1.

Record Nr.	UNINA9910483355603321
Titolo	Smart Card Research and Advanced Applications : 11th International Conference, CARDIS 2012, Graz, Austria, November 28-30, 2012, Revised Selected Papers / / edited by Stefan Mangard
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2013
ISBN	3-642-37288-0
Edizione	[1st ed. 2013.]
Descrizione fisica	1 online resource (XII, 297 p. 98 illus.)
Collana	Security and Cryptology ; ; 7771
Disciplina	004.6
Soggetti	Computer communication systems Data encryption (Computer science) Management information systems Computer science Algorithms Software engineering Computer security Computer Communication Networks Cryptology Management of Computing and Information Systems Algorithm Analysis and Problem Complexity Software Engineering Systems and Data Security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di contenuto	Towards the Hardware Accelerated Defensive Virtual Machine – Type and Bound Protection -- Dynamic Fault Injection Countermeasure: A New Conception of Java Card Security -- Java Card Combined Attacks with Localization-Agnostic Fault -- Improved (and Practical) Public-Key Authentication for UHF RFID. Unlinkable Attribute-Based Credentials with Practical Revocation on Smart-Cards -- On the Use of Shamir’s Secret Sharing against Side-Channel Analysis -- Secure Multiple SBoxes Implementation with Arithmetically Masked Input -- Low-Cost

Countermeasure against RPA -- Efficient Removal of Random Delays from Embedded Software Implementations Using Hidden Markov Models -- On the Implementation Aspects of Sponge-Based Authenticated Encryption for Pervasive Devices -- Compact Implementation and Performance Evaluation of Hash Functions in ATtiny Devices -- Putting together What Fits together - GrÆStl -- Memory Access Pattern Protection for Resource-Constrained Devices -- Multipurpose Cryptographic Primitive ARMADILLO3 -- Improving Side-Channel Analysis with Optimal Linear Transforms -- SCA with Magnitude Squared Coherence -- Strengths and Limitations of High-Resolution Electromagnetic Field Measurements for Side-Channel Analysis -- Efficient Template Attacks Based on Probabilistic Multi-class Support Vector Machines -- Defensive Leakage Camouflage.

Sommario/riassunto

This book constitutes the thoroughly refereed post-conference proceedings of the 11th International Conference on Smart Card Research and Advanced Applications, CARDIS 2012, held in Graz, Austria, in November 2012. The 18 revised full papers presented together with an invited talk were carefully reviewed and selected from 48 submissions. The papers are organized in topical sections on Java card security, protocols, side-channel attacks, implementations, and implementations for resource-constrained devices.