1. Record Nr. UNINA9910741184703321

Titolo	Advances in Cryptology – CRYPTO 2023 : 43rd Annual International Cryptology Conference, CRYPTO 2023, Santa Barbara, CA, USA, August 20–24, 2023, Proceedings, Part III / / edited by Helena Handschuh, Anna Lysyanskaya
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2023
ISBN	9783031385483 3031385489
Edizione	[1st ed. 2023.]
Descrizione fisica	1 online resource (XIX, 794 p. 112 illus., 62 illus. in color.)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 14083
Disciplina	005.824
Soggetti	Cryptography Data encryption (Computer science) Computer engineering Computer networks Computer networks - Security measures Coding theory Information theory Cryptology Computer Engineering and Networks Mobile and Network Security Coding and Information Theory
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Preface -- Organization -- Contents - Part III -- Cryptanalysis -- Fast Practical Lattice Reduction Through Iterated Compression -- 1 Introduction -- 1.1 Overview of Techniques -- 2 Background -- 2.1 Notation -- 2.2 History of Lattice Reduction Algorithms -- 2.3 Lattice Reduction Basics -- 2.4 Heuristic Assumptions -- 3 Lattice Profiles and Their Application -- 3.1 Example Profiles -- 3.2 Functions of the Lattice Profile -- 3.3 Profile Compression and Profile Drop -- 3.4 Lattice Reduction Condition -- 4 Improved Lattice Reduction Algorithm -- 4.1 Basis Compression -- 4.2 Reducing Sublattices -- 4.3 Lattice

Reduction of Partially Reduced Bases -- 4.4 Analyzing the Behavior of Left-Right Reduction -- 4.5 Reducing Generic Lattice Bases -- 5 Implementation Details -- 6 Experimental Evaluation -- 6.1 Knapsack Lattices -- 6.2 Gentry-Halevi Fully Homomorphic Encryption -- 6.3 Univariate Coppersmith -- 6.4 RSA Factorization with High Bits Known -- 6.5 q-Ary Lattice Reduction -- 6.6 Approximate GCD -- References
-- Does the Dual-Sieve Attack on Learning with Errors Even Work? -- 1 Introduction -- 1.1 Contributions -- 1.2 Conclusion -- 2 Preliminaries -- 2.1 Probabilities and Distributions -- 2.2 Lattices -- 2.3 Dual Distinguishing -- 3 Dual-Sieve-FFT Distinguishing, Generalized -- 3.1 Abstracting the Dual-Sieve-FFT Attack of Guo-Johansson -- 3.2 Implementation of the General Dual-Sieve-FFT Attack -- 3.3 Advantages of the Generalization -- 4 Contradictions from the Heuristic Analysis -- 4.1 Distinguishing the Indistinguishable -- 4.2 Candidates Closer Than the Solution (Asymptotic) -- 4.3 Candidates Closer Than the Solution (Concrete) -- 5 Experiments -- 5.1 Implementation Details -- 5.2 Distribution of Scores of Uniform Targets -- 5.3 Distribution of Scores of BDD Targets -- 5.4 Distribution of Scores, with Modulus Switching -- 6 Afterthoughts.
6.1 A Similar Result from Coding Theory -- 6.2 The Origin of Correlation -- 6.3 Is the Dual Attack Fixable? -- References --
Exploring Decryption Failures of BIKE: New Class of Weak Keys and Key Recovery Attacks -- 1 Introduction -- 1.1 Our Results -- 1.2 Related Works -- 1.3 Summary of Our Work -- 1.4 Organizations -- 2 Preliminary -- 2.1 Estimate of the Probability from the Frequency -- 2.2 BIKE -- 2.3 The Bit-Flipping Algorithm -- 3 The Gathering Property for QC-MDPC -- 3.1 The Frequency of Decryption Failures -- 3.2 An Explanation of the Gathering Property -- 3.3 Number of Keys and Errors Satisfying the Gathering Property -- 4 A New Class of Weak Keys -- 4.1 Extending Weak Keys Using Isomorphism -- 4.2 Lower Bound on the Average DFR -- 5 A Key Recovery Attack Using Decryption Failures -- 5.1 Attack Model -- 5.2 Information Set Decoding Using Extra Information -- 5.3 Complexity Analysis -- 6 A Key Recovery Attack with Ciphertexts Reusing -- 6.1 Attack Model (with Ciphertexts Reusing) -- 6.2 Complexity Analysis -- 7 Conclusion -- References --
Graph-Theoretic Algorithms for the Alternating Trilinear Form Equivalence Problem -- 1 Introduction -- 2 Preliminaries -- 3 The Graph of Alternating Trilinear Forms -- 4 Solving ATFE with Auxiliary Information via Gröbner Bases -- 5 Algorithms for the Alternating Trilinear Form Equivalence Problem -- 5.1 The Algorithms of ch4PKC: BFFP11,ch4EC:TDJPQS22 -- 5.2 A General MinRank-Based Algorithm -- 5.3 Graph-Walking Algorithms for Small n -- 5.4 A (Sketch of An) Algorithm Using Graph-Neighbourhood Invariants -- 6 A Class of Weak Keys for n=10 -- 7 The Curious Case of n=9 -- 7.1 Graph-Neighbourhood Invariants -- 7.2 A Mysterious Function H -- 7.3 Turning H into an Invariant -- 7.4 Using F to Solve the ATFE Problem -- References.
Analysis of the Security of the PSSI Problem and Cryptanalysis of the Durandal Signature Scheme -- 1 Introduction -- 2 Preliminaries -- 2.1 Notation and General Definitions -- 2.2 Dimension of an Intersection of Subspaces -- 2.3 Product Spaces -- 3 Durandal Signature Scheme -- 3.1 Description of the Scheme -- 3.2 Parameters -- 4 PSSI Problem -- 5 An Observation When m Is High -- 6 An Attack Against PSSI -- 6.1 General Overview of the Attack -- 6.2 Technical Results About 2-Sums -- 6.3 Proof of the Probability of Success of the Attack -- 6.4 Complexity of the Attack -- 6.5 Number of Signatures -- 7 Experimental Results -- 8 Conclusion and Perspectives -- References
-- Finding Short Integer Solutions When the Modulus Is Small -- 1

