1. Record Nr. UNISA996466297403316

Titolo	Advances in Cryptology -- ASIACRYPT 2012 [[electronic resource]] : 18th International Conference on the Theory and Application of Cryptology and Information Security, Beijing, China, December 2-6, 2012, Proceedings / / edited by Xiaoyun Wang, Kazue Sako
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2012
ISBN	3-642-34961-7
Edizione	[1st ed. 2012.]
Descrizione fisica	1 online resource (XVI, 780 p. 64 illus.)
Collana	Security and Cryptology ; ; 7658
Disciplina	005.8/2
Soggetti	Data encryption (Computer science) Algorithms Management information systems Computer science Computer science—Mathematics Computer security Applied mathematics Engineering mathematics Cryptology Algorithm Analysis and Problem Complexity Management of Computing and Information Systems Discrete Mathematics in Computer Science Systems and Data Security Applications of Mathematics Conference proceedings.
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Pairing-Based Cryptography -- Past, Present, and Future -- Some Mathematical Mysteries in Lattices -- Constant-Size Structure-Preserving Signatures: Generic Constructions and Simple Assumptions -- Dual Form Signatures: An Approach for Proving Security from Static Assumptions -- Breaking Pairing-Based Cryptosystems Using T

Pairing over GF(397) -- On the (Im)possibility of Projecting Property in Prime-Order Setting -- Optimal Reductions of Some Decisional Problems to the Rank Problem -- Signature Schemes Secure against Hard-to-Invert Leakage -- Completeness for Symmetric Two-Party Functionalities - Revisited -- Adaptively Secure Garbling with Applications to One-Time Programs and Secure Outsourcing -- The Generalized Randomized Iterate and Its Application to New Efficient Constructions of UOWHFs from Regular One-Way Functions -- Symmetric Cipher Perfect Algebraic Immune Functions -- Differential Analysis of the LED Block Cipher -- PRINCE – A Low-Latency Block Cipher for Pervasive Computing Applications: Extended Abstract -- Analysis of Differential Attacks in ARX Constructions -- Integral and Multidimensional Linear Distinguishers with Correlation Zero -- Differential Attacks against Stream Cipher ZUC -- An Asymptotically Tight Security Analysis of the Iterated Even-Mansour Cipher -- 3kf9: Enhancing 3GPP-MAC beyond the Birthday Bound -- Understanding Adaptivity: Random Systems Revisited -- RKA Security beyond the Linear Barrier: IBE, Encryption and Signatures -- Fully Secure Unbounded Inner-Product and Attribute-Based Encryption -- Computing on Authenticated Data: New Privacy Definitions and Constructions -- A Coding-Theoretic Approach to Recovering Noisy RSA Keys -- Certifying RSA -- Lattice-Based Cryptography and Number Theory Faster Gaussian Lattice Sampling Using Lazy Floating-Point Arithmetic -- Learning a Zonotope and More: Cryptanalysis of NTRUSign Countermeasures -- On Polynomial Systems Arising from a Weil Descent -- ECM at Work -- IND-CCA Secure Cryptography Based on a Variant of the LPN Problem -- Provable Security of the Knudsen-Preneel Compression Functions -- Optimal Collision Security in Double Block Length Hashing with Single Length Key -- Bicliques for Permutations: Collision and Preimage Attacks in Stronger Settings -- Investigating Fundamental Security Requirements on Whirlpool: Improved Preimage and Collision Attacks -- Generic Related-Key Attacks for HMAC -- The Five-Card Trick Can Be Done with Four Cards -- A Mix-Net from Any CCA2 Secure Cryptosystem -- How Not to Prove Yourself: Pitfalls of the Fiat-Shamir Heuristic and Applications to Helios -- Sequential Aggregate Signatureswith Lazy Verification from Trapdoor Permutations (Extended Abstract) -- Commitments and Efficient Zero-Knowledge Proofs from Learning Parity with Noise -- Calling Out Cheaters: Covert Security with Public Verifiability -- A Unified Framework for UC from Only OT -- Four-Dimensional Gallant-Lambert-Vanstone Scalar Multiplication -- Shuffling against Side-Channel Attacks: A Comprehensive Study with Cautionary Note -- Theory and Practice of a Leakage Resilient Masking Scheme.

Sommario/riassunto

This book constitutes the refereed proceedings of the 18th International Conference on the Theory and Application of Cryptology and Information Security, Asiacrypt 2012, held in Beijing, China, in December 2012. The 43 full papers presented were carefully reviewed and selected from 241 submissions. They are organized in topical sections named: public-key cryptography, foundation, symmetric cipher, security proof, lattice-based cryptography and number theory, hash function, cryptographic protocol, and implementation issues.