ECRYPT II

Sponsored by the ECRYPT Network of Excellence

COOPERATION

- Workshop on Lightweight Cryptography 2011 -

November 28-29, 2011, Louvain-la-Neuve, Belgium.

- Call for Papers -

The focus of the workshop is on all aspects related to low-cost cryptography, mixing symmetric and asymmetric techniques, algorithms and protocols, as well as hardware and software implementation issues. The workshop is a forum for presenting new solutions for securing small embedded devices (smart cards, RFIDs, sensor nodes) including their underlying mathematical foundations and practical applications. Topics of interest include, but are not limited to:

- *Low cost symmetric cryptographic primitives (block/stream ciphers, hash functions).*
- *Public key cryptography fitting the constraints of smart cards and RFIDs.*
- *Cryptanalysis of emerging (secret and public key) cryptographic primitives.*
- *Lightweight authentication protocols and their security analysis.*
- *Low-cost key distribution mechanisms in sensor networks.*
- *Efficient multi-purpose designs (e.g. encryption + hashing + authentication).*
- *Benchmarking of lightweight cryptographic algorithms in software and hardware.*
- *Implementation attacks and countermeasures for constrained devices.*
- *Random number generation and physically unclonable functions.*
- *Exploitation of new low power micro-/nano-electronic technologies.*
- *Industrial applications (e.g. automotive industry, smart metering in buildings, …).*
- *Privacy issues raised by the proliferation of embedded cryptography.*

Important dates.

Submission deadline: October 10, 2011.
Final version due: November 15, 2011.
Notification of acceptance: November 7, 2011.
Registration deadline: November 15, 2011.

Instructions for authors.

Authors are invited to submit their papers via electronic submission. Contributions should describe technical works related to the workshop topics. Papers must be at most 18 pages (excluding the bibliography and appendices), and be formatted according to the Springer Lecture Notes in Computer Science style (see http://www.springer.de/comp/lncs/author.html). The workshop will not have formal proceedings. Therefore, accepted papers can be re-submitted to other conferences or journals without risking infringing double-submission policies.

Program committee.

- Frederik Armknecht (Universität Mannheim, Germany).
- Jean-Philippe Aumasson (Nagravision, Switzerland).
- Gildas Avoine (Université catholique de Louvain, Belgium).
- Thomas Baignères (CryptoExperts, France).
- Lejla Batina (Radboud University Nijmegen, The Netherlands and KU Leuven, Belgium).
- Guido Bertoni (ST Microelectronics, Italy).
- Jean-Luc Beuchat (University of Tsukuba, Japan).
- Andrey Bogdanov (KU Leuven, Belgium).
- Christophe De Cannière (Google, Switzerland).
- Josep Domingo-Ferrer (Universitat Rovira i Virgili, Catalonia).
- Emmanuelle Dottax (Oberthur Technologies, France).
- Orr Dunkelman (University of Haifa, Israel).
- Benoît Gérard (Université catholique de Louvain, Belgium).
- Henri Gilbert (ANSSI, France).
- Thomas Gross (University of Newcastle, UK).
- Tim Güneysu (University of Bochum, Germany).
- Tanja Lange (Technische Universiteit Eindhoven, The Netherlands).
- Stefan Mangard (Infineon Technologies, Germany).
- María Naya-Plasencia (Fachhochschule Nordwestschweiz, Switzerland).
- David Naccache (Ecole Normale Supérieure, France).
- Thomas Peyrin (Nanyang Technological University, Singapore).
- Axel Poschmann (Nanyang Technological University, Singapore).
- Francisco Rodriguez-Henriquez (Centro de inv. y de Estudios Avanzados del IPN, Mexico).
- Kazuo Sakiyama (University of Electro Communications, Japan).
- Serge Vaudenay (EPFL, Switzerland).
- Erik Zenner (Technical University of Denmark).

Program committee co-chairs.

- Gregor Leander (Technical University of Denmark).
- François-Xavier Standaert (Université catholique de Louvain, Belgium).

Workshop website: http://www.uclouvain.be/crypto/ecrypt_lc11/
Submission website: https://www.easychair.org/conferences/?conf=lc2011