The Non-Invasive Attack Testing Workshop (NIAT 2011) Accepted Papers

- **Choosing Distinguishers for Differential Power Analysis Attacks**
  Elisabeth Oswald, Luke Mather, and Carolyn Whitnall
  University of Bristol, Department of Computer Science

- **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

- **Education and open benchmarking on side-channel analysis with the DPA contests**
  Jean-Luc Danger, Guillaume Duc, Sylvain Guilley and Laurent Sauvage
  DPA Contest

- **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)

- **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

- **Efficient FPGA Implementation of dual-rail countermeasures using Stochastic Models**
  Shivam Bhasin, Sylvain Guilley, Youssef Souissi, Jean-Luc Danger
  Telecom Paris-Tech

- **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

- 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)

- 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

- Practical Electro-Magnetic Analysis
  Fred de Beer, Marc Witteman, and Bartek Gedrojc
  Riscure

- Evaluation Tools for Side-Channel Attacks: An Overview
  François-Xavier Standaert
  UCL Crypto Group, Université catholique de Louvain