UNIVERSITY OF TORONTO
Identity, Privacy & Security Institute

The IPSI Lecture Series Presents:

Finding a Needle in an Encrypted Haystack

Professor Ali Miri
Ryerson University

As the world continues to become more connected, the amount of data generated continues to climb. As corporations and governments increasingly monitor many aspects of our lives, the security and privacy concerns that surround this stored data have also become more apparent. While anonymization is suggested for protecting user privacy, it has shown to be unreliable. In contrast, cryptographic techniques are well studied, and have provable and quantifiable security. In this talk, we will look at some of the most important results in the area of searchable encryption and encrypted data processing, including encrypted indeces, Bloom filters and Boneh's IBE-based searchable encryption scheme. We'll also discuss some of the most promising developments in recent years: performing range query through the use of order-preserving encryption and computing over ciphertext using homomorphic encryption. To better illustrate the techniques, the schemes are described in various sample applications involving text and media search. Time permitting, we will also describe a framework where practical scalable privacy-protected copyright detection can be performed, and we will show an application of sequence querying over generic data in the form of an Anti-Virus over encrypted cloud storage.

Tuesday, March 13, 2018

2:00 PM – 3:15 PM

University College, RM 140

15 King's College Cir, Toronto, ON M5S 3H7

Ali Miri has been a Full Professor at the School of Computer Science, Ryerson University, Toronto since 2009. He is the Research Director of the Privacy and Big Data Institute, Ryerson University, an Affiliated Scientist at the Li Ka Shing Knowledge Institute, St. Michael's Hospital, and a member of the Standards Council of Canada, Big Data Working Group. He has also been with the School of Information Technology and Engineering and the Department of Mathematics and Statistics of the University of Ottawa since 2001, and has held visiting positions at the Fields Institute for Research in Mathematical Sciences, Toronto in 2006, and Universite de Cergy-Pontoise, France in 2007, and Alicante and Albecete Universities in Spain in 2008. His research interests include cloud computing and big data, computer networks, digital communication, and security and privacy technologies and their applications. He has authored and co-authored more than 200 referred articles, 6 books, and 8 patents in these fields. Dr. Miri has chaired over a dozen international conferences and workshops, and had served on more than 85 technical program committees. He is a senior member of the IEEE, and a member of Professional Engineers Ontario.

IPSI
Bahen Centre, RM 4127
40 St. George Street, Toronto ON M5S 2E4
E ipsi@utoronto.ca W www.ipsi.utoronto.ca