Introduction -- 2 Preliminaries -- 2.1 Lattices and Computational Problems -- 2.2 Reduction Algorithms -- 2.3 Lattice Sieves -- 2.4 Elements of High Dimensional Geometry -- 3 Attack on Small Modulus SIS -- 3.1 On the Z-Shape of BKZ Reduced Bases for q-ary Lattices -- 3.2 Exploiting the Z-Shape -- 3.3 On Balls and Cubes -- 3.4 Putting It All Together -- 3.5 Extension to ISIS -- 4 Optimisations -- 4.1 On the Fly Lifting -- 5 Experimental Verification -- 5.1 The Lengths of Lifts -- 5.2 The Z-Shape Basis -- 6 Application and Practical Cryptanalysis -- 6.1 Small q Hash and Sign Signatures -- References -- Practical-Time Related-Key Attack on GOST with Secret S-Boxes -- 1 Introduction -- 2 Preliminaries -- 2.1 The Structure of GOST -- 2.2 Related-Key Differential Attacks -- 3 The New Related-Key Differential of GOST -- 3.1 The Basic 3-Round Iterative Related-Key Differential -- 3.2 The Full 32-Round Differential -- 3.3 The Related-Key Differential for GOST with Secret S-boxes -- 3.4 Other Variants of the Differential -- 4 The New Related-Key Attack on GOST with Secret S-boxes -- 4.1 The Strategy Used for S-box Recovery.
4.2 First Stage of the Attack - Recovering Two S-boxes -- 4.3 The Second Stage of the Attack - Recovering Two Additional S-boxes -- 4.4 The Third Stage of the Attack - Recovering One Additional S-box -- 4.5 The Fourth Stage of the Attack - Recovering the Rest of the S-Boxes and Eliminating More Wrong Candidates of K1 -- 4.6 Experimental Verification of the Attack -- 5 Possible Application to GOST-Based Hash Functions -- 5.1 Collision Attack on a Davies-Meyer Construction Using GOST -- 5.2 Observations on the GOST Hash Function -- 6 Summary and Conclusions -- References -- On Perfect Linear Approximations and Differentials over Two-Round SPNs -- 1 Introduction -- 2 Preliminaries -- 3 Perfect Linear Approximations -- 3.1 Unkeyed Permutations -- 3.2 Two Rounds -- 3.3 SPNs -- 4 Probability-One Differentials -- 4.1 Recent Results Regarding Round Function Decompositions -- 4.2 Implications of Two Different Decompositions -- 4.3 A Less Technical Interpretation -- 5 Conclusion -- References -- Differential Meet-In-The-Middle Cryptanalysis -- 1 Introduction -- 2 The New Attack: Differential MITM -- 2.1 General Framework -- 2.2 Improvement: Parallel Partitions for Layers with Partial Subkeys -- 2.3 Improvement: Reducing Data with Imposed Conditions -- 2.4 Discussion and Comparison -- 3 Differential Meet-the-Middle Attacks Against SKINNY-128-384 -- 3.1 Specifications of SKINNY -- 3.2 An Attack Against 23-Round SKINNY-128-384 -- 3.3 Enumeration Procedure of kout for the 23-Round Attack -- 3.4 Extension to 24 Rounds -- 3.5 An Attack Against 25 Rounds of SKINNY-128-384 -- 3.6 Comparison of the Attacks on SKINNY-128-384 with Differential Attacks -- 4 New Attack Against 12-Round AES-256 in the related-key setting -- 4.1 Description of AES-256 -- 4.2 Generation of the Related Keys -- 4.3 The Attack -- 5 Conclusion and Open Problems.
A Automatic Detection of Involved Keys -- References -- Moving a Step of ChaCha in Syncopated Rhythm -- 1 Introduction -- 2 Preliminaries -- 3 Reviewing Differential Cryptanalysis of ChaCha -- 3.1 Differential Attack Based on PNB Method -- 3.2 Recent Advances in Cryptanalysis of ChaCha -- 4 The PNB-Based Attack with Syncopation -- 4.1 Syncopation Technique -- 4.2 Refined PNB-Based Attack with Syncopation -- 5 Theoretical Analysis of Differential Equations -- 5.1 Reducing Complexities -- 5.2 Theoretical Interpretation of Strong Key -- 6 Applications: ChaCha7/7.5/6 -- 6.1 Attacks Against ChaCha7 -- 6.2 Attacks Against ChaCha7.5 -- 6.3 Attack Against ChaCha6 -- 7 Conclusion -- References -- Cryptanalysis of Symmetric Primitives over Rings and a Key Recovery Attack on Rubato -- 1 Introduction -- 1.1

