

1. Record Nr.	UNINA9910855383103321
Titolo	Advances in Cryptology – EUROCRYPT 2024 : 43rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zurich, Switzerland, May 26–30, 2024, Proceedings, Part I / / edited by Marc Joye, Gregor Leander
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2024
ISBN	3-031-58716-2
Edizione	[1st ed. 2024.]
Descrizione fisica	1 online resource (505 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 14651
Disciplina	005.8
Soggetti	Cryptography Data encryption (Computer science) Data protection Computer networks - Security measures Computer networks Information technology - Management Cryptology Security Services Mobile and Network Security Computer Communication Networks Computer Application in Administrative Data Processing
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 - Part I -- Awarded Papers -- SQISignHD: New Dimensions in Cryptography -- 1 Introduction -- 1.1 A Modular Overview of SQISignHD -- 2 Representing the Response Isogeny Efficiently in Higher Dimension -- 2.1 State of the Art Isogeny Representation: A Slow Signature Process -- 2.2 Embedding Isogenies in Higher Dimension with Kani's Lemma -- 2.3 Application of Kani's Lemma to SQISign -- 3 Key Generation, Commitment and Challenge -- 3.1 Accessible Torsion and Choice of the Prime Characteristic -- 3.2 Challenge Generation -- 3.3 Fast Key Generation and Commitment -- 4 Response and Verification -- 4.1

Overview of the Response Computation -- 4.2 Finding a Uniformly Random Tight Response Ideal -- 4.3 Dividing the Higher Dimensional Isogeny Computation in Two -- 4.4 Computing the Response Isogeny Representation -- 4.5 Verification -- 5 Security Analysis -- 5.1 Knowledge Soundness -- 5.2 Heuristic Zero-Knowledge Property -- 5.3 On Hardness of the Supersingular Endomorphism Problem with Access to an Auxiliary Oracle -- 6 The SQIsignHD Digital Signature Scheme -- 6.1 Compactness -- 6.2 Time Efficiency -- References -- Tight Indistinguishability Bounds for the XOR of Independent Random Permutations by Fourier Analysis -- 1 Introduction -- 1.1 The XoP Construction -- 1.2 Our Contribution -- 1.3 Paper Structure -- 2 Preliminaries -- 2.1 Probability -- 2.2 Fourier Analysis -- 2.3 Cryptographic Preliminaries and Sampling Without Replacement -- 3 Indistinguishability Bounds for XoP[r,n] Using Fourier Properties of Sampling Without Replacement -- 3.1 Basic Properties of n, k -- 3.2 Application to Indistinguishability Bounds for XoP[r,n] -- 4 Bounding $M=k[n, k]$ (Proof of Lemma 1) -- 4.1 Bounding $|n, k|^{0362n, k}|$ for Type $K = (k)$ -- 4.2 Classification of Masks -- 4.3 Bounding $|n, k|^{0362n, k}|$ for General.

5 Bounding $W=k[n, k]$ (Proof of Lemma 2) -- A Missing Proofs from Section 4 -- References -- AprèsSQL: Extra Fast Verification for SQIsign Using Extension-Field Signing -- 1 Introduction -- 2 Preliminaries -- 2.1 Elliptic Curves and Their Endomorphism Rings -- 2.2 Quaternion Algebras and the Deuring Correspondence -- 2.3 SQIsign -- 2.4 SQIsign-Friendly Primes -- 2.5 Computing Rational Isogenies from Irrational Generators -- 3 Signing with Extension Fields -- 3.1 Changes in the Signing Procedure -- 3.2 Increased Torsion Availability from Extension Fields -- 3.3 Cost of Signing Using Extension Fields -- 4 Effect of Increased 2-Torsion on Verification -- 4.1 Detailed Description of Verification -- 4.2 Impact of Large f on Verification -- 4.3 Implementation and Benchmark of Cost in F_p -Multiplications -- 5 Optimisations for Verification -- 5.1 Basis Generation for Full 2-Power Torsion -- 5.2 General Improvements to Verification -- 5.3 To Push, or Not to Push—that is, the Q . -- 5.4 Improved Challenge for f -- 6 Size-Speed Trade-Offs in SQIsign Signatures -- 6.1 Adding Seeds for the Torsion Basis in the Signature -- 6.2 Uncompressed Signatures -- 7 Primes and Performance -- 7.1 Performance of Optimised Verification -- 7.2 Finding Specific Primes -- 7.3 Performance for Specific Primes -- References -- Symmetric Cryptology -- The Exact Multi-user Security of (Tweakable) Key Alternating Ciphers with a Single Permutation -- 1 Introduction -- 1.1 Research Question -- 1.2 Contributions -- 1.3 Organization -- 2 Basic Notation -- 3 KACs: Specification and Security Definition -- 3.1 KACs with a Single Permutation -- 3.2 Definition of Mu-SPRP Security of KACs -- 4 Mu-Security of KACs with a Single Permutation -- 4.1 r -Wise Independent Subkeys -- 4.2 Mu-SPRP Security Bounds of KACs -- 4.3 Tools for the Mu-SPRP Security Proof.

