

# Table of Contents

## Keynote Speech

Can Code Polymorphism Limit Information Leakage? .....	1
<i>Antoine Amarilli, Sascha Müller, David Naccache, Daniel Page, Pablo Rauzy, and Michael Tunstall</i>	

## Mobile Authentication and Access Control

Mobile Electronic Identity: Securing Payment on Mobile Phones .....	22
<i>Chen Bangdao and A.W. Roscoe</i>	
Role-Based Secure Inter-operation and Resource Usage Management in Mobile Grid Systems .....	38
<i>Antonios Gouglidis and Ioannis Mavridis</i>	

## Lightweight Authentication

SSL/TLS Session-Aware User Authentication Using a GAA Bootstrapped Key .....	54
<i>Chunhua Chen, Chris J. Mitchell, and Shaohua Tang</i>	
An Almost-Optimal Forward-Private RFID Mutual Authentication Protocol with Tag Control .....	69
<i>Paolo D'Arco</i>	
Affiliation-Hiding Authentication with Minimal Bandwidth Consumption .....	85
<i>Mark Manulis and Bertram Poettering</i>	

## Algorithms

Formal Framework for the Evaluation of Waveform Resynchronization Algorithms .....	100
<i>Sylvain Guilley, Karim Khalfallah, Victor Lomne, and Jean-Luc Danger</i>	
Solving DLP with Auxiliary Input over an Elliptic Curve Used in TinyTate Library .....	116
<i>Yumi Sakemi, Tetsuya Izu, Masahiko Takenaka, and Masaya Yasuda</i>	
Information Leakage Discovery Techniques to Enhance Secure Chip Design .....	128
<i>Alessandro Barengi, Gerardo Pelosi, and Yannick Tégli</i>	

## Hardware Implementation

A Cryptographic Processor for Low-Resource Devices: Canning ECDSA and AES Like Sardines .....	144
<i>Michael Hutter, Martin Feldhofer, and Johannes Wolkerstorfer</i>	
An Evaluation of Hash Functions on a Power Analysis Resistant Processor Architecture .....	160
<i>Simon Hoerder, Marcin Wójcik, Stefan Tillich, and Daniel Page</i>	
A Comparison of Post-Processing Techniques for Biased Random Number Generators .....	175
<i>Siew-Hwee Kwok, Yen-Ling Ee, Guanhan Chew, Kanghong Zheng, Khoongming Khoo, and Chik-How Tan</i>	

## Security and Cryptography

AES Variants Secure against Related-Key Differential and Boomerang Attacks .....	191
<i>Jiali Choy, Aileen Zhang, Khoongming Khoo, Matt Henricksen, and Arel Poschmann</i>	
Leakage Squeezing Countermeasure against High-Order Attacks .....	208
<i>Housseem Maghrebi, Sylvain Guilley, and Jean-Luc Danger</i>	

## Security Attacks and Measures (Short Papers)

Differential Fault Analysis of the Advanced Encryption Standard Using a Single Fault .....	224
<i>Michael Tunstall, Debdeep Mukhopadhyay, and Subidh Ali</i>	
Entropy of Selectively Encrypted Strings .....	234
<i>Reine Lundin and Stefan Lindskog</i>	
Practical Attacks on HB and HB+ Protocols .....	244
<i>Zbigniew Golebiewski, Krzysztof Majcher, Filip Zagórski, and Marcin Zawada</i>	
Attacks on a Lightweight Mutual Authentication Protocol under EPC C-1 G-2 Standard .....	254
<i>Mohammad Hassan Habibi, Mahdi R. Alagheband, and Mohammad Reza Aref</i>	

## Security Attacks

A SMS-Based Mobile Botnet Using Flooding Algorithm .....	264
<i>Jingyu Hua and Kowichi Sakurai</i>	

FIRE: Fault Injection for Reverse Engineering .....	280
<i>Manuel San Pedro, Mate Soos, and Sylvain Guilley</i>	
Hardware Trojan Side-Channels Based on Physical Unclonable Functions .....	294
<i>Zheng Gong and Marc X. Makkes</i>	

## Security and Trust

Formal Analysis of Security Metrics and Risk .....	304
<i>Leanid Krautsevich, Fabio Martinelli, and Artsiom Yautsiukhin</i>	
STORM - Collaborative Security Management Environment .....	320
<i>Theodoros Ntouskas, George Pentafronimos, and Spyros Papastergiou</i>	
Trust Agreement in Wireless Mesh Networks .....	336
<i>Andreas Noack</i>	

## Mobile Application Security and Privacy (Short Papers)

Secure E-Auction for Mobile Users with Low-Capability Devices in Wireless Network .....	351
<i>Kun Peng</i>	
Privacy Respecting Targeted Advertising for Social Networks .....	361
<i>Christian Kahl, Stephen Crane, Markus Tschersich, and Kai Rannenberg</i>	
Privacy Protection for Smartphones: An Ontology-Based Firewall .....	371
<i>Johann Vincent, Christine Porquet, Maroua Borsali, and Harold Leboulanger</i>	
A Study on the Security, the Performance and the Penetration of Wi-Fi Networks in a Greek Urban Area.....	381
<i>Savvas Mousionis, Alex Vakaloudis, and Constantinos Hilas</i>	
Author Index .....	391