1. Record Nr. UNISA996466205803316

Titolo	Progress in Cryptology - AFRICACRYPT 2017 [[electronic resource]] : 9th International Conference on Cryptology in Africa, Dakar, Senegal, May 24-26, 2017, Proceedings / / edited by Marc Joye, Abderrahmane Nitaj
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2017
ISBN	3-319-57339-X
Edizione	[1st ed. 2017.]
Descrizione fisica	1 online resource (X, 231 p. 42 illus.)
Collana	Security and Cryptology ; ; 10239
Disciplina	005.82
Soggetti	Computer security Data encryption (Computer science) Coding theory Information theory Numerical analysis Computers Management information systems Computer science Systems and Data Security Cryptology Coding and Information Theory Numeric Computing Computation by Abstract Devices Management of Computing and Information Systems
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Intro -- Preface -- Organization AFRICACRYPT 2017 -- Contents -- Cryptographic Schemes -- RingRainbow -- An Efficient Multivariate Ring Signature Scheme -- 1 Introduction -- 2 Ring Signatures -- 3 Multivariate Cryptography -- 3.1 The Rainbow Signature Scheme -- 3.2 Multivariate Ring Signature Schemes -- 4 Our Ring Signature Scheme -- 4.1 Security -- 5 Parameters -- 6 Alternative Construction of a

Multivariate Ring Signature Scheme -- 6.1 Unforgeability -- 7 Reduction of Public Key Size -- 8 Implementation and Efficiency Results -- 9 Discussion -- 10 Conclusion -- References -- Pinocchio-Based Adaptive zk-SNARKs and Secure/Correct Adaptive Function Evaluation -- 1 Introduction -- 2 Preliminaries -- 2.1 Algebraic Tools, Notation, and Complexity Assumptions -- 2.2 Adaptive zk-SNARKs in the CRS Model -- 2.3 The Pinocchio zk-SNARK Construction from -- 3 Adaptive zk-SNARKs Based on Pinocchio -- 4 Smaller Proofs and Comparison to Literature -- 5 Secure/Correct Adaptive Function Evaluation -- 5.1 Our Construction -- 5.2 Efficient Instantiation Using Secret Sharing and Our zk-SNARK -- 6 Prototype and Distributed Medical Research Case -- 6.1 Prototype of Our zk-SNARK and Adaptive Trinocchio -- 6.2 Application to Medical Survival Analysis -- 7 Conclusion -- References -- Revisiting and Extending the AONT-RS Scheme: A Robust Computationally Secure Secret Sharing Scheme -- 1 Introduction -- 2 Preliminaries -- 2.1 Secret Sharing Schemes -- 2.2 Symmetric Key Encryption -- 2.3 Commitment Schemes -- 2.4 Error Correcting Codes -- 2.5 Information Dispersal Algorithms -- 3 The AONT-RS -- 3.1 Generalising the AONT-RS -- 3.2 Information Leakage -- 3.3 Proving the Privacy of AONT-RS -- 4 Extending AONT-RS to be Robust -- 4.1 Proof of Privacy -- 4.2 Proof of Robustness -- 5 Comparing RAONT-RS and HK2 -- 5.1 The SSMS and HK2 Scheme -- 5.2 Comparison -- 6 Conclusion.
References -- Side-Channel Analysis -- Climbing Down the Hierarchy: Hierarchical Classification for Machine Learning Side-Channel Attacks -- 1 Introduction -- 1.1 Idea and Contributions -- 1.2 Road Map -- 2 Machine Learning Techniques -- 2.1 Naive Bayes -- 2.2 Decision Tree - C4.5 -- 2.3 Rotation Forest -- 2.4 Support Vector Machines -- 3 The Hierarchical Approach Under Test -- 3.1 Experimental Data -- 3.2 Training Phase and Parameter Tuning -- 3.3 Testing Results -- 4 Realistic Testing -- 4.1 Hierarchical Attack -- 4.2 Structured Attack -- 4.3 Attack Results and Comparison with Template Attack -- 5 Discussion -- 6 Conclusions -- References -- Multivariate Analysis Exploiting Static Power on Nanoscale CMOS Circuits for Cryptographic Applications -- 1 Introduction -- 2 Background -- 3 Case Study -- 3.1 4-Bit PRESENT Crypto-Core -- 3.2 Full Implementation of PRESENT-80 Block Cipher -- 3.3 Testbench -- 4 Univariate Analysis of Information Leakage -- 4.1 4-Bit PRESENT Crypto-Core -- 4.2 Full Implementation of PRESENT-80 Block Cipher -- 5 Multivariate Analysis: Can We Exploit More? -- 6 Conclusion -- References -- Differential Bias Attack for Block Cipher Under Randomized Leakage with Key Enumeration -- 1 Introduction -- 1.1 Background -- 1.2 Contribution -- 2 Previous Works -- 2.1 Leakage Model for Side-Channel Attacks -- 2.2 Differential Bias Attack [2] -- 2.3 Key Enumeration and Rank Estimation -- 3 Reestimation of Complexity by Time-Data Tradeoff -- 3.1 New Hypothesis-Testing Method -- 3.2 Comparison to the Previous Method -- 4 Application of Key Enumeration and Rank Estimation -- 4.1 Differential Bias Attack with Key Enumeration -- 4.2 Experimental Evaluation -- 5 Conclusion -- References -- Differential Cryptanalysis -- Impossible Differential Cryptanalysis of Reduced-Round SKINNY -- 1 Introduction -- 2 Specifications of SKINNY.
3 An Impossible Differential Distinguisher of SKINNY -- 4 Impossible Differential Key-Recovery Attack on 20-Round SKINNY-n-2n (n=64 or 128) -- 4.1 Impossible Differential Key-Recovery Attack on SKINNY-64-128 -- 4.2 Impossible Differential Key-Recovery Attack on SKINNY-128-256 -- 5 Impossible Differential Key-Recovery Attack on 18-Round SKINNY-n-n (n=64 or 128) -- 6 Impossible Differential Key-Recovery Attack on 22-Round SKINNY-n-3n (n=64 or 128) -- 7