4.4 Re-Sampling Method for Triple Encryption ch4tdesspsccs2022 -- 4.5 Updating the Re-Sampling Method for Arbitrary Round KACs -- 4.6 Evaluation for Good Transcript -- 5 Proof of Theorem 1 -- 5.1 Notations and Definitions -- 5.2 Definition of Chain -- 5.3 Dummy Internal Values in the Ideal World -- 5.4 Adversary's View -- 5.5 Bad Events and Definitions of Good and Bad Transcripts -- 5.6 Deriving the Upper-Bound in Theorem 1 -- 5.7 Upper-Bounding $\Pr[TI \text{ Tbad}]$ -- 5.8 Lower-Bounding $\Pr[TR=] \Pr[TI=]$ -- 5.9 Proof of Lemma 2 -- 5.10 Proof of Lemma 3 -- 6 The Exact Mu-Security of Tweakable KACs -- 7 Conclusion -- References -- Partial Sums Meet FFT: Improved Attack on 6-Round AES -- 1 Introduction -- 2 Background -- 2.1 Description

of AES -- 2.2 The Square Attack on AES -- 2.3 The Partial Sums Attack -- 2.4 The FFT-Based Attack of Todo and Aoki -- 3 The New Technique: Partial Sums Meet FFT -- 3.1 The Basic Technique -- 3.2 Packing Several FFTs Together by Embedding into Z -- 3.3 Enhancements and Other Variants of the Basic Technique -- 3.4 Our Technique vs. Partial Sums and the Todo-Aoki Technique -- 3.5 Experimental Verification of Our Attack on 6-Round AES -- 4 Improved Attack on Kuznyechik -- 4.1 The Structure of Kuznyechik -- 4.2 The Multiset-Algebraic Attack of Biryukov et al. -- 4.3 Improvement Using Our Technique -- 5 Summary -- References -- New Records in Collision Attacks on SHA-2 -- 1 Introduction -- 2 Preliminaries -- 2.1 Notations -- 2.2 Description of SHA-2 -- 2.3 Previous Methods to Search for Differential Characteristics -- 3 SAT/SMT-Based Tools for the MD-SHA Hash Family -- 3.1 SAT/SMT Models for the Signed Difference Transitions -- 3.2 SAT/SMT Models for the Value Transitions -- 3.3 Models for SHA-2 -- 4 New (SFS/FS) Collision Attacks on SHA-2 -- 4.1 The First Practical SFS Collision for 39-Step SHA-256. 4.2 Improved Collision Attacks on 31-Step SHA-256 -- 4.3 The First Collision Attack on 31-Step SHA-512 -- 4.4 The Practical Collision Attack on 28-Step SHA-512 -- 4.5 The First Practical FS Collision for 40-Step SHA-224 -- 5 Summary and Future Work -- References -- Improving Linear Key Recovery Attacks Using Walsh Spectrum Puncturing -- 1 Introduction -- 2 Preliminaries -- 2.1 Binary Vector Spaces -- 2.2 Pseudoboolean Functions and Their Walsh Spectra -- 2.3 Vectorial Boolean Functions -- 2.4 Linear Approximations -- 2.5 Key Recovery Linear Attack Scenario -- 2.6 Distribution of the Experimental Correlation -- 3 Approximating the Key Recovery Map -- 3.1 Effect on the Data Complexity -- 3.2 Walsh Spectrum Puncturing -- 3.3 Experimental Verification -- 3.4 Relationship to Multiple and Multidimensional Attacks -- 4 Puncturing Walsh Spectra -- 4.1 Some Useful Results -- 4.2 Puncturing Strategies -- 5 Application to Serpent -- 5.1 Improved Key Recovery Attack Against 12-Round Serpent-256 -- 5.2 Improved Key Recovery Attack Against 12-Round Serpent-192 -- 6 Application to GIFT-128 -- 6.1 Application to GIFT-128 in the General Setting -- 6.2 Application to GIFT-128 on the COFB Setting -- 7 Application to the Data Encryption Standard -- 8 Application to Noekeon -- 9 Conclusion -- References -- A Generic Algorithm for Efficient Key Recovery in Differential Attacks - and its Associated Tool -- 1 Introduction -- 2 The Key Recovery Problem in Differential Cryptanalysis -- 2.1 Differential Cryptanalysis -- 2.2 Efficient Key Recovery -- 2.3 Considered Ciphers -- 3 Modeling the Key Recovery Problem -- 3.1 Our Modelization -- 3.2 Sieving of the Pairs Using the Differential Constraints of the S-Boxes -- 3.3 Precomputing Partial Solutions -- 3.4 Computing in Parallel -- 4 Algorithm and Its Associated Tool -- 4.1 High-Level Description of Our Algorithm. 4.2 Taking into Account the Techniques of Section3 -- 4.3 Parameters and Limitations -- 5 Applications -- 5.1 Validity and Experiments -- 5.2 RECTANGLE -- 5.3 PRESENT -- 5.4 GIFT-64 -- 5.5 Application to SPEEDY-7-192 -- 6 Conclusion and Open Problems -- References -- Tight Security of TNT and Beyond -- 1 Introduction -- 1.1 Motivation -- 1.2 Contributions -- 1.3 Impact of Our Birthday-Bound Attack -- 2 Preliminaries -- 2.1 (Tweakable) Block Ciphers and Random Permutations -- 2.2 Security Definition -- 2.3 The Expectation Method -- 3 Birthday-Bound Attack on -- 3.1 Comparing the Number of Collision Pairs in $-\frac{4}{3}0365 \cdot 4, m$ and $, m$ -- 3.2 The Collision Counting Distinguisher -- 3.3 Experimental Verification -- 4 Spotting the Flaw in the BBB Security Proof of -- 5 Birthday-Bound Security of and Its Variant -- 6 The Generalized LRW Paradigm -- 6.1 Security of

