1. Record Nr. UNINA9910557457203321

Titolo	Beyond Foucault: Excursions in Political Genealogy
Pubbl/distr/stampa	MDPI
ISBN	3-03897-245-2
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia

2. Record Nr. UNISA996465820303316

Titolo	Advances in cryptology - EUROCRYPT '90 : Workshop on the Theory and Application of Cryptographic Techniques, Aarhus, Denmark, May 21-24, 1990, proceedings / / I. B. Damgard (ed.)
Pubbl/distr/stampa	Berlin ; ; Heidelberg : , : Springer-Verlag, , [1991] Â©1991
ISBN	3-540-46877-3
Edizione	[1st ed. 1991.]
Descrizione fisica	1 online resource (VIII, 500 p.)
Collana	Lecture Notes in Computer Science ; ; 473
Disciplina	003.54
Soggetti	Coding theory Combinatorial analysis
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	Protocols -- All Languages in NP Have Divertible Zero-Knowledge Proofs and Arguments Under Cryptographic Assumptions -- On the Importance of Memory Resources in the Security of Key Exchange Protocols -- Provably Secure Key-Updating Schemes in Identity-Based Systems -- Oblivious transfer protecting secrecy -- Public-Randomness in Public-Key Cryptography -- An Interactive Identification Scheme Based on Discrete Logarithms and Factoring -- Number-Theoretic Algorithms -- Factoring with two large primes -- Which new RSA signatures can be computed from some given RSA

signatures? -- Implementation of a Key Exchange Protocol Using Real Quadratic Fields -- Distributed Primality Proving and the Primality of (23539 + 1)/3 -- Boolean Functions -- Properties of binary functions -- How to Construct Pseudorandom Permutations from Single Pseudorandom Functions -- Constructions of bent functions and difference sets -- Propagation Characteristics of Boolean Functions -- Binary Sequences -- The Linear Complexity Profile and the Jump Complexity of Keystream Sequences -- Lower Bounds for the Linear Complexity of Sequences over Residue Rings -- On the Construction of Run Permuted Sequences -- Correlation Properties of Combiners with Memory in Stream Ciphers (Extended Abstract) -- Correlation Functions of Geometric Sequences -- Implementations -- Exponentiating Faster with Addition Chains -- A Cryptographic Library for the Motorola DSP56000 -- VICTOR an efficient RSA hardware implementation -- Experimental Quantum Cryptography -- Combinatorial Schemes -- A Protocol to Set Up Shared Secret Schemes Without the Assistance of a Mutually Trusted Party -- Lower Bounds for Authentication Codes with Splitting -- Essentially ?-fold secure authentication systems -- On the construction of authentication codes with secrecy and codes withstanding spoofing attacks of order L ? 2 -- Cryptanalysis -- Cryptanalysis of a public-key cryptosystem based on approximations by rational numbers -- A Known-Plaintext Attack on Two-Key Triple Encryption -- Confirmation that Some Hash Functions Are Not Collision Free -- Inverting the Pseudo Exponentiation -- New Cryptosystems -- Cryptosystem for Group Oriented Cryptography -- A Provably-Secure Strongly-Randomized Cipher -- General public key residue cryptosystems and mental poker protocols -- A Proposal for a New Block Encryption Standard -- A new trapdoor in knapsacks -- Signatures and Authentication -- On the Design of Provably-Secure Cryptographic Hash Functions -- Fast Signature Generation with a Fiat Shamir — Like Scheme -- A Remark on a Signature Scheme Where Forgery can be Proved -- Membership Authentication for Hierarchical Multigroups Using the Extended Fiat-Shamir Scheme -- Zero-Knowledge Undeniable Signatures (extended abstract) -- Precautions taken against various potential attacks -- Impromptu Talks -- Software Run-Time Protection: A Cryptographic Issue -- An identity-based identification scheme based on discrete logarithms modulo a composite number -- A Noisy Clock-Controlled Shift Register Cryptanalysis Concept Based on Sequence Comparison Approach -- The MD4 Message Digest Algorithm -- A remark on the efficiency of identification schemes -- On an Implementation of the Mohan-Adiga Algorithm.

Sommario/riassunto

Eurocrypt is a conference devoted to all aspects of cryptologic research, both theoretical and practical, sponsored by the International Association for Cryptologic Research (IACR). Eurocrypt 90 took place in Åarhus, Denmark, in May 1990. From the 85 papers submitted, 42 were selected for presentation at the conference and for inclusion in this volume. In addition to the formal contributions, short abstracts of a number of informal talks are included in these proceedings. The proceedings are organized into sessions on protocols, number-theoretic algorithms, boolean functions, binary sequences, implementations, combinatorial schemes, cryptanalysis, new cryptosystems, signatures and authentication, and impromptu talks.

3. Record Nr. UNISANNIOFER0139069

Autore	Andrioli, Virgilio
Titolo	1: Disposizioni generali / Virgilio Andrioli
Pubbl/distr/stampa	Napoli, : E. Jovene, 1943
Edizione	[2. ed. riv. e aggiornata]
Descrizione fisica	XVI, 402 p. ; 25 cm.
Disciplina	347 347.05
Soggetti	Italia . Codice di procedura civile
Collocazione	D (AR) 27 046
Lingua di pubblicazione	Italiano
Formato	Materiale a stampa
Livello bibliografico	Monografia