1.

Record Nr.	UNINA9910484513503321
Titolo	Advances in cryptology : CRYPTO 2009, 29th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 16 - 20, 2009, proceedings / / Shai Halevi (ed.)
Pubbl/distr/stampa	Berlin ; ; Heidelberg ; ; New York, NY, : Springer, c2009
ISBN	3-642-03356-3
Edizione	[1st ed. 2009.]
Descrizione fisica	1 online resource (XIV, 692 p.)
Collana	Lecture notes in computer science ; ; 5677
Classificazione	DAT 465f SS 4800
Altri autori (Persone)	HaleviShai
Disciplina	004n/a
Soggetti	Cryptography Data encryption (Computer science)
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	International conference proceedings. Includes index.
Nota di contenuto	Key Leakage -- Reconstructing RSA Private Keys from Random Key Bits -- Public-Key Cryptosystems Resilient to Key Leakage -- Leakage-Resilient Public-Key Cryptography in the Bounded-Retrieval Model -- Hash-Function Cryptanalysis -- Short Chosen-Prefix Collisions for MD5 and the Creation of a Rogue CA Certificate -- Meet-in-the-Middle Preimage Attacks Against Reduced SHA-0 and SHA-1 -- Privacy and Anonymity -- Private Mutual Authentication and Conditional Oblivious Transfer -- Randomizable Proofs and Delegatable Anonymous Credentials -- Computational Differential Privacy -- Interactive Proofs and Zero-Knowledge -- Probabilistically Checkable Arguments -- On the Composition of Public-Coin Zero-Knowledge Protocols -- On the Amortized Complexity of Zero-Knowledge Protocols -- Linear Algebra with Sub-linear Zero-Knowledge Arguments -- Block-Cipher Cryptanalysis -- New Birthday Attacks on Some MACs Based on Block Ciphers -- Distinguisher and Related-Key Attack on the Full AES-256 -- Cryptanalysis of C2 -- Modes of Operation -- Message Authentication Codes from Unpredictable Block Ciphers -- How to Encipher Messages on a Small Domain -- Elliptic Curves -- How to Hash into Elliptic Curves -- Batch Binary Edwards -- Cryptographic Hardness -- Solving Hidden Number Problem with One Bit Oracle and

Advice -- Computational Indistinguishability Amplification: Tight Product Theorems for System Composition -- Merkle Puzzles -- Merkle Puzzles Are Optimal — An O(n 2)-Query Attack on Any Key Exchange from a Random Oracle -- Cryptography in the Physical World -- Position Based Cryptography -- Improving the Security of Quantum Protocols via Commit-and-Open -- Attacks on Signature Schemes -- Practical Cryptanalysis of iso/iec 9796-2 and emv Signatures -- How Risky Is the Random-Oracle Model? -- Invited Talk -- Abstraction in Cryptography -- Secret Sharing and Secure Computation -- Asymptotically Good Ideal Linear Secret Sharing with Strong Multiplication over Any Fixed Finite Field -- The Round Complexity of Verifiable Secret Sharing Revisited -- Somewhat Non-committing Encryption and Efficient Adaptively Secure Oblivious Transfer -- Cryptography and Game-Theory -- Collusion-Free Multiparty Computation in the Mediated Model -- Privacy-Enhancing Auctions Using Rational Cryptography -- Utility Dependence in Correct and Fair Rational Secret Sharing -- Cryptography and Lattices -- On Bounded Distance Decoding, Unique Shortest Vectors, and the Minimum Distance Problem -- Fast Cryptographic Primitives and Circular-Secure Encryption Based on Hard Learning Problems -- Identity-Based Encryption -- Dual System Encryption: Realizing Fully Secure IBE and HIBE under Simple Assumptions -- Cryptographers’ Toolbox -- The Group of Signed Quadratic Residues and Applications -- Short and Stateless Signatures from the RSA Assumption -- Smooth Projective Hashing for Conditionally Extractable Commitments.

Sommario/riassunto

This book constitutes the refereed proceedings of the 29th Annual International Cryptology Conference, CRYPTO 2009, held in Santa Barbara, CA, USA in August 2009. The 38 revised full papers presented were carefully reviewed and selected from 213 submissions. Addressing 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 key leakage, hash-function cryptanalysis, privacy and anonymity, interactive proofs and zero-knowledge, block-cipher cryptanalysis, modes of operation, elliptic curves, cryptographic hardness, merkle puzzles, cryptography in the physical world, attacks on signature schemes, secret sharing and secure computation, cryptography and game-theory, cryptography and lattices, identity-based encryption and cryptographers’ toolbox.