Advances in Cryptology - ASIACRYPT99 : International Conference on the Theory and Application of Cryptology and Information Security, Singapore, November 14-18, 1999. Proceedings /

Lam, Kwok-Yan
Okamoto, Eiji
Xing, Chaoping

Springer-Verlag Berlin Heidelberg,
1999

Monografía

This book constitutes the refereed proceedings of the 5th International Conference on the Theory and Application of Cryptology and Information Security, ASIACRYPT'99, held in Singapore in November 1999. The 31 revised full papers presented together with one invited paper were carefully reviewed and selected from a total of 96 submissions. The book is divided in topical sections on assymetric key cryptosystems, cryptanalysis, elliptic curve cryptosystems, public key cryptosystems, integers and computation, network security, random numbers, key management, and authentication

Título: Advances in Cryptology - ASIACRYPT99 International Conference on the Theory and Application of Cryptology and Information Security, Singapore, November 14-18, 1999. Proceedings edited by Kwok-Yan Lam, Eiji Okamoto, Chaoping Xing

Editorial: Berlin Heidelberg Springer-Verlag Berlin Heidelberg 1999

Descripción física: 1 online resource

Mención de serie: Lecture Notes in Computer Science 1716 0302-9743

Documento fuente: Springer Nature eBook

Bibliografía: With index

Contenido: Invited Talk -- Modulus Search for Elliptic Curve Cryptosystems -- Asymmetric Key Cryptosystems -- On the Lai-Massey Scheme -- On Cryptographically Secure Vectorial Boolean Functions -- Analysis -- Equivalent Keys of HPC -- Cryptanalysis of Five Rounds of CRYPTON Using Impossible Differentials -- Cryptanalysis of Two Cryptosystems Based on Group Actions -- Probabilistic Higher Order Differential Attack and Higher Order Bent Functions -- Elliptic Curve Cryptosystems -- Fast Algorithms for Elliptic Curve Cryptosystems over Binary Finite Field -- Optimizing the Menezes-Okamoto-Vanstone (MOV) Algorithm for Non-supersingular Elliptic Curves -- Speeding up the Discrete Log Computation on Curves with Automorphisms -- ECC: Do We Need to Count? -- Elliptic Scalar Multiplication Using Point Halving -- Public Key Cryptosystems -- On the Design of RSA with Short Secret Exponent -- Efficient Public-Key Cryptosystems Provably Secure Against Active Adversaries -- Adaptively-Secure Optimal-Resilience Proactive RSA -- Integers and Computation -- Factorization of RSA-140 Using the Number Field Sieve -- How to Prove That a Committed Number Is Prime -- Reducing Logarithms in Totally Non-maximal Imaginary Quadratic Orders to Logarithms in Finite Fields -- General Adversaries in Unconditional Multi-party Computation -- Network Security -- Approximation Hardness and Secure Communication in Broadcast Channels -- Mix-Networks on Permutation Networks -- Secure Communication in an Unknown Network Using Certificates -- Random Number -- Linear Complexity versus Pseudorandomness: On Beth and Dai's Result -- A Class of Explicit Perfect Multi-sequences -- Cryptanalysis of LFSR-Encrypted Codes with Unknown Combining Function -- Key Management -- Doing More with Fewer Bits -- A Quick Group Key Distribution Scheme with "Entity Revocation" -- An Efficient Hierarchical Identity-Based Key-Sharing Method Resistant against Collusion-Attacks -- Periodical Multi-secret Threshold Cryptosystems -- Authentication -- A Signature Scheme with Message Recovery as Secure as Discrete Logarithm -- A 3-Codes under Collusion Attacks -- Broadcast Authentication in Group Communication

Lengua: English

ISBN: 9783540480006 electronic bk.) 3540480005 electronic bk.) 3540666664 9783540666660 9788354048008 6) 8354048004

Materia: Computer science Computer Communication Networks Operating systems (Computers) Data encryption (Computer science) Computer software Computational complexity Computer science- Mathematics Data Encryption Operating Systems Algorithm Analysis and Problem Complexity Computational Mathematics and Numerical Analysis Discrete Mathematics in Computer Science Electronic data processing Computer programs Informatique Systèmes d'exploitation (Ordinateurs) Chiffrement (Informatique) Logiciels Complexité de calcul (Informatique) Informatique- Mathématiques computer science. data processing. operating systems. Software Computational complexity. Computer science. Computer science- Mathematics. Computer software. Data encryption (Computer science) Operating systems (Computers)

Autores: Lam, Kwok-Yan Okamoto, Eiji Xing, Chaoping

Enlace a formato físico adicional: Advances in cryptology, ASIACRYPT'99 (NL-LeOCL)188203648 (OCoLC) 898995503

Punto acceso adicional serie-Título: Lecture notes in computer science 1716 0302-9743 (OCoLC)818889120

Baratz Innovación Documental

- Gran Vía, 59 28013 Madrid
- (+34) 91 456 03 60
- informa@baratz.es