEO Satellite Network -- 2.2 Denial-of-Service Attack -- 2.3 LSN Simulation -- 3 DoSat Attack -- 3.1 Threat Model -- 3.2 Feasibility Analysis -- 3.3 DoSat Overview -- 3.4 Attack Mechanism -- 4 Simulation and Evaluation -- 4.1 Simulation Setup -- 4.2 Network Setup -- 4.3 Evaluation Metrics -- 4.4 Results -- 5 Mitigations -- 6 Conclusion -- References -- DDoSMiner: An Automated Framework for DDoS Attack Characterization and Vulnerability Mining -- 1 Introduction -- 2 Background and Related Work -- 2.1 TCP-Based DDoS Attacks -- 2.2 DDoS Mining/Exploit Schemes -- 2.3 Exploration TCP Stack with Symbolic Execution -- 3 Threat Model and Problem Definition -- 3.1 Threat Model -- 3.2 Problem Definition -- 4 Workflow of DDoSMiner -- 4.1 Generation of Attack Call Flow Graph -- 4.2 Selective Symbolic Execution -- 5 Evaluation -- 5.1 Experiment Configuration -- 5.2 Attack Call Flow Graph Analysis -- 5.3 Symbol

Execution Experiment Setup -- 5.4 Symbolic Execution Results -- 5.5 Evasion Evaluation Against IDS -- 6 Conclusion -- 7 Limitations and Future Work -- A Visualization and Analysis of System Calls -- B The Kernel Address Corresponding to the Full Drop Nodes for Six Categories of Attacks -- References -- Privacy and Homomorphic Encryption.

Memory Efficient Privacy-Preserving Machine Learning Based on Homomorphic Encryption.