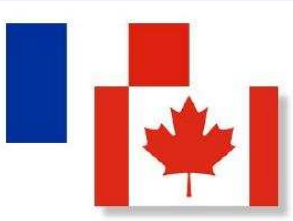
MITACS 2009



2nd Canada-France Workshop on

Foundations & Practice of Security

Friday June 26 - Saturday June 27, 2009

Grenoble, France

Workshop of CAV 09

http://www-mitacs2009.imag.fr/

MITACS 2009

GOAL: Network in Security and cryptography between FRANCE and CANADA

ACTIONS:

- 2 Master french students at Calgary for 1 year
- PhD visit of 2 months in Waterloo
- Visits between Calgary, Victoria and Grenoble
- Start of universities agreements ...

Workshops

- 2008 i n Montreal
- 2009 in Grenoble
- 2010 in CANADA, but where???

DAY 1

- 8:15 08:30 Welcome
- 8:30 9:15 C. Castelluccia: "Tracking Malicious Servers on the Internet"
- 9:15 10:00 Jose M. Fernandez "Botnets: No calm after the Storm"
- 10:00 10:30 Break I
- 10:30 11:15 Joaquin Garcia-Alfaro Security and Privacy on EPC Networks
- 11:15 12:00 M. Abdalla: Robust Public-Key and Identity-Based Encryption.
- **12:00 1:30** Lunch
- 1:30 - 2:00 Rei Safavi-Naini Unconditionally secure key agreement over noisy channels
- 2:00 3:30 Tutorial A: Fault attacks from theory to practise: what is possible to do?
- 3:30 4:00 Break II
- 4:00 5:30 Tutorial B: New Techniques in Privacy-Preserving Data Mining and Machine Learning

DAY 2

- 8:30 9:15 Student Presentation
  - M. Gagné: "Automated Security Proof for Symmetric Encryption Modes."
  - A. Chaabane: "Revisiting unstructured overlay network security"
  - Chris Ware: "Applications of Geometric Programming in Information Security"
- 9:15 10:00 Kumar Murty: The ERINDALE Hash Function
- 10:00 10:30 Break I
- 10:30 11:15 Bruce Kapron: Computational Indistinguishablility Logic
- 11:15 12:00 Blanchet Bruno: CryptoVerif
- **12:00 1:30** Lunch
- 1:30 2:00 Marine Minier: Some integral properties of Rijndael
- 2:00 3:30 Tutorial B 2nd Part
- 3:30 4:00 Break II
- 4:00 5:30 Tutorial A 2nd part
- 5:30 - 6:00 **BUISNESS Meeting**
- WORKSHOP DINER 7:30 PM at the "bubble" cable

Social Event

WORKSHOP DINER

7:30 PM Saturday, using the "bubble" cable to go "La Bastille".

5:30 - 6:00 **BUISNESS Meeting**

PUB: VETO 2009

3rd International Workshop on
Security and Electronic Voting
Sunday 28 June 2009
http://www-veto2009.imag.fr/

Piece of Program

- Peter Ryan (University of Luxembourg)
- Jacques Traoré (Orange) "Towards Practical Coercion-Resistant Electronic Elections".
- Damien Vergnaud (ENS ULM) "Traceable Anonymous Encryption"
- Olivier de Marneffe (UCL Belgium)
- Mark Ryan (University of Birmingham UK)...