The Non-Invasive Attack Testing Workshop (NIAT 2011)

September 25-27, 2011
Nara Hotel (Reception)
Todai-ji Cultural Center (Technical Programs)
Nara, JAPAN

Organized by:

Cryptographic Module Validation Program (CMVP)
National Institute of Advanced Industrial Science and Technology (AIST)

Sponsored by:

Cryptography Research
Riscure

Day 0 (Nara Hotel) Sunday, September 25, 2011	
17:30	**Registration**
18:00 – 20:00 (2 hours)	**Reception**

Day 1 (Todai-ji Cultural Celter) Monday, September 26, 2011	
9:00	**Registration**
9:30-10:30 (60 minutes)	**Introduction**
9:30 9:40 9:50	• Opening Remarks *Randall Easter,* CMVP NIST • Workshop Overview *Akashi Satoh,* AIST • CMVP and FIPS Development *Randall Easter,* CMVP NIST
10:30-11:10 (40 minutes)	**Break / Vendor Demo**

11:10-12:20 (70 minutes)	**Technical Session 1 - Attack Methods 1 –** *Session Chair: Hirofumi Sakane*
11:10 11:45	• Novel Applications of Wavelet Transforms based Side-Channel Analysis *Youssef Souissi[1], M.Aziz el Aabid[1,2], Jean-Luc Danger[1,3], Sylvain Guilley[1,3], Nicolas Debande[1,4]* [1] Telecom Paris-Tech, [2] UniversitéParis 8, [3] Secure-IC SAS, [4] Morpho • An Equidistant Message Power Attack Using Restricted Number of Traces on Reduction Algorithm *Jong-Yeon Park[1], Dong-Guk Han[1], Okyeon Yi[1], and Dooho Choi[2]* [1] Cryptography and Information Security Institute(CISI), Department of Mathematics Kookmin University [2] Electronic and Telecommunication Research Institute(ETRI)
12:20-14:00 (1 hour 40 minutes)	**Lunch (Yumekaze Hiroba)**
14:00-15:10 (70 minutes)	**Technical Session 2 - Attack Methods 2-** *Session Chair: Caroline Scace*
14:00 14:35	• Practical Electro-Magnetic Analysis *Fred de Beer, Marc Witteman, and Bartek Gedrojc* Riscure • Non-invasive Trigger-free Fault Injection Method Based on Intentional Electromagnetic Interference *Yu-ichi Hayashi, Naofumi Homma, Takeshi Sugawara, Takaaki Mizuki, Takafumi Aoki, and Hideaki Sone* Tohoku University
15:10-15:50 (40 minutes)	**Break / Vendor Demo**
15:50-17:00 (70 minutes)	**Technical Session 3 - Attack Methods 3 and Countermeasures –** *Session Chair: Kim Schaffer*
15:50 16:25	• Choosing Distinguishers for Differential Power Analysis Attacks *Elisabeth Oswald, Luke Mather, and Carolyn Whitnall* University of Bristol, Department of Computer Science • Efficient FPGA Implementation of dual-rail countermeasures using Stochastic Models *Shivam Bhasin, Sylvain Guilley, Youssef Souissi, Jean-Luc Danger* Telecom Paris-Tech
17:00	END of Day 1

Day 2 (Todai-ji Cultural Celter) Tuesday, September 27, 2011	
8:30	**Registration**
9:00-10:00 (60 minutes)	**DPA Contest Session** *Session Chair: Caroline Scace*
	• Education and open benchmarking on side-channel analysis with the DPA contests *Jean-Luc Danger, Guillaume Duc, Sylvain Guilley and Laurent Sauvage* DPA Contest • Round table discussion *Moderator: Sylvain Guilley*
10:00-10:30 (30 minutes)	**Break / Vendor Demo**
10:30-12:00 (90 minutes)	**Technical Session 4 - Test Methods and Metrics –** *Session Chair: Hirofumi Sakane*
10:30 11:05 11:40	• A testing methodology for side-channel resistance validation *Gilbert Goodwill, Benjamin Jun, Josh Jaffe, and Pankaj Rohatgi* Cryptography Research Inc. • Efficient side-channel testing for public key algorithms: RSA case study *Josh Jaffe[1], Pankaj Rohatgi[1], and Marc Witteman[2]* [1] Cryptography Research Inc. [2] Riscure • Extended discussion
12:00-13:40 (1 hour 40 minutes)	**Lunch (Yumekaze Hiroba)**
13:40-14:40 (60 minutes)	**Panel Discussion – Tool Vendor / Laboratory –** *Theme: Test Automation and Metrics* *Moderator: Randall Easter* *Panelists : BrightSight, Cryptography Research, Riscure, Secure-IC*
14:40-15:10 (30 minutes)	**Break / Vendor Demo**
15:10-17:15 (125 minutes)	**Technical Session 5 - Test Tools and Methods –** *Session Chair: Kim Schaffer*

15:10	• Side-Channel Attack Standard Evaluation Board SASEBO-W for Smartcard Testing *Toshihiro Katashita, Yohei Hori, Hirofumi Sakane, and Akashi Satoh* National Institute of Advanced Industrial Science and Technology (AIST)
15:45	• Test Apparatus for Side-Channel Resistance Compliance Testing *Michael Hutter, Jörn-Marc Schmidt, Thomas Plos, and Mario Kirschbaum* Institute for Applied Information Processing and Communications (IAIK), Graz University of Technology
16:20	• Evaluation Tools for Side-Channel Attacks: An Overview *François-Xavier Standaert* UCL Crypto Group, Université catholique de Louvain
16:55	• Extended discussion
17:15-17:25	**Concluding Remarks** *Randall Easter,* CMVP NIST
17:25	END of Day 2

Technical session presentation : 35 minutes per presenter. (25-minute presentation including introduction followed by 10-minute discussion)

Updated: 09/22/2011