Graduate Seminar (EEL 6936)
Department of Electrical Engineering
http://ee.eng.usf.edu/Grad_Seminar

Sara Zafar Jafarzadeh

Département d'Informatique et de Recherche Opérationnelle
Université de Montréal, Montreal, Canada
&
ISARA Corporation, Waterloo, Canada

Friday, November 3rd, 2017, 3:00 p.m. - 4:00 p.m.
College of Engineering (ENB) Room 118

Cryptography in Quantum World

Abstract

Cryptography, although practiced as an art and science for thousands of years, had to wait until the end of the 1940s before Claude Shannon gave it a strong mathematical foundation. However, Shannon's approach was rooted is his own information theory, itself inspired by the classical physics of Newton. But our world is ruled by the laws of quantum mechanics. When quantum-mechanical phenomena are considered, new vistas open up both for cryptographers (code makers) and cryptanalysts (code breakers). Some theorems (including by Shannon) remain mathematically correct, but become irrelevant in our quantum world. Most strikingly, it is possible for two people who do not share ahead of time a long secret key to communicate in perfect secrecy under the nose of an eavesdropper with unlimited computing power and whose technology is limited only by the known laws of physics. Conversely, quantum mechanics provides powerful tools to threaten the mechanisms that are currently used on the Internet to protect electronic transactions. Furthermore, it seems—but is not yet proven—that quantum mechanics provides more benefits to cryptanalysts than cryptographers if the latter are restricted to using only classical communication channels. So, in the end, is quantum mechanics a blessing or a curse to the protection of privacy? The jury is still out. No prior knowledge in quantum mechanics or cryptography will be expected from the audience.

Biography

Sara Zafar Jafarzadeh is currently a doctoral candidate under the supervision of Prof. Gilles Brassard and co-supervison of Prof. Louis Salvail in the Laboratoire d'Informatique Théorique et Quantique (LITQ) in the Department of Computer Science and Operation Research at University of Montreal. Currently she is also working as a security researcher at ISARA Corporation, Canada, a cutting-edge security solutions company that offers companies and government agencies quantum-readiness planning and quantum computer-resistant products. Here she is working on developing quantum-safe standards to ensure compliance for vulnerable hardware and software systems. She received her M.Sc. in Artificial Intelligence from the Computer Engineering Department at Ferdowsi University of Mashhad in 2014, where her thesis was titled "Routing in Wireless Sensor Network Using Reinforcement Learning". Her current research interests include security, quantum cryptography and post-quantum cryptography. She is a Member of CryptoWorks21 and the Institut Transdisciplinaire d'Information Quantique (INTRIQ), a highly-interdisciplinary group of university researchers in computer science, engineering, and physics spread across several universities in Quebec, Canada.