Program of PROOFS

UCSB, USA, CA — Saturday August 24th, 2013

8h30–9h00	Registration, at Corwin Pavilion lobby (same location as the CHES registration), coffee. The workshop will take place in Flying A Room
9h00–9h15	Opening – Welcome, presentation of PROOFS 2013
9h15–10h15	Session 1: formal analysis of fault attacks Chair: Rob Bekkers.
• "**Formal verification of a software countermeasure against instruction skip attacks**", by *Karine Heydemann, Nicolas Moro, Emmanuelle Encrenaz and Bruno Robisson.*	
• "**A formal proof of countermeasures against fault injection attacks on CRT-RSA**", by *Pablo Rauzy and Sylvain Guilley.*	
10h15–10h30	Coffee break
10h30–11h30	Session 2: formal analysis of countermeasures against side-channel attacks Chair: Jean-Pierre Seifert.
• "**Towards Fresh Re-Keying with Leakage-Resilient PRFs: Cipher Design Principles and Analysis**", by *Sonia Belaid, Fabrizio De Santis, Johann Heyszl, Stefan Mangard, Marcel Medwed, Jörn-Marc Schmidt, François-Xavier Standaert and Stefan Tillich.*	
• "**Understanding the Limitations and Improving the Relevance of SPICE Simulations in Side-Channel Security Evaluations**", by *Dina Kamel, Mathieu Renauld, Denis Flandre and François-Xavier Standaert.*	
11h30–12h30	Invited keynote talk
• "**Better Provability through Computer Architecture**", by *Timothy Sherwood.*	
12h30–14h00	Lunch
14h00–15h00	Session 3: Formal design methods Chair: Kris Gaj.
• "**Formal Design of Composite Physically Unclonable Function**", by *Durga Prasad Sahoo, Debdeep Mukhopadhyay and Rajat Subhra Chakraborty.*	
• "**A hierarchical graph-based approach to generating formally-proofed Galois-field multipliers**", by *Kotaro Okamoto, Naofumi Homma and Takafumi Aoki.*	
• "**Trojan-Resilient Circuits**", by *Christoph Bayer and Jean-Pierre Seifert.*	
15h00–15h25	"Work in Progress" session
15h25–15h30	Wrap-up