LightSec 2014: Call For Papers

Third International Workshop on
Lightweight Cryptography for Security and Privacy

September 1–2, 2014, Istanbul (Turkey)
http://www.light-sec.org

Program Chairs
Thomas Eisenbarth
Erdinç Öztürk

General Chair
Erdinç Öztürk

Program Committee
Tolga Acar
Onur Aciicmez
Elena Andreeva
Jean-Phillipe Aumasson
Paulo Barreto
Lejla Batina
Guido Bertoni
Andrey Bogdanov
Elke De Mulder
Chris Gaj
Berndt Gammel
Shay Gueron
Julio Hernandez-Castro
Pascal Junod
Jens-Peter Kaps
Xuejia Lai
Albert Levi
Amir Moradi
Mehran Mozaffari Kermani
Axel Poschmann
Francesco Regazzoni
Arash Reyhani-Masoleh
Francisco Rodríguez Henríquez
Mehmet Sabir Kiraz
Erkay Savas
Nitesh Saxena
Ali Aydin Selçuk
Georg Sigl
Meltem Sonmez Turan
Mike Tunstall
Kerem Varici
Amr Youssef

General Information
LightSEC 2014 will promote and initiate novel research on the security & privacy issues for applications that can be termed as lightweight security, due to the associated constraints on metrics such as available power, energy, computing ability, area, execution time, and memory requirements. As such applications are becoming ubiquitous, providing an immense value to society, they are also affecting a greater portion of the public & leading to a plethora of economical & security and privacy related concerns.

Topics of Interest
- Design, analysis and implementation of lightweight cryptographic protocols
- Cryptographic hardware development for constrained domains
- Security & privacy solutions for wireless embedded systems
- Lightweight privacy-preserving protocols & systems
- Design and analysis of fast and compact cryptographic algorithms
- Wireless network security for low-resource devices
- Low-power crypto architectures
- Scalable protocols and architectures for security and privacy
- Formal methods for analysis of lightweight cryptographic protocols
- Security and privacy issues in RFID and NFC
- Embedded systems security
- PUF based crypto protocols
- Security of ubiquitous and pervasive computing
- Side channel analysis and countermeasures on lightweight devices
- Efficient and scalable cryptographic protocols for the Next Generation Secure Cloud

Important Dates

Paper submission deadline:	**June 1, 2014**
Author notification:	July 11, 2014
Camera ready papers due:	July 20, 2014
Workshop date:	September 1 - 2, 2014

Instructions for Authors
The submission must be anonymous with no author names, affiliations or obvious references. Only original unpublished work should be included in the manuscript. The manuscripts must be compliant with Springer's LNCS template. Each paper will be reviewed by at least three reviewers. The proceedings will be published in Springer-Verlag's LNCS series.
Submission website: http://www.easychair.org/conferences/?conf=lightsec14