1. Record Nr. UNISA996199938303316

Titolo	Advances in Information and Computer Security [[electronic resource]] : 10th International Workshop on Security, IWSEC 2015, Nara, Japan, August 26-28, 2015, Proceedings / / edited by Keisuke Tanaka, Yuji Suga
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2015
ISBN	3-319-22425-5
Edizione	[1st ed. 2015.]
Descrizione fisica	1 online resource (XIII, 357 p. 51 illus.)
Collana	Security and Cryptology ; ; 9241
Disciplina	005.8
Soggetti	Computer security Data encryption (Computer science) Computer science—Mathematics Algorithms Computer communication systems Systems and Data Security Cryptology Discrete Mathematics in Computer Science Algorithm Analysis and Problem Complexity Computer Communication Networks
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di contenuto	Intro -- Preface -- IWSEC 2015 10th International Workshop on Security -- Contents -- Identity-Based Encryption -- Identity-Based Lossy Encryption from Learning with Errors -- 1 Introduction -- 1.1 Background -- 1.2 Our Contributions -- 1.3 Related Work -- 1.4 Organization -- 2 Preliminaries -- 2.1 Notations -- 2.2 Min-Entropy -- 2.3 Learning with Errors -- 2.4 Discrete Gaussians -- 2.5 Lossy Encryption -- 2.6 Some Results About Randomness -- 3 Identity-Based Lossy Encryption -- 3.1 Selective Opening Security -- 3.2 Construction from LWE -- 4 Conclusion -- References -- Adaptive-ID Secure Revocable Hierarchical Identity-Based Encryption -- 1 Introduction -- 2 Preliminaries -- 3 Revocable Hierarchical Identity-Based Encryption --

4 Proposed Adaptive-ID Secure RHIBE -- 5 Conclusion -- References -- Elliptic Curve Cryptography -- Invalid Curve Attacks in a GLS Setting -- 1 Introduction -- 2 Preliminaries -- 3 Invalid Curve Attack on GLS Scalar Multiplication -- 4 Complexity Analysis -- 5 Implementations -- 6 Conclusion -- A Computation of (u) on u [1, 3] -- References -- New Fast Algorithms for Elliptic Curve Arithmetic in Affine Coordinates -- 1 Introduction -- 2 Preliminary -- 3 Speeding up Some Elliptic Curve Operations in Affine Coordinates -- 4 Comparisons -- 4.1 Point Operations -- 4.2 Scalar Multiplications -- 5 Conclusions -- References -- Factoring -- Implicit Factorization of RSA Moduli Revisited (Short Paper) -- 1 Introduction -- 2 Preliminaries -- 3 Previous Method of Factoring Two RSA Moduli with Implicitly Common Middle Bits -- 4 Our Improvement -- 5 Conclusion -- References -- Symmetric Cryptanalysis -- Improved (Pseudo) Preimage Attacks on Reduced-Round GOST and Grøstl-256 and Studies on Several Truncation Patterns for AES-like Compression Functions -- 1 Introduction -- 2 The Hash Function Family.
3 Improved Preimage Attacks on Reduced-Round GOST -- 3.1 Overview of the Preimage Attack on 5-Round GOST-256 -- 3.2 Phase 1. Construct the Multicollisions -- 3.3 Phase 2. Invert the Output Transformation -- 3.4 Phase 3. Generate the Preimage -- 3.5 Summarize the 5-Round Attack -- 3.6 Extend the Preimage Attack to More Rounds -- 4 Conclusion and Open Problems -- References -- Improvement on the Method for Automatic Differential Analysis and Its Application to Two Lightweight Block Ciphers DESL and LBlock-s -- 1 Introduction -- 2 MILP Based Framework for Automatic Differential Cryptanalysis -- 3 Techniques for Obtaining Better Characteristics -- 4 Application to DESL and LBlock-s -- 4.1 Improved Single-Key and Related-Key Differential Characteristics for DESL -- 4.2 Tighter Security Bound for LBlock-s -- 5 Conclusion and Discussion -- References -- Provable Security -- NM-CPA Secure Encryption with Proofs of Plaintext Knowledge -- 1 Introduction -- 2 Preliminaries -- 2.1 Public Key Encryption -- 2.2 Proofs of Knowledge -- 3 Our Scheme -- 4 Security Proof -- 5 Applications: Electronic Voting -- 5.1 Election Schemes -- 5.2 Sufficient Conditions for Ballot Secrecy -- 5.3 Towards a Secure Variant of Helios -- 6 Related Work -- 7 Conclusion -- A Proof of Theorem 1 -- A.1 Game 0: IND-1-CPA -- A.2 Game 1: Simulate Decryption Oracle -- A.3 Game 2: Simulate the Challenge Oracle -- A.4 Game 3: Embed a Challenge Ciphertext -- References -- Improvement of UC Secure Searchable Symmetric Encryption Scheme -- 1 Introduction -- 2 Verifiable Searchable Symmetric Encryption -- 2.1 System Model -- 2.2 Security Definition -- 2.3 Kurosawa-Ohtaki Scheme (KO-Scheme) -- 2.4 Inefficiency of KO-Scheme -- 3 Improvement of KO-Scheme -- 3.1 Concrete Description of Our Scheme -- 3.2 Security -- 3.3 Comparison -- 4 Conclusion -- References.
Fully Leakage-Resilient Non-malleable Identification Schemes in the Bounded-Retrieval Model -- 1 Introduction -- 1.1 Our Contribution -- 1.2 Related Work -- 2 Preliminaries -- 2.1 Bilinear Groups and Hardness Assumptions -- 3 Definition of Fully Leakage Resilient Non-malleable Identification Schemes -- 3.1 Tag-Based Fully Leakage-Resilient Non-malleable Identification Schemes -- 4 A Tag-Based Fully Leakage-Resilient Non-malleable Identification Scheme -- 4.1 Proof of Theorem 1 -- 5 A Fully Leakage-Resilient Non-malleable Identification Scheme -- 5.1 Proof of Security -- References -- LWE-Based Encryption -- LWE-Based FHE with Better Parameters -- 1 Introduction -- 1.1 Motivation and Techniques -- 1.2 Contribution -- 1.3 Other Related Works -- 1.4 Roadmap -- 2 Preliminaries -- 2.1

