1. Record Nr. UNISA996466163203316

Titolo	Advances in Cryptology – EUROCRYPT 2001 [[electronic resource]] : International Conference on the Theory and Application of Cryptographic Techniques Innsbruck, Austria, May 6–10, 2001, Proceedings / / edited by Birgit Pfitzmann
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2001
ISBN	3-540-44987-6
Edizione	[1st ed. 2001.]
Descrizione fisica	1 online resource (XIII, 544 p. 23 illus.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 2045
Disciplina	652.8
Soggetti	Data encryption (Computer science) Computer science—Mathematics Management information systems Computer science Computer communication systems Algorithms Computer mathematics Cryptology Mathematics of Computing Management of Computing and Information Systems Computer Communication Networks Algorithm Analysis and Problem Complexity Computational Mathematics and Numerical 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 at the end of each chapters and index.
Nota di contenuto	Elliptic Curves -- A Memory Efficient Version of Satoh's Algorithm -- Finding Secure Curves with the Satoh-FGH Algorithm and an Early-Abort Strategy -- How Secure Are Elliptic Curves over Composite Extension Fields? -- Commitments -- Efficient and Non-interactive Non-malleable Commitment -- How to Convert the Flavor of a Quantum Bit Commitment -- Anonymity -- Cryptographic Counters

and Applications to Electronic Voting -- An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation -- Priced Oblivious Transfer: How to Sell Digital Goods -- Signatures and Hash Functions -- A Secure Three-Move Blind Signature Scheme for Polynomially Many Signatures -- Practical Threshold RSA Signatures without a Trusted Dealer -- Hash Functions: From Merkle-Damgård to Shoup -- XTR and NTRU -- Key Recovery and Message Attacks on NTRU-Composite -- Evidence that XTR Is More Secure than Supersingular Elliptic Curve Cryptosystems -- NSS: An NTRU Lattice-Based Signature Scheme -- Assumptions -- The Bit Security of Paillier's Encryption Scheme and Its Applications -- Assumptions Related to Discrete Logarithms: Why Subtleties Make a Real Difference -- Multiparty Protocols -- On Adaptive vs. Non-adaptive Security of Multiparty Protocols -- Multiparty Computation from Threshold Homomorphic Encryption -- On Perfect and Adaptive Security in Exposure-Resilient Cryptography -- Block Ciphers -- Cryptanalysis of Reduced-Round MISTY -- The Rectangle Attack — Rectangling the Serpent -- Primitives -- Efficient Amplification of the Security of Weak Pseudo-random Function Generators -- Min-round Resettable Zero-Knowledge in the Public-Key Model -- Symmetric Ciphers -- Structural Cryptanalysis of SASAS -- Hyper-bent Functions -- New Method for Upper Bounding the Maximum Average Linear Hull Probability for SPNs -- Key Exchange and Multicast -- Lower Bounds for Multicast Message Authentication -- Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels -- Efficient Password-Authenticated Key Exchange Using Human-Memorable Passwords -- Authentication and Identification -- Identification Protocols Secure against Reset Attacks -- Does Encryption with Redundancy Provide Authenticity? -- Encryption Modes with Almost Free Message Integrity.

Sommario/riassunto

EUROCRYPT 2001, the 20th annual Eurocrypt conference, was sponsored by the IACR, the International Association for Cryptologic Research, see http://www. iacr. org/, this year in cooperation with the Austrian Computer - ciety (OCG). The General Chair, Reinhard Posch, was responsible for local or- nization, and registration was handled by the IACR Secretariat at the University of California, Santa Barbara. In addition to the papers contained in these proceedings, we were pleased that the conference program also included a presentation by the 2001 IACR d- tinguished lecturer, Andrew Odlyzko, on "Economics and Cryptography" and an invited talk by Silvio Micali, "Zero Knowledge Has Come of Age. " Furthermore, there was the rump session for presentations of recent results and other (p- sibly satirical) topics of interest to the crypto community, which Jean-Jacques Quisquater kindly agreed to run. The Program Committee received 155 submissions and selected 33 papers for presentation; one of them was withdrawn by the authors. The review process was therefore a delicate and challenging task for the committee members, and I wish to thank them for all the e? ort they spent on it. Each committee member was responsible for the review of at least 20 submissions, so each paper was carefully evaluated by at least three reviewers, and submissions with a program committee member as a (co-)author by at least six.