4th Workshop on Fault Diagnosis and Tolerance in Cryptography

General Co-chairs: Luca Breveglieri\textsuperscript{1} and Israel Koren\textsuperscript{2}

Program Co-chairs: David Naccache\textsuperscript{3} and Jean Pierre Seifert\textsuperscript{4}

\textsuperscript{1} Politecnico di Milano, Milano, Italy
\textsuperscript{2} University of Massachusetts, Amherst, USA
\textsuperscript{3} École Normale Supérieure de Paris, France
\textsuperscript{4} Sisa, Samsung, USA
1st Workshop on Fault Diagnosis and Tolerance in Cryptography

Florence, ITALY    June 30, 2004

DSN 2004 – Intern’l Conference on Dependable Systems and Networks

25 participants
No official proceedings
2nd Workshop on Fault Diagnosis and Tolerance in Cryptography

Edinburgh, UK  September 2, 2005

CHES 2005 – Workshop on Cryptographic Hardware and Embedded Systems

118 participants

No official proceedings

IEEE Transactions on Computers, Sept. 2006

SPECIAL SECTION ON FAULT DIAGNOSIS AND TOLERANCE IN CRYPTOGRAPHY
3rd Workshop on Fault Diagnosis and Tolerance in Cryptography

Yokohama, Japan  October 10, 2006

CHES 2006 – Workshop on Cryptographic Hardware and Embedded Systems

103 participants

The 1st FDTC to have official proceedings (by Springer-Verlag)
4th Workshop on Fault Diagnosis and Tolerance in Cryptography

