1. Record Nr. UNINA9910483520403321

Titolo	Constructive Side-Channel Analysis and Secure Design : 5th International Workshop, COSADE 2014, Paris, France, April 13-15, 2014. Revised Selected Papers / / edited by Emmanuel Prouff
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2014
ISBN	3-319-10175-7
Edizione	[1st ed. 2014.]
Descrizione fisica	1 online resource (X, 313 p. 110 illus.)
Collana	Security and Cryptology ; ; 8622
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	A note on the use of margins to compare distinguishers -- A Theoretical Study of Kolmogorov-Smirnov Distinguishers: Side-Channel Analysis vs. Differential Cryptanalysis -- Pragmatism vs. Elegance: comparing two approaches to Simple Power Attacks on AES -- Addition with Blinded Operands -- On the Use of RSA Public Exponent to Improve Implementation Efficiency and Side-Channel Resistance -- Common Points on Elliptic Curves: The Achille's Heel of Fault Attack Countermeasures -- On Adaptive Bandwidth Selection for Efficient MIA

	-- Generic DPA attacks: curse or blessing? -- Template Attacks on Different Devices -- Using the Joint Distributions of a Cryptographic Function in Side Channel Analysis -- A Multiple-Fault Injection Attack by Adaptive Timing Control under Black-Box Conditions and a Countermeasure -- Adjusting laser injections for fully controlled faults.
Sommario/riassunto	This book constitutes the thoroughly refereed post-conference proceedings of the 5th International Workshop, COSADE 2014, held in Paris, France, in April 2014. The 20 revised full papers presented together with two invited talks were carefully selected from 51 submissions and collect truly existing results in cryptographic engineering, from concepts to artifacts, from software to hardware, from attack to countermeasure.