1. Record Nr. UNINA9910785814603321

Titolo	Public-key cryptography and computational number theory [[electronic resource]] : proceedings of the international conference organized by the Stefan Banach International Mathematical Center, Warsaw, Poland, September 11-15, 2000 / / editors, Kazimierz Alster, Jerzy Urbanowicz, Hugh C. Williams
Pubbl/distr/stampa	Berlin ; ; New York, : Walter de Gruyter, c2001
ISBN	3-11-088103-9
Edizione	[Reprint 2011]
Descrizione fisica	xii, 331 p
Collana	De Gruyter Proceedings in Mathematics
Classificazione	SD 2000
Altri autori (Persone)	AlsterKazimierz UrbanowiczJerzy <1951-> WilliamsHugh C
Disciplina	003/.54
Soggetti	Coding theory Public key cryptography
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.
Nota di contenuto	Front matter -- Preface -- Mathematics, cryptology, and technology / Odlyzko, Andrew -- Table of contents -- A survey on IQ cryptography / Buchmann, Johannes / Hamdy, Safuat -- Algebraic groups and discrete logarithm / Couveignes, Jean-Marc -- Fermat numbers, Wieferich and Wilson primes: computations and generalizations / Dilcher, Karl / Enge, Andreas -- How to distinguish hyperelliptic curves in even characteristic / Enge, Andreas -- Limitations of constructive Weil descent / Galbraith, Steven D. -- On the security of a public-key cryptosystem / Grošek, Otokar / Magliveras, Spyros S. / Wei, Wandi -- Optimizations for NTRU / Hoffstein, Jeffrey / Silverman, Joseph -- The efficiency and security of a real quadratic field based key exchange protocol / Jacobson, Michael J. / Scheidler, Renate / Williams, Hugh C. -- Extending the binary gcd algorithms / Kubiak, Przemysaw -- Stochastic kleptography detection / Kucner, Daniel / Kutylowski, Miroslaw -- An overview of the XTR public key system / Lenstra, Arjen K. / Verheul, Eric R. -- A survey of IND-CCA secure public-key encryption schemes relative to factoring / Müller, Siguna -- Efficient point multiplication for elliptic curves over special optimal extension

fields / Müller, Volker -- Error-correcting codes and cryptography / Niederreiter, Harald -- Secret public key schemes / Patarin, Jacques -- Index form surfaces and construction of elliptic curves over large finite fields / Peth, Attila -- On the size of solutions of the inequality (ax + b) < (ax) / Riele, Herman te -- Security of DL-encryption and signatures against generic attacks-a survey / Schnorr, Claus Peter -- Square-root algorithms for the discrete logarithm problem (a survey) / Teske, Edlyn -- Height functions on elliptic curves / Zimmer, Horst G. -- List of participants -- List of contributors

Sommario/riassunto

The Proceedings contain twenty selected, refereed contributions arising from the International Conference on Public-Key Cryptography and Computational Number Theory held in Warsaw, Poland, on September 11-15, 2000. The conference, attended by eightyfive mathematicians from eleven countries, was organized by the Stefan Banach International Mathematical Center. This volume contains articles from leading experts in the world on cryptography and computational number theory, providing an account of the state of research in a wide variety of topics related to the conference theme. It is dedicated to the memory of the Polish mathematicians Marian Rejewski (1905-1980), Jerzy Róøycki (1909-1942) and Henryk Zygalski (1907-1978), who deciphered the military version of the famous Enigma in December 1932 - January 1933. A noteworthy feature of the volume is a foreword written by Andrew Odlyzko on the progress in cryptography from Enigma time until now.