1.

Record Nr.	UNISA996466018603316
Titolo	Advances in Cryptology – EUROCRYPT 2009 [[electronic resource]] : 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cologne, Germany, April 26-30, 2009, Proceedings / / edited by Antoine Joux
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2009
ISBN	3-642-01001-6
Edizione	[1st ed. 2009.]
Descrizione fisica	1 online resource (XV, 611 p.)
Collana	Security and Cryptology ; ; 5479
Classificazione	DAT 465f SS 4800
Disciplina	005.82
Soggetti	Data encryption (Computer science) Coding theory Information theory Computer communication systems Computer security Algorithms Computer science—Mathematics Cryptology Coding and Information Theory Computer Communication Networks Systems and Data Security Algorithm Analysis and Problem Complexity Discrete Mathematics in Computer Science Kongress. Koln (2009) Koln <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	Security, Proofs and Models (1) -- Possibility and Impossibility Results for Encryption and Commitment Secure under Selective Opening --

Breaking RSA Generically Is Equivalent to Factoring -- Resettably Secure Computation -- On the Security Loss in Cryptographic Reductions -- Hash Cryptanalysis -- On Randomizing Hash Functions to Strengthen the Security of Digital Signatures -- Cryptanalysis of MDC-2 -- Cryptanalysis on HMAC/NMAC-MD5 and MD5-MAC -- Finding Preimages in Full MD5 Faster Than Exhaustive Search -- Group and Broadcast Encryption -- Asymmetric Group Key Agreement -- Adaptive Security in Broadcast Encryption Systems (with Short Ciphertexts) -- Traitors Collaborating in Public: Pirates 2.0 -- Cryptosystems (1) -- Key Agreement from Close Secrets over Unsecured Channels -- Order-Preserving Symmetric Encryption -- A Double-Piped Mode of Operation for MACs, PRFs and PROs: Security beyond the Birthday Barrier -- Cryptanalysis -- On the Security of Cryptosystems with Quadratic Decryption: The Nicest Cryptanalysis -- Cube Attacks on Tweakable Black Box Polynomials -- Smashing SQUASH-0 -- Cryptosystems (2) -- Practical Chosen Ciphertext Secure Encryption from Factoring -- Realizing Hash-and-Sign Signatures under Standard Assumptions -- A Public Key Encryption Scheme Secure against Key Dependent Chosen Plaintext and Adaptive Chosen Ciphertext Attacks -- Invited Talk -- Cryptography without (Hardly Any) Secrets ? -- Security, Proofs and Models (2) -- Salvaging Merkle-Damgård for Practical Applications -- On the Security of Padding-Based Encryption Schemes – or – Why We Cannot Prove OAEP Secure in the Standard Model -- Simulation without the Artificial Abort: Simplified Proof and Improved Concrete Security for Waters' IBE Scheme -- On the Portability of Generalized Schnorr Proofs -- Side Channels -- A Unified Framework for the Analysis of Side-Channel Key Recovery Attacks -- A Leakage-Resilient Mode of Operation -- Curves -- ECM on Graphics Cards -- Double-Base Number System for Multi-scalar Multiplications -- Endomorphisms for Faster Elliptic Curve Cryptography on a Large Class of Curves -- Generating Genus Two Hyperelliptic Curves over Large Characteristic Finite Fields -- Randomness -- Verifiable Random Functions from Identity-Based Key Encapsulation -- Optimal Randomness Extraction from a Diffie-Hellman Element -- A New Randomness Extraction Paradigm for Hybrid Encryption.

Sommario/riassunto

This book constitutes the refereed proceedings of the 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2009, held in Cologne, Germany, in April 2009. The 33 revised full papers presented together with 1 invited lecture were carefully reviewed and selected from 148 submissions. The papers address all current foundational, theoretical and research aspects of cryptology, cryptography, and cryptanalysis as well as advanced applications. The papers are organized in topical sections on security, proofs, and models, hash cryptanalysis, group and broadcast encryption, cryptosystems, cryptanalysis, side channels, curves, and randomness.