1. Record Nr. UNISA996465560903316

Titolo	Advances in Cryptology - CRYPTO 2002 [[electronic resource]] : 22nd Annual International Cryptology Conference Santa Barbara, California, USA, August 18-22, 2002. Proceedings / / edited by Moti Yung
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2002
ISBN	3-540-45708-9
Edizione	[1st ed. 2002.]
Descrizione fisica	1 online resource (XIV, 630 p.)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 2442
Disciplina	005.8/2
Soggetti	Cryptography Data encryption (Computer science) Data protection Computer science—Mathematics Discrete mathematics Algorithms Operating systems (Computers) Electronic data processing—Management Cryptology Data and Information Security Discrete Mathematics in Computer Science Operating Systems IT Operations
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	Block Ciphers -- Essential Algebraic Structure within the AES -- Blockwise-Adaptive Attackers Revisiting the (In)Security of Some Provably Secure Encryption Modes: CBC, GEM, IACBC -- Tweakable Block Ciphers -- Multi-user Oriented Cryptosystems -- The LSD Broadcast Encryption Scheme -- Dynamic Accumulators and Application to Efficient Revocation of Anonymous Credentials -- Foundations and Methodology -- Provably Secure Steganography --

Flaws in Applying Proof Methodologies to Signature Schemes -- Separating Random Oracle Proofs from Complexity Theoretic Proofs: The Non-committing Encryption Case -- Security of Practical Protocols -- On the Security of RSA Encryption in TLS -- Security Analysis of IKE's Signature-Based Key-Exchange Protocol -- GQ and Schnorr Identification Schemes: Proofs of Security against Impersonation under Active and Concurrent Attacks -- Secure Multiparty Computation -- On 2-Round Secure Multiparty Computation -- Private Computation — k-Connected versus 1-Connected Networks -- Public-Key Encryption -- Analysis and Improvements of NTRU Encryption Paddings -- Universal Padding Schemes for RSA -- Cryptanalysis of Unbalanced RSA with Small CRT-Exponent -- Information Theory and Secret Sharing -- Hyper-encryption against Space-Bounded Adversaries from On-Line Strong Extractors -- Optimal Black-Box Secret Sharing over Arbitrary Abelian Groups -- Cipher Design and Analysis -- A Generalized Birthday Problem -- (Not So) Random Shuffles of RC4 -- Black-Box Analysis of the Block-Cipher-Based Hash-Function Constructions from PGV -- Elliptic Curves and Abelian Varieties -- Supersingular Abelian Varieties in Cryptology -- Efficient Algorithms for Pairing-Based Cryptosystems -- Computing Zeta Functions of Hyperelliptic Curves over Finite Fields of Characteristic 2 -- Password-Based Authentication -- Threshold Password-Authenticated Key Exchange -- Distributed Cryptosystems -- A Threshold Pseudorandom Function Construction and Its Applications -- Efficient Computation Modulo a Shared Secret with Application to the Generation of Shared Safe-Prime Products -- Pseudorandomness and Applications -- Hidden Number Problem with the Trace and Bit Security of XTR and LUC -- Expanding Pseudorandom Functions; or: From Known-Plaintext Security to Chosen-Plaintext Security -- Variations on Signatures and Authentication -- Threshold Ring Signatures and Applications to Ad-hoc Groups -- Deniable Ring Authentication -- SiBIR: Signer-Base Intrusion-Resilient Signatures -- Stream Ciphers and Boolean Functions -- Cryptanalysis of Stream Ciphers with Linear Masking -- The Filter-Combiner Model for Memoryless Synchronous Stream Ciphers -- A Larger Class of Cryptographic Boolean Functions via a Study of the Maiorana-McFarland Construction -- Commitment Schemes -- Linear VSS and Distributed Commitments Based on Secret Sharing and Pairwise Checks -- Perfect Hiding and Perfect Binding Universally Composable Commitment Schemes with Constant Expansion Factor -- Signature Schemes -- Unique Signatures and Verifiable Random Functions from the DH-DDH Separation -- Security Proof for Partial-Domain Hash Signature Schemes.

Sommario/riassunto

Crypto 2002, the 22nd Annual Crypto Conference, was sponsored by IACR, the International Association for Cryptologic Research, in cooperation with the IEEE Computer Society Technical Committee on Security and Privacy and the Computer Science Department of the University of California at Santa Barbara. It is published as Vol. 2442 of the Lecture Notes in Computer Science (LNCS) of Springer Verlag. Note that 2002, 22 and 2442 are all palindromes... (Don't nod!) Theconferencereceived175submissions,ofwhich40wereaccepted;twos-missionsweremergedintoasinglepaper, yieldingthetotalof39papersaccepted for presentation in the technical program of the conference. In this proceedings volume you will ?nd the revised versions of the 39 papers that were presented at the conference. The submissions represent the current state of work in the cryptographic community worldwide, covering all areas of cryptologic research. In fact, many high-quality works (that surely will be published elsewhere) could not be accepted. This is due to the competitive nature

of the conference and the challenging task of selecting a program. I wish to thank the authors of all submitted papers. Indeed, it is the authors of all papers who have made this conference possible, regardless of whether or not their papers were accepted. The conference program was also immensely bene?ted by two plenary talks.