

| | |
|-------------------------|---|
| 1. Record Nr. | UNISA996465856603316 |
| Titolo | Advances in Cryptology – EUROCRYPT 2000 [[electronic resource]] : International Conference on the Theory and Application of Cryptographic Techniques Bruges, Belgium, May 14-18, 2000 Proceedings / / edited by Bart Preneel |
| Pubbl/distr/stampa | Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2000 |
| ISBN | 3-540-45539-6 |
| Edizione | [1st ed. 2000.] |
| Descrizione fisica | 1 online resource (XIII, 612 p.) |
| Collana | Lecture Notes in Computer Science, , 0302-9743 ; ; 1807 |
| Disciplina | 618.9268 |
| Soggetti | Data encryption (Computer science) Computer communication systems Algorithms Operating systems (Computers) Computer mathematics Cryptology Computer Communication Networks Algorithm Analysis and Problem Complexity Operating Systems Computational Mathematics and Numerical Analysis |
| Lingua di pubblicazione | Inglese |
| Formato | Materiale a stampa |
| Livello bibliografico | Monografia |
| Note generali | Includes index. |
| Nota di contenuto | Factoring and Discrete Logarithm -- Factorization of a 512-Bit RSA Modulus -- An Algorithm for Solving the Discrete Log Problem on Hyperelliptic Curves -- Analysis and Optimization of the TWINKLE Factoring Device -- Cryptanalysis I: Digital Signatures -- Noisy Polynomial Interpolation and Noisy Chinese Remaindering -- A Chosen Messages Attack on the ISO/IEC 9796-1 Signature Scheme -- Cryptanalysis of Countermeasures Proposed for Repairing ISO 9796-1 -- Security Analysis of the Gennaro-Halevi-Rabin Signature Scheme -- Invited Talk -- On the Security of 3GPP Networks -- Private Information Retrieval -- One-Way Trapdoor Permutations Are Sufficient for Non-trivial Single-Server Private Information Retrieval -- Single Database |

Private Information Retrieval Implies Oblivious Transfer -- Key Management Protocols -- Authenticated Key Exchange Secure against Dictionary Attacks -- Provably Secure Password-Authenticated Key Exchange Using Diffie-Hellman -- Fair Encryption of RSA Keys -- Threshold Cryptography and Digital Signatures -- Computing Inverses over a Shared Secret Modulus -- Practical Threshold Signatures -- Adaptively Secure Threshold Cryptography: Introducing Concurrency, Removing Erasures -- Confirmer Signature Schemes Secure against Adaptive Adversaries -- Public-Key Encryption -- Public-Key Encryption in a Multi-user Setting: Security Proofs and Improvements -- Using Hash Functions as a Hedge against Chosen Ciphertext Attack -- Quantum Cryptography -- Security Aspects of Practical Quantum Cryptography -- Perfectly Concealing Quantum Bit Commitment from any Quantum One-Way Permutation -- Multi-party Computation and Information Theory -- General Secure Multi-party Computation from any Linear Secret-Sharing Scheme -- Minimal-Latency Secure Function Evaluation -- Information-Theoretic Key Agreement: From Weak to Strong Secrecy for Free -- Cryptanalysis II: Public-Key Encryption -- New Attacks on PKCS#1 v1.5 Encryption -- A NICE Cryptanalysis -- Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations -- Cryptanalysis of Patarin's 2-Round Public Key System with S Boxes (2R) -- Invited Talk -- Colossus and the German Lorenz Cipher — Code Breaking in WW II -- Zero-Knowledge -- Efficient Concurrent Zero-Knowledge in the Auxiliary String Model -- Efficient Proofs that a Committed Number Lies in an Interval -- Symmetric Cryptography -- A Composition Theorem for Universal One-Way Hash Functions -- Exposure-Resilient Functions and All-or-Nothing Transforms -- The Sum of PRPs Is a Secure PRF -- Boolean Functions and Hardware -- Construction of Nonlinear Boolean Functions with Important Cryptographic Properties -- Propagation Characteristics and Correlation-Immunity of Highly Nonlinear Boolean Functions -- Cox-Rower Architecture for Fast Parallel Montgomery Multiplication -- Voting Schemes -- Efficient Receipt-Free Voting Based on Homomorphic Encryption -- How to Break a Practical MIX and Design a New One -- Cryptanalysis III: Stream Ciphers and Block Ciphers -- Improved Fast Correlation Attacks Using Parity-Check Equations of Weight 4 and 5 -- Advanced Slide Attacks.
