

Table of Contents

WLC Preface	1
<i>Josep M. Miret and Francesc Sebé</i>	
Hummingbird: Ultra-Lightweight Cryptography for Resource-Constrained Devices	3
<i>Daniel Engels, Xinxin Fan, Guang Gong, Honggang Hu, and Eric M. Smith</i>	
Lighten Encryption Schemes for Secure and Private RFID Systems	19
<i>Sébastien Canard, Iwen Coisel, and Jonathan Etrog</i>	
Analysis and Improvement of a Pseudorandom Number Generator for EPC Gen2 Tags	34
<i>J. Melia-Segui, J. Garcia-Alfaro, and J. Herrera-Joancomarti</i>	
A Note on a Fatal Error of Optimized LFC Private Information Retrieval Scheme and Its Corrected Results	47
<i>Jin Tamura, Kazukuni Kobara, Hanane Fathi, and Hideki Imai</i>	
Reliable Food Traceability Using RFID Tagging	57
<i>Guillermo Azuara, José L. Salazar, José L. Tornos, and Joan J. Piles</i>	
Lightweight Cryptography and DPA Countermeasures: A Survey	68
<i>Amir Moradi and Axel Poschmann</i>	
Securing the Use of RFID-Enabled Banknotes	80
<i>Santi Martínez, Concepció Roig, and Magda Valls</i>	
Increasing Privacy Threats in the Cyberspace: The Case of Italian E-Passports	94
<i>Vincenzo Auletta, Carlo Blundo, Angelo De Caro, Emiliano De Cristofaro, Giuseppe Persiano, and Ivan Visconti</i>	
RLCPS Preface	105
<i>Aggelos Kiayias and Kazuo Sako</i>	
SPAKE: A Single-Party Public-Key Authenticated Key Exchange Protocol for Contact-Less Applications	107
<i>Jean-Sébastien Coron, Aline Gouget, Pascal Paillier, and Karine Villegas</i>	
A Secure and Privacy-Preserving Targeted Ad-System	123
<i>Elli Androulaki and Steven M. Bellovin</i>	

Cryptographic Cloud Storage	136
<i>Seny Kamara and Kristin Lauter</i>	
Extending IPsec for Efficient Remote Attestation	150
<i>Ahmad-Reza Sadeghi and Steffen Schulz</i>	
Open Mobile Alliance Secure Content Exchange: Introducing Key Management Constructs and Protocols for Compromise-Resilient Easing of DRM Restrictions	166
<i>David William Kravitz</i>	
How to Evaluate the Security of Real-Life Cryptographic Protocols? The Cases of ISO/IEC 29128 and CRYPTREC	182
<i>Shin'ichiro Matsuo, Kunihiko Miyazaki, Akira Otsuka, and David Basin</i>	
WECSR Preface	195
<i>Sven Dietrich</i>	
Preaching What We Practice: Teaching Ethical Decision-Making to Computer Security Professionals (Keynote Talk)	197
<i>Kenneth R. Fleischmann</i>	
A Case Study on Measuring Statistical Data in the Tor Anonymity Network	203
<i>Karsten Loesing, Steven J. Murdoch, and Roger Dingledine</i>	
A Case Study in Ethical Decision Making Regarding Remote Mitigation of Botnets	216
<i>David Dittrich, Felix Leder, and Tillmann Werner</i>	
Ethical Proactive Threat Research (Position Paper)	231
<i>John Aycock and John Sullins</i>	
A Framework for Understanding and Applying Ethical Principles in Network and Security Research (Position Paper)	240
<i>Erin Kenneally, Michael Bailey, and Douglas Maughan</i>	
Ethical Concerns in Computer Security and Privacy Research Involving Human Subjects (Panel)	247
<i>Lorrie Faith Cranor</i>	
Ethical Guidelines for Computer Security Researchers: "Be Reasonable" (Panel)	250
<i>Len Sassaman</i>	
Author Index	257