2nd Workshop on Fault Diagnosis and Tolerance in Cryptography

Luca Breveglieri[1] and Israel Koren[2]

[1]Dipartimento di Elettronica e Informazione, Politecnico di Milano, Milano, ITALY

[2]Department of Electrical & Computer Engineering, University of Massachusetts, Amherst, USA

1st Workshop on Fault Diagnosis and Tolerance in Cryptography

Florence, ITALY June 30, 2004

DSN 2004 – Intern'l Conf. on Dependable Systems and Networks

IEEE Transactions on Computers, June 2006

SPECIAL SECTION ON FAULT DIAGNOSIS AND TOLERANCE IN CRYPTOGRAPHY

9:00 – 09:15	**Welcome and Opening Remarks** ***Luca Breveglieri*, Politecnico di Milano, Milano, Italy,** ***Israel Koren*, University of Massachusetts, Amherst, MA, USA**
9:15 – 10:25	**Session 1: Cryptographic Systems and Fault Attacks – Overview** ***Invited lecture*: On Fault Attacks and Trusted Computing,** ***Jean Pierre Seifert*.** **Robust Codes for Fault Attack Resistant Cryptographic Hardware,** ***Konrad Kulikowski, Mark Karpovsky, Alexander Taubin***
10:25 – 10:45	**Coffee break**
10:45 – 12:25	**Session 2: Attack and Protection Methods of Secret and Public Key** **1. Round Reduction Using Faults, *Michael Tunstall, Hamid Choukri*** **2. Sign Change Fault Attacks On Elliptic Curve Cryptosystems,** ***Martin Otto, Johannes Bloemer, Jean Pierre Seifert*** **3. Robust Finite Field Arithmetic for Fault-Tolerant Public-Key Cryptography, *Gunnar Gaubatz, Berk Sunar*** **4. A Fault Attack on Pairing Based Cryptography,** ***Daniel Page, Fre Vercauteren***
12:25 – 13:45	**Buffet lunch in hotel quadrangle**

13:45 – 15.25	**Session 3: Evaluation Models for Fault Attacks & Countermeasures** **1. Cryptographic Key Reliable Lifetimes: Bounding the Risk of Key Exposure in the Presence of Faults, *Alfonso De Gregorio*** **2. An Adversarial Model for Fault Analysis against Low-Cost Cryptographic Devices, *Kerstin Lemke, Christof Paar*** **3. Crypto BIST: A Built-In Self Test Architecture for Crypto Chips, *Bo Yang, Ramesh Karri*** **4. A Comparative Cost / Security Analysis of Fault Attack Countermeasures, *Francois-Xavier Standaert, Tal Malkin, Moti Yung***
15.25 – 15.45	**Coffee Break**
15.45 – 17.10	**Session 4: Attack and Protection Methods for RSA** **1. Practical Fault Countermeasures for Chinese Remaindering Based RSA, *Marc Joye, Mathieu Ciet*** **2. Incorporating Error Detection in a RSA Architecture, *Paolo Maistri, Luca Breveglieri, Israel Koren*** **3. Fault-resistant RSA Implementation, *Christophe Giraud*** **4. Injection of Multiple Bit-Flips for Counter Measures Validation, *Régis Leveugle, K. Hadjiat, A. Ammari***
17.10-17.15	**Closing Remarks and Farewell**

Program committee:

- **Luca BREVEGLIERI, Politecnico di Milano, Milano, Italy**
- **Joan DAEMEN, STMicroelectronics, Zaventem, Belgium**
- **Christophe GIRAUD, Oberthur Card Systems, Puteaux, France**
- **Shay GUERON, Intel Corporation, Israel, and University of Haifa, Israel**
- **Marc JOYE, Gemplus & CIM-PACA, La Ciotat , France**
- **Mark KARPOVSKY, University of Boston, Boston, Massachusetts, USA**
- **Çetin KAYA KOÇ, Oregon State University, Corvallis, Oregon, USA**
- **Israel KOREN, University of Massachusetts, Amherst, Massachusetts, USA**
- **Régis LEVEUGLE, TIMA Laboratory, Grenoble, France**
- **Ramesh KARRI, Polytechnic University, Brooklyn, New York, USA**
- **David NACCACHE, Sorbonne, Paris**
- **Christof PAAR, University of Ruhr, Bochum, Germany**
- **Jean Pierre SEIFERT, Intel Corp., Oregon, USA**

20 manuscripts submitted

13 papers accepted for presentation

118 participants