

1. Record Nr.	UNINA9910483836703321
Titolo	Progress in Cryptology – Mycrypt 2005 : First International Conference on Cryptology in Malaysia, Kuala Lumpur, Malaysia, September 28-30, 2005, Proceedings // edited by Ed Dawson, Serge Vaudenay
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2005
Edizione	[1st ed. 2005.]
Descrizione fisica	1 online resource (XI, 329 p.)
Collana	Security and Cryptology ; ; 3715
Classificazione	54.62
Disciplina	005.809595
Soggetti	Data encryption (Computer science) Coding theory Information theory Computer communication systems Algorithms Computer science—Mathematics Management information systems Computer science Cryptology Coding and Information Theory Computer Communication Networks 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 and index.
Nota di contenuto	Invited Talk I -- Trends and Challenges for Securer Cryptography in Practice -- Stream Ciphers Analysis -- Distinguishing Attacks on T-Functions -- Introducing a New Variant of Fast Algebraic Attacks and Minimizing Their Successive Data Complexity -- Cryptography Based on Combinatorics -- Equivalent Keys in HFE, C*, and Variations -- A New Structural Attack for GPT and Variants -- A Family of Fast Syndrome Based Cryptographic Hash Functions -- Cryptographic

Protocols -- Optimization of Electronic First-Bid Sealed-Bid Auction Based on Homomorphic Secret Sharing -- Identity Based Delegation Network -- On Session Key Construction in Provably-Secure Key Establishment Protocols -- On the Security of Probabilistic Multisignature Schemes and Their Optimality -- Invited Talk II -- Efficient Secure Group Signatures with Dynamic Joins and Keeping Anonymity Against Group Managers -- Implementation Issues -- An Analysis of Double Base Number Systems and a Sublinear Scalar Multiplication Algorithm -- Power Analysis by Exploiting Chosen Message and Internal Collisions -- Vulnerability of Checking Mechanism for RSA-Decryption -- Optimization of the MOVA Undeniable Signature Scheme -- Unconventional Cryptography -- Questionable Encryption and Its Applications -- Twin RSA -- Invited Talk III -- Security of Two-Party Identity-Based Key Agreement -- Block Cipher Cryptanalysis -- Related-Key Differential Attacks on Cobra-S128, Cobra-F64a, and Cobra-F64b -- Advanced Slide Attacks Revisited: Realigning Slide on DES -- New Multiset Attacks on Rijndael with Large Blocks -- Homomorphic Encryption -- Paillier's Cryptosystem Modulo  $p^2q$  and Its Applications to Trapdoor Commitment Schemes -- Homomorphic Cryptosystems Based on Subgroup Membership Problems.

---