1. Record Nr. UNISA996465720103316

Titolo	Advances in Cryptology – ASIACRYPT 2005 [[electronic resource]] : 11th International Conference on the Theory and Application of Cryptology and Information Security, Chennai, India, December 4-8, 2005, Proceedings / / edited by Bimal Kumar Roy
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2005
Edizione	[1st ed. 2005.]
Descrizione fisica	1 online resource (XIV, 706 p.)
Collana	Security and Cryptology ; ; 3788
Disciplina	003.54
Soggetti	Coding theory Information theory Data encryption (Computer science) Operating systems (Computers) Algorithms Management information systems Computer science Computer communication systems Coding and Information Theory Cryptology Operating Systems Algorithm Analysis and Problem Complexity Management of Computing and Information Systems Computer Communication Networks
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 and index.
Nota di contenuto	Algebra and Number Theory -- Discrete-Log-Based Signatures May Not Be Equivalent to Discrete Log -- Do All Elliptic Curves of the Same Order Have the Same Difficulty of Discrete Log? -- Adapting Density Attacks to Low-Weight Knapsacks -- Efficient and Secure Elliptic Curve Point Multiplication Using Double-Base Chains -- Multiparty Computation -- Upper Bounds on the Communication Complexity of

Optimally Resilient Cryptographic Multiparty Computation -- Graph-Decomposition-Based Frameworks for Subset-Cover Broadcast Encryption and Efficient Instantiations -- Revealing Additional Information in Two-Party Computations -- Zero Knowledge and Secret Sharing -- Gate Evaluation Secret Sharing and Secure One-Round Two-Party Computation -- Parallel Multi-party Computation from Linear Multi-secret Sharing Schemes -- Updatable Zero-Knowledge Databases -- Information and Quantum Theory -- Simple and Tight Bounds for Information Reconciliation and Privacy Amplification -- Quantum Anonymous Transmissions -- Privacy and Anonymity -- Privacy-Preserving Graph Algorithms in the Semi-honest Model -- Spreading Alerts Quietly and the Subgroup Escape Problem -- A Sender Verifiable Mix-Net and a New Proof of a Shuffle -- Universally Anonymizable Public-Key Encryption -- Cryptanalytic Techniques -- Fast Computation of Large Distributions and Its Cryptographic Applications -- An Analysis of the XSL Algorithm -- Stream Cipher Cryptanalysis -- New Applications of Time Memory Data Tradeoffs -- Linear Cryptanalysis of the TSC Family of Stream Ciphers -- A Practical Attack on the Fixed RC4 in the WEP Mode -- A Near-Practical Attack Against B Mode of HBB -- Block Ciphers and Hash Functions -- New Improvements of Davies-Murphy Cryptanalysis -- A Related-Key Rectangle Attack on the Full KASUMI -- Some Attacks Against a Double Length Hash Proposal -- A Failure-Friendly Design Principle for Hash Functions -- Bilinear Maps -- Identity-Based Hierarchical Strongly Key-Insulated Encryption and Its Application -- Efficient and Provably-Secure Identity-Based Signatures and Signcryption from Bilinear Maps -- Verifier-Local Revocation Group Signature Schemes with Backward Unlinkability from Bilinear Maps -- Key Agreement -- Modular Security Proofs for Key Agreement Protocols -- A Simple Threshold Authenticated Key Exchange from Short Secrets -- Examining Indistinguishability-Based Proof Models for Key Establishment Protocols -- Provable Security -- Server-Aided Verification: Theory and Practice -- Errors in Computational Complexity Proofs for Protocols -- Signatures -- Universal Designated Verifier Signature Proof (or How to Efficiently Prove Knowledge of a Signature) -- Efficient Designated Confirmer Signatures Without Random Oracles or General Zero-Knowledge Proofs -- Universally Convertible Directed Signatures.