1.

Record Nr.	UNISA996485666803316
Titolo	Information and communications security : 24th International Conference, ICICS 2022, Canterbury, UK, September 5-8, 2022, proceedings / / Cristina Alcaraz [and three others] (editors)
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2022] ©2022
ISBN	3-031-15777-X
Descrizione fisica	1 online resource (649 pages)
Collana	Lecture notes in computer science ; ; Volume 13407
Disciplina	005.8
Soggetti	Computer security Cryptography Telecommunication - Security measures
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 -- Cryptography -- BS: Blockwise Sieve Algorithm for Finding Short Vectors from Sublattices -- 1 Introduction -- 1.1 Related Work -- 1.2 Our Contribution -- 1.3 Organization of the Paper -- 2 Preliminaries -- 2.1 Lattice -- 2.2 Lattice Reduction Algorithms -- 2.3 Learning with Errors -- 3 Block Sieve Algorithm -- 3.1 Basic Block Sieve Algorithm -- 3.2 Progressive Block Sieve Algorithm -- 4 Analysis of BS and PBS -- 4.1 Complexity Analysis -- 4.2 Performance on Challenge Lattices -- 4.3 Performance of PBS on LWE Instances -- 5 Conclusion -- References -- Calibrating Learning Parity with Noise Authentication for Low-Resource Devices -- 1 Introduction -- 2 Preliminaries -- 2.1 Notation -- 2.2 LPN Basics -- 2.3 Assumptions -- 3 Exploring Precision -- 3.1 Statistical Bounds -- 3.2 Computational Simulations -- 3.3 Summary of Precision Results -- 4 Exploring Key Lengths -- 4.1 Key Length Recommendation -- 4.2 Effectiveness of Known Attacks -- 4.3 Effectiveness of Guessing -- 4.4 Effectiveness of Incomplete Attacks -- 4.5 Cryptanalytic Progress -- 4.6 Summary of Key Length Results -- 5 Conclusion -- A Algorithm Pseudocode -- References -- New Results of Breaking the CLS Scheme from ACM-CCS 2014 -- 1 Introduction -- 2 Preliminaries -- 2.1 Notation -- 2.2 co-ACD Problem -- 2.3 CLS Additive Homomorphic

Probability -- 3.1 Decryption Failures -- 3.2 Formula Derivation -- 3.3 The Deviation Between the Theoretical Failure Probability and the Actual Failure Probability -- 4 Experiment and Sample Test -- References -- Authentication -- Improving Deep Learning Based Password Guessing Models Using Pre-processing -- 1 Introduction -- 1.1 Related Work -- 1.2 Our Contributions -- 2 Background -- 2.1 LSTM Based Models -- 2.2 PassGAN -- 3 Preliminaries -- 3.1 Datasets -- 3.2 Ethical Considerations.

4 Preprocessing Methods -- 4.1 Important Abbreviations -- 4.2 Character Feature Based Encoding Method -- 4.3 Refined PCFG -- 4.4 PassGAN Using PCFG for Preprocessing -- 4.5 Chunk+PCFG Preprocessing Method -- 5 Experiments -- 5.1 Attacking Strategies Design -- 5.2 Evaluation Results -- 6 Conclusion -- 1 Some Statistics About User-Chosen Passwords -- 2 Exploratory Experiments -- References -- Exploring Phone-Based Authentication Vulnerabilities in Single Sign-On Systems -- 1 Introduction -- 2 Background and Related Work -- 3 Understanding PBA Goals, Options, and Impacts -- 3.1 Threat Model and Experiment Setup -- 3.2 Impact of Malicious Relying Party Sites -- 3.3 Timing Attacks on Unassociated PBA Approvals -- 3.4 Observable Characteristics of the Attack Scenarios -- 4 User Study and Findings -- 4.1 IRB Process and Participant Recruiting -- 4.2 Experimental Setup -- 4.3 Participant Responses to the Malicious Relying Party Scenario -- 4.4 Participant Responses to Timing Attack Scenario -- 4.5 Participant Feedback and Study Limitations -- 4.6 Potential Mitigations for Deployment -- 5 Concluding Remarks -- References -- FRACTAL: Single-Channel Multi-factor Transaction Authentication Through a Compromised Terminal -- 1 Introduction -- 2 Scenario and Adversary Model -- 2.1 Scenario -- 2.2 Adversarial Model -- 3 Protocol Description -- 3.1 Basic Protocol Flow -- 3.2 Scenario #1 -- 3.3 Scenario #2 -- 4 Security Considerations -- 4.1 Security Features -- 4.2 Formal Security Analysis via ProVerif -- 5 Implementation and Performance Assessment -- 5.1 Implementation Details -- 5.2 Experimental Performance Assessment -- 6 Related Work and Qualitative Comparison -- 7 Conclusion -- References -- Privacy and Anonymity -- Lightweight and Practical Privacy-Preserving Image Masking in Smart Community -- 1 Introduction -- 2 Related Work -- 3 Preliminaries.

3.1 Yolo v5 Object Detection Algorithm -- 3.2 ChaCha20-Poly1305 Stream Encryption Algorithm -- 3.3 Bilinear Map -- 3.4 Proxy Re-encryption -- 4 Our Proposed Scheme -- 4.1 Preparation and Image Pre-processing Phase -- 4.2 Membrane Generation and Image Masking Phase -- 4.3 Proxy Re-encryption Phase -- 4.4 Image Recovery Phase -- 5 Evaluation and Results -- 5.1 Evaluation Setup -- 5.2 Findings and Results -- 5.3 Efficiency Analysis -- 5.4 Security Analysis -- 6 Conclusions -- References -- Using Blockchains for Censorship-Resistant Bootstrapping in Anonymity Networks -- 1 Introduction -- 2 Background -- 2.1 Tor Network -- 2.2 Blockchain Network -- 2.3 Public Key Encryption -- 2.4 Elliptic Curve Diffie-Hellman -- 3 Overview -- 3.1 System Model -- 3.2 Threat Model -- 3.3 Design Goals -- 4 Antiblok Details -- 4.1 Client Request -- 4.2 BridgeDB Response -- 4.3 Circuit Creation -- 5 Security -- 6 Evaluation -- 6.1 Experimental Setup -- 6.2 Functionality Evaluation -- 7 Discussion -- 8 Conclusion -- References -- Repetitive, Oblivious, and Unlinkable SkNN Over Encrypted-and-Updated Data on Cloud -- 1 Introduction -- 1.1 Background -- 1.2 Motivations -- 1.3 Possible Solutions and Technical Challenges -- 1.4 Paper Organization -- 2 Related Work -- 2.1 SkNN -- 2.2 Privacy-Preserving Range Querying -- 3 Problem Formulation -- 3.1 System Model -- 3.2 Threat Model -- 3.3 Design Objectives -- 4