

# **2011 Workshop on Lightweight Security & Privacy: Devices, Protocols and Applications**

**(LightSec 2011)**

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



**IEEE Catalog Number: CFP1131N-PRT  
ISBN: 978-1-61284-170-0**

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

## LightSec 2011

### Table of Contents

Message from Program Chairs .....	vii
Organizing Committee .....	viii
Additional Reviewers .....	ix

---

### Workshop Papers

Practical and Secure Software-Based Attestation .....	1
<i>Markus Jakobsson and Karl-Anders Johansson</i>	
An Efficient Verifiable Implicit Asking Protocol for Diffie-Hellman Key Exchange .....	10
<i>Kazuomi Oishi and Tsutomu Matsumoto</i>	
Cryptanalysis of Lightweight Mutual Authentication and Ownership Transfer for RFID Systems .....	20
<i>Süleyman Kardaş, Mete Akgün, Mehmet Sabir Kiraz, and Hüseyin Demirci</i>	
On Hardware-Oriented Message Authentication with Applications towards RFID .....	26
<i>Martin Ågren, Martin Hell, and Thomas Johansson</i>	
Secure Network Discovery in Wireless Sensor Networks Using Combinatorial Key Pre-distribution .....	34
<i>Kevin Henry and Douglas R. Stinson</i>	
Short Group Signatures with Controllable Linkability .....	44
<i>Jung Yeon Hwang, Sokjoon Lee, Byung-Ho Chung, Hyun Sook Cho, and DaeHun Nyang</i>	
F-HB: An Efficient Forward Private Protocol .....	53
<i>Xiaolin Cao and Máire O'Neill</i>	
Scalable and Efficient FPGA Implementation of Montgomery Inversion .....	61
<i>Ertuğrul Murat, Süleyman Kardaş, and Erkay Savaş</i>	

Short-Key Certificateless Encryption .....	69
<i>George Stephanides</i>	
Towards an Ultra Lightweight Crypto Processor .....	76
<i>Begul Bilgin, Elif Bilge Kavun, and Tolga Yalcin</i>	
<b>Author Index</b> .....	<b>84</b>