1. Record Nr. UNINA9910483148603321

Titolo	Public Key Cryptography - PKC 2005 : 8th International Workshop on Theory and Practice in Public Key Cryptography / / edited by Serge Vaudenay
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2005
ISBN	3-540-30580-7
Edizione	[1st ed. 2005.]
Descrizione fisica	1 online resource (XIV, 436 p.)
Collana	Security and Cryptology, , 2946-1863 ; ; 3386
Altri autori (Persone)	VaudenaySerge
Disciplina	005.8
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 -- A New Related Message Attack on RSA -- Breaking a Cryptographic Protocol with Pseudoprimes -- Experimenting with Faults, Lattices and the DSA -- Key Establishment -- Securing RSA-KEM via the AES -- One-Time Verifier-Based Encrypted Key Exchange -- Password-Based Authenticated Key Exchange in the Three-Party Setting -- Optimization -- On the Optimization of Side-Channel Attacks by Advanced Stochastic Methods -- Symmetric Subgroup Membership Problems -- Building Blocks -- Optimizing Robustness While Generating Shared Secret Safe Primes -- Fast Multi-computations with Integer Similarity Strategy -- Efficient Proofs of Knowledge of Discrete Logarithms and Representations in Groups with Hidden Order -- Efficient k-Out-of-n Oblivious Transfer Schemes with Adaptive and

Non-adaptive Queries -- RSA Cryptography -- Converse Results to the Wiener Attack on RSA -- RSA with Balanced Short Exponents and Its Application to Entity Authentication -- The Sampling Twice Technique for the RSA-Based Cryptosystems with Anonymity -- From Fixed-Length to Arbitrary-Length RSA Encoding Schemes Revisited -- Multivariate Asymmetric Cryptography -- Tractable Rational Map Signature -- Cryptanalysis of the Tractable Rational Map Cryptosystem -- Large Superfluous Keys in ultivariate uadratic Asymmetric Systems -- Cryptanalysis of HFEv and Internal Perturbation of HFE -- Signature Schemes -- A Generic Scheme Based on Trapdoor One-Way Permutations with Signatures as Short as Possible -- Cramer-Damgård Signatures Revisited: Efficient Flat-Tree Signatures Based on Factoring -- The Security of the FDH Variant of Chaum's Undeniable Signature Scheme -- Efficient Threshold RSA Signatures with General Moduli and No Extra Assumptions -- Identity-Based Cryptography -- Improved Identity-Based Signcryption -- EfficientMulti-receiver Identity-Based Encryption and Its Application to Broadcast Encryption -- CBE from CL-PKE: A Generic Construction and Efficient Schemes -- Best Paper Award -- A Verifiable Random Function with Short Proofs and Keys.

Sommario/riassunto

The 2005 issue of the International Workshop on Practice and Theory in Public Key Cryptography (PKC 2005) was held in Les Diablerets, Switzerland during January 23-26, 2005. It followed a series of successful PKC workshops which started in 1998 in Paci'co Yokohama, Japan. Previous workshops were succ- sively held in Kamakura (Japan), Melbourne (Australia), Cheju Island (South Korea),Paris(France),Miami (USA), andSingapore.Since 2003,PKChasbeen sponsoredbytheInternationalAssociationforCryptologicResearch(IACR). As in previous years, PKC 2005 was one of the major meeting points of worldwide research experts in public-key cryptography. I had the honor to co-chair the workshop together with Jean Monnerat and to head the program committee. Inspired by the fact that the RSA cryptosystem was invented on ski lifts, we decided that the best place for PKC was at a ski resort. Jean Monnerat and I hope that this workshop in a relaxed atmosphere will lead us to 25 more years of research fun. PKC 2005 collected 126 submissions on August 26, 2004. This is a record number. The program committee carried out a thorough review process. In - tal, 413 review reports were written by renowned experts, program committee members as well as external referees. Online discussions led to 313 additional discussionmessagesand 238emails. The reviewprocesswasrun using email and the Webreview software by Wim Moreau and Joris Claessens. Every submitted paperreceivedatleast3reviewreports. Weselected28papersforpublicationon October 28, 2004. Authors were then given a chance to revise their submission over the following two weeks. This proceedings includes all the revised papers.