1. Record Nr. UNISA996490354403316

| | |
|---|---|
| Titolo | Post-quantum cryptography : 13th international workshop, PQCrypto 2022, virtual event, September 28-30, 2022, proceedings / / Jung Hee Cheon and Thomas Johansson, editors |
| Pubbl/distr/stampa | Cham, Switzerland : , : Springer International Publishing, , [2022]<br>©2022 |
| ISBN | 3-031-17234-5 |
| Descrizione fisica | 1 online resource (523 pages) |
| Collana | Lecture Notes in Computer Science |
| Disciplina | 005.8 |
| Soggetti | Data encryption (Computer science)<br>Quantum computers |
| Lingua di pubblicazione | Inglese |
| Formato | Materiale a stampa |
| Livello bibliografico | Monografia |
| Nota di contenuto | Intro -- Preface -- Organization -- Contents -- Code-Based Cryptography -- Hybrid Decoding - Classical-Quantum Trade-Offs for Information Set Decoding -- 1 Introduction -- 2 Preliminaries -- 3 A Quantum ISD Circuit Design -- 3.1 Reducing the Width for Free -- 4 Classical-Time Quantum-Memory Trade-Offs -- 4.1 Shortening the Code -- 4.2 Puncturing the Code -- 4.3 Combined Hybrid -- References -- How to Backdoor (Classic) McEliece and How to Guard Against Backdoors -- 1 Introduction -- 2 Background -- 2.1 McEliece and Binary Goppa Codes -- 2.2 SETUP Mechanism -- 3 Backdooring Vanilla McEliece -- 3.1 Key Generation for Vanilla McEliece -- 3.2 Vanilla McEliece Strong SETUP -- 3.3 From Strong to Weak SETUP -- 4 How to Backdoor Classic McEliece -- 5 How to Use McEliece Encryption Against Classic McEliece -- A Appendix: A Simpler (But Flawed) SETUP Mechanism -- A.1 A Flawed SETUP -- A.2 The distinguisher -- References -- LRPC Codes with Multiple Syndromes: Near Ideal-Size KEMs Without Ideals -- 1 Introduction and Previous Work -- 2 Background on Rank Metric Codes -- 2.1 General Definitions -- 2.2 Ideal Codes -- 2.3 Difficult Problems in Rank Metric -- 3 LRPC Codes and their Decoding -- 3.1 Low Rank Parity Check Codes -- 3.2 A Basic Decoding Algorithm -- 3.3 LRPC Codes Indistinguishability -- 4 LRPC with Multiple Syndromes -- 4.1 General Idea -- 4.2 Description of the |

Scheme (LRPC-MS) -- 4.3 Description of the Scheme with Ideal Structure (ILRPC-MS) -- 4.4 Decoding Failure Rate of Our Scheme -- 4.5 Impact on the Asymptotic Range of Parameters -- 5 Security -- 5.1 Definitions -- 5.2 IND-CPA Proof -- 5.3 Known Attacks -- 6 Parameters -- 7 Conclusion and Future Work -- A Dimension of the Support of the Product of Homogeneous Matrices -- A.1 Preliminary Results on Binary Matrices -- A.2 Proof of Theorem 1 -- B Performance -- References.
