Table of Contents
2008 5th Workshop on Fault Diagnosis and Tolerance in Cryptography

Preface
Organizing Committee
Program Committee

Section One - Overview of Side Channel Attacks and Countermeasures
Silicon-level Solutions to Counteract Passive and Active Attacks
Sylvain Guilley, Laurent Sauvage, Jean-Luc Danger, Nidhal Selmane, and Renaud Pacalet
Aspects of the Development of Secure and Fault-Resistant Hardware
Wieland Fischer

Section Two - Differential Fault Analysis
Improved Differential Fault Analysis on CLEFIA
Junko Takahashi and Toshinori Fukunaga
Masking Does Not Protect Against Differential Fault Attacks
Arnaud Boscher and Helena Handschuh
Comparative Analysis of Robust Fault Attack Resistant Architectures for Public and Private Cryptosystems
Konrad J. Kulikowski, Zhen Wang, and Mark G. Karpovsky

Section Three - Fault Security of Hardware and Software
A Practical Fault Attack on Square and Multiply
Jörn-Marc Schmidt and Christoph Herbst
Exploiting Hardware Performance Counters
Leif Uhsadel, Andy Georges, and Ingrid Verbauwhede
A Generic Fault Countermeasure Providing Data and Program Flow Integrity
Marcel Medwed and Jörn-Marc Schmidt

Section Four - Fault Security of Elliptic Curve Cryptography
Error Detection for Borrow-Save Adders Dedicated to ECC Unit
Julien Francq, Jean-Baptiste Rigaud, Pascal Manet, Assia Tria, and Arnaud Tisserand
On the Security of a Unified Countermeasure
Marc Joye
Fault Attack on Elliptic Curve Montgomery Ladder Implementation
Pierre-Alain Fouque, Reynald Lercier, Denis Réal, and Frédéric Valette

Section Five - Fault Security of Public Key Cryptography

In(security) Against Fault Injection Attacks for CRT-RSA Implementations
Alexandre Berzati, Cécile Canovas, and Louis Goubin

Attacks on Authentication and Signature Schemes Involving Corruption of Public Key (Modulus)
Michael Kara-Ivaniov, Eran Iceland, and Aviad Kipnis

Author Index

vi