Vienna, Austria  September 10, 2007

CHES 2007 – Workshop on Cryptographic Hardware and Embedded Systems

73 participants

FDTC 2007 Fault Diagnosis and Tolerance in Cryptography

Official proceedings by IEEE Computer Society Press
<table>
<thead>
<tr>
<th>Time</th>
<th>Session 1: Fault Attacks on Public Key Cryptosystems</th>
<th>1st Invited Talk: Securing Flash Technology</th>
<th>Session 2: Fault Attacks on ECCs</th>
</tr>
</thead>
<tbody>
<tr>
<td>8:45 – 9:00</td>
<td>Welcome and Opening Remarks</td>
<td>1st Invited Talk: Securing Flash Technology</td>
<td>11:15 - 12:05</td>
</tr>
<tr>
<td>9:00 – 9:40</td>
<td>Israel Koren, University of Massachusetts, Amherst, MA, USA</td>
<td>Helena Handshuh, Elena Trichina</td>
<td>11:15 - 12:05</td>
</tr>
<tr>
<td></td>
<td>1. How can we overcome both Side Channel Analysis and Fault Attacks on RSA-CRT ?</td>
<td>1. How can we overcome both Side Channel Analysis and Fault Attacks on RSA-CRT ?</td>
<td>11:15 - 12:05</td>
</tr>
<tr>
<td></td>
<td>Chong Hee Kim, Jean-Jacques Quisquater</td>
<td>Chong Hee Kim, Jean-Jacques Quisquater</td>
<td>11:15 - 12:05</td>
</tr>
<tr>
<td></td>
<td>Michael Tunstall</td>
<td>Michael Tunstall</td>
<td>11:15 - 12:05</td>
</tr>
<tr>
<td></td>
<td>Arash Hariri, Arash Reyhani-Masoleh</td>
<td>Arash Hariri, Arash Reyhani-Masoleh</td>
<td>11:15 - 12:05</td>
</tr>
<tr>
<td>11:15 - 12:05</td>
<td>Session 2: Fault Attacks on ECCs</td>
<td>1st Invited Talk: Securing Flash Technology</td>
<td>11:15 - 12:05</td>
</tr>
<tr>
<td></td>
<td>1. Tate Pairing with Strong Fault Resiliency</td>
<td>1st Invited Talk: Securing Flash Technology</td>
<td>11:15 - 12:05</td>
</tr>
<tr>
<td></td>
<td>Erdinc Ozturk, Gunnar Gaubatz, Berk Sunar</td>
<td>1st Invited Talk: Securing Flash Technology</td>
<td>11:15 - 12:05</td>
</tr>
<tr>
<td></td>
<td>2. Register Transfer Level Concurrent Error Detection in Elliptic Curve Crypto Implementations</td>
<td>2. Register Transfer Level Concurrent Error Detection in Elliptic Curve Crypto Implementations</td>
<td>11:15 - 12:05</td>
</tr>
<tr>
<td></td>
<td>Richard Stern, Nikhil Joshi, Kaijie Wu, Ramesh Karri</td>
<td>2. Register Transfer Level Concurrent Error Detection in Elliptic Curve Crypto Implementations</td>
<td>11:15 - 12:05</td>
</tr>
<tr>
<td>Time</td>
<td>Event</td>
<td>Chair</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------------------------------------------------</td>
<td>----------------</td>
<td></td>
</tr>
<tr>
<td>12:05 – 13:40</td>
<td>Lunch</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1. A Structure-independent Approach for Fault Detection Hardware Implementations of the AES</td>
<td>M. Mozaffari-Kermani, A. Reyhani-Masoleh</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. A Novel Double-Data-Rate AES Architecture Resistant against Fault Injection</td>
<td>P. Maistri, P. Vanhauwaert, R. Leveugle</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. DFA Mechanism on the AES Key Schedule</td>
<td>Junko Takahashi, Toshinori Fukunaga, Kimihiro Yamakoshi</td>
<td></td>
</tr>
<tr>
<td>15:35 – 16:00</td>
<td>Coffee break</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16:00 – 17:15</td>
<td>Session 4: Countermeasures and Attack Techniques</td>
<td>Guido Bertoni</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1. Countermeasures Against Branch Target Buffer Attacks</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>G. Agosta, L. Breveglieri, I. Koren, G. Pelosi, M. Sykora</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Cheap Hardware Parallelism Implies Cheap Security</td>
<td>Onur Acicmez, Jean-Pierre Seifert</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Passive and Active Combined Attacks Combining Fault Attacks and Side Channel Analysis  (Presented by Michael Tunstall)</td>
<td>Frederic Amiel, Benoit Feix, Louis Marcel, Karine Villegas</td>
<td></td>
</tr>
<tr>
<td>17:15 – 17:30</td>
<td>Closing remarks and Farewell</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Program co-chairs:

David Naccache
École Normale
Supérieure de Paris,
France

Jean Pierre Seifert
SISA, Samsung, USA

Program committee:

Hervé Chabannes  Sagem Défense Sécurité, France
Christophe Clavier  Gemplus Corporation, France
Wieland Fischer  Infineon Corporation, Germany
Shay Gueron  University of Haifa and Intel Corporation, Israel
Ramesh Karri  Polytechnic University of Brooklyn, USA
Christof Paar  University of Ruhr
Johannes Bloemer  University of Paderborn
Régis Leveugle  TIMA Lab. Grenoble
Paul Karger  IBM
Çetin Kaya Koç  Oregon State University, USA
Pierre-Yvan Liardet  STMicroelectronics Corporation, France
Sandra Marcello  Thales Corporation, France
Elisabeth Oswald  Graz University of Technology, Austria
Elena Trichina  Spansion Corporation, USA
Helena Handschuh  Spanion
Michael Tunstall  Royal Holloway University of London, UK
Kaiji Wu  University of Illinois at Chicago, USA
Mehdi Laurent Akka  Texas Instruments
Nora Dabbous  Ingenico
Onur Aciicmez  Samsung
Eran Tromer  Weizman Institute
Special Thanks to the registration support

Mrs. Irmgard Kühn, Communication Security Center, Ruhr University, Bochum, Germany

Prof. Christof Paar, General Chair, SHARCS
Statistics

16 manuscripts submitted

11 papers accepted for presentation

Participants:

- France  18
- Germany  14
- Japan  9
- USA  7
- Belgium, Czech Republic  4
- UK, Israel  3
- Canada, Italy, Netherlands  2
- Austria, Slovakia, Ireland, S. Korea, Switzerland, Singapore, Iran  1