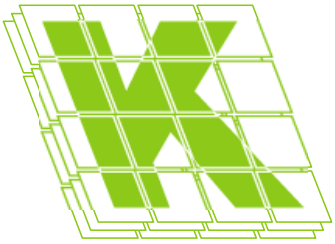
IAIK

TUG

Graz University of Technology



IAIK Krypto Group

VLSI

IAIK VLSI Group

PHILIPS

SIEMENS

ECRYPT

Program Committee

- Vincent Rijmen, TUG (chair)
- Phong Nguyen, ENS
- Christof Paar, RUB
- Bart Preneel, KULeuven
- Matt Robshaw, RHUL

This workshop is organized by the European Network of Excellence in Cryptology (ECRYPT) in Graz, Austria.

www.iaik.tugraz.at/research/krypto

Workshop on RFID and Light-Weight Crypto

Program, Wednesday July 13th

19.00 - Welcome reception at the Murinsel

Program, Thursday July 14th

9.00 - 9.30: Registration, Welcome
9.30 - 10.30: Introductory talk (Chair: Vincent Rijmen)
Johannes Wolkerstorfer
10.30 - 11.00: Break
11.00 - 12.30: Protocols (1) (Chair: Tanja Lange)
A scalable, delegatable, pseudonym protocol enabling ownership transfer of RFID tags by
David Molnar, Andrea Soppera, David Wagner

Mutual authentication protocol for low-cost RFID by Jeongkyu Yang, Jaemin Park, Hyunrok Lee, Kui Ren, Kwangjo Kim

Symmetric authentication for RFID systems in practice by
Sandra Dominikus, Elisabeth Oswald, Martin Feldhofer
12.30 - 14.00: Lunch
14.00 - 15.00: Invited talk (Chair: Bart Preneel)
RFID: The Problems of Cloning and Counterfeiting by
Ari Juels
15.00 - 15.30: Break
15.30 - 17.00: Hardware (Chair: Markus Volkmer)
8-bit microcontroller system with area efficient AES coprocessor for transponder applications by
Mark Jung, Horst Fiedler, Reneé Lerch

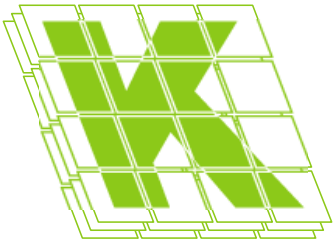
Electromagnetic side channel analysis of a contactless smart card: first results by Dario Carluccio, Kerstin Lemke, Christof Paar

Design of instruction set extensions and functional units for energy-efficient public-key cryptography by
Johann Großschädl, Stefan Tillich
18.15 - 19.15: City tour
19.30 - … : Conference dinner at Mayers

IAIK

TUG

Graz University of Technology



IAIK Krypto Group

VLSI

IAIK VLSI Group

PHILIPS

SIEMENS

ECRYPT

Program Committee

- Vincent Rijmen, TUG (chair)
- Phong Nguyen, ENS
- Christof Paar, RUB
- Bart Preneel, KULeuven
- Matt Robshaw, RHUL

This workshop is organized by the European Network of Excellence in Cryptology (ECRYPT) in Graz, Austria.

www.iaik.tugraz.at/research/krypto

Workshop on RFID and Light-Weight Crypto

Program, Friday July 15th

9.00 - 10.00: Invited talk (Chair: Matt Robshaw)
Protocol Design: Coming Down from the Cloud by Dieter Gollmann

10.00 - 10.30: Break

10.30 - 11.30: Curves (Chair: Francois-Xavier Standaert)
Arithmetic on binary genus 2 curves suitable for small devices by Tanja Lange

Is Elliptic-Curve Cryptography Suitable to Secure RFID Tags?
by Johannes Wolkerstorfer

11.30 - 12.30: Protocols (2) (Chair: Andrea Soppera)
Noisy cryptographic protocols for low cost RFID tags by Hervé Chabanne, Guillaume Fumaroli

Lightweight key exchange and stream cipher based solely on tree parity machines by Markus Volkmer, Sebastian Wallner

12.30 - 14.00: Lunch

14.00 - 15.00: Invited talk (Chair: Vincent Rijmen)
Scalability Issues in RFID Systems by Gildas Avoine

15.00 - 15.30: Break

15.30 - 17.00: Ciphers (Chair: Kerstin Lemke)
Grain - a stream cipher for constrained environments by Martin Hell, Thomas Johansson, Willi Meier

Small scale variants of the secure hash standard by Marco Macchetti, Philippe Rivard

SEA, a scalable encryption algorithm for small embedded applications by Francois-Xavier Standaert, Gilles Piret, Neil Gershenfeld, Jean-Jacques Quisquater