1. Record Nr. UNISA996478865503316

Titolo	Applied cryptography and network security : 20th International Conference, ACNS 2022, Rome, Italy, June 20-23, 2022, proceedings / / edited by Giuseppe Ateniese and Daniele Venturi
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2022] ©2022
ISBN	3-031-09234-1
Descrizione fisica	1 online resource (916 pages)
Collana	Lecture Notes in Computer Science ; ; v.13269
Disciplina	005.82
Soggetti	Computer networks - Security measures Cryptography
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Intro -- Preface -- Organization -- Contents -- Encryption -- Keyed-Fully Homomorphic Encryption Without Indistinguishability Obfuscation -- 1 Introduction -- 1.1 Background -- 1.2 Contribution -- 1.3 Technical Overview -- 2 Preliminaries -- 2.1 Non-Interactive Zero-Knowledge Argument -- 2.2 Dual-System Simulation-Sound NIZK -- 2.3 (Keyed-)Fully Homomorphic Encryption -- 3 Generic Construction of Keyed-FHE -- 4 Strong DSS-NIZK from Smooth PHPS and Unbounded Simulation-Sound NIZK -- 5 Feasibility of Our Construction -- References -- A Performance Evaluation of Pairing-Based Broadcast Encryption Systems -- 1 Introduction -- 2 An ElGamal Baseline and Other Related Works -- 3 Broadcast Encryption Implementations and Analysis -- 3.1 Boneh-Gentry-Waters Scheme Using Asymmetric Pairings -- 3.2 Gentry-Waters: A Semi-static Variant of the BGW System -- 3.3 Waters Dual System Broadcast Encryption System -- 3.4 Comparison of General Broadcast Encryption Systems -- 4 Applications of Broadcast Encryption -- References -- An Optimized GHV-Type HE Scheme: Simpler, Faster, and More Versatile -- 1 Introduction -- 2 Preliminaries -- 2.1 Cryptographic Problem -- 2.2 Trapdoor Sampling Algorithms -- 2.3 The Gentry-Halevi-Vaikuntanathan Encryption Scheme -- 2.4 Other Preliminaries -- 3 Efficiency Analyses of GHV -- 3.1 On the Density of Trapdoor Matrix Pair (T, T-1) -- 3.2 Theoretical

Efficiency of GHV -- 4 Our Optimized GHV-Type Encryption Scheme -- 4.1 Using a Sparse Matrix to Replace T-1 -- 4.2 Generic Construction of oGHV -- 4.3 Homomorphic Operations and Concrete Parameters -- 4.4 Computational Optimizations -- 4.5 Property Analysis -- 5 Conclusions -- References -- Attacks -- Analyzing the Provable Security Bounds of GIFT-COFB and Photon-Beetle -- 1 Introduction -- 2 Preliminaries -- 2.1 Notations -- 2.2 Cryptographic Components -- 2.3 Authenticated Encryption.
3 Analysis of GIFT-COFB -- 3.1 Our Attack -- 3.2 Brief Analysis on Security Proof -- 4 Analysis of Photon-Beetle -- 4.1 Claimed Security Bound and Our Attack -- 4.2 Analysis of the Bound in ch4ToSC: ChaJhaNan20 -- 4.3 Related-Key Attack -- 5 Conclusions -- A Specifications of GIFT-COFB and Photon-Beetle -- References -- Beware of Your Vibrating Devices! Vibrational Relay Attacks on Zero-Effort Deauthentication -- 1 Introduction -- 2 Background: ZEBRA Review -- 3 Overview and Threat Model -- 4 Design and Implementation -- 4.1 Implementation of ZEBRA -- 4.2 Implementation of Relay Attack -- 4.3 Design of VibRaze's Attack Scenarios -- 5 Data Collection -- 6 Analysis and Results -- 6.1 Performance of ZEBRA -- 6.2 Performance of VibRaze Against ZEBRA -- 7 Potential Mitigations -- 8 Related Work -- 9 Conclusion and Future Work -- References -- ZLeaks: Passive Inference Attacks on Zigbee Based Smart Homes -- 1 Introduction -- 2 Background and Motivation -- 2.1 Zigbee Overview -- 2.2 System and Threat Model -- 3 Passive Inference Attacks on Zigbee -- 3.1 Attack Overview -- 3.2 Passive Network Mapping -- 3.3 Device and Event Identification Using Inferred APL Command -- 3.4 Device Identification Using Periodic Reporting Patterns -- 4 Experimental Setup and Results -- 4.1 Automating Passive Inference Attacks with ZLeaks Tool -- 4.2 Experimental Setup -- 4.3 Evaluation Metrics -- 4.4 Device and Event Identification Using Inferred APL Command -- 4.5 Device Identification Using Periodic Reporting Patterns -- 5 Discussion and Related Work -- 5.1 Security Implications of Leaked Data -- 5.2 Potential Countermeasures -- 5.3 Related Work -- 6 Conclusion -- References -- Passive Query-Recovery Attack Against Secure Conjunctive Keyword Search Schemes -- 1 Introduction -- 2 Related Work -- 3 Preliminaries -- 3.1 Searchable Symmetric Encryption.
