1. Record Nr. UNINA9910484591603321

Titolo	Progress in cryptology : AFRICACRYPT 2009 :second international conference on cryptology in Africa, Gammarth, Tunisia, June 21-15, 2009 : proceedings / / Serge Vaudenay (ed.)
Pubbl/distr/stampa	Berlin ; ; Heidelberg, : Springer, c2009
ISBN	3-642-02384-3
Edizione	[1st ed. 2009.]
Descrizione fisica	1 online resource (XI, 435 p.)
Collana	Lecture notes in computer science ; ; 5580
Classificazione	DAT 465f SS 4800
Altri autori (Persone)	VaudenaySerge
Disciplina	005.8
Soggetti	Computer security Computers - Access control Cryptography
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 author index.
Nota di contenuto	Hash Functions -- Second Preimage Attack on 5-Pass HAVAL and Partial Key-Recovery Attack on HMAC/NMAC-5-Pass HAVAL -- Cryptanalysis of Vortex -- Two Passes of Tiger Are Not One-Way -- Block Ciphers -- Generic Attacks on Feistel Networks with Internal Permutations -- Distinguishers for Ciphers and Known Key Attack against Rijndael with Large Blocks -- Asymmetric Encryption -- Reducing Key Length of the McEliece Cryptosystem -- Cryptanalysis of RSA Using the Ratio of the Primes -- Digital Signatures -- New RSA-Based (Selectively) Convertible Undeniable Signature Schemes -- A Schnorr-Like Lightweight Identity-Based Signature Scheme -- On the Theoretical Gap between Group Signatures with and without Unlinkability -- Practical Threshold Signatures with Linear Secret Sharing Schemes -- Asymmetric Encryption and Anonymity -- Certified Encryption Revisited -- Threshold Attribute-Based Signatures and Their Application to Anonymous Credential Systems -- Anonymity from Public Key Encryption to Undeniable Signatures -- Key Agreement Protocols -- Security Analysis of Standard Authentication and Key Agreement Protocols Utilising Timestamps -- Password-Authenticated Group Key Agreement with Adaptive Security and Contributiveness -- Cryptographic Protocols -- Unifying Zero-Knowledge Proofs of

Knowledge -- Co-sound Zero-Knowledge with Public Keys -- Another Look at Extended Private Information Retrieval Protocols -- Constructing Universally Composable Oblivious Transfers from Double Trap-Door Encryptions -- Efficient Implementations -- Exponent Recoding and Regular Exponentiation Algorithms -- Efficient Acceleration of Asymmetric Cryptography on Graphics Hardware -- Fast Elliptic-Curve Cryptography on the Cell Broadband Engine -- On Modular Decomposition of Integers -- Implementation Attacks -- Breaking KeeLoq in a Flash: On Extracting Keys at Lightning Speed -- An Improved Fault Based Attack of the Advanced Encryption Standard.

Sommario/riassunto

This book constitutes the proceedings of the Second International Conference on Cryptology in Africa, AFRICACRYPT 2009, held in Gammarth, Tunisia, on June 21-25, 2009. The 25 papers presented together with one invited talk were carefully reviewed and selected from 70 submissions. The topics covered are hash functions, block ciphers, asymmetric encryption, digital signatures, asymmetric encryption and anonymity, key agreement protocols, cryptographic protocols, efficient implementations, and implementation attacks.