1. Record Nr. UNINA9910484544903321

Titolo	Advances in Cryptology – EUROCRYPT 2015 : 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part I / / edited by Elisabeth Oswald, Marc Fischlin
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2015
ISBN	3-662-46800-X
Edizione	[1st ed. 2015.]
Descrizione fisica	1 online resource (XVII, 818 p. 123 illus.)
Collana	Security and Cryptology ; ; 9056
Disciplina	004
Soggetti	Data encryption (Computer science) Algorithms Computer security Management information systems Computer science Cryptology Algorithm Analysis and Problem Complexity Systems and Data Security Management of Computing and Information Systems
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di contenuto	Cryptanalysis of the Multilinear Map over the Integers -- Robust Authenticated-Encryption AEZ and the Problem That It Solves -- On the Behaviors of Affine Equivalent Sboxes Regarding Differential and Linear Attacks -- A Provable-Security Analysis of Intel’s Secure Key RNG -- A Formal Treatment of Backdoored Pseudorandom Generators -- Improving NFS for the Discrete Logarithm Problem in Non-prime Finite Fields -- The Multiple Number Field Sieve with Conjugation and Generalized -- Better Algorithms for LWE and LWR -- On Computing Nearest Neighbors with Applications to Decoding of Binary Linear Codes -- Cryptanalytic Time-Memory-Data Tradeoffs for FX-Constructions with Applications to PRINCE and PRIDE -- A Generic Approach to Invariant Subspace Attacks: Cryptanalysis of Robin,

iSCREAM and Zorro -- Structural Evaluation by Generalized Integral Property -- Cryptanalysis of SP Networks with Partial Non-Linear Layers -- The Sum Can Be Weaker Than Each Part -- SPHINCS: Practical Stateless Hash-Based Signatures -- Making Masking Security Proofs Concrete: Or How to Evaluate the Security of Any Leaking Device -- Ciphers for MPC and FHE -- Verified Proofs of Higher-Order Masking -- Inner Product Masking Revisited -- Fully Homomophic Encryption over the Integers Revisited -- (Batch) Fully Homomorphic Encryption over Integers for Non-Binary Message Spaces -- KDM-CCA Security from RKA Secure Authenticated Encryption -- On the Provable Security of the Iterated Even-Mansour Cipher Against Related-Key and Chosen-Key Attacks -- FHEW: Bootstrapping Homomorphic Encryption in Less Than a Second -- Bootstrapping for HElib -- More Efficient Oblivious Transfer Extensions with Security for Malicious Adversaries -- How to Efficiently Evaluate RAM Programs with Malicious Security -- Cube Attacks and Cube-Attack-Like Cryptanalysis on the Round-Reduced Keccak Sponge Function -- Twisted Polynomials and Forgery Attacks on GCM -- Quadratic Time, Linear Space Algorithms for Gram-Schmidt Orthogonalization and Gaussian Sampling in Structured Lattices.

Sommario/riassunto

The two-volume proceedings LNCS 9056 + 9057 constitutes the proceedings of the 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2015, held in Sofia, Bulgaria, in April 2015. The 57 full papers included in these volumes were carefully reviewed and selected from 194 submissions. The papers are organized in topical sections named: honorable mentions, random number generators, number field sieve, algorithmic cryptanalysis, symmetric cryptanalysis, hash functions, evaluation implementation, masking, fully homomorphic encryption, related-key attacks, fully monomorphic encryption, efficient two-party protocols, symmetric cryptanalysis, lattices, signatures, zero-knowledge proofs, leakage-resilient cryptography, garbled circuits, crypto currencies, secret sharing, outsourcing computations, obfuscation and e-voting, multi-party computations, encryption, resistant protocols, key exchange, quantum cryptography, and discrete logarithms.