1. Record Nr. UNISA996495572203316

Titolo	Progress in cryptology - AFRICACRYPT 2022 : 13th International Conference on Cryptology in Africa, AFRICACRYPT 2022, Fes, Morocco, July 18-20, 2022, proceedings / / Lejla Batina and Joan Daemen (editors)
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2022] ©2022
ISBN	3-031-17433-X
Descrizione fisica	1 online resource (599 pages)
Collana	Lecture notes in computer science ; ; Volume 13503
Disciplina	005.82
Soggetti	Data encryption (Computer science) Cryptography
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 -- Symmetric Cryptography -- Construction of Recursive MDS Matrices Using DLS Matrices -- 1 Introduction -- 2 Definition and Preliminaries -- 2.1 Finite Fields and MDS Matrices -- 2.2 XOR Count -- 3 Construction of MDS Matrices from DLS Matrices -- 3.1 Diagonal-Like Sparse (DLS) Matrices -- 3.2 Equivalence Classes of DLS Matrices to Construct Recursive MDS Matrices -- 3.3 Equivalence of DLS Matrices with Sparse DSI Matrices -- 4 Construction of MDS Matrices from Generalized DLS Matrices -- 4.1 Construction of 44 Recursive MDS Matrices -- 4.2 Construction of 55 Recursive MDS Matrices -- 4.3 Construction of 66 Recursive MDS Matrices -- 4.4 Construction of 77 Recursive MDS Matrices -- 4.5 Importance of GDLS Matrices -- 5 Conclusion and Future Work -- References -- FUTURE: A Lightweight Block Cipher Using an Optimal Diffusion Matrix -- 1 Introduction -- 2 Definition and Preliminaries -- 2.1 MDS Matrix -- 2.2 Boolean Function and Sbox -- 3 Structure of FUTURE -- 3.1 Round Function -- 4 Design Decision -- 4.1 SubCell -- 4.2 MixColumn -- 4.3 Round Key -- 5 Security Analysis -- 5.1 Differential and Linear Cryptanalysis -- 5.2 Impossible Differential Attacks -- 5.3 Boomerang Attack -- 5.4 Integral Attack -- 5.5 Invariant Subspace Attacks -- 5.6 Meet-in-the-Middle Attacks -- 5.7 Algebraic

Attacks -- 6 Hardware Implementations, Performance and Comparison -- 6.1 FPGA Implementation -- 6.2 ASIC Implementation -- 7 Conclusions -- A Test Vectors -- References -- A Small GIFT-COFB: Lightweight Bit-Serial Architectures -- 1 Introduction -- 1.1 Contributions -- 1.2 Roadmap -- 2 Preliminaries -- 2.1 GIFT-COFB -- 2.2 Swap-and-Rotate Methodology -- 3 GIFT-COFB-SER-S -- 3.1 Implementing the Feedback Function -- 3.2 Multiplication by 2 and 3 -- 3.3 GIFT-COFB-SER-S Total Latency -- 4 GIFT-COFB-SER-F. 4.1 Tweaking the Feedback Function -- 4.2 Reordering Data Bits -- 4.3 Enhancing the Multiplier -- 4.4 GIFT-COFB-SER-F Total Latency -- 5 First-Order Threshold Implementation -- 5.1 GIFT-COFB-SER-TI First-Order Threshold Implementation -- 5.2 Evaluation -- 6 Implementation -- 7 Conclusion -- A Swap-and-Rotate GIFT-128 State Pipeline -- B ANF Equations of the 3-Share GIFT-128S-Box -- References -- Attribute and Identity Based Encryption -- Identity-Based Encryption in DDH Hard Groups -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Related Work -- 2 Preliminaries -- 2.1 Notations and Conventions -- 2.2 Identity-Based Key Encryption -- 2.3 Signature Schemes -- 2.4 Witness Encryption -- 2.5 Smooth Projective Hash Functions -- 2.6 The Generic Group Model -- 3 Construction -- 3.1 Unique Signatures Based on DDH -- 3.2 Witness Encryption Based on DDH -- 3.3 Modified Generic Construction -- 4 Discussion -- 4.1 The PVR Impossibility Result ch4EPRINT:PapRacVah12 -- 4.2 Shortcomings of the PVR Impossibility Result -- 5 Conclusions -- References -- TinyABE: Unrestricted Ciphertext-Policy Attribute-Based Encryption for Embedded Devices and Low-Quality Networks -- 1 Introduction -- 1.1 Our Contributions -- 2 High-level Overview and Details About TinyABE -- 3 Preliminaries -- 3.1 Notation -- 3.2 Access Structures -- 3.3 Ciphertext-policy ABE -- 3.4 Security Model -- 3.5 Pairings (or Bilinear Maps) -- 3.6 Pair Encoding Schemes -- 4 Our Construction: TinyABE -- 4.1 Removing the Bounds from AC16 -- 4.2 The Scheme -- 4.3 The Associated Pair Encoding Scheme -- 5 Security Proof -- 5.1 ``Unbounding'' the AC17 Proof of AC16 -- 5.2 The Selective Property -- 5.3 The Co-selective Property -- 6 Performance Analysis -- 6.1 Computational Costs of TinyABE -- 6.2 Comparison with RW13 and AC16/Att19 -- 6.3 Advantages in Low-Quality Networks and Constrained Devices -- 7 Future Work.
References -- Symmetric Cryptanalysis -- Cryptanalysis of Reduced Round SPEEDY -- 1 Introduction -- 2 Preliminaries -- 2.1 Specification of SPEEDY -- 2.2 SPEEDY Instances and Security Claims -- 2.3 Cube Attacks -- 3 Practical Distinguishers for Two Rounds SPEEDY -- 3.1 Core Idea of Distinguishers -- 3.2 Distinguishers with 214 Data -- 3.3 Distinguishers with 213 Data -- 3.4 Discussion on the Proofs of Distinguishers -- 4 Key Recovery Attacks -- 4.1 3-Round Key Recovery Attack -- 4.2 On Improving Number of Rounds for Key Recovery -- 5 Conclusion -- A SPEEDY Round Constants -- References -- And Rijndael? -- 1 Introduction -- 2 Rijndael -- 3 The Solving Process -- 3.1 Constraint Programming -- 3.2 Two-Step Solving Process -- 3.3 Step 1 -- 3.4 Step 2 -- 4 Results -- 5 Attacks -- 5.1 Attack on 12 Rounds of Rijndael-128-224 -- 5.2 Attack on 12 Rounds of Rijndael-160-256 -- 6 Conclusion -- References -- Breaking Panther -- 1 Introduction -- 2 Specification of Panther -- 2.1 State Update Function F -- 3 Main Observation on Panther -- 3.1 An Observation on F4 -- 3.2 Consequences in a Known Ciphertext only Setting -- 4 Cryptanalysis of Panther -- 4.1 Key-Recovery Attack with One Plaintext/Ciphertext Pair -- 4.2 Plaintext-Recovery Attack with One Known Ciphertext -- 4.3 Forging Attacks -- 5 Implementation -- 5.1 Repairing Panther -- 6 Conclusion -- References -- Automated Key Recovery Attacks on

Round-Reduced Orthros -- 1 Introduction -- 2 Preliminaries -- 2.1 Specification of Orthros -- 2.2 Differential Cryptanalysis -- 2.3 Differential-Linear Cryptanalysis -- 3 Differential-Linear Attack on 7-Round Orthros -- 3.1 Previous Approaches for Automated Key Recovery Attacks -- 3.2 Framework of Mounting Key Recovery Attacks on Orthros -- 3.3 Implement Our Framework with STP -- 3.4 Key Recovery Attack on 7-Round Orthros -- 4 Differential Attack on Orthros.
