1. Record Nr. UNINA9910483102703321

Titolo	Selected Areas in Cryptography -- SAC 2014 : 21st International Conference, Montreal, QC, Canada, August 14-15, 2014, Revised Selected Papers / / edited by Antoine Joux, Amr Youssef
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2014
ISBN	3-319-13051-X
Edizione	[1st ed. 2014.]
Descrizione fisica	1 online resource (X, 381 p. 66 illus.)
Collana	Security and Cryptology, , 2946-1863 ; ; 8781
Disciplina	005.82
Soggetti	Cryptography Data encryption (Computer science) Data protection Algorithms Coding theory Information theory Computer science - Mathematics Discrete mathematics Cryptology Data and Information Security Coding and Information Theory Discrete Mathematics in Computer Science
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di contenuto	Intro -- Preface -- Organization -- Contents -- Malicious Hashing: Eve's Variant of SHA-1 -- 1 Introduction -- 2 Malicious Hashing -- 2.1 Malicious Cryptography and Backdoors -- 2.2 Definitions -- 3 Eve's Variant of SHA-1 -- 3.1 Short Description of SHA-1 -- 3.2 Differential Attack Strategy for SHA-1 -- 3.3 Malicious Collision Attack -- 4 Building Meaningful Collisions -- 4.1 Constraints -- 4.2 Binary File Format Overview -- 4.3 Example Files -- A Full Characteristic for Malicious SHA-1 -- References -- Binary Elligator Squared -- 1 Introduction -- 2 Preliminaries -- 2.1 Well-Bounded Encodings -- 2.2

Elligator Squared -- 2.3 Shallue--van de Woestijne in Characteristic 2 -- 2.4 Lambda Affine Coordinates -- 3 Algorithmic Aspects -- 3.1 The Subroutine SWCHAR2 -- 3.2 The Subroutine PREIMAGESSW -- 3.3 Operation Counts -- 4 Implementation Aspects -- 5 Experimental Results -- 6 Comparison of Elligator 2 and Elligator Squared on Prime Finite Fields -- References -- Batch NFS -- 1 Introduction -- 1.1 Contents of this paper. -- 1.2 Security consequences. -- 1.3 Previous work. -- 2 Exponents -- 2.1 QS: the Quadratic sieve (1982). -- 2.2 NFS: the number-field sieve (1993). -- 2.3 RAM cost analysis (1993). -- 2.4 AT cost analysis (2001). -- 2.5 The factorization factory (1993). -- 2.6 Batch NFS (new). -- 2.11 Comparison and numerical parameter optimization. -- 3 Early-abort ECM -- 3.1 Early-abort trial division. -- 3.2 Early aborts in more generality. -- 3.3 Performance of early aborts. -- 3.4 Understanding the heuristics. -- 3.5 Impact of early aborts on smoothness probabilities. -- A ECM -- References -- An Improvement of Linear Cryptanalysis with Addition Operations with Applications to FEAL-8X -- 1 Introduction -- 2 The Cipher FEAL-8X -- 2.1 An Equivalent Description of FEAL-8X -- 3 First Attack -- Finding the Key Using 215 Known Plaintexts.
3.1 The Linear Approximations -- 3.2 The Basic Attack -- 3.3 Matching Subkeys from the Backward and Forward Directions -- 3.4 Retrieving the Rest of the Subkeys -- 4 The Partitioning Technique -- Finding the Key Using 214 Known Plaintexts -- 4.1 A Simplified Example -- 4.2 The Attack -- 5 Attacking FEAL-8X Using 210 Known Plaintexts with Complexity 262 -- 6 Attacks with a Few Known or Chosen Plaintexts -- 6.1 Differential and Linear Exhaustive Search Attacks -- 6.2 Meet in the Middle Attacks -- 7 Summary -- A Efficient Implementation -- B The Linear Approximations Used in Our Attacks -- References -- Colliding Keys for SC2000-256 -- 1 Introduction -- 2 Description of SC2000-256 -- 3 Key Collisions for SC2000-256 -- 3.1 Specifying the Difference for the Second Phase -- 3.2 Finding Pairs in the First Phase -- 4 Results and Applications -- 5 Conclusion -- References -- Faster Binary-Field Multiplication and Faster Binary-Field MACs -- 1 Introduction -- 1.1 Integer-Multiplication Hardware -- 1.2 New Speeds for Binary-Field MACs -- 1.3 New Bit-Operation Records for Binary-Field Multiplication -- 1.4 Polynomial-Multiplication Hardware: PCLMULQDQ -- 2 Field Arithmetic in F28 -- 2.1 Review of Tower Fields -- 2.2 Variable Multiplications -- 2.3 Constant Multiplications -- 2.4 Subfields and Decomposability -- 3 Faster Additive FFTs -- 3.1 Size-4 FFTs: The Lowest Level of Recursion -- 3.2 The Size-8 FFTs: The First Recursive Case -- 3.3 The Size-16 FFTs: Saving Additions for Radix Conversions -- 3.4 Size-16 FFTs Continued: Decomposition at Field-Element Level -- 3.5 Improvements: A Summary -- 3.6 Polynomial Multiplications: A Comparison with Karatsuba and Toom -- 4 The Auth256 Message-Authentication Code: Major Features -- 4.1 Output Size: Bigger-Birthday-Bound Security -- 4.2 Pseudo Dot Products and FFT Addition.
4.3 Embedding Invertible Linear Operations into FFT Inputs -- 5 Software Implementation -- 5.1 Minimizing Memory Operations in Radix Conversions -- 5.2 Minimizing Memory Operations in Muladdadd Operations -- 5.3 Implementing the Size-16 Additive FFT -- 6 Auth256: Minor Details -- 6.1 Review of Wegman--Carter MACs -- 6.2 Field Representation -- 6.3 Hash256 Padding and Conversion -- 6.4 Hash256 and Auth256 Keys and Authenticators -- References -- A Security Proof -- OMD: A Compression Function Mode of Operation for Authenticated Encryption -- 1 Introduction -- 2 Preliminaries -- 3 Definitions and Security Goals -- 4 The OMD Mode of Operation -- 5 Security Analysis -- 5.1 Generalized OMD Using a Tweakable Random

