Concordia University
ENCS
Engineering & Computer Science

Concordia Institute for Information Systems Engineering

THE CONCORDIA INSTITUTE FOR INFORMATION SYSTEMS ENGINEERING
IS PLEASED TO PRESENT THE FOLLOWING GUEST LECTURE IN OUR CIISE DISTINGUISHED SEMINAR SERIES

Dr. Ali Miri, Professor

School of Computer Science at Ryerson University, Toronto

A New Multibase Number Representation and its Application to Elliptic and Hyperelliptic Cryptosystems

In many coding and cryptography algorithms, representations of numbers and in particular their Hamming distances have a direct impact on their computational complexity. One such algorithm, scalar multiplication is the central and most time-consuming operation in many public-key curve-based systems such as Elliptic Curve (ECC), Hyperelliptic Curve (HECC) and Pairing-based cryptosystems. Its algorithmic and computational structure has been the focus of extensive research in recent years in a growing effort to reduce its execution time and power/memory requirements and, thus, make the corresponding system suitable for implementation in the myriad of new applications using ubiquitous devices such as PDAs, smartcards, cellphones, RFID tags and wireless sensor networks.

In this talk, we present a new method for scalar multiplication that uses a generic multibase representation to reduce the number of required operations. Further, a multibase NAF-like algorithm that efficiently converts numbers to such representations without impacting memory or speed performance is developed and shown to be sublinear in terms of the number of nonzero terms. Additional representation reductions are discussed with the introduction of window-based variants that use an extended set of precomputations. Extensive testing is carried out to show that our multibase scalar multiplication is the fastest method to date in the setting of ECC/HECC and exhibits a small footprint, which makes it ideal for implementation on constrained devices.

Biography: Ali Miri is a Professor with the School of Computer Science at Ryerson University, Toronto, Canada. He is also a Professor at the School of Information Technology and Engineering, and the Department of Mathematics and Statistics at the University of Ottawa, Ottawa, Canada. His research interests include applied cryptography, digital communication, signal processing, distributed systems, and mobile computing. He is a member of Professional Engineers Ontario, ACM and a senior member of IEEE.

Thursday, March 25, 2010

14:30

EV003.309

Université Concordia University

1455 De Maisonneuve Blvd. West, EV 7.640, Montreal, Quebec, Canada H3G 1M8
Tel: 514-848-2424 ext. 5847 Fax: 514-848-3171 www.ciise.concordia.ca