Interleaved Prange: A New Generic Decoder for Interleaved Codes -- 1 Introduction -- 2 Preliminaries -- 3 Decoding Algorithms -- 3.1 SD-Based Algorithms -- 3.2 CF-Based Algorithms -- 3.3 Novel Approach: Interleaved Prange -- 3.4 Recognizing Failures -- 3.5 Comparison -- 4 Conclusion -- References -- A Study of Error Floor Behavior in QC-MDPC Codes -- 1 Introduction -- 2 Background -- 2.1 Coding Theory and QC-MDPC Codes -- 2.2 BIKE -- 2.3 Weak Keys and Near Codewords -- 3 Methods -- 4 Average DFR over Full Message Space -- 5 DFR on At,(S) Sets -- 6 Distribution of Syndrome Weight -- 7 Conclusion -- References -- Multivariate Cryptography
and the MinRank Problem -- Improvement of Algebraic Attacks for Solving Superdetermined MinRank Instances -- 1 Introduction -- 2 Notation and Preliminaries -- 3 Relations Between the Various Modelings -- 4 Complexity of Solving Superdetermined Systems -- 5 Application to DAGS -- 5.1 Principle of the Attack -- 5.2 Original Modeling -- 5.3 Modeling Update -- A  Appendix -- References -- A New Fault Attack on UOV Multivariate Signature Scheme -- 1 Introduction -- 2 Preliminaries -- 2.1 Multivariate Signature Schemes -- 2.2 Unbalanced Oil and Vinegar Signature Scheme -- 2.3 Attacks on UOV -- 2.4 Existing Fault Attacks on UOV or Its Variant -- 3 New Fault Attack on UOV -- 3.1 Attack Model -- 3.2 Description -- 4 Analysis of Our Proposed Attack -- 4.1 Application of Key Recovery Attacks -- 4.2 Simulations of Our Proposed Attack -- 4.3 Limited Faults Cases -- 5 Conclusion -- References -- MR-DSS - Smaller MinRank-Based (Ring-) Signatures -- 1 Introduction -- 1.1 Related Work -- 1.2 Contribution -- 2 Preliminaries -- 2.1 Sigma Protocols with Helper -- 2.2 Commitment Schemes -- 3 The Sigma Protocol of Courtois -- 4 Improved MinRank-Based Signature Scheme -- 4.1 Sigma Protocol with Helper for ZK Proof of MinRank.
4.2 Removing the Helper -- 4.3 Further Improvements -- 4.4 Public Key Size -- 4.5 Signature Size -- 4.6 Parameters -- 5 MinRank-Based Ring Signatures -- 5.1 Extending to Ring Signatures -- 5.2 Parameters of the Scheme -- 5.3 Public Key and Signature Size -- A Commitment Scheme -- B Ring Signatures -- B.1 Security Definitions -- B.2 Proofs -- C A Note on Santoso et al.'s Scheme -- References -- IPRainbow -- 1 Introduction -- 2 UOV and Rainbow -- 2.1 Oil and Vinegar -- 2.2 Rainbow -- 3 Known Attacks of Rainbow -- 3.1 Background -- 3.2 Rectangular MinRank Attack -- 3.3 Simple Attack -- 4 IPRainbow -- 4.1 Description of IPRainbow -- 4.2 Security Analysis -- 4.3 Efficiency and Key Size -- 5 Conclusion -- A  Algorithms -- References -- 2F - A New Method for Constructing Efficient Multivariate Encryption Schemes -- 1 Introduction -- 2 Multivariate Encryption Schemes -- 2.1 HFE -- 2.2 SQUARE -- 2.3 ABC Simple Matrix -- 2.4 PCBM -- 3 2F Modulus Switching -- 4 An Instance of 2F Multivariate Encryption -- 5 Security Analysis -- 5.1 MinRank Attacks -- 5.2 Differential -- 5.3 Direct -- 5.4 Lattice Attacks -- 6 Parameters and Performance -- 7 Conclusion -- References -- Quantum Algorithms, Attacks and Models -- Quantum Attacks on Lai-Massey Structure -- 1 Introduction -- 2 Preliminaries -- 2.1 Notation -- 2.2 Pseudo-Random Permutation -- 2.3 Quantum Algorithms -- 3 Quantum Attacks on Lai-Massey Structures -- 3.1

