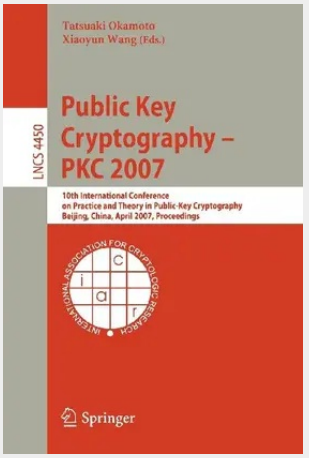
Okamoto / Wang

Public Key Cryptography - PKC 2007

10th International Conference on Practice and Theory in Public-Key Cryptography, Beijing, China, April 16-20, 2007, Proceedings

This book constitutes the refereed proceedings of the 10th International Conference on Practice and Theory in Public-Key Cryptography, PKC 2007, held in Beijing, China in April 2007. The 29 revised full papers presented together with two invited lectures are organized in topical sections on signatures, cryptanalysis, protocols, multivariate cryptosystems, encryption, number theoretic techniques, and public-key infrastructure.

Signatures I.- Full-Domain Subgroup Hiding and Constant-Size Group Signatures.- A Direct Anonymous Attestation Scheme for Embedded Devices.- Anonymous Signatures Made Easy.- On the Generic and Efficient Constructions of Secure Designated Confirmer Signatures.- Invited Talk I.- Cryptanalysis of Group-Based Key Agreement Protocols Using Subgroup Distance Functions.- Cryptanalysis.- Length Based Attack and Braid Groups: Cryptanalysis of Anshel-Anshel-Goldfeld Key Exchange Protocol.- New Chosen-Ciphertext Attacks on NTRU.- Cryptanalysis of the Paeng-Jung-Ha Cryptosystem from PKC 2003.- Protocols I.- Optimistic Fair Exchange in a Multi-user Setting.- Multi-party Stand-Alone and Setup-Free Verifiably Committed Signatures.- Knowledge-Binding Commitments with Applications in Time-Stamping.- Signatures II.- Efficient Ring Signatures Without Random Oracles.- Traceable Ring Signature.- Two-Tier Signatures, Strongly Unforgeable Signatures, and Fiat-Shamir Without Random Oracles.- Improved On-Line/Off-Line Threshold Signatures.- Multivariate Cryptosystems.- High Order Linearization Equation (HOLE) Attack on Multivariate Public Key Cryptosystems.- Cryptanalysis of HFE with Internal Perturbation.- ?-Invertible Cycles for ultivariate uadratic ( ) Public Key Cryptography.- Encryption.- Chosen-Ciphertext Secure Key-Encapsulation Based on Gap Hashed Diffie-Hellman.- Parallel Key-Insulated Public Key Encryption Without Random Oracles.- Multi-bit Cryptosystems Based on Lattice Problems.- Protocols II.- Practical and Secure Solutions for Integer Comparison.- Multiparty Computation for Interval, Equality, and Comparison Without Bit-Decomposition Protocol.- Identity-Based Traitor Tracing.- Verifiable Shuffle of Large Size Ciphertexts.- Invited Talk II.- A Survey of Single-DatabasePrivate Information Retrieval: Techniques and Applications.- Number Theoretic Techniques.- Deterministic Polynomial Time Equivalence Between Factoring and Key-Recovery Attack on Takagi's RSA.- Efficient Pseudorandom Generators Based on the DDH Assumption.- Fast Batch Verification of Multiple Signatures.- Public-Key Infrastructure.- A Closer Look at PKI: Security and Efficiency.- Self-Generated-Certificate Public Key Encryption Without Pairing.



53,49 €
49,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9783540716761
Medium: Buch
ISBN: 978-3-540-71676-1
Verlag: Springer
Erscheinungstermin: 30.03.2007
Sprache(n): Englisch
Auflage: Erscheinungsjahr 2007
Serie: Lecture Notes in Computer Science
Produktform: Kartoniert
Gewicht: 1570 g
Seiten: 498
Format (B x H): 155 x 235 mm