
Welcome to PROOFS!

PROOFS:

"Security Proofs for Embedded Systems"

Introduction to the third workshop

Presentation Outline

Presentation Outline

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

Program of the Day

- Overview
  - Two invited talks
  - Six contributed talks (5 regular, 1 short)

Invited talks

1. Keynote talks:
   - "*Verified cryptographic implementations: how far can we go?*", by Gilles Barthe
   - "*Error-Correcting Codes for Cryptography*", by Jon-Lark Kim

Contributed talks (regular)

1. David Galindo, Johann Großschädl, Zhe Liu, Praveen Kumar Vadnala and Srinivas Vivek:
   - "*Implementation and Evaluation of a Leakage-Resilient ElGamal Key Encapsulation Mechanism*"
2. Pablo Rauzy, Sylvain Guilley and Zakaria Najm:
   - "*Formally Proved Security of Assembly Code Against Power Analysis: A Case Study on Balanced Logic*"
3. Fatemeh Ganji, Shahin Tajik and Jean-Pierre Seifert:
   - "*PAC Learning of Arbiter PUFs*"
4. Bruno Robisson and Hélène Le Bouder:
   - "*Physical functions : the common factor of side-channel and fault attacks?*"
5. Xuan Thuy Ngo, Zakaria Najm, Shivam Bhasin, Sylvain Guilley and Jean-Luc Danger:
   - "*Method Taking into Account Process Dispersions to Detect Hardware Trojan Horse by Side-Channel*"

Contributed talks (short)

1. Jean-Luc Danger, Florent Lozac'h and Zouha Cherif:
   - "*Methods to Enhance the Reliability of Key Generation from Physically Unclonable Functions*"

- 10 submissions
- 13 PC members

Proceedings

- Soft copies can be downloaded from the website:
  http://www.proofs-workshop.org/program.html.

  Login: `proofs2014` Password: `pwd_4_proofs2014`
- This year, no LNCS volume
- We would like the put presentation slides online
- Long talks can be revised and submitted for a JCEN special section on PROOFS

wifi

- PARADISE_BQ
- No password, but one must accept the conditions:
  http://www.busanparadisehotel.co.kr/