1.	Record Nr.	UNISA996465545703316
	Titolo	Topics in Cryptology - CT-RSA 2009 [[electronic resource]] : The Cryptographers' Track at the RSA Conference 2009, San Francisco,CA, USA, April 20-24, 2009, Proceedings / / edited by Marc Fischlin
	Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2009
	ISBN	3-642-00862-3
	Edizione	[1st ed. 2009.]
	Descrizione fisica	1 online resource (XI, 482 p.)
	Collana	Security and Cryptology ; ; 5473
	Classificazione	DAT 465f SS 4800
	Disciplina	005.82
	Soggetti	Data encryption (Computer science) Coding theory Information theory Computer science—Mathematics Computer security Computer communication systems Algorithms Cryptology Coding and Information Theory Discrete Mathematics in Computer Science Systems and Data Security Computer Communication Networks Algorithm Analysis and Problem Complexity Kongress. San Francisco (Calif., 2009)
	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	Identity-Based Encryption -- Adaptive-ID Secure Revocable Identity-Based Encryption -- An Efficient Encapsulation Scheme from Near Collision Resistant Pseudorandom Generators and Its Application to IBE-to-PKE Transformations -- Universally Anonymous IBE Based on the Quadratic Residuosity Assumption -- Protocol Analysis -- Attacks

on the DECT Authentication Mechanisms -- Comparison-Based Key Exchange and the Security of the Numeric Comparison Mode in Bluetooth v2.1 -- Two-Party Protocols -- Key Insulation and Intrusion Resilience over a Public Channel -- Statistically Hiding Sets -- Adaptively Secure Two-Party Computation with Erasures -- More Than Signatures -- Short Redactable Signatures Using Random Trees -- Divisible On-Line/Off-Line Signatures -- Collisions for Hash Functions -- Speeding up Collision Search for Byte-Oriented Hash Functions -- Hard and Easy Components of Collision Search in the Zémor-Tillich Hash Function: New Attacks and Reduced Variants with Equivalent Security -- Cryptanalysis -- A Statistical Saturation Attack against the Block Cipher PRESENT -- Practical Attacks on Masked Hardware -- Cryptanalysis of CTC2 -- Alternative Encryption -- A CCA2 Secure Public Key Encryption Scheme Based on the McEliece Assumptions in the Standard Model -- Square, a New Multivariate Encryption Scheme -- Privacy and Anonymity -- Communication-Efficient Private Protocols for Longest Common Subsequence -- Key-Private Proxy Re-encryption -- Dynamic Universal Accumulators for DDH Groups and Their Application to Attribute-Based Anonymous Credential Systems -- Effciency Improvements -- Practical Short Signature Batch Verification -- Single-Layer Fractal Hash Chain Traversal with Almost Optimal Complexity -- Recursive Double-Size Modular Multiplications without Extra Cost for Their Quotients -- Multi-Party Protocols -- Constant-Rounds, Almost-Linear Bit-Decomposition of Secret Shared Values -- Local Sequentiality Does Not Help for Concurrent Composition -- Security of Encryption Schemes -- Breaking and Repairing Damgård et al. Public Key Encryption Scheme with Non-interactive Opening -- Strengthening Security of RSA-OAEP -- Faults and Countermeasures -- Fault Attacks on RSA Public Keys: Left-To-Right Implementations Are Also Vulnerable -- Fault Analysis Attack against an AES Prototype Chip Using RSL -- Countermeasures and Faults -- Evaluation of the Detached Power Supply as Side-Channel Analysis Countermeasure for Passive UHF RFID Tags -- Securing RSA against Fault Analysis by Double Addition Chain Exponentiation.

Sommario/riassunto

This book constitutes the refereed proceedings of the Cryptographers' Track at the RSA Conference 2009, CT-RSA 2009, held in San Francisco, CA, USA in April 2009. The 31 revised full papers presented were carefully reviewed and selected from 93 submissions. The papers are organized in topical sections on identity-based encryption, protocol analysis, two-party protocols, more than signatures, collisions for hash functions, cryptanalysis, alternative encryption, privacy and anonymity, efficiency improvements, multi-party protocols, security of encryption schemes as well as countermeasures and faults.