This volume contains the proceedings of the 4th Canada-France MITACS Workshop on Foundations and Practice of Security (FPS 2011). The FPS workshop was initiated in 2008, following the Canada-France Meeting on Security held at the Simon Fraser University, Vancouver, during December 6–8, 2007. Since then, the FPS workshop has been held annually, alternating between Canadian and French locations, including Montreal, Grenoble and Toronto. This fourth edition of the FPS workshop was held in Paris, France, during May 12–13, and was co-located with the NOTERE 2011 conference hosted by Télécom ParisTech.

In response to the call for participation, 30 contributions from 15 different countries were submitted to the workshop. These contributions were evaluated on the basis of their significance, novelty, and technical quality. This volume contains a revised version of ten full papers, accompanied by three keynote addresses, two short papers, and five ongoing research reports. These papers cover a wide and rich spectrum of research in security and privacy of electronic services.

We would like to express our sincere appreciation for all the support we received from the General and Organizing Chairs of FPS 2011, Evangelos Kranakis, Rei Safavi-Naini, Frédéric Cuppens, and Nora Cuppens-Boulahia. Thanks very much for your contribution to the success of the event. Our special thanks go, also, to our keynote speakers, Abdullatif Shikfa (Alcatel-Lucent Bell Labs), Ali Miri (Ryerson University), Marc Frappier (University of Sherbrooke), Gimer Cervera (Carleton University), Christoph Neumann (Technicolor), and Rei Safavi-Naini (Calgary University), for accepting our invitation and for their presence during the event and talks.

We acknowledge the financial support from MITACS (thank you Rebecca Marsh and Michael Lynch), INRIA (thank you Claude Kirchner and Helene Kirchner), UOC/IN3 (thank you David Megias), and Institut Télécom (thank you David Sadek). We also acknowledge the support from the following projects: ARES-CONSOLIDER INGENIO 2010 CSD2007-00004 and eAEGIS TSI2007-65406-C03-03 from the Spanish MICINN; and the DEMONS project FP7-ICT-2009-5 from the European Commission.

Finally, we express our gratitude to the NOTERE 2011 organization team. Thank you Ahmed Serhrouchni, Isabelle Demeuere, Thomas Robert, and Gael Thomas, for all your help with the local arrangements of FPS. Many thanks go, also, to the FPS 2011 Program Committee members and the external referees, for their help, availability and commitment. Last, but by no means least, we thank all the authors who submitted papers and talks, and all the workshop attendees.

September 2011

Joaquin Garcia-Alfaro
Pascal Lafourcade
FPS 2011 Workshop Organization

General Chairs
Evangelos Kranakis  Carleton University, Canada
Rei Safavi-Naini  Calgary University, Canada

Program Chairs
Joaquin Garcia-Alfaro  TELECOM Bretagne, France
Pascal Lafourcade  Joseph Fourier University, France

Organizing Chairs
Frédéric Cuppens  TELECOM Bretagne, France
Nora Cuppens-Boulahia  TELECOM Bretagne, France
Joaquin Garcia-Alfaro  TELECOM Bretagne, France

Publication Chair
Joaquin Garcia-Alfaro  TELECOM Bretagne, France

Program Committee
Carlos Aguilar Melchor  XLIM Research Institute, France
Michel Barbeau  Carleton University, Canada
Mike Burmester  Florida State University, USA
Christophe Bidan  Supelec, Rennes, France
Joan Borrell-Viader  Autonomous University of Barcelona, Spain
Ana Cavalli  TELECOM SudParis, France
Jordi Castella-Roca  Rovira i Virgili University, Spain
Frederic Cuppens  TELECOM Bretagne, France
Nora Cuppens-Boulahia  TELECOM Bretagne, France
Ernesto Damiani  University of Milan, Italy
Josep Domingo-Ferrer  Rovira i Virgili University, Spain
David Evans  University of Cambridge, UK
Jose M. Fernandez  Ecole Polytechnique de Montreal, Canada
Sara Foresti  University of Milan, Italy
Sebastien Gambs
Joaquin Garcia-Alfaro
Stefanos Gritzalis
Jordi Herrera-Joancomartí
Thomas Jensen
Wei Jiang
Bruce Kapron
Claude Kirchner
Evangelos Kranakis
Pascal Lafourcade
Yassine Lakhnech
Jean Leneutre
Georgios Lioudakis
Luigi Logrippo
Fabio Massacci
Ludovic Me
Ali Miri
Kumar Murty
Guillermo Navarro-Arribas
Andreas Pashalidis
Rei Safavi-Naini
Douglas Stinson
Nicola Zannone

Université de Rennes 1, France
TELECOM Bretagne, France
University of the Aegean, Greece
Autonomous University of Barcelona, Spain
INRIA Rennes, France
Missouri University of Science and Technology, USA
Victoria University, Canada
INRIA, Rocquencourt, France
Carleton University, Canada
Joseph Fourier University, France
Joseph Fourier University, France
TELECOM ParisTech, France
National Technical University of Athens, Greece
Université du Quebec en Outaouais, France
Università di Trento, Italy
Supelec, Rennes, France
Ryerson University, Canada
University of Toronto, Canada
UAB, Spain
K.U. Leuven, Belgium
Calgary University, Canada
University of Waterloo, Canada
Eindhoven University of Technology, The Netherlands