3.2 Considered Conjunctive Keyword Search Model -- 3.3 Attacker Model -- 3.4 Attacker Knowledge -- 4 CKWS-Adapted Refined Score Attack -- 4.1 Score Attacks -- 4.2 Generic Extension -- 4.3 Transform Key Steps of Refined Score Attack -- 4.4 Revised Algorithm -- 4.5 Complexity -- 5 Experiments -- 5.1 Setup -- 5.2 Results -- 6 Discussion -- 7 Conclusion -- References -- Gummy Browsers: Targeted Browser Spoofing Against State-of-the-Art Fingerprinting Techniques -- 1 Introduction -- 2 Background and Related Work -- 2.1 Browser Fingerprinting -- 2.2 Representative Fingerprinting Techniques -- 2.3 Applications of Browser Fingerprinting -- 3 Attack Model and Spoofing Methods -- 3.1 Attack Model -- 3.2 Spoofing Methods -- 4 Attack Implementation -- 4.1 Acquiring User Browser Fingerprint -- 4.2 Visual Attack -- 4.3 Algorithm Attack: Attacking Prominent Fingerprinting Based Techniques -- 5 Dataset and Evaluation Methodology -- 5.1 FP-Stalker Dataset -- 5.2 Evaluation Methodology -- 6 Results -- 6.1 Visual Attack Results -- 6.2 Algorithm Attack Results -- 7 Implications of Our Attack -- 8 Discussion -- 9 Conclusion -- References -- Identifying Near-Optimal Single-Shot Attacks on ICSs with Limited Process Knowledge -- 1 Introduction -- 2 Background -- 2.1 Closed Control Loops -- 2.2 Process Knowledge Data Sources -- 3 Identifying Near-Optimal Single-Shot Attacks -- 3.1

System Model -- 3.2 Attacker Model -- 3.3 Research Questions and Challenges -- 3.4 Identifying Near-Optimal Single-Shot Attacks in CCL Graphs -- 3.5 Motivating Example -- 4 Implementation -- 5 Experimental Evaluation -- 5.1 Tennessee Eastman Plant -- 5.2 Experimental Attacks -- 6 Discussion -- 7 Related Work -- 8 Conclusion -- References -- RSA Key Recovery from Digit Equivalence Information -- 1 Introduction -- 2 Background -- 2.1 RSA -- 2.2 Fixed-Window Exponentiation.
