1. Record Nr. UNINA9910755088303321

Titolo	Code-Based Cryptography : 11th International Workshop, CBCrypto 2023, Lyon, France, April 22–23, 2023, Revised Selected Papers / / edited by Andre Esser, Paolo Santini
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2023
ISBN	3-031-46495-8
Edizione	[1st ed. 2023.]
Descrizione fisica	1 online resource (183 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 14311
Disciplina	003.54
Soggetti	Cryptography Data encryption (Computer science) Computer networks Computer science - Mathematics Application software Data protection Cryptology Computer Communication Networks Mathematics of Computing Computer and Information Systems Applications Data and Information Security
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 -- An Analysis of the RankSign Signature Scheme with Rank Multipliers -- 1 Introduction -- 2 Rank Metric Properties and Bounds -- 2.1 The Rank Metric -- 2.2 Bounds in the Rank Metric -- 2.3 A Difficult Problem in the Rank Metric -- 3 LRPC Codes -- 3.1 Erasure Decoder for LRPC Codes -- 4 The RankSign Signature Scheme -- 4.1 KeyGen -- 4.2 Sign -- 4.3 Verify -- 5 Attack by Debris-Alazard and Tillich -- 6 Repairing RankSign -- 6.1 KeyGen -- 6.2 Sign -- 6.3 Verify -- 6.4 Key and Signature Size -- 6.5 Discussion of Parameters -- 7 Conclusion -- References -- Fast Gao-Like Decoding of Horizontally Interleaved Linearized Reed-Solomon Codes -- 1 Introduction -- 2 Preliminaries -- 2.1 Skew-Polynomial

Rings -- 2.2 The Sum-Rank Metric and the Corresponding Interleaved Channel Model -- 2.3 Horizontally Interleaved Linearized Reed-Solomon (HILRS) Codes -- 3 A Gao-Like Decoder for HILRS Codes -- 4 A Fast Variant of the Gao-Like Decoder for HILRS Codes -- 4.1 Minimal Approximant Bases -- 4.2 Solving the Gao-Like Key Equation via Minimal Approximant Bases -- 5 Conclusion -- References -- Theoretical Analysis of Decoding Failure Rate of Non-binary QC-MDPC Codes -- 1 Introduction -- 2 Analysis of Guaranteed Error-correction Capability of Non-binary QC-MDPC Codes -- 2.1 One-Step Majority Logic Decoding -- 3 Plausibility Analysis of 1-iteration Parallel Symbol Flipping Decoder -- 3.1 Distribution of Counters -- 3.2 Analysis of Parallel Symbol-Flipping Decoder -- 4 Choice of Cryptosystem Parameters -- 5 Conclusion -- References -- FuLeeca: A Lee-Based Signature Scheme -- 1 Introduction -- 2 Preliminaries -- 2.1 Notation -- 2.2 Basic Cryptographic Tools -- 2.3 Lee-Metric Codes -- 3 System Description -- 3.1 Key Generation -- 3.2 Signature Generation -- 3.3 Signature Verification -- 3.4 Encoding and Decoding.
4 Security Analysis -- 4.1 Hardness of Underlying Problem and Generic Solvers -- 4.2 Analysis of the Algorithm with Respect to Known Attacks -- 4.3 Lattice-Based Attacks -- 5 Efficiency and Performance -- 5.1 Parameters -- 5.2 Reason for Choice of Parameters -- 5.3 Detailed Performance Analysis -- 6 Preliminary Attack on FuLeeca -- 7 Conclusion -- References -- Algebraic Algorithm for the Alternating Trilinear Form Equivalence Problem -- 1 Introduction -- 2 Preliminaries -- 3 Previous Algorithms for Solving ATFE -- 3.1 Graph-Theoretic Algorithm of Bouillaguet et al. ch5BFV12 -- 3.2 Graph-Theoretic Algorithm of Beullens ch5Beu22 -- 4 A Coding Theory Perspective of ATFE -- 5 Algebraic Algorithms for Solving ATFE -- 5.1 Direct Modelling -- 5.2 Improved Matrix-Code Modelling -- 5.3 Removing Invalid Solutions -- 6 Complexity Analysis -- 6.1 Non-trivial Syzygies -- 6.2 Hilbert Series and the Solving Degree -- 7 Experimental Results -- 7.1 Computing Syzygies -- 7.2 Running Gröbner Basis Computations -- References -- Modeling Noise-Accepting Key Exchange -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Related Work -- 2 Prerequisites -- 3 Key Exchange over Unreliable Networks -- 3.1 Modeling Noise -- 3.2 Noisy Matching Conversations -- 4 The Validity of Our Model -- 4.1 Secure in a Noise-Free Environment -- 4.2 Canonical Extension to a Noisy Environment -- 5 Tools for Constructing Noisy Key Exchange -- 5.1 Other Error-Resistant Security Notions -- 5.2 Error Tolerant FO-Transform -- 5.3 Error-Resistant KEA Construction -- 6 Existence of Error-Resistant PKE -- A Proof of Modified FO-transform Theorem 2 -- References -- Generic Error SDP and Generic Error CVE -- 1 Introduction -- 2 Preliminaries -- 3 Generic Error Sets -- 3.1 Error Detectability and Correctability -- 3.2 Generic Gilbert-Varshamov Bound -- 3.3 Density of Codes Correcting a Generic Error Set.
4 Generic Error SDP -- 5 Generic Error CVE -- 5.1 Completeness -- 5.2 Soundness -- 5.3 Zero-Knowledge -- 6 On Polynomial Instances of GE-SDP -- 6.1 Vulnerability of R-SDP and R-CVE -- 7 Conclusions -- References -- PALOMA: Binary Separable Goppa-Based KEM -- 1 Introduction -- 1.1 Trapdoor -- 1.2 KEM Structure -- 1.3 Parameter Sets -- 2 Specification -- 2.1 Parameter Sets -- 2.2 Key Generation -- 2.3 Encryption and Decryption -- 2.4 Encapsulation and Decapsulation -- 3 Performance Analysis -- 3.1 Description of C Implementation -- 3.2 Data Size -- 3.3 Speed -- 4 Security -- 4.1 OW-CPA-secure PKE= (GenKey, Encrypt, Decrypt) -- 4.2 IND-CCA2-Secure KEM= (GenKey, Encap, Decap) -- 5 Conclusion -- A Mathematical Background -- A.1 Syndrome Decoding Problem -- A.2 Binary Separable Goppa Code --

A.3 Extended Patterson for Binary Separable Goppa code -- B Pseudo codes for PALOMA -- References -- Author Index.

Sommario/riassunto

This book constitutes the refereed proceedings of the 11th International Conference on Code-Based Cryptography, CBCrypto 2023, held in Lyon, France, during April 22–23, 2023. The 8 full papers included in this book were carefully reviewed and selected from 28 submissions. The conference offers a wide range of many important aspects of code-based cryptography such as cryptanalysis of existing schemes, the proposal of new cryptographic systems and protocols as well as improved decoding algorithms. .