Function -- 5.2 Instantiating Tweakable RFs with PRFs -- 6 Instantiations -- 6.1 OMD-SHA256 -- 6.2 OMD-SHA512 -- 6.3 Instantiating G-OMD with a Native Tweakable PRF -- References -- Security Amplification for the Composition of Block Ciphers: Simpler Proofs and New Results -- 1 Introduction -- 2 Preliminaries -- 2.1 Notation and Definitions -- 2.2 Security Definitions and Classical Lemmas -- 3 A Simple Proof of the ``Two Weak Make One Strong'' Theorem -- 4 Many Weak Make One Even Stronger -- 5 On the Tightness of the Bound -- A Omitted Proofs -- References -- Improved Differential Cryptanalysis of Round-Reduced Speck -- 1 Introduction -- 2 Notations and Conventions -- 3 Description of Speck -- 4 Summary of Previous and New Attacks on Speck -- 5 Auxiliary Algorithms Used by Our Attacks -- 5.1 Key-Schedule Inversion -- 5.2 Overview of the 2-Round Attack on Speck -- 6 Details of the Full Differential Attacks -- 7 The 2-Round Attack -- 7.1 A Basic 2-Round Attack -- 7.2 Optimizing the Basic 2-Round Attack Using Filters -- 7.3 The Optimized 2-Round Attack -- 8 Conclusions -- A Details of the Basic 2-Round Attack -- References.
Differential Cryptanalysis of SipHash -- 1 Introduction -- 2 Description of SipHash -- 3 Automatic Search for Differential Characteristics -- 3.1 Generalized Conditions -- 3.2 Propagation of Conditions -- 3.3 Basic Search Strategy -- 4 Improvements in the Automatic Search for SipHash -- 4.1 Extended Search Strategy -- 4.2 Calculating the Probability Using Cyclic S-Functions -- 4.3 Bitsliced Description of SipHash -- 5 Results -- 5.1 Colliding Characteristics for SipHash-1-x and SipHash-2-x -- 5.2 Characteristic for Finalization of SipHash-2-4 -- 6 Conclusion -- A Results Without Secret Key -- B An Example for Cyclic S-Functions -- References -- Weak Instances of PLWE -- 1 Introduction -- 2 Background -- 2.1 Distances and Distributions -- 2.2 Lattices -- 2.3 Number Fields -- 2.4 Definition of the Ring-LWE Distribution and Problem -- 2.5 Worst-Case Hardness of Search Version of Ring-LWE -- 2.6 Known Attacks -- 3 Overview of Results -- 4 Search to Decision Reduction for the Ring-LWE Problem -- 5 Reduction from R-DLWEq to PLWE -- 5.1 The PLWE Problem -- 5.2 Reduction -- 6 Breaking Certain Instances of PLWE -- 6.1 The Attack -- 6.2 A Family of Examples -- 6.3 Extension of the Attack on PLWE -- 6.4 Security Implications for RLWE and PLWE-based Cryptosystems -- References -- The Usage of Counter Revisited: Second-Preimage Attack on New Russian Standardized Hash Function -- 1 Introduction -- 2 Specifications of Streebog -- 2.1 Domain Extension of Streebog -- 2.2 The Compression Function of Streebog -- 3 Our Observation -- 4 Second-Preimage Attack on Full Streebog with a Diamond -- 4.1 The Diamond Structure -- 4.2 Details of the Attack -- 5 Second-Preimage Attack on Full Streebog with an Expandable Message -- 5.1 The Expandable Message -- 5.2 Details of the Attack -- 6 Open Discussion and Conclusion -- References.
Side-Channel Analysis of Montgomery's Representation Randomization -- 1 Introduction -- 2 On Randomized Implementations of Modular Operations -- 2.1 Background on Elliptic Curves and Montgomery Multiplication -- 2.2 Randomized Montgomery Domain -- 3 Our Attack -- 3.1 Core Idea -- 3.2 Attack Description -- 4 Simulations -- 5 Analysis and Conclusion -- A Examples of Algorithms for Elliptic Curve Scalar Multiplication -- References -- Practical Cryptanalysis of PAES -- 1 Introduction -- 2 Description of PAES -- 3 Practical Universal Forgery Attack Against PAES-8 -- 3.1 Differential Trail and Detection of Difference Cancellation -- 3.2 Recovery of State Words -- 3.3 The Attack -- 4 Practical Distinguisher for a Weak-Key Class of PAES -- 4.1 Symmetric Properties of the AES Round Function -- 4.2 Symmetric Properties of the PAES Transformations -- 4.3 The Distinguisher -- 5