Homomorphism -- 2.2 Useful Tools -- 2.3 Learning with Errors -- 3 Building Block -- 4 A New LWE-Based PK-FHE -- 4.1 FHE Scheme: YAP -- 4.2 Homomorphic Property of YAP -- 4.3 Bootstrapping and Unbounded PK-FHE -- 5 Conclusions -- References -- Improved Efficiency of MP12 -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Related Works -- 2 Preliminaries -- 2.1 Tag-Based Encryption -- 2.2 Selective-Tag Weak CCA Security -- 2.3 Lattices -- 3 The Learning with Errors (LWE) Problem -- 3.1 Knapsack LWE -- 3.2 Extended-(knapsack) LWE -- 3.3 The Gadget Matrix G -- 4 Description of Our Scheme -- 4.1 Our Scheme -- 5 Conclusion -- References -- Secret Sharing -- Almost Optimum Secret Sharing Schemes with Cheating Detection for Random Bit Strings -- 1 Introduction -- 2 Preliminaries -- 2.1 Secret Sharing Scheme -- 2.2 Cheating Detectable Secret Sharing Schemes -- 2.3 Existing Schemes Secure Under the OKS Model -- 3 Proposed Schemes -- 3.1 Generalization -- 4 Concluding Remarks -- References -- Privacy-Preserving and Anonymity -- k-Anonymous Microdata Release via Post Randomisation Method.
1 Introduction -- 1.1 Motivations -- 1.2 Contributions -- 1.3 Related Work -- 2 Preliminaries -- 2.1 Publishing Scenario -- 2.2 Notation -- 2.3 PRAM -- 2.4 k-Anonymity -- 2.5 Anonymization and Privacy Mechanisms -- 3 Pk-Anonymity -- 3.1 Background Knowledge of Adversary -- 3.2 Definition of Pk-Anonymity -- 4 Applying Pk-Anonymity to PRAM -- 5 Conclusions -- References -- On Limitations and Alternatives of Privacy-Preserving Cryptographic Protocols for Genomic Data -- 1 Introduction -- 2 Protecting Genome Privacy By Cryptography -- 2.1 Example: Privacy-Preserving Data Mining for Allele Frequency -- 2.2 Limitation of Computationally Secure Cryptographic Tools -- 2.3 Everlasting Security -- 3 An Example of Everlasting Security -- 3.1 Observation for the Desired Security -- 3.2 Security Definition -- 4 Preliminaries for Protocol Construction -- 5 Proposed Oblivious Transfer Protocol -- 5.1 Overview of the Construction -- 5.2 Construction -- 5.3 Security Analysis -- 5.4 Execution Cost -- 6 Discussion -- 7 Conclusion -- References -- Anonymous Credential System with Efficient Proofs for Monotone Formulas on Attributes -- 1 Introduction -- 1.1 Backgrounds -- 1.2 Previous Works -- 1.3 Our Contributions -- 2 Preliminaries -- 2.1 Bilinear Maps -- 2.2 Complexity Assumptions -- 2.3 AHO Structure-Preserving Signatures -- 2.4 Groth-Sahai (GS) Proof -- 3 Accumulator to Verify Monotone Formulas -- 3.1 Tag Assignment Algorithm -- 3.2 Correctness of Tag Assignment Algorithm -- 3.3 Accumulator to Verify Monotone Formulas -- 3.4 Correctness and Security of Accumulator -- 4 Syntax and Security Model of Anonymous Credential System -- 4.1 Syntax -- 4.2 Security Model -- 5 Proposed Anonymous Credential System -- 5.1 Construction Overview -- 5.2 Construction -- 5.3 Security -- 6 Efficiency Consideration -- 7 Conclusions -- A Security Model of Anonymous Credential System.
A.1 Misauthentication Resistance -- A.2 Anonymity -- References -- Secure Protocol -- Secure Multi-Party Computation Using Polarizing Cards -- 1 Introduction -- 1.1 Background -- 1.2 Our Contribution -- 1.3 Related Works -- 2 Polarizing Cards -- 2.1 Polarizing Cards -- 2.2 Operations -- 3 Multi-party Computation Using Polarizing Cards -- 3.1 Model -- 3.2 Security -- 4 COPY, XOR, and AND Protocols -- 4.1 COPY Protocol -- 4.2 XOR Protocol -- 4.3 AND Protocol -- 5 Applications -- 5.1 Input-Preserving Protocols -- 5.2 Applications -- 6 Discussions -- 6.1 One-Card-Per-Bit Scheme -- 6.2 Attacks from Outside of Our Model -- References -- Systems Security -- An Analysis Platform for the Information Security of In-Vehicle Networks Connected with External Networks -- Abstract -- 1 Introduction -- 2 Information

