1. Record Nr. UNISA996465822703316

Titolo	Advances in cryptology - EUROCRYPT '88 : workshop on the theory and application of cryptographic techniques Davos, Switzerland, May 25-27, 1988 proceedings / / edited by D. Barstow [and ten others]
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer-Verlag, , [1988] ©1988
ISBN	1-280-80454-8 9786610804542 3-540-45961-8
Edizione	[1st ed. 1988.]
Descrizione fisica	1 online resource (441 p.)
Collana	Lecture Notes in Computer Science ; ; 330
Disciplina	004
Soggetti	Computer science Data encryption (Computer science) Electronic data processing
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Key Distribution -- Key Agreements Based on Function Composition -- Security of Improved Identity-based Conference Key Distribution Systems -- Authentication -- Subliminal-free Authentication and Signature -- Zero-Knowledge Proofs of Identity and Veracity of Transaction Receipts -- Authentication Codes with Multiple Arbiters -- Some Constructions for Authentication - Secrecy Codes -- Efficient Zero-Knowledge Identification Scheme for Smart Cards -- Signatures -- A Smart Card Implementation of the Fiat-Shamir Identification Scheme -- Manipulations and Errors, Detection and Localization -- Privacy Protected Payments — Realization of a Protocol That Guarantees Payer Anonymity -- A Practical Zero-Knowledge Protocol Fitted to Security Microprocessor Minimizing Both Transmission and Memory -- A Generalized Birthday Attack -- Protocols -- An Interactive Data Exchange Protocol Based on Discrete Exponentiation -- Anonymous and Verifiable Registration in Databases -- Elections with Unconditionally-Secret Ballots and Disruption Equivalent to Breaking RSA -- Passports and Visas Versus IDs -- Complexity and Number

Theory -- The Probabilistic Theory of Linear Complexity -- A Probabilistic Primality Test Based on the Properties of Certain Generalized Lucas Numbers -- On the Construction of Random Number Generators and Random Function Generators -- Numerical Methods -- Factorization of Large Integers on a Massively Parallel Computer -- A Fast Modular Arithmetic Algorithm Using a Residue Table -- Fast Exponentiation in GF(2n) -- Fast RSA-Hardware: Dream or Reality? -- Cryptanalysis -- Properties of the Euler Totient Function Modulo 24 and Some of Its Cryptographic Implications -- An Observation on the Security of McEliece's Public-Key Cryptosystem -- How to Break Okamoto's Cryptosystem by Reducing Lattice Bases -- Cryptanalysis of F.E.A.L. -- Fast Correlation Attacks on Stream Ciphers -- Running-Key Ciphers -- A New Class of Nonlinear Functions for Running-key Generators -- Windmill Generators A generalization and an observation of how many there are -- Lock-in Effect in Cascades of Clock-Controlled Shift-Registers -- Proof of Massey's Conjectured Algorithm -- Linear Recurring m-Arrays -- Cipher Theory and Threshold -- Substantial Number of Cryptographic Keys and Its Application to Encryption Designs -- A Measure of Semiequivocation -- Some New Classes of Geometric Threshold Schemes -- New Ciphers -- A Universal Algorithm for Homophonic Coding -- A New Probabilistic Encryption Scheme -- Public Quadratic Polynomial-Tuples for Efficient Signature-Verification and Message-Encryption -- Some Applications of Multiple Key Ciphers.

Sommario/riassunto

The International .4ssociation for Cryptologic Research (1.4CR) organizes tmo - ternational conferences every year, one in Europe and one in the 1-nited States. EUROCRYI'T'88. held in the beautiful environment of the S\~isb mountains in Davos, was the sixth European conference. The number of contributions and of participants at the meeting has increased substantiall!.. which is an indication of the high interest in cryptography and system security in general. The interest has not only increased but has also further moved towards - thentication. signatures and other protocols. This is easy to understand in view of the urgent needs for such protocols, in particular in connection with open - formation systems, and in view of the exciting problems in this area. The equally fascinating classical field of secrecy, 2.e. the theory, design and analysis of stream or block ciphers and of public key cryptosystems. was however also well represented and several significant results mere communicated. The present proceedings contain all contributions which were accepted for presentation. The chapters correspond to the sessions at the conference.