1.

Record Nr.	UNISA996465998803316
Titolo	Constructive Side-Channel Analysis and Secure Design [[electronic resource]] : Third International Workshop, COSADE 2012, Darmstadt, Germany, May 3-4, 2012. Proceedings / / edited by Werner Schindler, Sorin Huss
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2012
ISBN	3-642-29912-1
Edizione	[1st ed. 2012.]
Descrizione fisica	1 online resource (280 p. 103 illus.)
Collana	Security and Cryptology ; ; 7275
Classificazione	SS 4800
Disciplina	005.82
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 Kongress2012.Darmstadt Conference 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	Exploiting the Difference of Side-Channel Leakages / Michael Hutter, Mario Kirschbaum, Thomas Plos, Jorn-Marc Schmidt and Stefan Mangard -- Attacking an AES-Enabled NFC Tag: Implications from Design to a Real-World Scenario / Thomas Korak, Thomas Plos and Michael Hutter -- 700+ Attacks Published on Smart Cards: The Need

for a Systematic Counter Strategy / Mathias Wagner -- An Interleaved EPE-Immune PA-DPL Structure for Resisting Concentrated EM Side Channel Attacks on FPGA Implementation / Wei He, Eduardo de la Torre and Teresa Riesgo -- An Architectural Countermeasure against Power Analysis Attacks for FSR-Based Stream Ciphers / Shohreh Sharif Mansouri and Elena Dubrova -- Conversion of Security Proofs from One Leakage Model to Another: A New Issue / Jean-Sebastien Coron, Christophe Giraud, Emmanuel Prouff, Soline Renner and Matthieu Rivain, et al. -- Attacking Exponent Blinding in RSA without CRT / Sven Bauer -- A New Scan Attack on RSA in Presence of Industrial Countermeasures / Jean Da Rolt, Amitabh Das, Giorgio Di Natale, Marie-Lise Flottes and Bruno Rouzeyre, et al.

RSA Key Generation: New Attacks / Camille Vuillaume, Takashi Endo and Paul Wooderson -- A Fault Attack on the LED Block Cipher / Philipp Jovanovic, Martin Kreuzer and Ilia Polian -- Differential Fault Analysis of Full LBlock / Liang Zhao, Takashi Nishide and Kouichi Sakurai -- Contactless Electromagnetic Active Attack on Ring Oscillator Based True Random Number Generator / Pierre Bayon, Lilian Bossuet, Alain Aubert, Viktor Fischer and Francois Poucheret, et al. -- A Closer Look at Security in Random Number Generators Design / Viktor Fischer -- Same Values Power Analysis Using Special Points on Elliptic Curves / Cedric Murdica, Sylvain Guilley, Jean-Luc Danger, Philippe Hoogvorst and David Naccache -- The Schindler-Itoh-attack in Case of Partial Information Leakage / Alexander Kruger -- Butterfly-Attack on Skein's Modular Addition / Michael Zohner, Michael Kasper and Marc Stottinger -- MDASCA: An Enhanced Algebraic Side-Channel Attack for Error Tolerance and New Leakage Model Exploitation / Xinjie Zhao, Fan Zhang, Shize Guo, Tao Wang and Zhijie Shi, et al. -- Intelligent Machine Homicide / Breaking Cryptographic Devices Using Support Vector Machines / Annelie Heuser and Michael Zohner.

Sommario/riassunto

This book constitutes the refereed proceedings of the Third International Workshop on Constructive Side-Channel Analysis and Secure Design, COSADE 2012, held in Darmstadt, Germany, May 2012. The 16 revised full papers presented together with two invited talks were carefully reviewed and selected from 49 submissions. The papers are organized in topical sections on practical side-channel analysis; secure design; side-channel attacks on RSA; fault attacks; side-channel attacks on ECC; different methods in side-channel analysis.