From Traditional Symmetric Primitives to Symmetric Primitives over Integer Rings Modulo Composites -- 1.2 Our Contributions -- 2 General Security of Symmetric Primitives: Fields Versus Integers Modulo q -- 2.1 Notation and Preliminaries -- 2.2 Solving Polynomial Systems Modulo q -- 2.3 Impact on Security -- 3 Algebraic Methods over Zq for Composite q -- 3.1 Linearization Attacks -- 3.2 Gröbner Basis Attack -- 3.3 Interpolation Attack -- 3.4 Higher-Order Differential Attack -- 4 Designing a Non-linear (S-box) Function over Zq -- 4.1 Polynomial Non-linear Function over Zq -- 4.2 Learning from Elisabeth: Look-Up Tables -- 4.3 ``Cut and Sew'' Approach -- 5 Rubato -- 5.1 Description of Rubato -- 5.2 About the Value of q: Rubato in the RtF Framework -- 5.3 Non-invertible And/Or Non-MDS Matrices for Rubato -- 6 Key Recovery Attack on Rubato -- 6.1 Recovering Key and Noise Modulo a Small Factor of q -- 6.2 Recovering the Key Modulo a Larger Factor of q and Positions in the Key Stream with No Noise -- 6.3 Key-Recovery of the Full Rubato Key.
7 Assumptions and Cost of the Attack on Rubato.

Sommario/riassunto

The five-volume set, LNCS 14081, 140825, 14083, 14084, and 14085 constitutes the refereed proceedings of the 43rd Annual International Cryptology Conference, CRYPTO 2023. The conference took place at Santa Barbara, USA, during August 19-24, 2023. The 124 full papers presented in the proceedings were carefully reviewed and selected from a total of 479 submissions. The papers are organized in the following topical sections: Part I: Consensus, secret sharing, and multi-party computation; Part II: Succinctness; anonymous credentials; new paradigms and foundations; Part III: Cryptanalysis; side channels; symmetric constructions; isogenies; Part IV: Faster fully homomorphic encryption; oblivious RAM; obfuscation; secure messaging; functional encryption; correlated pseudorandomness; proof systems in the discrete-logarithm setting. .