Proceedings

FDTC 2008

Fault Diagnosis and Tolerance in Cryptography

10 August 2008
Washington, DC, USA

CPS Conference Publishing Services

Los Alamitos, California

Washington • Tokyo

IEEE computer society

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

Preface vii
Organizing Committee ix
Program Committee x

Section One - Overview of Side Channel Attacks and Countermeasures

Silicon-level Solutions to Counteract Passive and Active Attacks 3
Sylvain Guilley, Laurent Sauvage, Jean-Luc Danger, Nidhal Selmane, and Renaud Pacalet

Aspects of the Development of Secure and Fault-Resistant Hardware 18
Wieland Fischer

Section Two - Differential Fault Analysis

Improved Differential Fault Analysis on CLEFIA 25
Junko Takahashi and Toshinori Fukunaga

Masking Does Not Protect Against Differential Fault Attacks 35
Arnaud Boscher and Helena Handschuh

Comparative Analysis of Robust Fault Attack Resistant Architectures for Public and Private Cryptosystems 41
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 53
Jörn-Marc Schmidt and Christoph Herbst

Exploiting Hardware Performance Counters 59
Leif Uhsadel, Andy Georges, and Ingrid Verbauwhede

A Generic Fault Countermeasure Providing Data and Program Flow Integrity 68
Marcel Medwed and Jörn-Marc Schmidt

Section Four - Fault Security of Elliptic Curve Cryptography

Error Detection for Borrow-Save Adders Dedicated to ECC Unit 77
Julien Francq, Jean-Baptiste Rigaud, Pascal Manet, Assia Tria, and Arnaud Tisserand

On the Security of a Unified Countermeasure 87
Marc Joye

Fault Attack on Elliptic Curve Montgomery Ladder Implementation 92
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 101
Alexandre Berzati, Cécile Canovas, and Louis Goubin

Attacks on Authentication and Signature Schemes Involving Corruption of Public Key (Modulus) 108
Michael Kara-Ivaniov, Eran Iceland, and Aviad Kipnis

Author Index 116