

Table of Contents

Keynote Address

Preserving Privacy in Online Social Networks	1
<i>Fatemeh Raji, Ali Miri, and Mohammad Davarpanah Jazi</i>	

Short Papers

TTP SmartCard-Based ElGamal Cryptosystem Using Threshold Scheme for Electronic Elections	14
<i>Jordi Pujol-Ahulló, Roger Jardí-Cedó, Jordi Castellà-Roca, and Oriol Farràs</i>	
Automated Verification of Block Cipher Modes of Operation, an Improved Method	23
<i>Martin Gagné, Pascal Lafourcade, Yassine Lakhnech, and Reihaneh Safavi-Naini</i>	

Pervasive Security and Threshold Cryptography

(SC) ² : Secure Communication over Smart Cards: How to Secure Off-Card Matching in Security-by-Contract for Open Multi-application Smart Cards	32
<i>Nicola Dragoni, Eduardo Lostal, Davide Papini, and Javier Fabra</i>	
Private Identification of RFID Tags	49
<i>Behzad Malek and Ali Miri</i>	
Threshold Encryption into Multiple Ciphertexts	62
<i>Martin Stanek</i>	

Encryption, Cryptanalysis and Automatic Verification

A Novel Commutative Blinding Identity Based Encryption Scheme	73
<i>Yu Chen, Song Luo, Jianbin Hu, and Zhong Chen</i>	
A Related-Key Attack on Block Ciphers with Weak Recurrent Key Schedules	90
<i>Marina Pudovkina</i>	
A Computational Indistinguishability Logic for the Bounded Storage Model	102
<i>Gilles Barthe, Mathilde Duclos, and Yassine Lakhnech</i>	

Keynote Addresses

Preventing the Cluster Formation Attack against the Hierarchical OLSR Protocol	118
<i>Gimer Cervera, Michel Barbeau, Joaquin Garcia-Alfaro, and Evangelos Kranakis</i>	
Secret Key Establishment over Noisy Channels	132
<i>Hadi Ahmadi and Reihaneh Safavi-Naini</i>	

Formal Methods and Network Security

Formal Specification and Validation of Security Policies	148
<i>Tony Bourdier, Horatiu Cirstea, Mathieu Jaume, and Hélène Kirchner</i>	
Vote-Independence: A Powerful Privacy Notion for Voting Protocols	164
<i>Jannik Dreier, Pascal Lafourcade, and Yassine Lakhnech</i>	
Black-Box Property of Cryptographic Hash Functions	181
<i>Michal Rjasko</i>	
Phishing Detection with Popular Search Engines: Simple and Effective	194
<i>Jun Ho Huh and Hyoungshick Kim</i>	

Ongoing Research

A Contextual Privacy-Aware Access Control Model for Network Monitoring Workflows: Work in Progress	208
<i>Eugenia I. Papagiannakopoulou, Maria N. Koukovini, Georgios V. Lioudakis, Joaquin Garcia-Alfaro, Dimitra I. Kaklamani, and Iakovos S. Venieris</i>	
A Metamodel for the Design of Access-Control Policy Enforcement Managers: Work in Progress	218
<i>Michel Embe Jiague, Marc Frappier, Frédéric Gervais, Régine Laleau, and Richard St-Denis</i>	
Specification and Verification of Access Control Policies in EB ³ SEC: Work in Progress	227
<i>Pierre Konopacki, Hakim Belhaouari, Marc Frappier, and Régine Laleau</i>	

A Metamodel of the B Modeling of Access-Control Policies: Work in Progress	234
<i>Jérémy Milhau, Marc Frappier, and Régine Laleau</i>	
Formal Verification of a Key Establishment Protocol for EPC Gen2 RFID Systems: Work in Progress	242
<i>Wiem Tounsi, Nora Cuppens-Boulahia, Frédéric Cuppens, and Joaquín García-Alfaro</i>	
Author Index	253