Constructive Side-Channel Analysis and Secure Design [6th International Workshop, COSADE 2015, Berlin, Germany, April 13-14, 2015. Revised Selected Papers /

Mangard, Stefan
Poschmann, Axel Y

Computer science | Computer Communication Networks | Data protection | Data encryption (Computer science) | Computer software | Computational complexity | Information Systems | Computer Science | Data Encryption | Computer Communication Networks | Systems and Data Security | Management of Computing and Information Systems | Algorithm Analysis and Problem Complexity | Discrete Mathematics in Computer Science

Monografía

This book constitutes the thoroughly refereed post-conference proceedings of the 6th International Workshop, COSADE 2015, held in Berlin, Germany, in April 2015. The 17 revised full papers presented were carefully selected from 48 submissions. the focus of this workshop was on following topics: side-channel attacks, FPGA countermeasures, timing attacks and countermeasures, fault attacks, countermeasures, and Hands-on Side-channel analysis

Título: Constructive Side-Channel Analysis and Secure Design Recurso electrónico] :] 6th International Workshop, COSADE 2015, Berlin, Germany, April 13-14, 2015. Revised Selected Papers edited by Stefan Mangard, Axel Y. Poschmann

Mención de serie: Lecture Notes in Computer Science 9064

Contenido: Side-Channel Attacks -- Improving Non-Profiled Attacks on Exponentiations Based on Clustering and Extracting Leakage from Multi-Channel High-Resolution EM Measurements -- Template Attacks vs. Machine Learning Revisited (and the Curse of Dimensionality in Side-Channel Analysis) -- Efficient Selection of Time Samples for Higher-Order DPA with Projection Pursuits -- Exploring the Resilience of Some Lightweight Ciphers Against Profiled Single Trace Attacks -- Two Operands of Multipliers in Side-Channel Attack -- FPGA

Countermeasures -- Evaluating the Duplication of Dual-Rail Precharge Logics on FPGAs -- Side-Channel Protection by Randomizing Look-Up Tables on Reconfigurable Hardware -- Timing Attacks and Countermeasures -- A Faster and More Realistic Flush+Reload Attack on AES -- Faster software for fast endomorphisms -- Toward Secure Implementation of McEliece Decryption -- Fault Attacks -- Fault Injection with a new favor: Memetic Algorithms make a difference -- Differential Fault Intensity Analysis on PRESENT and LED Block Ciphers -- A Biased Fault Attack on the Time Redundancy Countermeasure for AES -- Countermeasures -- Faster Mask Conversion with Lookup Tables -- Towards Evaluating DPA Countermeasures for Keccak on a Real ASIC -- Hands-on Side-Channel Analysis Side-Channel Security Analysis of Ultra-Low-Power FRAM-based MCUs -- Side Channel Attacks on Smartphones and Embedded Devices using Standard Radio Equipment

Detalles del sistema: Modo de acceso: world wide web

Fuente de adquisición directa: Springer (e-Books)

ISBN: 9783319214764 978-3-319-21476-4 9783319214757

Autores: Mangard, Stefan Poschmann, Axel Y
