

An aerial photograph of a coastal town, likely Santa Barbara, California. The town is built on a peninsula with a bay in the foreground. The water is a deep blue, and the sky is clear. In the background, there are rolling hills and mountains. The text "Welcome to PROOFS!" is overlaid in the center of the image.

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



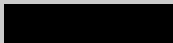
- Overview
 - Two invited talks
 - Six contributed talks

- 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”*

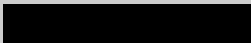
- 1 **Using Modular Extension to Provably Protect Edwards Curves Against Fault Attacks**, *Margaux Dugardin, Sylvain Guilley, Martin Moreau, Zakaria Najm and Pablo Rauzy.*
- 2 **Mistakes Are Proof That You Are Trying: On Verifying Software Encoding Schemes' Resistance to Fault Injection Attacks**, *Jakub 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.*

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

Login:



Password:



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

