FDTC 2011
Fault Diagnosis and Tolerance in Cryptography

8th Workshop on Fault Diagnosis and Tolerance in Cryptography

September 28, 2011 • Nara, Japan

(one day before CHES 2011)

Nara (Todai-ji Culture Center)

Important dates

Submission deadline: **May 2, 2011**
Notification of acceptance: June 6, 2011
Camera-ready version: July 8, 2011
Workshop: September 28, 2011

In recent years applied cryptography has developed considerably, to satisfy the increasing security requirements of various information technology disciplines, e.g., telecommunications, networking, data base systems and mobile applications. Cryptosystems are inherently computationally complex and in order to satisfy the high throughput requirements of many applications, they are often implemented by means of either VLSI devices (crypto-accelerators) or highly optimised software routines (crypto-libraries) and are used via suitable (network) protocols.

The high complexity of such implementations raises concerns regarding their reliability. Research is therefore needed to develop methodologies and techniques for designing robust cryptographic systems (both hardware and software), and to protect them against both accidental faults and intentional intrusions and attacks, in particular those based on the malicious injection of faults into the device for the purpose of extracting the secret key.

This annual workshop was started in 2004 and had follow-ups in 2005, 2006, 2007, 2008, 2009, and 2010.

Topics of interest include but are not limited to:

- modeling the reliability of cryptographic systems and protocols;
- inherently reliable cryptographic systems and algorithms;
- faults and fault models for cryptographic devices (HW and SW);
- reliability-based attack procedures on cryptographic systems (fault-injection attacks) and protocols;
- adapting classical fault diagnosis and tolerance techniques to cryptographic systems;
- novel fault diagnosis and tolerance techniques for cryptographic systems;
- attacks exploiting micro-architecture components (cache, branch predictor, etc.);
- physical protection against attacks;
- fault injection based attacks using FIB laser and chemistry;
- case studies of attacks, reliability and fault diagnosis and tolerance techniques in cryptographic systems.

Instructions for authors

Submissions must not substantially duplicate work that any of the authors have published elsewhere or that have been submitted in parallel with any other conference or workshop. Submissions should be anonymous, with no author names, affiliations, acknowledgments or obvious references. Papers should be at most 10 pages (including the bibliography and appendices), with at least 11pt font and reasonable margins.

At least one author of each accepted paper must register with the workshop and present the paper in order to be included in the proceedings.

For submission instructions and further information please point your web-browser to:

`http://conferenze.dei.polimi.it/FDTC11/`

Proceedings

Accepted papers will be published by Conference Publishing Services (CPS) and will be distributed at the time of the workshop.