WORKSHOP ON FAULT DIAGNOSIS AND TOLERANCE IN CRYPTOGRAPHY - FDTC 2008 - PROGRAMME

The workshop is located in the Colonial Room of the Mayflower Marriot Renaissance Hotel, Whashington DC.

Time	Session & Title	Authors
07:30-08:30	**Registration and Continental Breakfast**	
08:30-08:45	**Opening Remarks - L. Breveglieri and I. Koren**	
08:45-09:25	**Silicon-Level Solutions to counteract Passive and Active Attacks - invited paper**	**Sylvain Guilley**, Laurent Sauvage, Jean-Luc Danger, Nidhal Selmane, Renaud Pacalet **- introduced by L. Breveglier**
	Session 1 - Differential Fault Analysis - Chair: G. Bertoni	
09:25-09:50	Improved Differential Fault Analysis on CLEFIA	**Junko Takahashi**, Toshinori Fukunaga
09:50-10:15	Masking does not protect against Differential Fault Attacks	Helena Handschuh, **Arnaud Boscher**
10:15-10:40	Comparative Analysis of Robust Fault Attack Resistant Architectures for Public and Private Cryptosystems	Konrad J. Kulikowski, Zhen Wang, **Mark G. Karpovsky**
10:40-11:00	**Coffee Break**	
	Session 2 - Fault Security of HW and SW - Chair: M. Joye	
11:00-11:25	A Practical Attack on Square and Multiply	**Jörn-Marc Schmidt**, Christoph Herbst
11:25-11:50	Exploiting Hardware Performance Counters	**Leif Uhsadel**, Andy Georges, Ingrid Verbauwhede
11:50-12:15	A Generic Fault Countermeasure providing Data and Program Flow Integrity	**Marcel Medwed,** Jörn-Marc Schmidt
12:15-13:45	**Lunch**	
13:45-14:25	**Aspects of the Development of Fault Resistant Hardware - invited paper**	**Wieland Fischer - introduced by J-P Seifert**
	Session 3 - Fault Security of Elliptic Curves - Chair: J-P Seifert	
14:25-14:50	Fault-Tolerant ECC Unit using Parity preserving Logic Gates	**Julien Francq**, Jean-Baptiste Rigaud, Pascal Manet, Assia Tria
14:50-15:15	On the Security of a Unified Countermeasure	**Marc Joye**
15:15-15:40	Fault Attack on Elliptic Curve with Montgomery Ladder Implementation	Pierre-Alain Fouque, Reynald Lercier, **Denis Réal**, Frédéric Valette
15:40-16:00	**Coffee Break**	
	Session 4 - Fault Security of Public Key - Chair: A. Tria	
16:00-16:25	Security against Fault Injection Attacks for CRT-RSA Implementations	**Alexandre Berzati**, Cecile Canovas, Louis Goubin
16:25-16:50	Attacks on Authentication and Signature Schemes involving Corruption of Public Key (Modulus)	**Michael Kara-Ivanov**, Eran Iceland, Aviad Kipnis
16.50-17:00	**Closing Remarks and Farewell - L. Breveglieri and I. Koren**	