Conclusion -- References -- Impossible Differential Attack on Reduced Round SPARX-64/128 -- 1 Introduction -- 2 Description of SPARX-64/128 -- 2.1 Specifications of SPARX-64/128 -- 3 Impossible Differentials of SPARX-64/128 -- 4 Impossible Differential Cryptanalysis of SPARX-64/128 -- 4.1 15-Round Impossible Differential Attack on SPARX-64/128 -- 4.2 16-Round Impossible Differential Attack on SPARX-64/128 -- 5 Conclusion -- References -- Applications -- Private Conjunctive Query over Encrypted Data -- 1 Introduction -- 1.1 Review of Recent Works -- 1.2 Our Contribution -- 2 Security Tool -- 2.1 Asymmetric SwHE Scheme -- 2.2 Security of SwHE Scheme -- 2.3 Correctness of SwHE Scheme -- 3 Private Conjunctive Query Protocol -- 3.1 Boosting Performance Using the Batch Technique -- 3.2 Batch Private Conjunctive Query Protocol -- 3.3 Data Representation for Conjunctive Query Processing -- 3.4 Packing Method of Data -- 4 Secure Computation of Private Conjunctive Query -- 4.1 Batch Private Conjunctive Query Protocol -- 4.2 Solving Additional Information Leakage Problem -- 5 Performance Analysis -- 5.1 Theoretical Evaluation -- 5.2 Experimental Settings -- 5.3 Experimental Evaluation -- 6 Conclusions -- References -- Efficient Oblivious Transfer from Lossy Threshold Homomorphic Encryption -- 1 Introduction -- 2 Background -- 3 Definition of Two-Party Lossy Threshold PKE Scheme.
4 A New Two-Party Lossy Threshold Homomorphic Encryption Scheme -- 5 Security of the DKG Protocol DKG -- 6 Security of Encryption Scheme ELTA2E -- 7 Oblivious Transfer Against One-Sided Active Adaptive Adversaries -- 8 Security of Protocol OTAA -- 9 Efficiency and Comparison with Related Work -- 10 Efficiency of the OT Protocol by Hazay and Patra -- 11 Adaptive Zero Knowledge Arguments -- 12 Future Work -- References -- Privacy-Friendly Forecasting for the Smart Grid Using Homomorphic Encryption and the Group Method of Data Handling -- 1 Introduction -- 2 The Smart Grid and Privacy Concerns -- 3 Neural Networks versus the Group Method of Data Handling -- 4 The Fan-Vercauteren SHE Scheme -- 5 Representing Fixed-Point Numbers in Plaintext Space -- 6 Prediction Approach for the Smart Grid -- 6.1 Prediction Model: Apartment Complexes -- 6.2 Design of the Network -- 6.3 Benchmark Results -- 7 Conclusions and Future Work -- References -- Number Theory -- On Indifferentiable Hashing into the Jacobian of Hyperelliptic Curves of Genus 2 -- 1 Introduction -- 2 Preliminaries -- 3 Almost-Injective and Invertible Encodings into Three Families of Hyperellitic Curves -- 3.1 An Almost-Injective Encoding on H1 -- 3.2 An Almost-Injective Encoding on H2 -- 3.3 An Almost-Injective Encoding on H3 -- 4 Applications to the Jacobian -- 4.1 General Framework on Indifferentiable Hashing into the Jacobian -- 4.2 Indifferentiable Hashing into the Jacobian of Hi, 1i3 -- 5 Conclusion -- References -- Cryptanalysis of Some Protocols Using Matrices over Group Rings -- 1 Introduction -- 2 Irreducible Representations of S5 -- 3 Cryptanalysis of Protocols -- 4 An Example -- 5 Conclusion -- References -- Author Index.

Sommario/riassunto

This book constitutes the refereed proceedings of the 9th International Conference on the Theory and Application of Cryptographic Techniques in Africa, AFRICACRYPT 2017, held in Dakar, Senegal, in May 2017. The 13 papers presented in this book were carefully reviewed and selected from 40 submissions. The papers are organized in topical sections on cryptographic schemes, side-channel analysis, differential cryptanalysis, applications, and number theory.