1. Record Nr. UNISA996465879203316

Titolo	Advances in Cryptology -- CRYPTO 2003 [[electronic resource]] : 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings / / edited by Dan Boneh
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2003
ISBN	3-540-45146-3
Edizione	[1st ed. 2003.]
Descrizione fisica	1 online resource (XII, 636 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 2729
Disciplina	005.8205
Soggetti	Data encryption (Computer science) Computer communication systems Operating systems (Computers) Algorithms Computer science—Mathematics Management information systems Computer science Cryptology Computer Communication Networks Operating Systems Algorithm Analysis and Problem Complexity Discrete Mathematics in Computer Science 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	Public Key Cryptanalysis I -- Factoring Large Numbers with the TWIRL Device -- New Partial Key Exposure Attacks on RSA -- Algebraic Cryptanalysis of Hidden Field Equation (HFE) Cryptosystems Using Gröbner Bases -- Alternate Adversary Models -- On Constructing Locally Computable Extractors and Cryptosystems in the Bounded Storage Model -- Unconditional Authenticity and Privacy from an Arbitrarily Weak Secret -- Invited Talk I -- On Cryptographic

Assumptions and Challenges -- Protocols -- Scalable Protocols for Authenticated Group Key Exchange -- Practical Verifiable Encryption and Decryption of Discrete Logarithms -- Extending Oblivious Transfers Efficiently -- Symmetric Key Cryptanalysis I -- Algebraic Attacks on Combiners with Memory -- Fast Algebraic Attacks on Stream Ciphers with Linear Feedback -- Cryptanalysis of Safer++ -- Public Key Cryptanalysis II -- A Polynomial Time Algorithm for the Braid Diffie-Hellman Conjugacy Problem -- The Impact of Decryption Failures on the Security of NTRU Encryption -- Universal Composability -- Universally Composable Efficient Multiparty Computation from Threshold Homomorphic Encryption -- Universal Composition with Joint State -- Zero-Knowledge -- Statistical Zero-Knowledge Proofs with Efficient Provers: Lattice Problems and More -- Derandomization in Cryptography -- On Deniability in the Common Reference String and Random Oracle Model -- Algebraic Geometry -- Primality Proving via One Round in ECPP and One Iteration in AKS -- Torus-Based Cryptography -- Public Key Constructions -- Efficient Universal Padding Techniques for Multiplicative Trapdoor One-Way Permutation -- Multipurpose Identity-Based Signcryption -- Invited Talk II -- SIGMA: The ‘SIGn-and-MAc’ Approach to Authenticated Diffie-Hellman and Its Use in the IKE Protocols -- New Problems -- On Memory-Bound Functions for Fighting Spam -- Lower and Upper Bounds on Obtaining History Independence -- Private Circuits: Securing Hardware against Probing Attacks -- Symmetric Key Constructions -- A Tweakable Enciphering Mode -- A Message Authentication Code Based on Unimodular Matrix Groups -- Luby-Rackoff: 7 Rounds Are Enough for 2 n(1????) Security -- New Models -- Weak Key Authenticity and the Computational Completeness of Formal Encryption -- Plaintext Awareness via Key Registration -- Relaxing Chosen-Ciphertext Security -- Symmetric Key Cryptanalysis II -- Password Interception in a SSL/TLS Channel -- Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication -- Making a Faster Cryptanalytic Time-Memory Trade-Off.

Sommario/riassunto

Crypto 2003, the 23rd Annual Crypto Conference, was sponsored by the Int- national Association for Cryptologic Research (IACR) 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. The conference received 169 submissions, of which the program committee selected 34 for presentation. These proceedings contain the revised versions of the 34 submissions that were presented at the conference. These revisions have not been checked for correctness, and the authors bear full responsibility for the contents of their papers. Submissions to the conference represent cutti- edge research in the cryptographic community worldwide and cover all areas of cryptography. Many high-quality works could not be accepted. These works will surely be published elsewhere. The conference program included two invited lectures. Moni Naor spoke on cryptographic assumptions and challenges. Hugo Krawczyk spoke on the ‘SI- and-MAc’ approachtoauthenticatedDi?e-HellmananditsuseintheIKEpro- cols. The conference program also included the traditional rump session, chaired by Stuart Haber, featuring short, informal talks on late-breaking research news. Assembling the conference program requires the help of many many people. To all those who pitched in, I am forever in your debt. I would like to ?rst thank the many researchers from all over the world who submitted their work to this conference. Without them, Crypto could not exist. I thank Greg Rose, the general chair, for shielding me from innumerable logistical headaches, and showing great

generosity in supporting my e?orts.