1. Record Nr. UNISA996466031103316

Titolo	Constructive Side-Channel Analysis and Secure Design [[electronic resource]] : 4th International Workshop, COSADE 2013, Paris, France, March 6-8, 2013, Revised Selected Papers / / edited by Emmanuel Prouff
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2013
ISBN	3-642-40026-4
Edizione	[1st ed. 2013.]
Descrizione fisica	1 online resource (X, 215 p. 51 illus.)
Collana	Security and Cryptology ; ; 7864
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
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di contenuto	Differential Photonic Emission Analysis -- Electromagnetic Glitch on the AES Round Counter -- Defeating with Fault Injection a Combined Attack Resistant Exponentiation -- Fault Attacks on Projective-to-Affine Coordinates Conversion -- Improved Algebraic Fault Analysis: A Case Study on Piccolo and Applications to Other Lightweight Block Ciphers -- Updated Recommendations for Blinded Exponentiation vs. Single Trace Analysis -- On 3-Share Threshold Implementations for 4-Bit S-

	boxes -- Collision-Correlation Attack against Some 1st-Order Boolean Masking Schemes in the Context of Secure Devices -- Exploring the Relations between Fault Sensitivity and Power Consumption -- Improved Side Channel Attacks on Pairing Based Cryptography -- Semi-Supervised Template Attack.
Sommario/riassunto	This book constitutes the thoroughly refereed post-conference proceedings of the 4th International Workshop, COSADE 2013, held in Paris, France, in March 2013. The 13 revised full papers presented together with two invited talks were carefully selected from 39 submissions and collect truly existing results in cryptographic engineering, from concepts to artifacts, from software to hardware, from attack to countermeasure.