1. Record Nr. UNISA996466361603316

Titolo	Advances in Cryptology - ASIACRYPT 2004 [[electronic resource]] : 10th International Conference on the Theory and Application of Cryptology and Information Security, Jeju Island, Korea, December 5-9, 2004, Proceedings / / edited by Pil Joong Lee
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2004
ISBN	3-540-30539-4
Edizione	[1st ed. 2004.]
Descrizione fisica	1 online resource (XVI, 548 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 3329
Disciplina	005.8/2
Soggetti	Coding theory Information theory Data encryption (Computer science) Operating systems (Computers) Algorithms Management information systems Computer science Computer communication systems Coding and Information Theory Cryptology Operating Systems Algorithm Analysis and Problem Complexity Management of Computing and Information Systems Computer Communication Networks
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Block Ciphers -- On Feistel Ciphers Using Optimal Diffusion Mappings Across Multiple Rounds -- Efficient Instantiations of Tweakable Blockciphers and Refinements to Modes OCB and PMAC -- Eliminating Random Permutation Oracles in the Even-Mansour Cipher -- Public Key Encryption -- Towards Plaintext-Aware Public-Key Encryption Without Random Oracles -- OAEP 3-Round:A Generic and Secure Asymmetric

Encryption Padding -- Invited Talk I -- Stream Ciphers: Dead or Alive? -- Number Theory and Algebra -- On the Generalized Linear Equivalence of Functions Over Finite Fields -- Sieving Using Bucket Sort -- Right-Invariance: A Property for Probabilistic Analysis of Cryptography Based on Infinite Groups -- Secure Computation -- Practical Two-Party Computation Based on the Conditional Gate -- Privacy in Non-private Environments -- Asynchronous Proactive Cryptosystems Without Agreement -- Lattice-Based Threshold-Changeability for Standard Shamir Secret-Sharing Schemes -- Hash Functions -- Masking Based Domain Extenders for UOWHFs: Bounds and Constructions -- Higher Order Universal One-Way Hash Functions -- The MD2 Hash Function Is Not One-Way -- Key Management -- New Approaches to Password Authenticated Key Exchange Based on RSA -- Constant-Round Authenticated Group Key Exchange for Dynamic Groups -- A Public-Key Black-Box Traitor Tracing Scheme with Sublinear Ciphertext Size Against Self-Defensive Pirates -- Identification -- Batching Schnorr Identification Scheme with Applications to Privacy-Preserving Authorization and Low-Bandwidth Communication Devices -- Secret Handshakes from CA-Oblivious Encryption -- k-Times Anonymous Authentication (Extended Abstract) -- XL-Algorithms -- The XL-Algorithm and a Conjecture from Commutative Algebra -- Comparison Between XL and Gröbner Basis Algorithms -- Digital Signatures -- Generic Homomorphic Undeniable Signatures -- Efficient and Provably Secure Trapdoor-Free Group Signature Schemes from Bilinear Pairings -- Public Key Cryptanalysis -- On the Security of MOR Public Key Cryptosystem -- Cryptanalyzing the Polynomial-Reconstruction Based Public-Key System Under Optimal Parameter Choice -- Colluding Attacks to a Payment Protocol and Two Signature Exchange Schemes -- Invited Talk II -- Information Security in Korea IT839 Strategy -- Symmetric Key Cryptanalysis -- How Far Can We Go Beyond Linear Cryptanalysis? -- The Davies-Murphy Power Attack -- Time-Memory Trade-Off Attacks on Multiplications and T-Functions -- Cryptanalysis of Bluetooth Keystream Generator Two-Level E0 -- Protocols -- On Provably Secure Time-Stamping Schemes -- Strong Conditional Oblivious Transfer and Computing on Intervals -- Improved Setup Assumptions for 3-Round Resettable Zero Knowledge.

Sommario/riassunto

The 10th Annual ASIACRYPT 2004 was held in Jeju Island, Korea, d- ing December 5–9, 2004. This conference was organized by the International Association for Cryptologic Research (IACR) in cooperation with KIISC (- rean Institute of Information Security and Cryptology) and IRIS (International Research center for Information Security) at ICU (Information and Communi- tionsUniversity),andwas? nanciallysupportedbyMIC(MinistryofInformation and Communication) in Korea. The conference received, from 30 countries, 208 submissions that represent the current state of work in the cryptographic community worldwide, covering all areas of cryptologic research. Each paper, without the authors' information, was reviewed by at least three members of the program committee, and the papers (co-)authored by members of the program committee were reviewed by at least six members. We also blinded the reviewers' names among the reviewers until the ?nal decision, by using pseudonyms. The reviews were then followed by deep discussions on the papers, which greatly contributed to the quality of the ?nal selection. In most cases, extensive comments were sent to the authors. Among 208 submissions, the program committee selected 36 papers. Two submissions were merged into a single paper, yielding the total of 35 papers acceptedforpresentationinthetechnicalprogramoftheconference.

Manyhi- quality works could not be accepted because of the competitive nature of the conference and the challenging task of selecting a program. These proceedings contain revised versions of the accepted papers. These revisions have not been checked for correctness, and the authors bear full responsibility for the contents of their papers.