ECRYPT Workshop on Lightweight Cryptography.
November 28-29, 2011, Louvain-la-Neuve, Belgium.

Monday, November 28.

08:30 - 09:15 Registration.
09:15 - 09:30 Opening remarks.

09:30 - 10:45 Session 1: *Cryptanalysis*.

- Differential Cryptanalysis of PUFFIN and PUFFIN2
  - Céline Blondeau and Benoît Gérard
- Meet-in-the-Middle Cryptanalysis of KATAN
  - Simon Knellwolf
- Some Preliminary Studies on the Differential Behavior of the Lightweight Block Cipher LBlock
  - Marine Minier and María Naya-Plasencia

10:45 - 11:15 Coffee break.

11:15 - 12:15 Invited talk 1: *Challenges in Embedded Cryptography* (Joan Daemen).

12:15 - 14:15 Lunch break.

14:15 - 15:30 Session 2: *Implementation issues.*

- Compact Hardware Implementations of the Ultra-Lightweight Blockcipher Piccolo
  - Harunaga Hiwatari, Kyoji Shibutani, Takanori Isobe, Atsushi Mitsuda, Toru Akishita, Taizo Shirai
- Compact Implementation and Performance Evaluation of Block Ciphers in ATtiny Devices
  - Thomas Eisenbarth, Zheng Gong, Tim Güneysu, Stefan Heyse, Sebastiaan Indesteege, Stéphanie Kerckhof, François Koeune, Tomislav Nad, Thomas Plos, Francesco Regazzoni, Francois-Xavier Standaert and Loic Van Oldeneel
- High Speed Implementation of Authenticated Encryption for the MSP430X Microcontroller
  - Conrado P. L. Gouvea and Julio López

15:30 - 16:00 Coffee break.

16:00 - 17:00 Invited talk 2: *Bridging Theory and Practice in Cryptography* (Pascal Junod).

19:00 - 21:00 Workshop dinner

Tuesday November 29.

09:20 - 10:10 Session 3: *LPN.*

- An Efficient Authentication Protocol Based on Ring-LPN
  - Stefan Heyse, Eike Kiltz, Vadim Lyubashevsky, Christof Paar and Krzysztof Pietrzak
- The Cryptographic Power of Random Selection
  - Matthias Krause and Matthias Hamann

10:10 - 11:00 Session 4: *New designs.*

- TWINE: A Lightweight, Versatile Block Cipher
  - Tomoyasu Suzaki, Kazuhiko Minematsu, Sumio Morioka and Eita Kobayashi
- SPONGENT: The Design Space of Lightweight Cryptographic Hashing
  - Andrey Bogdanov, Miroslav Knezevic, Gregor Leander, Deniz Toz, Kerem Varici and Ingrid Verbauwhede

11:00 - 11:30 Coffee break

11:30 - 12:30 Invited talk 3: *Cryptography for RFIDs* (Matt Robshaw).

12:30 - 14:30 Lunch break.

14:30 - 15:45 Session 5: *Authentication.*

- A new generic protocol for authentication and key agreement in lightweight systems
  - Naïm Qachri, Olivier Markowitch and Frédéric Lafitte
- Relation among the Security Models for RFID Authentication Protocol
  - Daisuke Moriyama, Shin'Ichiro Matsuo and Miyako Ohkubo
- CANAuth - A Simple, Backward Compatible Broadcast Authentication Protocol for CAN bus
  - Anthony Van Herrewege, Dave Singelee and Ingrid Verbauwhede

15:45 - 16:15 Coffee break

16:15 - 17:30 Session 6: *Implementation issues.*

- The Technology Dependence of Lightweight Hash Implementation Cost
  - Xu Guo and Patrick Schaumont
- Enabling Standardized Cryptography on Ultra-Constrained 4-bit Microcontrollers
  - Tino Kaufmann and Axel Poschmann
- Elliptic Curve Cryptography in JavaScript
  - Laurie Haustenne, Quentin De Neyer and Olivier Pereira

17:30 - 17:35 Concluding remarks