1. Record Nr. UNINA9910484728403321

Titolo	Constructive Side-Channel Analysis and Secure Design : 7th International Workshop, COSADE 2016, Graz, Austria, April 14-15, 2016, Revised Selected Papers / / edited by François-Xavier Standaert, Elisabeth Oswald
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2016
ISBN	3-319-43283-4
Edizione	[1st ed. 2016.]
Descrizione fisica	1 online resource (X, 219 p. 74 illus.)
Collana	Security and Cryptology ; ; 9689
Disciplina	005.82
Soggetti	Data encryption (Computer science) Computer security Management information systems Computer science Algorithms Computer science—Mathematics Computer hardware Cryptology Systems and Data Security Management of Computing and Information Systems Algorithm Analysis and Problem Complexity Discrete Mathematics in Computer Science Computer Hardware
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Security and Physical Attacks -- Exploiting the Physical Disparity: Side-Channel Attacks on Memory Encryption -- Co-location detection on the Cloud -- Simple Photonic Emission Attack with Reduced Data Complexity -- Side-Channel Analysis (case studies) -- Power Analysis Attacks against IEEE 802.15.4 Node -- Improved Side-Channel Analysis Attacks on Xilinx Bitstream Encryption of 5, 6, and 7 Series -- Dismantling real-world ECC with Horizontal and Vertical Template

	Attacks -- Fault Analysis -- Algorithmic Countermeasures Against Fault Attacks and Power Analysis for RSA-CRT -- Improved Differential Fault Analysis on Camellia-128 -- A Note on the Security of CHES 2014 Symmetric Infective Countermeasure -- Side-Channel Analysis (tools) -- Simpler, Faster, and More Robust T-test Based Leakage Detection -- Design and implementation of a waveform-matching based triggering system -- Robust and One-Pass Parallel Computation of Correlation-Based Attacks at Arbitrary Order.
Sommario/riassunto	This book constitutes revised selected papers from the 7th International Workshop on Constructive Side-Channel Analysis and Secure Design, COSADE 2016, held in Graz, Austria, in April 2016. The 12 papers presented in this volume were carefully reviewed and selected from 32 submissions. They were organized in topical sections named: security and physical attacks; side-channel analysis (case studies); fault analysis; and side-channel analysis (tools).