Annual Research Review Seminar for NSERC Strategic Project Grant Collaborated with RIM

University of Waterloo
December 3, 2008

Organizers: Guang Gong
Anwar Hasan
Herb Little

Program

Program

EIT 3151/53: 9:30-11:50am

9:30 – 9:35 am	Opening Remark
9:35 – 9:55 am	On Practicality of Identity-Based Batch Verification, Xinxin Fan
9:55 – 10:15 am	Exotic Number Systems for ECC, Nicolas Méloni
10:15 – 10:35 am	MIMO and LDPC Based Schemes for Physical Layer Security in Wireless Networks, Hong Wen
10:35 – 10:50 am	Coffee Break
10:50 – 11:10 am	Error Detection and Recovery in EC Scalar Multiplication, Abdulaziz Alkhoraidly
11:10 – 11:30 am	On the Security of Pseudorandom Sequences Generated via the Additive Order, Honggang Hu
11:30 – 11:50 am	Two Bitwise-Operation-Based Entity Authentication Protocols, Zhijun Li

EIT 3145: 12:00 – 2:30 pm

11:50 – 1:00 pm	Lunch Break (lunch provided)
1:00 – 2:00 pm	Discussions
2:00 – 2:30 pm	Concluding Remarks