Research Review Seminar
for NSERC Strategic Project Grant
Collaborated with RIM

University of Waterloo
February 25, 2010

Organizers: Guang Gong
Anwar Hasan

Program

DC 1302: 9:00-11:55am

9:00 – 9:05 am	Opening Remark
9:05 – 9:20 am	Selective DFT Attacks on Stream Ciphers and the Spectral Immunity of Boolean Functions, Honggang Hu
9:20 – 9:35 am	An Adaptive Idle-Wait Countermeasure Against Timing Attacks on Public-Key Cryptosystems, Carlos Moreno
9:35 – 9:50 am	Compressing Pairing Values, Koray Karabina
9:50 – 10:05 am	Adaptive Recovery for Transient Errors in Elliptic Curve Scalar Multiplication, Abdulaziz Alkhoraidly
10:05 – 10:20 am	Hummingbird: Ultra-Lightweight Cryptography for Resource-Constrained Devices, Xinxin Fan
10:20 – 10:40 am	Coffee Break
10:40 – 10:55 am	Merging Precomputation and Scalar Multiplication Using Large-Digit Representation, Nicolas Méloni
10:55 – 11:10 am	Implementation of the Compression Function for Selected SHA-3 Candidates on FPGA, Ashkan H. Namin
11:10 – 11:25 am	On the (In)Security of a Pairing-Based Group Signature Protocol, Sanjit Chatterjee
11:25 – 11:40 am	Cloud Computing Security and Privacy Concerns, Anuchart Tassanaviboon
11:40 – 11:55 am	Randomly Directed Exploration: An Efficient Node Clone Detection Protocol in Wireless Sensor Networks, Zhijun Li

DC 1302: 12:00-1:25pm

12:00 – 1:20 pm	Lunch Break (lunch provided) and Discussions
1:20 – 1:25 pm	Concluding Remarks