Welcome to PROOFS!

PROOFS:
“Security Proofs for Embedded Systems”

Introduction to the workshop

Presentation Outline

1. Goal of PROOFS
2. Practical Aspects
   - Program
   - Invited Talk
   - Contributed Talks
   - Proceedings

Presentation Outline

1. Goal of PROOFS

2. Practical Aspects
   - Program
   - Invited Talk
   - Contributed Talks
   - Proceedings

What we intend to do:

- **For designers**: get more *confidence* in
  - security-oriented designs;
  - security-oriented CAD tools;
- **For evaluators**: do independent tests / attacks.

Presentation Outline

1. Goal of PROOFS
2. Practical Aspects
   - Program
   - Invited Talk
   - Contributed Talks
   - Proceedings

Program of the Day

- Overview
  - One invited talk
  - Seven contributed talks (4 regular, 3 short)
- The program is also in your booklet, at page 8.

1. Keynote talk:
   - “*Better Provability through Computer Architecture*”, by Timothy Sherwood

Contributed talks (regular)

1. Karine Heydemann, Nicolas Moro, Emmanuelle Encrenaz and Bruno Robisson:
    - “*Formal verification of a software countermeasure against instruction skip attacks*”
2. Pablo Rauzy and Sylvain Guilley:
    - “*A formal proof of countermeasures against fault injection attacks on CRT-RSA*”
3. Sonia Belaid, Fabrizio De Santis, Johann Heyszl, Stefan Mangard, Marcel Medwed, Jörn-Marc Schmidt, François-Xavier Standaert and Stefan Tillich:
    - “*Towards Fresh Re-Keying with Leakage-Resilient PRFs: Cipher Design Principles and Analysis*”
4. Dina Kamel, Mathieu Renauld, Denis Flandre and François-Xavier Standaert:
    - “*Understanding the Limitations and Improving the Relevance of SPICE Simulations in Side-Channel Security Evaluations*”

Contributed talks (short)

1. Durga Prasad Sahoo, Debdeep Mukhopadhyay and Rajat Subhra Chakraborty:
   - “*Formal Design of Composite Physically Unclonable Function*”
2. Kotaro Okamoto, Naofumi Homma and Takafumi Aoki:
   - “*A hierarchical graph-based approach to generating formally-proofed Galois-field multipliers*”
3. Christoph Bayer and Jean-Pierre Seifert:
   - “*Trojan-Resilient Circuits*”

- 12 submissions
- 11 PC members

Proceedings

- Hard copies are available
- Soft copies can be downloaded from the website:
  - http://perso.enst.fr/guilley/proofs2013_proceedings.pdf
- Long talks can be revised an submitted for a JCEN special section on PROOFS
- PROOFS 2014:
  1. The steering committee will mount a file for Springer/LNCS
  2. The goal is to have the best papers formally published