1. 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 / / Phong Q. Nguyen (ed.)
Pubbl/distr/stampa	Berlin ; ; New York, : Springer, c2006
ISBN	3-540-68800-5
Edizione	[1st ed. 2006.]
Descrizione fisica	1 online resource (XI, 388 p.)
Collana	Lecture notes in computer science, , 0302-9743 ; ; 4341 LNCS sublibrary. SL 4, Security and cryptology
Altri autori (Persone)	NguyenPhong, Q (Phong Quang)
Disciplina	005.8
Soggetti	Computer security - Vietnam Computer systems - Access control Cryptography - Vietnam
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.