Steering Committee

Guillaume Hanrot
Bruce Kapron
Evangelos Kranakis
Pascal Lafourcade
Henry Lee

LORIA, France
Victoria University, Canada
Carleton University, Canada
Joseph Fourier University, France
Government of BC, Canada

External Referees

Theodoros Balopoulos
Nataliia Bielova
Jannik Dreier
Arnau Erola
Oriol Farras
Laurent Fousse
Olga Gadyatskaya

University of the Aegean, Greece
Università di Trento, Italy
Joseph Fourier University, France
Rovira i Virgili University, Spain
Rovira i Virgili University, Spain
Joseph Fourier University, France
Università di Trento, Italy
Martin Gagné, Joseph Fourier University, France
Iksoon Hwang, TELECOM SudParis, France
Behzad Malek, University of Ottawa, Canada
Joan Melia-Segui, Open University of Catalonia, Spain
Anderson Morais, TELECOM SudParis, France
Kris Narayan, Calgary University, Canada
Thomas Peyrin, Nanyang Technological University, Singapore
Guillaume Piolle, Supelec, Rennes, France
Bruno Pontes Soares Rocha, Eindhoven University of Technology, The Netherlands
Jordi Pujol-Ahullo, Rovira i Virgili University, Spain
Alfredo Rial, K.U. Leuven, Belgium
Bharath Samanthula, Missouri University of Science and Technology, USA
Hoi Ting Poon, University of Ottawa, Canada
Elmar Tischhauser, K.U. Leuven, Belgium
Eric Totel, Supelec, Rennes, France
Meilof Veeningen, Eindhoven University of Technology, The Netherlands
# Table of Contents

## Keynote Address

Preserving Privacy in Online Social Networks ............................. 1  
*Fatemeh Raji, Ali Miri, and Mohammad Davarpanah Jazi*

## Short Papers

TTP SmartCard-Based ElGamal Cryptosystem Using Threshold  
Scheme for Electronic Elections ............................................. 14  
*Jordi Pujol-Ahulló, Roger Jardí-Cedó, Jordi Castellà-Roca, and Oriol Farràs*

Automated Verification of Block Cipher Modes of Operation, an  
Improved Method .............................................................. 23  
*Martin Gagné, Pascal Lafourcade, Yassine Lakhnech, and Reihaneh Safavi-Naini*

## 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  
*Nicola Dragoni, Eduardo Lostal, Davide Papini, and Javier Fabra*

Private Identification of RFID Tags ......................................... 49  
*Behzad Malek and Ali Miri*

Threshold Encryption into Multiple Ciphertexts .......................... 62  
*Martin Stanek*

## Encryption, Cryptanalysis and Automatic Verification

A Novel Commutative Blinding Identity Based Encryption Scheme ..... 73  
*Yu Chen, Song Luo, Jianbin Hu, and Zhong Chen*

A Related-Key Attack on Block Ciphers with Weak Recurrent Key  
Schedules .............................................................................. 90  
*Marina Pudovkina*

A Computational Indistinguishability Logic for the Bounded Storage  
Model .................................................................................... 102  
*Gilles Barthe, Mathilde Duclos, and Yassine Lakhnech*
Table of Contents

Keynote Addresses

Preventing the Cluster Formation Attack against the Hierarchical OLSR Protocol ............................................. 118  
Gimer Cervera, Michel Barbeau, Joaquin Garcia-Alfaro, and Evangelos Kranakis

Secret Key Establishment over Noisy Channels .................. 132  
Hadi Ahmadi and Reihaneh Safavi-Naini

Formal Methods and Network Security

Formal Specification and Validation of Security Policies .......... 148  
Tony Bourdier, Horatiu Cirstea, Mathieu Jaume, and Hélène Kirchner

Vote-Independence: A Powerful Privacy Notion for Voting Protocols . 164  
Jannik Dreier, Pascal Lafourcade, and Yassine Lakhnech

Black-Box Property of Cryptographic Hash Functions ............ 181  
Michal Rjaško

Phishing Detection with Popular Search Engines: Simple and Effective ......................................................... 194  
Jun Ho Huh and Hyoungshick Kim

Ongoing Research

A Contextual Privacy-Aware Access Control Model for Network Monitoring Workflows: Work in Progress .................... 208  
Eugenia I. Papagiannakopoulou, Maria N. Koukovini, Georgios V. Lioudakis, Joaquin Garcia-Alfaro, Dimitra I. Kaklamani, and Iakovos S. Venieris

A Metamodel for the Design of Access-Control Policy Enforcement Managers: Work in Progress .......................... 218  
Michel Embe Jiaque, Marc Frappier, Frédéric Gervais, Régine Laleau, and Richard St-Denis

Specification and Verification of Access Control Policies in EB³SEC:  
Work in Progress ..................................................... 227  
Pierre Konopacki, Hakim Belhaouari, Marc Frappier, and Régine Laleau
   Jérémie Milhau, Marc Frappier, and Régine Laleau

Formal Verification of a Key Establishment Protocol for EPC Gen2 RFID Systems: Work in Progress .......................... 242
   Wiem Tounsi, Nora Cuppens-Boulahia, Frédéric Cuppens, and Joaquin Garcia-Alfaro

Author Index .......................................................... 253