1. Record Nr. UNINA9910461968403321

Autore	Hirschler Konrad
Titolo	The written word in the medieval Arabic lands [[electronic resource]] : a social and cultural history of reading practices / / Konrad Hirschler
Pubbl/distr/stampa	Edinburgh, : Edinburgh University Press, c2012
ISBN	0-7486-5421-6
Descrizione fisica	1 online resource (257 p.)
Disciplina	028.909174927
Soggetti	Written communication - Arab countries - History - To 1500 Books and reading - Arab countries - History - To 1500 Electronic books.
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.

2. Record Nr. UNINA9910484937903321

Titolo	Progress in Cryptology - VIETCRYPT 2006 : First International Conference on Cryptology in Vietnam, Hanoi, Vietnam, September 25-28, 2006, Revised Selected Papers / / edited by Phong Q. Nguyen
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2006
ISBN	3-540-68800-5
Edizione	[1st ed. 2006.]
Descrizione fisica	1 online resource (XI, 388 p.)
Collana	Security and Cryptology, , 2946-1863 ; ; 4341
Altri autori (Persone)	NguyenPhong, Q (Phong Quang)
Disciplina	005.8
Soggetti	Cryptography Data encryption (Computer science) Algorithms Computer science - Mathematics Discrete mathematics Data protection Computer networks Electronic data processing - Management Cryptology Discrete Mathematics in Computer Science Data and Information Security Computer Communication Networks 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 and index.
Nota di contenuto	Signatures and Lightweight Cryptography -- Probabilistic Multivariate Cryptography -- Short 2-Move Undeniable Signatures -- Searching for Compact Algorithms: cgen -- Invited Talk -- On Pairing-Based Cryptosystems -- Pairing-Based Cryptography -- A New Signature Scheme Without Random Oracles from Bilinear Pairings -- Efficient Dynamic k-Times Anonymous Authentication -- Side Channel Analysis of Practical Pairing Implementations: Which Path Is More Secure? -- Algorithmic Number Theory -- Factorization of Square-Free Integers

with High Bits Known -- Scalar Multiplication on Koblitz Curves Using Double Bases -- Compressed Jacobian Coordinates for OEF -- Ring Signatures and Group Signatures -- On the Definition of Anonymity for Ring Signatures -- Escrowed Linkability of Ring Signatures and Its Applications -- Dynamic Fully Anonymous Short Group Signatures -- Hash Functions -- Formalizing Human Ignorance -- Discrete Logarithm Variants of VSH -- How to Construct Sufficient Conditions for Hash Functions -- Cryptanalysis -- Improved Fast Correlation Attack on the Shrinking and Self-shrinking Generators -- On the Internal Structure of Alpha-MAC -- A Weak Key Class of XTEA for a Related-Key Rectangle Attack -- Key Agreement and Threshold Cryptography -- Deniable Group Key Agreement -- An Ideal and Robust Threshold RSA -- Towards Provably Secure Group Key Agreement Building on Group Theory -- Public-Key Encryption -- Universally Composable Identity-Based Encryption -- Traitor Tracing for Stateful Pirate Decoders with Constant Ciphertext Rate -- Reducing the Spread of Damage of Key Exposures in Key-Insulated Encryption.

Sommario/riassunto

This book constitutes the thoroughly refereed post-proceedings of the First International Conference on Cryptology in Vietnam, VIETCRYPT 2006, held in Hanoi, Vietnam, September 2006. The 25 papers cover signatures and lightweight cryptography, pairing-based cryptography, algorithmic number theory, ring signatures and group signatures, hash functions, cryptanalysis, key agreement and threshold cryptography, as well as public-key encryption.