Welcome to PROOFS!

PROOFS:
“Security Proofs for Embedded Systems”
Introduction to the fifth workshop

5th edition of PROOFS

PROOFS 2012: Leuven

PROOFS 2013: UCSB

PROOFS 2014: Busan

PROOFS 2015: Saint Malo

Program of the Day

- Overview
  - Two invited talks
  - Six contributed talks

Invited talks

1. Ryan KASTNER, UCSD, USA.
    - “*Moving Hardware from “Security through Obscurity” to “Secure by Design*”
2. Yuval YAROM, the University of Adelaide, Australia.
    - “*Thwarting cache-based side-channel attacks*”

Contributed talks

1. **Using Modular Extension to Provably Protect Edwards Curves Against Fault Attacks**, *Margaux Dugardin, Sylvain Guilley, Martin Moreau, Zakaria Najm and Pablo Rauzy*.
2. **Mistakes Are Proof That You Are Trying: On Verifying Software Encoding Schemes' Resistance to Fault Injection Attacks**, *Jakub Breier, Dirmanto Jap and Shivam Bhasin*.
3. **Optimal Side-Channel Attacks for Multivariate Leakages and Multiple Models**, *Nicolas Bruneau, Sylvain Guilley, Annelie Heuser, Damien Marion and Olivier Rioul*.
4. **Algebraic Security Analysis of Key Generation with Physical Unclonable Functions**, *Matthias Hiller, Michael Pehl, Gerhard Kramer and Georg Sigl*.
5. **Formal Fault Analysis of Branch Predictors: Attacking countermeasures of Asymmetric key ciphers**, *Sarani Bhattacharya and Debdeep Mukhopadhyay*.
6. **Template Attack vs. Bayes Classifier**, *Stjepan Picek, Annelie Heuser and Sylvain Guilley*.

Proceedings

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

Login: [redacted] Password: [redacted]

- We would like the put presentation slides online
- Contributed talks can be revised and submitted for a JCEN special section on PROOFS

Springer

Journal of Cryptographic Engineering