1. Record Nr. UNINA9910143607803321

Titolo	Progress in Cryptology - INDOCRYPT 2000 : First International Conference in Cryptology in India, Calcutta, India, December 10-13, 2000. Proceedings / / edited by Bimal Kumar Roy, Eiji Okamoto
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2000
ISBN	3-540-44495-5
Edizione	[1st ed. 2000.]
Descrizione fisica	1 online resource (X, 302 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 1977
Disciplina	005.8/2
Soggetti	Data encryption (Computer science) Computer communication systems Computer programming Algorithms Management information systems Computer science Operating systems (Computers) Cryptology Computer Communication Networks Programming Techniques Algorithm Analysis and Problem Complexity Management of Computing and Information Systems Operating 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 and index.
Nota di contenuto	Stream Ciphers and Boolean Functions -- The Correlation of a Boolean Function with Its Variables -- On Choice of Connection-Polynomials for LFSR-Based Stream Ciphers -- On Resilient Boolean Functions with Maximal Possible Nonlinearity -- Cryptanalysis I : Stream Ciphers -- Decimation Attack of Stream Ciphers -- Cryptanalysis of the A5/1 GSM Stream Cipher -- Cryptanalysis II : Block Ciphers -- On Bias Estimation in Linear Cryptanalysis -- On the Incomparability of Entropy and Marginal Guesswork in Brute-Force Attacks -- Improved Impossible

Differentials on Twofish -- Electronic Cash & Multiparty Computation -- An Online, Transferable E-Cash Payment System -- Anonymity Control in Multi-bank E-Cash System -- Efficient Asynchronous Secure Multiparty Distributed Computation -- Tolerating Generalized Mobile Adversaries in Secure Multiparty Computation -- Digital Signatures -- Codes Identifying Bad Signatures in Batches -- Distributed Signcryption -- Fail-Stop Signature for Long Messages (Extended Abstract) -- Elliptic Curves -- Power Analysis Breaks Elliptic Curve Cryptosystems Even Secure against the Timing Attack -- Efficient Construction of Cryptographically Strong Elliptic Curves -- Fast Arithmetic -- High-Speed Software Multiplication in F2m -- On Efficient Normal Basis Multiplication -- Cryptographic Protocols -- Symmetrically Private Information Retrieval -- Two-Pass Authenticated Key Agreement Protocol with Key Confirmation -- Anonymous Traceability Schemes with Unconditional Security -- Block Ciphers & Public Key Cryptography -- New Block Cipher DONUT Using Pairwise Perfect Decorrelation -- Generating RSA Keys on a Handheld Using an Untrusted Server -- A Generalized Takagi-Cryptosystem with a Modulus of the Form prqs.

Sommario/riassunto

The field of Cryptology witnessed a revolution in the late seventies. Since then it has been expanded into an important and exciting area of research. Over the last two decades, India neither participated actively nor did it contribute sig- nificantly towards the development in this field. However, recently a number of active research groups engaged in important research and developmental work have crystalized in different parts of India. As a result, their interaction with the international crypto community has become necessary. With this backdrop, it was proposed that a conference on cryptology - INDOCRYPT, be organized for the first time in India. The Indian Statistical Institute was instrumental in hosting this conference. INDOCRYPT has generated a large amount of enthu- siasm amongst the Indians as well as the International crypto communities. An INDOCRYPT steering committee has been formed and the committee has plans to make INDOCRYPT an annual event. For INDOCRYPT 2000, the program committee considered a total of 54 pa- pers and out of these 25 were selected for presentation. The conference program also included two invited lectures by Prof. Adi Shamir and Prof. Eli Biham. These proceedings include the revised versions of the 25 papers accepted by the program committee. These papers were selected from all the submissions based on originality, quality and relevance to the field of Cryptology. Revisions were not checked and the authors bear the full responsibility for the contents of the papers in these proceedings.