Quantum Chosen-Plaintext Attack Against 3-Round Lai-Massey Structure -- 3.2 Quantum Chosen-Ciphertext Attack Against 4 Round Lai-Massey Structure -- 3.3 Quantum Key-Recovery Attack on 4-Round Lai-Massey Structure -- 4 Lai-Massey and Quasi-Feistel Structures -- 4.1 Quasi-Feistel Structure -- 4.2 Lai-Massey and Quasi-Feistel Structures -- 5 Quantum Attacks Against Quasi-Feistel Structures. 5.1 Quantum Chosen-Plaintext Attack Against 3-Round Quasi-Feistel Structure -- 5.2 Quantum Chosen-Ciphertext Attack Against 4-Round Quasi-Feistel Structure -- 6 Conclusion and Discussion -- A Intermediate Parameters in the Decryption Process of 4-round Lai-Massey Structure in Sect.3.2 -- B  Proof of Theorem 4 -- References -- Sponge-Based Authenticated Encryption: Security Against Quantum Attackers -- 1 Introduction -- 2 Preliminaries -- 2.1 Notation -- 2.2 Definitions -- 3 The Sponge Construction and Slae -- 3.1 Sponge Construction -- 3.2 The FGHF' Construction and Slae -- 4 Post-Quantum (QS1) Security -- 4.1 Security of SlFunc -- 4.2 Security of SPrg -- 4.3 Security of SvHash -- 4.4 Security of Slae -- 5 Quantum (QS2) Security -- 5.1 QS2 Security Notions for SKE -- 5.2 Left-or-Right Security of SlEnc -- 5.3 Real-or-Random Security of SlEnc -- 5.4 IND-qCPA Security of Slae and FGHF' -- 6 Conclusion -- A  Additional Preliminaries -- A.1  Authenticated Encryption -- A.2  Message Authentication Code -- A.3  Hash Function -- B  QS1 Proofs -- B.1 Proof of Theorem 8 -- B.2  Proof of Theorem 9 -- B.3  Proof of Theorem 10 -- B.4  Proof of Theorem 11 -- B.5  Proof of Theorem 12 -- C  QS2 Proofs -- C.1  Proof of Theorem 14 -- References -- Post-quantum Plaintext-Awareness -- 1 Introduction -- 1.1 Motivation -- 1.2 Challenges and Our Contribution -- 1.3 Our Contribution -- 1.4 Organization -- 2 Preliminaries -- 2.1 Definitions -- 3 Post-quantum Plaintext-Awareness -- 3.1 Post-quantum PA0, PA1 -- 3.2 Post-quantum PA2 -- 4 Relationships Between Notions -- 4.1 Relationships Between PA Notions -- 4.2 Relation with IND-qCCA -- 5 Achievability -- A  Preliminaries -- A.1  Commitment Scheme -- A.2  Basics of Quantum Computing -- B  Discussion on Quantum Eavesdropping -- C Proof of Theorem 8 -- D  Achievability -- D.1  OAEP transform -- References.
On Quantum Ciphertext Indistinguishability, Recoverability, and OAEP -- 1 Introduction -- 1.1 Our Contribution -- 1.2 Related Work -- 1.3 Outline -- 2 Preliminaries -- 2.1 Notation -- 2.2 Public-Key Cryptography -- 2.3 Quantum Computing -- 3 (Quantum) Ciphertext Indistinguishability -- 3.1 The qINDqCPA Security Notion -- 3.2 Interpretation of Ciphertext Indistinguishability -- 4 Observations on Recoverability -- 4.1 Recoverability -- 4.2 Equivalent Recoverable PKE Schemes -- 5 OAEP -- 5.1 Recoverability of OAEP -- 5.2 Quantum Operators for OAEP -- References -- Implementation and Side Channel Attacks -- Efficiently Masking Polynomial Inversion at Arbitrary Order -- 1 Introduction -- 2 Preliminaries -- 2.1 Notation -- 2.2 Masking -- 2.3 Polynomial Inversion Applications -- 3 Masking Polynomial Inversion -- 3.1 Conversion from Additive to Multiplicative Sharing -- 3.2 Conversion from Multiplicative to Additive Sharing -- 3.3 Reducing the Number of Inversions -- 3.4 Reducing the Number of Multiplications -- 4 Implementation and Evaluation -- 4.1 Implementation Results -- 4.2 Side-Channel Evaluation -- 5 Conclusion -- References -- A Power Side-Channel Attack on the Reed-Muller Reed-Solomon Version of the HQC Cryptosystem -- 1 Introduction -- 2 Preliminaries -- 2.1 Notation -- 2.2 HQC -- 2.3 Choice of Error Correcting Code C -- 3 Novel Oracle-Based Side-Channel Attack -- 3.1 Support Distribution of y -- 3.2 General Attack Idea -- 3.3 Description of the Attack Strategy -- 3.4 Retrieval of y from

Partial Information with Information Set Decoding -- 4 Side-Channel Targets to Build the Required Oracle -- 4.1 Power Side-Channel of the RS Decoder -- 4.2 Power Side-Channel of the Used Hash Functions G,H -- 4.3 Timing Side-Channel of the Used Sampler -- 5 Conclusion -- A Counterexample to the Attack Strategy in ch16Ueno2021, ch16Xagawa21archive.
B  Modified Variant of Stern's Algorithm.