# Workshop on Lightweight Security & Privacy: Devices, Protocols, and Applications (LightSec 2011)

http://www.light-sec.org

*March 14-15, 2011*
*Istanbul, Turkey*

## Call for Papers

### Organizational Committee

***Program Chairs***

Erkay Savas
*Sabanci University*

Ali Aydin Selcuk
*Bilkent University*

Umut Uludag
*TUBITAK - UEKAE*

***Local Chairs***

Huseyin Demirci
*TUBITAK - UEKAE*

Orhun Kara
*TUBITAK - UEKAE*

The main goal of this workshop is to 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, definitely providing an immense value to the society, they are also affecting a greater portion of the public & leading to a plethora of economical & security and privacy related concerns. The goal of this workshop is to create a platform where these concerns can be addressed and proposed solutions are discussed and evaluated. The solutions should be economically applicable in constrained environments such as wireless embedded systems. Due to the nature of the problem, good scalability properties are also expected requirements of the proposed systems. Providing implementation results & demonstrating the applicability of the proposed solutions are among the essentials. Metrics to evaluate different aspects of lightweight security solutions and combined metrics for overall evaluations thereof for a given application scenario are useful for implementers and engineers. Compactness and efficiency are the properties which are commonly sought.

Topics of interest include, but are not limited to:

- Design, analysis and implementation of lightweight cryptographic protocols & applications
- Cryptographic hardware development for constrained domains
- Design, analysis and implementation of security & privacy solutions for wireless embedded systems
- Design, analysis and implementation of 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
- Fast and compact biometric-based algorithms for authentication and identification
- Scalable protocols and architectures for security and privacy
- Formal methods for analysis of lightweight cryptographic protocols

### *Important Dates*

*Submission deadline:* October 22, 2010 – October 27, 2010, 23:59 UTC (Extended)
*Acceptance notification:* November 12, 2010 – November 17, 2010 (Extended)
*Final papers due:* December 17, 2010

## *Program Committee*

Onur Aciicmez, *Samsung Information Systems, USA*
Gildas Avoine, *UCL, Louvain-la-Neuve, Belgium*
Paulo Barreto, *University of Sao Paulo, Brazil*
Lejla Batina, *Katholieke Universiteit Leuven, Belgium*
Guido Bertoni, *STMicroelectronics, Italy*
Orr Dunkelman, *Weizmann Institute of Science, Israel*
Kris Gaj, *George Mason University, USA*
Helena Handschuh, *Intrinsic-ID Inc., USA*
Francisco Rodriguez Henriquez, *Ins. Politecnico Nacional, Mexico*
Anil Jain, *Michigan State University, USA*
Marc Joye, *Technicolor, France*
Cetin Kaya Koc, *Istanbul Sehir University, Turkey*
Albert Levi, *Sabanci University, Turkey*
Christof Paar, *Ruhr-University Bochum, Germany*
Thomas Pedersen, *TUBITAK-UEKAE, Turkey*
Bart Preneel, *Katholieke Universiteit Leuven, Belgium*
Arash Reyhani-Masoleh, *University of Western Ontario, Canada*
Vincent Rijmen, *K. Universiteit Leuven, Belgium & TU Graz, Austria*
Pankaj Rohatgi, *Cryptography Research, USA*
Arun Ross, *West Virginia University, USA*
Ahmad-Reza Sadeghi, *Ruhr-University Bochum, Germany*
Gokay Saldamli, *Bogazici University, Turkey*
Mike Scott, *Dublin City University, Ireland*
Berk Sunar, *Worcester Polytechnic Institute, USA*
Serge Vaudenay, *EPFL, Switzerland*
Berna Ors Yalcin, *Istanbul Technical University, Turkey*
Berrin Yanikoglu, *Sabanci University, Turkey*

## *Instructions for Paper Submission*

The submission must be anonymous with no author names or other identifying information. Only original/previously unpublished work should be included in the paper. Maximum paper length is 8 pages, with double-column formatting. Each paper conforming to these specifications will be reviewed by at least 3 anonymous reviewers, to be selected from the Program Committee.

The authors should use the template at http://www.computer.org/portal/web/cscps/formatting. Paper submission website is https://www.easychair.org/account/signin.cgi?conf=lightsec2011.

## *Workshop Proceedings*

The workshop proceedings will be published by Conference Publishing Services (CPS)( www.**computer**.org/portal/web/cs**cps** ). CD proceedings will be available at the workshop.

## *Invited Speakers*

- Prof. Dr. Josep Domingo-Ferrer, Universitat Rovira i Virgili, Catalonia, http://crises-deim.urv.cat/jdomingo/. "Making security and privacy compatible with VANET performance requirements", Tuesday, March 15, 2011.
- Prof. Dr. Bart Preneel, Katholieke Universiteit Leuven, Belgium, http://homes.esat.kuleuven.be/~preneel/,"A Perspective on Lightweight Cryptographic Algorithms", Monday, March 14, 2011.

## *Stipends*

A limited number of stipends will be available to student authors of accepted papers.