Program of PROOFS

Leuven, Belgium. Thursday September 13rd, 2012

8h15–9h00	Registration, at College de Valk	
9h00–9h15	Opening – Welcome, presentation of PROOFS	
9h15–10h15	Invited talk #1	Chair: Stefan Mangard.
• "**Understanding the reasons for the side-channel leakage is indispensable for secure design**", by *Werner Schindler*.		
10h15–10h30	Coffee break	
10h30–12h00	Submitted papers session	Chair: Svetla Nikova.
• Contributed talk #1, "**A formal study of two physical countermeasures against side channel attacks**", by *Sébastien Briais, Sylvain Guilley and Jean-Luc Danger*.		
• Contributed talk #2, "**Formal verification of an implementation of CRT-RSA Vigilant's algorithm**", by *Maria Christofi, Boutheina Chetali, Louis Goubin and David Vigilant*.		
• Contributed talk #3, "**Toward A Taxonomy of Communications Security Models**", by *Mark Brown*.		
12h00–13h30	Lunch, at Alma cafeteria	
13h30–14h30	Invited talk #2	Chair: Éliane Jaulmes.
• "**Toward Formal Design of Cryptographic Processors Based on Galois Field Arithmetic**", by *Naofumi Homma*.		
14h30–15h30	Invited talk #3	Chair: Louis Goubin.
• "**Analysing Cryptographic Hardware Interfaces with Tookan**", by *Graham Steel*.		
15h30–16h00	Coffee break	
16h00–16h30	Round-table and Q&A with the audience	
16h30–16h35	Wrap-up	