1.	Record Nr.	UNINA9910483857703321
	Titolo	Smart Card Research and Advanced Applications : 15th International Conference, CARDIS 2016, Cannes, France, November 7–9, 2016, Revised Selected Papers / / edited by Kerstin Lemke-Rust, Michael Tunstall
	Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2017
	ISBN	3-319-54669-4
	Edizione	[1st ed. 2017.]
	Descrizione fisica	1 online resource (XII, 265 p. 93 illus.)
	Collana	Security and Cryptology ; ; 10146
	Disciplina	006
	Soggetti	Data encryption (Computer science) Computer security Programming languages (Electronic computers) Management information systems Computer science Algorithms Cryptology Systems and Data Security Programming Languages, Compilers, Interpreters Management of Computing and Information Systems Algorithm Analysis and Problem Complexity
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Nota di contenuto	Kernel Discriminant Analysis for Information Extraction in the Presence of Masking -- Second Order Side-Channel Analysis on ISO9797-1 MAC Algorithm 3 -- Side-Channel Analysis of the TUAK Algorithm Used for Authentication and Key Agreement in 3G/4G Networks -- Reverse Engineering Flash EEPROM Memories Using Scanning Electron Microscopy -- Spectre: A Tiny Side-Channel Resistant Speck Core for FPGAs -- Concealing Secrets in Embedded Processors Designs -- The Hell Forgery, Self-Modifying Codes Shoot again -- Logical Attacks on Secured Containers of the Java Card Platform -- Single-Trace Side-Channel Attacks on Scalar Multiplications with Pre-Computations -- A

Compact and Exception-Free Ladder for All Short Weierstrass Elliptic Curves -- Inner Product Masking for Bit-slice Ciphers and Security Order Amplification for Linear Leakages -- Squeezing Polynomial Masking in Tower Fields -- PRNGs for Masking Applications and Their Mapping to Evolvable Hardware -- Automated Detection of Instruction Cache Leaks in Modular Exponentiation Software -- An Analysis of the Learning Parity with Noise Assumption against Fault Attacks.

Sommario/riassunto

This book constitutes the thoroughly refereed post-conference proceedings of the 15th International Conference on Smart Card Research and Advanced Applications, CARDIS 2016, held in Cannes, France, in November 2016. The 15 revised full papers presented in this book were carefully reviewed and selected from 29 submissions. The focus of the conference was on all aspects of the design, development, deployment, validation, and application of smart cards or smart personal devices.