1.

Record Nr.	UNINA9910483457903321
Titolo	Progress in Cryptology - AFRICACRYPT 2008 : First International Conference on Cryptology in Africa, Casablanca, Morocco, June 11-14, 2008, Proceedings / / edited by Serge Vaudenay
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2008
ISBN	3-540-68164-7
Edizione	[1st ed. 2008.]
Descrizione fisica	1 online resource (XI, 420 p.)
Collana	Security and Cryptology, , 2946-1863 ; ; 5023
Altri autori (Persone)	VaudenaySerge
Disciplina	005.8
Soggetti	Cryptography Data encryption (Computer science) Coding theory Information theory Computer networks Data protection Algorithms Computer science - Mathematics Discrete mathematics Cryptology Coding and Information Theory Computer Communication Networks Data and Information Security Discrete Mathematics in Computer Science
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	AES -- Improving Integral Attacks Against Rijndael-256 Up to 9 Rounds -- Implementation of the AES-128 on Virtex-5 FPGAs -- Analysis of RFID Protocols -- Weaknesses in a Recent Ultra-Lightweight RFID Authentication Protocol -- Differential Cryptanalysis of Reduced-Round PRESENT -- Invited Talk -- The Psychology of Security -- Cryptographic Protocols -- An (Almost) Constant-Effort Solution-Verification Proof-of-Work Protocol Based on Merkle Trees -- Robust

Threshold Schemes Based on the Chinese Remainder Theorem -- An Authentication Protocol with Encrypted Biometric Data -- Authentication -- Authenticated Encryption Mode for Beyond the Birthday Bound Security -- Cryptanalysis of the TRMS Signature Scheme of PKC’05 -- Public-Key Cryptography -- New Definition of Density on Knapsack Cryptosystems -- Another Generalization of Wiener’s Attack on RSA -- An Adaptation of the NICE Cryptosystem to Real Quadratic Orders -- Pseudorandomness -- A Proof of Security in O(2 n) for the Benes Scheme -- Analysis of Stream Ciphers -- Yet Another Attack on Vest -- Chosen IV Statistical Analysis for Key Recovery Attacks on Stream Ciphers -- Correlated Keystreams in Moustique -- Stream Ciphers Using a Random Update Function: Study of the Entropy of the Inner State -- Analysis of Grain’s Initialization Algorithm -- Hash Functions -- Password Recovery on Challenge and Response: Impossible Differential Attack on Hash Function -- How (Not) to Efficiently Dither Blockcipher-Based Hash Functions? -- Broadcast Encryption -- Attribute-Based Broadcast Encryption Scheme Made Efficient -- Lower Bounds for Subset Cover Based Broadcast Encryption -- Invited Talk -- A Brief History of Provably-Secure Public-Key Encryption -- Implementation -- On Compressible Pairings and Their Computation -- Twisted Edwards Curves -- EfficientMultiplication in , m???1 and 5???????18.

Sommario/riassunto

This book constitutes the refereed proceedings of the First International Conference on Cryptology hosted in Africa, held in Casablanca, Morocco, in June 2008. The 25 revised full papers presented together with 2 invited papers were carefully selected during two rounds of reviewing and improvement from 82 submissions. The papers are organized in topical sections on AES, analysis of RFID protocols, cryptographic protocols, authentication, public-key cryptography, pseudorandomness, analysis of stream ciphers, hash functions, broadcast encryption, and implementation.