

Contents

Part I Introductory Material

- 1 Side-Channel Analysis and Its Relevance to Fault Attacks 3**
Elisabeth Oswald and François-Xavier Standaert

Part II Fault Analysis in Secret Key Cryptography

- 2 Attacking Block Ciphers. 19**
Christophe Clavier
- 3 Differential Fault Analysis of DES. 37**
Matthieu Rivain
- 4 Differential Fault Analysis of the Advanced
Encryption Standard 55**
Christophe Giraud
- 5 Countermeasures for Symmetric Key Ciphers. 73**
Jörn-Marc Schmidt and Marcel Medwed
- 6 On Countermeasures Against Fault Attacks
on the Advanced Encryption Standard 89**
Kaouthar Bousselam, Giorgio Di Natale, Marie-Lise Flottes
and Bruno Rouzeyre

Part III Fault Analysis in Public Key Cryptography

7	A Survey of Differential Fault Analysis Against Classical RSA Implementations.	111
	Alexandre Berzati, Cécile Canovas-Dumas and Louis Goubin	
8	Fault Attacks Against RSA-CRT Implementation	125
	Chong Hee Kim and Jean-Jacques Quisquater	
9	Fault Attacks on Elliptic Curve Cryptosystems	137
	Abdulaziz Alkhoraidly, Agustín Domínguez-Oviedo and M. Anwar Hasan	
10	On Countermeasures Against Fault Attacks on Elliptic Curve Cryptography Using Fault Detection.	157
	Arash Hariri and Arash Reyhani-Masoleh	
11	Design of Cryptographic Devices Resilient to Fault Injection Attacks Using Nonlinear Robust Codes.	171
	Kahraman D. Akdemir, Zhen Wang, Mark Karpovsky and Berk Sunar	
12	Lattice-Based Fault Attacks on Signatures.	201
	Phong Q. Nguyen and Mehdi Tibouchi	
13	Fault Attacks on Pairing-Based Cryptography.	221
	Nadia El Mrabet, Dan Page and Frederik Vercauteren	

Part IV Miscellaneous

14	Fault Attacks on Stream Ciphers	239
	Alessandro Barengi and Elena Trichina	
15	Interaction Between Fault Attack Countermeasures and the Resistance Against Power Analysis Attacks	257
	Francesco Regazzoni, Luca Breveglieri, Paolo Ienne and Israel Koren	

Part V Implementing Fault Attacks

16 Injection Technologies for Fault Attacks on Microprocessors 275
Alessandro Barengi, Guido M. Bertoni, Luca Breveglieri,
Mauro Pelliccioli and Gerardo Pelosi

17 Global Faults on Cryptographic Circuits 295
Sylvain Guilley and Jean-Luc Danger

**18 Fault Injection and Key Retrieval Experiments
on an Evaluation Board** 313
Junko Takahashi, Toshinori Fukunaga, Shigeto Gomisawa,
Yang Li, Kazuo Sakiyama and Kazuo Ohta

References 333

Fault Analysis in Cryptography

Joye, M.; Tunstall, M. (Eds.)

2012, XVI, 356 p., Hardcover

ISBN: 978-3-642-29655-0