2.3 Attacks on Fixed-Window Exponentiation -- 2.4 The Heninger-Shacham Algorithm -- 2.5 Markov Chains -- 3 Attacker Model -- 4 Our Approach -- 4.1 Algorithm Overview -- 4.2 Complexity Analysis of the Aligned Case -- 4.3 Independent Markov Chains -- 4.4 Unaligned Case -- 5 Results and Comparisons -- 5.1 Theoretical Results -- 5.2 Experimental Results -- 6 Conclusions -- References -- Practical Seed-Recovery of Fast Cryptographic Pseudo-Random Number Generators -- 1 Introduction -- 2 Description of Arrow -- 3 Attacks on Arrow -- 3.1 Simple Guess-and-Determine Attack on Arrow-II -- 3.2 Longer Guess-and-Determine Attack on Arrow-I -- 3.3 An Attack Against Arrow-III, the Software Version of Arrow -- 4 Description of Trifork -- 5 Attack on Trifork -- 5.1 Recovering Z-r3 -- 5.2 Recovering Y-r2 -- References -- Autoguess: A Tool for Finding Guess-and-Determine Attacks and Key Bridges -- 1 Introduction -- 2 Preliminaries -- 2.1 Guess-and-Determine Technique -- 2.2 Key-Bridging Technique -- 2.3 Connection Relations -- 2.4 A Naive Guess-and-Determine Approach -- 3 Constraint Programming for GD and Key-Bridging -- 3.1 Modelling Knowledge Propagation -- 3.2 Encoding Using CP -- 4 From Guess Basis to Gröbner Basis -- 5 Autoguess -- 5.1 Preprocessing Phase -- 5.2 Early-Abort Technique -- 6 Application to Automatic Search for Key Bridges -- 6.1 Application to PRESENT -- 6.2 Application to LBlock with Nonlinear Key Schedule -- 7 Application to GD Attack on Block Ciphers -- 7.1 Automatic GD Attack on AES -- 8 Application to GD Attack on Stream Ciphers -- 8.1 Automatic GD Attack on ZUC -- 9 Key-Recovery-Friendly Distinguishers -- 9.1 DS-MITM Attack on SKINNY-{64-192, 64-128, 128-256} -- 9.2 Improved DS-MITM Attack on TWINE-80 -- 10 Conclusion -- References -- Cryptographic Protocols -- KEMTLS with Delayed Forward Identity Protection in (Almost) a Single Round Trip.
1 Introduction -- 1.1 Contributions -- 2 Preliminaries -- 3 Protocol -- 4 Security Model -- 5 Security Analysis -- 6 Discussion -- 7 Implementation -- 8 Benchmarking -- References -- Improving the Privacy of Tor Onion Services -- 1 Introduction -- 1.1 Related Work -- 2 Attacks -- 2.1 Tor and Hidden Service Directories -- 2.2 Attacks Targeting Clients -- 2.3 Attacks Targeting Onion Services -- 3 PIR for Descriptor Lookups -- 4 Privacy Analysis for PIR Schemes -- 5 Benchmarking and Results -- 5.1 Hardware-Assisted PIR Benchmarks -- 5.2 CPIR Microbenchmarks -- 5.3 Tor Integration Results -- 6 Conclusion -- References -- Privacy-Preserving Authenticated Key Exchange for Constrained Devices -- 1 Introduction -- 1.1 Related Work -- 1.2 Contributions -- 2 Description of the SAKE Protocol -- 2.1 SAKE -- 2.2 SAKE-AM -- 3 A Flawed Proposal -- 3.1 Issues -- 3.2 Countermeasures -- 4 Security Model -- 4.1 Execution Environment -- 4.2 Security Definitions of the Building Blocks -- 5 Privacy-Preserving SAKE/SAKE-AM -- 6 Security of Privacy-Preserving SAKE/SAKE-AM -- 7 Conclusion -- References -- Relations Between Privacy, Verifiability, Accountability and Coercion-Resistance in Voting Protocols -- 1 Introduction -- 2 Related Work -- 3 Preliminaries -- 3.1 Protocols -- 3.2 Notation Related to Voting Protocols -- 3.3 Verifiability and Accountability -- 3.4 Privacy and Coercion-Resistance -- 4 Relations

Between Definitions -- 4.1 Coercion-Resistance and Privacy -- 4.2 Accountability and Verifiability -- 4.3 Privacy and Verifiability -- 4.4 Verifiability and Coercion-Resistance -- 4.5 Privacy and Accountability -- 5 Conclusions and Future Work -- References -- System Security -- An Approach to Generate Realistic HTTP Parameters for Application Layer Deception -- 1 Introduction -- 2 Method -- 2.1 Data Collection and Training -- 2.2 Generation of Parameter Names.
3 Evaluation.