| | | |
|---|---|---|
| 1. | Record Nr. | UNISA996465405503316 |
| | Titolo | Advances in Cryptology – EUROCRYPT 2004 [[electronic resource] ] : International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May 2-6, 2004. Proceedings / / edited by Christian Cachin, Jan Camenisch |
| | Pubbl/distr/stampa | Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2004 |
| | ISBN | 1-280-30737-4<br>9786610307371<br>3-540-24676-2 |
| | Edizione | [1st ed. 2004.] |
| | Descrizione fisica | 1 online resource (XII, 630 p.) |
| | Collana | Lecture Notes in Computer Science, , 0302-9743 ; ; 3027 |
| | Disciplina | 005.82 |
| | Soggetti | Data encryption (Computer science)<br>Computer communication systems<br>Operating systems (Computers)<br>Algorithms<br>Computer science—Mathematics<br>Management information systems<br>Computer science<br>Cryptology<br>Computer Communication Networks<br>Operating Systems<br>Algorithm Analysis and Problem Complexity<br>Discrete Mathematics in Computer Science<br>Management of Computing and Information Systems |
| | 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 at the end of each chapters and index. |
| | Nota di contenuto | Private Computation -- Efficient Private Matching and Set Intersection -- Positive Results and Techniques for Obfuscation -- Secure Computation of the k th -Ranked Element -- Signatures I -- Short Signatures Without Random Oracles -- Sequential Aggregate Signatures |

from Trapdoor Permutations -- Unconditional Security -- On the Key-Uncertainty of Quantum Ciphers and the Computational Security of One-Way Quantum Transmission -- The Exact Price for Unconditionally Secure Asymmetric Cryptography -- On Generating the Initial Key in the Bounded-Storage Model -- Distributed Cryptography -- Practical Large-Scale Distributed Key Generation -- Optimal Communication Complexity of Generic Multicast Key Distribution -- Foundations I -- An Uninstantiable Random-Oracle-Model Scheme for a Hybrid-Encryption Problem -- Black-Box Composition Does Not Imply Adaptive Security -- Identity-Based Encryption -- Chosen-Ciphertext Security from Identity-Based Encryption -- Efficient Selective-ID Secure Identity-Based Encryption Without Random Oracles -- Elliptic Curves -- Construction of Secure Random Curves of Genus 2 over Prime Fields -- Projective Coordinates Leak -- Signatures II -- Security Proofs for Identity-Based Identification and Signature Schemes -- Concurrent Signatures -- The Hierarchy of Key Evolving Signatures and a Characterization of Proxy Signatures -- Public-Key Cryptography -- Public-Key Steganography -- Immunizing Encryption Schemes from Decryption Errors -- Secure Hashed Diffie-Hellman over Non-DDH Groups -- Foundations II -- On Simulation-Sound Trapdoor Commitments -- Hash Function Balance and Its Impact on Birthday Attacks -- Multiparty Computation -- Multi-party Computation with Hybrid Security -- On the Hardness of Information-Theoretic Multiparty Computation -- Dining Cryptographers Revisited -- Cryptanalysis -- Algebraic Attacks and Decomposition of Boolean Functions -- Finding Small Roots of Bivariate Integer Polynomial Equations Revisited -- New Applications -- Public Key Encryption with Keyword Search -- Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data -- Algorithms and Implementation -- Merkle Tree Traversal in Log Space and Time -- Can We Trust Cryptographic Software? Cryptographic Flaws in GNU Privacy Guard v1.2.3 -- Anonymity -- Traceable Signatures -- Handcuffing Big Brother: an Abuse-Resilient Transaction Escrow Scheme -- Anonymous Identification in Ad Hoc Groups.

Sommario/riassunto

These are the proceedings of Eurocrypt 2004, the 23rd Annual Eurocrypt C- ference. The conference was organized by members of the IBM Zurich Research Laboratory in cooperation with IACR, the International Association for Cr- tologic Research. Theconferencereceivedarecordnumberof206submissions,outofwhichthe program committee selected 36 for presentation at the conference (three papers were withdrawn by the authors shortly after submission). These proceedings contain revised versions of the accepted papers. These revisions have not been checked for correctness, and the authors bear full responsibility for the contents of their papers. The conference program also featured two invited talks. The ?rst one was the 2004 IACR Distinguished Lecture given by Whit?eld Di?e. The second invited talk was by Ivan Damg? ard who presented “Paradigms for Multiparty Computation. ” The traditional rump session with short informal talks on recent results was chaired by Arjen Lenstra. The reviewing process was a challenging task, and many good submissions had to be rejected. Each paper was reviewed independently by at least three members of the program committee, and papers co-authored by a member of the program committee were reviewed by at least six (other) members. The individual reviewing phase was followed by profound and sometimes lively d- cussions about the papers, which contributed a lot to the quality of the ?nal selection. Extensive comments were sent to the authors in most cases.