1.	Record Nr.	UNISA996465928203316
	Titolo	Advances in Cryptology - ASIACRYPT 2009 [[electronic resource]] : 15th International Conference on the Theory and Application of Cryptology and Information Security, Tokyo, Japan, December 6-10, 2009, Proceedings / / edited by Mitsuri Matsui
	Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2009
	ISBN	3-642-10366-9
	Edizione	[1st ed. 2009.]
	Descrizione fisica	1 online resource (XIV, 722 p.)
	Collana	Security and Cryptology ; ; 5912
	Disciplina	005.8
	Soggetti	Data encryption (Computer science) Computer programming Discrete mathematics Algorithms Data structures (Computer science) Computer science—Mathematics Cryptology Programming Techniques Discrete Mathematics Algorithm Analysis and Problem Complexity Data Structures and Information Theory Discrete Mathematics in Computer Science Kongress. Tokio (2009)
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	International conference proceedings.
	Nota di bibliografia	Includes bibliographical references and index.
	Nota di contenuto	Block Ciphers -- Related-Key Cryptanalysis of the Full AES-192 and AES-256 -- The Key-Dependent Attack on Block Ciphers -- Cascade Encryption Revisited -- Quantum and Post-Quantum -- Quantum-Secure Coin-Flipping and Applications -- On the Power of Two-Party Quantum Cryptography -- Security Bounds for the Design of Code-Based Cryptosystems -- Hash Functions I -- Rebound Attack on the

Full Lane Compression Function -- Rebound Distinguishers: Results on the Full Whirlpool Compression Function -- MD5 Is Weaker Than Weak: Attacks on Concatenated Combiners -- The Intel AES Instructions Set and the SHA-3 Candidates -- Encryption Schemes -- Group Encryption: Non-interactive Realization in the Standard Model -- On Black-Box Constructions of Predicate Encryption from Trapdoor Permutations -- Hierarchical Predicate Encryption for Inner-Products -- Hedged Public-Key Encryption: How to Protect against Bad Randomness -- Multi Party Computation -- Secure Two-Party Computation Is Practical -- Secure Multi-party Computation Minimizing Online Rounds -- Improved Non-committing Encryption with Applications to Adaptively Secure Protocols -- Cryptographic Protocols -- Non-malleable Statistically Hiding Commitment from Any One-Way Function -- Proofs of Storage from Homomorphic Identification Protocols -- Simple Adaptive Oblivious Transfer without Random Oracle -- Hash Functions II -- Improved Generic Algorithms for 3-Collisions -- A Modular Design for Hash Functions: Towards Making the Mix-Compress-Mix Approach Practical -- How to Confirm Cryptosystems Security: The Original Merkle-Damgård Is Still Alive! -- Models and Frameworks I -- On the Analysis of Cryptographic Assumptions in the Generic Ring Model -- Zero Knowledge in the Random Oracle Model, Revisited -- A Framework for Universally Composable Non-committing Blind Signatures -- Cryptanalysis: Sqaure and Quadratic -- Cryptanalysis of the Square Cryptosystems -- Factoring pq 2 with Quadratic Forms: Nice Cryptanalyses -- Attacking Power Generators Using Unravelled Linearization: When Do We Output Too Much? -- Models and Frameworks II -- Security Notions and Generic Constructions for Client Puzzles -- Foundations of Non-malleable Hash and One-Way Functions -- Hash Functions III -- Improved Cryptanalysis of Skein -- Linearization Framework for Collision Attacks: Application to CubeHash and MD6 -- Preimages for Step-Reduced SHA-2 -- Lattice-Based -- Fiat-Shamir with Aborts: Applications to Lattice and Factoring-Based Signatures -- Efficient Public Key Encryption Based on Ideal Lattices -- Smooth Projective Hashing and Password-Based Authenticated Key Exchange from Lattices -- Side Channels -- PSS Is Secure against Random Fault Attacks -- Cache-Timing Template Attacks -- Memory Leakage-Resilient Encryption Based on Physically Unclonable Functions -- Signature Schemes with Bounded Leakage Resilience.

Sommario/riassunto

This book constitutes the refereed proceedings of the 15th International Conference on the Theory and Application of Cryptology and Information Security, ASIACRYPT 2009, held in Tokyo, Japan, in December 2009. The 41 revised full papers presented were carefully reviewed and selected from 298 submissions. The papers are organized in topical sections on block ciphers, quantum and post-quantum, hash functions I, encryption schemes, multi party computation, cryptographic protocols, hash functions II, models and frameworks I, cryptoanalysis: square and quadratic, models and framework II, hash functions III, lattice-based, and side channels.