Security of an Automobile -- 2.1 Security Issues of an Automobile Connected to External Networks -- 2.2 Drawbacks of CAN -- 2.3 Related Work -- 3 Development of the Analysis Platform -- 3.1 Outline -- 3.2 Message Analysis Platform -- 3.3 Attack Evaluation Platform -- 4 Experiments with an Actual Car -- 4.1 Acquisition of Automotive Status -- 4.2 Spoofing Attack -- 4.3 DoS Attack -- 4.4 Consideration Over Protection Mechanism -- 5 Conclusion -- References -- Beyond Scale: An Efficient Framework for Evaluating Web Access Control Policies in the Era of Big Data -- 1 Introduction -- 2 Preliminaries -- 2.1 Overview of XACML -- 2.2 Processing Attributes -- 3 Two-Stage Clustering -- 3.1 First Stage Clustering -- 3.2 Transition Work -- 3.3 Second Stage Clustering -- 3.4 Other Work -- 4 Experimental Results -- 5 Related Work -- 6 Conclusion -- A Appendix -- References -- Artifact-Metric-Based Authentication for Bottles of Wine (Short Paper) -- 1 Introduction -- 1.1 Our Contributions -- 2 Design of Authentication System -- 2.1 Construction of Authentication System. 2.2 Authentication Algorithm and Preparation.

Sommario/riassunto

This book constitutes the proceedings of the 10th International Workshop on Security, IWSEC 2015, held in Nara, Japan, in August 2015. The 18 full papers and 3 short papers presented in this volume were carefully reviewed and selected from 58 submissions. They were organized in topical sections named: identity-based encryption; elliptic curve cryptography; factoring; symmetric cryptanalysis; provable security; LWE-based encryption; privacy-preserving and anonymity; secure protocol; systems security; and security in hardware.