Call for participation

FDTC 2009
Fault Diagnosis and Tolerance in Cryptography

6th Workshop on Fault Diagnosis and Tolerance in Cryptography – FDTC 2009

September 6, 2009 Lausanne, Switzerland

Co-located with CHES 2009, 7-9 September, 2009, in Lausanne

Workshop web site: http://conferenze.dei.polimi.it/FDTC09/

General co-chairs: Luca Breveglieri and Israel Koren

Program co-chairs: David Naccache and Elisabeth Oswald

Invited talks chair: Jean-Pierre Seifert

Technical Program

Invited paper: *Blinded fault resistant exponentiation revisited,* A. Boscher, H. Handshuh and E. Trichina

Session 1 - Novel fault attacks 1

1. Optical fault attacks on AES: a threat in violet , J.M. Schmidt, M. Hutter and T. Plos

2. Low voltage fault attacks on the RSA cryptosystem, A. Barenghi, G. Bertoni, E. Parrinello and G. Pelosi

Fault attack on Schnorr based identification and signature schemes, P.A. Fouque, D. Masgana and F. Valette

Session 2 - Protecting against fault attacks

1. Protecting RSA against fault attacks: the embedding method, M. Joye

2. Securing the elliptic curve Montgomery ladder against fault attacks, N. Ebeid and R. Lambert

3. Securing AES implementation against fault attacks, L. Genelle, C. Giraud and E. Prouff

Invited paper: *KeeLoq and side-channel analysis - Evolution of an attack,* Christof Paar

Session 3 - Novel fault attacks 2

1. WDDL is protected against fault attacks, N. Selmane, S. Bhasin, S. Guilley, T. Graba and J.L. Danger

2. Practical fault attack on a cryptographic LSI with ISO/IEC 18033-3 block ciphers, Fukunaga and J. Takahashi

3. A fault attack on ECDSA, J.M. Schmidt and M. Medwed

Session 4 - Implementations of fault attacks

1. Fault analysis of the stream cipher Snow 3G, B. Debraize and I.M. Corbella

2. Using optical emission analysis for estimating contribution to power analysis, S. Skorobogatov

3. Differential fault analysis on SHACAL-1, R. Li, C. Li and C. Gong