1.

Record Nr.	UNINA9910337635903321
Titolo	Automated Methods in Cryptographic Fault Analysis / / edited by Jakub Breier, Xiaolu Hou, Shivam Bhasin
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2019
ISBN	3-030-11333-7
Edizione	[1st ed. 2019.]
Descrizione fisica	1 online resource (342 pages)
Disciplina	005.82 005.8
Soggetti	Electronic circuits Microprocessors Electronics Microelectronics Circuits and Systems Processor Architectures Electronics and Microelectronics, Instrumentation
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Chapter 1. Introduction to Fault Analysis in Cryptography -- Part I. Automated Fault Analysis of Symmetric Block Ciphers -- Chapter 2. ExpFault: An Automated Framework for Block Cipher Fault Analysis -- Chapter 3. Exploitable Fault Space Characterization: A Complementary Approach -- Chapter 4. Differential Fault Analysis Automation on Assembly Code -- Chapter 5. An Automated Framework for Analysis and Evaluation of Algebraic Fault Attacks on Lightweight Block Ciphers -- Chapter 6. Automatic construction of fault attacks on cryptographic hardware implementations -- Part II. Automated Design and Deployment of Fault Countermeasures -- Chapter 7. Automated Deployment of Software Encoding Countermeasure -- Chapter 8. Idempotent Instructions to Counter Fault Analysis Attacks -- Chapter 9. Differential Fault Attack Resistant Hardware Design Automation -- Part III. Automated Analysis of Fault Countermeasures -- Chapter 10. Automated Evaluation of Software Encoding Schemes -- Chapter 11.

Automated Evaluation of Concurrent Error Detection Code Protected Hardware Implementations -- Chapter 12. Fault Analysis Assisted by Simulation -- Part IV. Automated Fault Attack Experiments -- Chapter 13. Optimizing Electromagnetic Fault Injection with Genetic Algorithms -- Chapter 14. Automated Profiling Method for Laser Fault Injection in FPGAs.

Sommario/riassunto

This book presents a collection of automated methods that are useful for different aspects of fault analysis in cryptography. The first part focuses on automated analysis of symmetric cipher design specifications, software implementations, and hardware circuits. The second part provides automated deployment of countermeasures. The third part provides automated evaluation of countermeasures against fault attacks. Finally, the fourth part focuses on automating fault attack experiments. The presented methods enable software developers, circuit designers, and cryptographers to test and harden their products. Offers a complete perspective on protecting block ciphers against fault attacks – from analysis to deployment; Provides automated methods for each stage, supported by evaluation and case studies; Describes current fault analysis approaches, together with countermeasures; Includes detailed description of prototypes for each automation method that can be easily implemented and put into industrial applications.