1. Record Nr. UNINA9910483440203321

Titolo	Public Key Cryptography - PKC 2006 [[electronic resource]] : 9th International Conference on Theory and Practice in Public-Key Cryptography, New York, NY, USA, April 24-26, 2006. Proceedings / / edited by Moti Yung, Yevgeniy Dodis, Aggelos Kiayias, Tal Malkin
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2006
ISBN	3-540-33852-7
Edizione	[1st ed. 2006.]
Descrizione fisica	1 online resource (XIV, 543 p.)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 3958
Disciplina	005.82
Soggetti	Cryptography Data encryption (Computer science) Algorithms Computer networks Computers and civilization Electronic data processing—Management Cryptology Computer Communication Networks Computers and Society IT Operations
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	Cryptanalysis and Protocol Weaknesses -- New Attacks on RSA with Small Secret CRT-Exponents -- An Attack on a Modified Niederreiter Encryption Scheme -- Cryptanalysis of an Efficient Proof of Knowledge of Discrete Logarithm -- Distributed Crypto-computing -- Efficient Polynomial Operations in the Shared-Coefficients Setting -- Generic On-Line/Off-Line Threshold Signatures -- Linear Integer Secret Sharing and Distributed Exponentiation -- Encryption Methods -- Encoding-Free ElGamal Encryption Without Random Oracles -- Parallel Key-Insulated Public Key Encryption -- Provably Secure Steganography with Imperfect Sampling -- Cryptographic Hash and Applications -- Collision-Resistant No More: Hash-and-Sign Paradigm Revisited --

Higher Order Universal One-Way Hash Functions from the Subset Sum Assumption -- Number Theory Algorithms -- An Algorithm to Solve the Discrete Logarithm Problem with the Number Field Sieve -- Efficient Scalar Multiplication by Isogeny Decompositions -- Curve25519: New Diffie-Hellman Speed Records -- Pairing-Based Cryptography -- Strongly Unforgeable Signatures Based on Computational Diffie-Hellman -- Generalization of the Selective-ID Security Model for HIBE Protocols -- Identity-Based Aggregate Signatures -- On the Limitations of the Spread of an IBE-to-PKE Transformation -- Cryptosystems Design and Analysis -- Inoculating Multivariate Schemes Against Differential Attacks -- Random Subgroups of Braid Groups: An Approach to Cryptanalysis of a Braid Group Based Cryptographic Protocol -- High-Order Attacks Against the Exponent Splitting Protection -- Signature and Identification -- New Online/Offline Signature Schemes Without Random Oracles -- Anonymous Signature Schemes -- The Power of Identification Schemes -- Authentication and Key Establishment -- Security Analysis of KEA Authenticated Key Exchange Protocol -- SAS-Based Authenticated Key Agreement -- The Twist-AUgmented Technique for Key Exchange -- Password-Based Group Key Exchange in a Constant Number of Rounds -- Multi-party Computation -- Conditional Oblivious Cast -- Efficiency Tradeoffs for Malicious Two-Party Computation -- PKI Techniques -- On Constructing Certificateless Cryptosystems from Identity Based Encryption -- Building Better Signcryption Schemes with Tag-KEMs -- Security-Mediated Certificateless Cryptography -- k-Times Anonymous Authentication with a Constant Proving Cost.

Sommario/riassunto

The 9th International Conference on Theory and Practice of Public-Key Cr- tography(PKC 2006) took place in New York City. PKC is the premier inter- tional conference dedicated to cryptology focusing on all aspects of public-key cryptography. The event is sponsored by the International Association of Cr- tologic Research (IACR), and this year it was also sponsored by the Columbia University Computer Science Department as well as a number of sponsors from industry, among them: EADS and Morgan Stanley, which were golden sponsors, as well as Gemplus, NTT DoCoMo, Google, Microsoft and RSA Security, which were silver sponsors. We acknowledge the generous support of our industrial sponsors; their support was a major contributing factor to the success of this year’s PKC. PKC 2006 followed a series of very successful conferences that started in 1998in Yokohama,Japan.Further meetingswereheld successivelyinKamakura (Japan), Melbourne (Australia), Jeju Island (Korea), Paris (France), Miami (USA), Singapore and Les Diablerets (Switzerland). The conference became an IACR sponsored event (o?cially designated as an IACR workshop) in 2003 and has been sponsored by IACR continuously since then. The year 2006 found us all in New York City where the undertone of the conference was hummed in the relentless rhythm of the city that never sleeps.