1.

Record Nr.	UNISA996465273703316
Titolo	Security, Privacy, and Applied Cryptography Engineering [[electronic resource]] : Second International Conference, SPACE 2012, Chennai, India, November 3-4, 2012, Proceedings / / edited by Andrey Bogdanov, Somitra Sanadhya
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2012
ISBN	3-642-34416-X
Edizione	[1st ed. 2012.]
Descrizione fisica	1 online resource (XII, 173 p. 29 illus.)
Collana	Security and Cryptology ; ; 7644
Disciplina	005.8
Soggetti	Computer communication systems Data encryption (Computer science) Management information systems Computer science Algorithms Computer security Computers and civilization Computer Communication Networks Cryptology Management of Computing and Information Systems Algorithm Analysis and Problem Complexity Systems and Data Security Computers and Society Conference papers and proceedings.
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	A Novel Circuit Design Methodology to Reduce Side Channel Leakage -- The Schedulability of AES as a Countermeasure against Side Channel Attacks -- Impact of Extending Side Channel Attack on Cipher Variants: A Case Study with the HC Series of Stream Ciphers -- Performance and Security Evaluation of AES S-Box-Based Glitch PUFs on FPGAs -- Relaxing IND-CCA: Indistinguishability against Chosen Ciphertext

Verification Attack -- Towards Formal Analysis of Key Control in Group Key Agreement Protocols -- Some Results on Related Key-IV Pairs of Grain -- A Differential Fault Attack on Grain-128a Using MACs -- Breaking Hitag 2 Revisited -- Reduction in Lossiness of RSA Trapdoor Permutation -- Adaptively Secure Efficient Lattice (H)IBE in Standard Model with Short Public Parameters.

Sommario/riassunto

This book constitutes the refereed proceedings of the Second International Conference on Security, Privacy and Applied Cryptography Engineering held in Chennai, India, in November 2012. The 11 papers presented were carefully reviewed and selected from 61 submissions. The papers are organized in topical sections on symmetric-key algorithms and cryptanalysis, cryptographic implementations, side channel analysis and countermeasures, fault tolerance of cryptosystems, physically unclonable functions, public-key schemes and cryptanalysis, analysis and design of security protocol, security of systems and applications, high-performance computing in cryptology and cryptography in ubiquitous devices.