Workshop on Fault Diagnosis and Tolerance in Cryptography
FDTC 2007

10 September 2007
Vienna, Austria
Preface .......................................................................................................... vii
Program Organization ................................................................................... ix
Program Committee .........................................................................................x

Invited Paper

Securing Flash Technology.................................................................................................................. 3
Helena Handschuh and Elena Trichina

Session 1: Fault Attacks against Public Key Cryptosystems

How Can We Overcome Both Side Channel Analysis and Fault Attacks on RSA-CRT? ......................... 21
Chong Hee Kim and Jean-Jacques Quisquater
Montgomery Multiplication with Redundancy Check ............................................................................. 30
Khanh Nguyen and Michael Tunstall
Fault Detection Structures for the Montgomery Multiplication over Binary Extension Field.................. 37
Arash Hariri and Arash Reyhani-Masoleh

Session 2: Fault Attacks against AES Implementations

A Structure-Independent Approach for Fault Detection Hardware Implementations
of the Advanced Encryption Standard .................................................................................................. 47
Mehran Mozaffari-Kermani and Arash Reyhani-Masoleh
A Novel Double-Data-Rate AES Architecture Resistant against Fault Injection............................... 54
P. Maistri, P. Vanhauwaert, and R. Leveugle
DFA Mechanism on the AES Key Schedule .......................................................................................... 62
Junko Takahashi, Toshinori Fukunaga, and Kimihiro Yamakoshi

Session 3: Countermeasures and Attack Techniques

Countermeasures against Branch Target Buffer Attacks ...................................................................... 75
Giovanni Agosta, Luca Breveglieri, Gerardo Pelosi, and Israel Koren
Cheap Hardware Parallelism Implies Cheap Security ............................................................................ 80
Onur Aciqmez and Jean-Pierre Seifert
Passive and Active Combined Attacks: Combining Fault Attacks and Side Channel Analysis.............. 92
Frederic Amiel, Karine Villegas, Benoit Feix, and Louis Marcel
Session 4: Fault Attacks against ECC Implementations

Tate Pairing with Strong Fault Resiliency ................................................................. 103
   Erdinc Öztürk, Gunnar Gaubatz, and Berk Sunar

Register Transfer Level Concurrent Error Detection in Elliptic Curve Crypto Implementations ........ 112
   Richard Stern, Nikhil Joshi, Kaijie Wu, and Ramesh Karri

Author Index .............................................................................................................. 120