1. Record Nr. UNINA9910484630103321

Titolo	Provable Security : Third International Conference, ProvSec 2009, Guangzhou, China, November 11-13, 2009. Proceedings / / edited by Josef Pawel Pieprzyk, Fangguo Zhang
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2009
ISBN	3-642-04642-8
Edizione	[1st ed. 2009.]
Descrizione fisica	1 online resource (XII, 275 p.)
Collana	Security and Cryptology, , 2946-1863 ; ; 5848
Classificazione	004 DAT 465f SS 4800
Altri autori (Persone)	PieprzykJosef <1949-> ZhangFangguo
Disciplina	005.8
Soggetti	Cryptography Data encryption (Computer science) Data structures (Computer science) Information theory Computer science - Mathematics Discrete mathematics Coding theory Cryptology Data Structures and Information Theory Mathematics of Computing Discrete Mathematics in Computer Science Symbolic and Algebraic Manipulation Coding and Information Theory
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 Talks -- A Brief History of Security Models for Confidentiality -- Symbolic Methods for Provable Security -- Encryption -- Efficient Non-interactive Universally Composable String-Commitment Schemes -- Spatial Encryption under Simpler Assumption -- Chosen-Ciphertext Secure RSA-Type Cryptosystems -- Anonymous Conditional Proxy Re-

encryption without Random Oracle -- Breaking and Fixing of an Identity Based Multi-Signcryption Scheme -- Digital Signatures -- Identity-Based Verifiably Encrypted Signatures without Random Oracles -- How to Prove Security of a Signature with a Tighter Security Reduction -- Twin Signature Schemes, Revisited -- On the Insecurity of the Fiat-Shamir Signatures with Iterative Hash Functions -- Is the Notion of Divisible On-Line/Off-Line Signatures Stronger than On-Line/Off-Line Signatures? -- Anonymous Signatures Revisited -- Cryptographic Protocols -- An eCK-Secure Authenticated Key Exchange Protocol without Random Oracles -- Password Authenticated Key Exchange Based on RSA in the Three-Party Settings -- Comparing SessionStateReveal and EphemeralKeyReveal for Diffie-Hellman Protocols -- Zero-Knowledge Protocols for NTRU: Application to Identification and Proof of Plaintext Knowledge -- Server-Controlled Identity-Based Authenticated Key Exchange -- Reductions and Privacy -- Oracle Separation in the Non-uniform Model -- GUC-Secure Set-Intersection Computation -- Self-enforcing Private Inference Control.

Sommario/riassunto

This book constitutes the refereed proceedings of the Third International Conference on Provable Security, ProvSec 2009, held in Guangzhou, China, November 11-13, 2009. The 19 revised full papers and two invited talks presented were carefully reviewed and selected from 64 submissions. The papers are organized in topical sections on encryption, digital signature, cryptographic protocols and reduction and privacy.