LRW+ -- 6.2 Instantiating LRW+ -- 7 Conclusion and Future Directions
-- References -- Improved Differential Meet-in-the-Middle
Cryptanalysis -- 1 Introduction -- 2 Preliminaries: Differential Meet-in-the-Middle -- 2.1 Framework of the Differential MITM Attack -- 2.2 Improvement: Parallel Partitions for Layers with Partial Subkeys -- 2.3 Reducing Data Needed with Imposed Conditions -- 3 Truncated Differential Meet-in-the-Middle Attack -- 3.1 Framework of the Truncated Differential MITM Attack -- 3.2 Attack Complexities -- 4 New Improvements to Differential MITM Attacks -- 4.1 Improving the Parallel Partitioning -- 4.2 Probabilistic Key Recovery Technique -- 4.3 Applying the State-Test Technique -- 5 MILP Modeling of the Truncated Differential-MITM Attack -- 5.1 MILP Model of the Basic Attack -- 5.2 MILP Model of the Improved Attack -- 6 Application on 23-Round CRAFT -- 6.1 An Attack on 23 Rounds of CRAFT -- 6.2 Other Attacks on CRAFT and Conclusion -- 7 Applications: SKINNY-64-192 and SKINNY-128-384.
7.1 Attack on 23-Round SKINNY-64-192.

Sommario/riassunto

The 7-volume set LNCS 14651 - 14657 conference volume constitutes the proceedings of the 43rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2024, held in Zurich, Switzerland, in May 2024. The 105 papers included in these proceedings were carefully reviewed and selected from 500 submissions. They were organized in topical sections as follows: Part I: Awarded papers; symmetric cryptology; public key primitives with advanced functionalities; Part II: Public key primitives with advances functionalities; Part III: AI and blockchain; secure and efficient implementation, cryptographic engineering, and real-world cryptography; theoretical foundations; Part IV: Theoretical foundations; Part V: Multi-party computation and zero-knowledge; Part VI: Multi-party computation and zero-knowledge; classic public key cryptography, Part VII: Classic public key cryptography.