Conclusion -- References -- Diffusion Matrices from Algebraic-Geometry Codes with Efficient SIMD Implementation -- 1 Introduction -- 2 Preliminaries -- 3 Efficient Algorithms for Matrix-Vector Multiplication -- 3.1 Table Implementation -- 3.2 A Generic Constant-Time Algorithm -- 3.3 A Faster Algorithm Exploiting Matrix Structure -- 3.4 Performance -- 4 Diffusion Matrices from Algebraic-Geometry Codes -- 4.1 A Short Introduction to Algebraic-Geometry Codes -- 4.2 Compact Encoders Using Code Automorphisms -- 4.3 Fast Random Encoders -- 5 Applications and Performance -- 6 Conclusion -- References -- Error-Tolerant Side-Channel Cube Attack Revisited -- 1 Introduction -- 2 Preliminaries -- 2.1 Cube Attack -- 2.2 Error-Tolerant Side-Channel Cube Attack(ET-SCCA) -- 3 A New ET-SCCA with Higher Error-Tolerant Rate -- 3.1 Polynomial Approximation -- 3.2 A New Variant of Cube Attack -- 4 Error Probability Evaluation -- 5 Simulations on PRESENT -- 5.1 Off-Line Phase.
5.2 Polynomial Approximation for PRESENT-80.

Sommario/riassunto

This book constitutes the proceedings of the 21st International Conference on Selected Areas in Cryptography, SAC 2014, held in Montreal, QC, Canada, in August 2014. The 22 papers presented in this volume were carefully reviewed and selected from 103 submissions. There are four areas covered at each SAC conference. The three permanent areas are: design and analysis of symmetric key primitives and cryptosystems, including block and stream ciphers, hash function, MAC algorithms, cryptographic permutations, and authenticated encryption schemes; efficient implementations of symmetric and public key algorithms; mathematical and algorithmic aspects of applied cryptology. This year, the fourth area for SAC 2014 is: algorithms for cryptography, cryptanalysis and their complexity analysis.