5 Conclusion and Future Work -- A Integral Key Recovery Attacks on Orthros -- B Differential-Like Attacks Considering Two Rounds Prepended -- C Permutations Adopted in Orthros -- D DDT, LAT and DLCT for the Sbox of Orthros -- References -- Post-quantum Cryptography -- Dilithium for Memory Constrained Devices -- 1 Introduction -- 2 Preliminaries -- 2.1 Dilithium -- 3 Dilithium Signature Generation -- 3.1 Streaming A and y -- 3.2 Compressing w -- 3.3 Compressing cs1, cs2, and ct0 -- 3.4 Variable Allocation -- 3.5 Summary of Optimizations -- 4 Dilithium Key Generation and Signature Verification -- 4.1 Key Generation -- 4.2 Signature Verification -- 5 Results and Discussion -- 6 Conclusions and Future Work -- References -- Lattice-Based Inner Product Argument -- 1 Introduction -- 2 Preliminaries -- 3 Lattice-Based Inner Product -- 3.1 The Protocol -- 3.2 Security Analysis -- 3.3 Efficiency Analysis and Parameters Setting -- 4 Optimized Inner Product Argument -- 4.1 Splitting Rings -- 4.2 Ring Isomorphism -- 4.3 Algebraic Structure of Our Commitment -- 4.4 Correctness of the Inner Product -- 4.5 Zero-Knowledge Inner Product Argument over Splitting Rings -- 4.6 Efficiency Analysis and Parameters Setting -- References -- Streaming SPHINCS+ for Embedded Devices Using the Example of TPMs -- 1 Introduction -- 2 Preliminaries -- 2.1 SPHINCS+ -- 2.2 Trusted Platform Modules -- 3 Design and Implementation -- 3.1 Streaming Interface -- 3.2 TPM Prototype and Streaming Extension -- 3.3 Considerations on Fault Attacks -- 4 Evaluation -- 4.1 Streaming Interface -- 4.2 TPM Integration -- 5 Conclusion -- References -- Post-quantum (Crypt)analysis -- Solving the Learning Parity with Noise Problem Using Quantum Algorithms -- 1 Introduction -- 2 Preliminaries -- 2.1 Fourier Analysis over Finite Abelian Groups -- 2.2 Significant Fourier Coefficients -- 2.3 Quantum Computing.
2.4 Learning Parity with Noise -- 3 Solving Techniques -- 3.1 Gaussian Elimination and Information Set Decoding -- 3.2 Exhaustive Search -- 3.3 Walsh-Hadamard Transform -- 3.4 Quantum Complexity Analysis for EXH and WHT Solvers -- 3.5 Significant Fourier Transform -- 4 Results -- 5 Conclusion -- A Reductions -- A.1 Reduction: Sparse-Secret -- A.2 Reduction: Part-Reduce (LF1) and Xor-Reduce (LF2) -- A. 3 Reduction: Drop-Reduce -- A.4 Reduction: Code-Reduce -- A.5 Reduction: Guess-Reduce -- B Graph of Reductions -- B.1 Finding Optimal -valid Chains -- B.2 Optimizing the build() Algorithm -- References -- An Estimator for the Hardness of the MQ Problem -- 1 Introduction -- 2 Preliminaries -- 2.1 General Notation -- 2.2 Computational Complexity -- 2.3 The MQ Problem -- 2.4 General Strategies for Underdetermined Systems -- 3 Algorithms for Solving MQ -- 3.1 Exhaustive Search -- 3.2 Algorithms Designed for Underdetermined Systems -- 3.3 Gröbner Basis -- 3.4 Hybrid Algorithms -- 3.5 Probabilistic Algorithms -- 4 Algorithms Not Considered in Our Estimator -- 5 The Estimator -- 5.1 Description/Usage -- 5.2 Numerical Results -- 5.3 Security of MPKCs Against the Direct Attack -- References -- Recovering Rainbow's Secret Key with a First-Order Fault Attack -- 1 Introduction -- 1.1 Organization -- 2 Background -- 2.1 The Rainbow Signature Scheme