

Contents

1	Introduction to Fault Analysis in Cryptography	1
	Jakub Breier and Xiaolu Hou	
Part I Automated Fault Analysis of Symmetric Block Ciphers		
2	ExpFault: An Automated Framework for Block Cipher Fault Analysis	13
	Sayandeep Saha, Debdeep Mukhopadhyay, and Pallab Dasgupta	
3	Exploitable Fault Space Characterization: A Complementary Approach	59
	Sayandeep Saha, Dirmanto Jap, Sikhar Patranabis, Debdeep Mukhopadhyay, Shivam Bhasin, and Pallab Dasgupta	
4	Differential Fault Analysis Automation on Assembly Code	89
	Jakub Breier, Xiaolu Hou, and Yang Liu	
5	An Automated Framework for Analysis and Evaluation of Algebraic Fault Attacks on Lightweight Block Ciphers.....	121
	Fan Zhang, Bolin Yang, Shize Guo, Xinjie Zhao, Tao Wang, Francois-Xavier Standaert, and Dawu Gu	
6	Automatic Construction of Fault Attacks on Cryptographic Hardware Implementations	151
	Ilia Polian, Mael Gay, Tobias Paxian, Matthias Sauer, and Bernd Becker	
Part II Automated Design and Deployment of Fault Countermeasures		
7	Automated Deployment of Software Encoding Countermeasure	173
	Jakub Breier and Xiaolu Hou	

8	Idempotent Instructions to Counter Fault Analysis Attacks	195
	Sikhar Patranabis and Debdeep Mukhopadhyay	
9	Differential Fault Attack Resistant Hardware Design Automation ...	209
	Mustafa Khairallah, Jakub Breier, Shivam Bhasin, and Anupam Chattopadhyay	
 Part III Automated Analysis of Fault Countermeasures		
10	Automated Evaluation of Software Encoding Schemes	223
	Jakub Breier, Dirmanto Jap, and Shivam Bhasin	
11	Automated Evaluation of Concurrent Error Detection Code Protected Hardware Implementations	247
	Dirmanto Jap, Jakub Breier, Shivam Bhasin, and Anupam Chattopadhyay	
12	Fault Analysis Assisted by Simulation	263
	Kais Chibani, Adrien Facon, Sylvain Guilley, Damien Marion, Yves Mathieu, Laurent Sauvage, Youssef Souissi, and Sofiane Takarabt	
 Part IV Automated Fault Attack Experiments		
13	Optimizing Electromagnetic Fault Injection with Genetic Algorithms.....	281
	Antun Maldini, Niels Samwel, Stjepan Picek, and Lejla Batina	
14	Automated Profiling Method for Laser Fault Injection in FPGAs	301
	Jakub Breier, Wei He, Shivam Bhasin, Dirmanto Jap, Samuel Chef, Hock Guan Ong, and Chee Lip Gan	
	Index.....	327