I-SENSE Distinguished Seminar Series

TOPIC

Post-quantum Group-based Cryptography

Group-based cryptography is a relatively new family in post-quantum cryptography. In the first part of my talk, I speak about the first dedicated security analysis of one of the central problems in group-based cryptography, the so-called Semidirect Discrete Logarithm Problem (SDLP). We provide a connection between SDLP and group actions, a context in which quantum sub exponential algorithms are known to apply. We are therefore able to construct a sub exponential quantum algorithm for solving SDLP, thereby classifying the complexity of SDLP and its relation to known computational problems. In the second part of my talk, I will speak about Post-quantum hash functions using special linear groups with implication to post-quantum blockchain technologies.

SPEAKER

Delaram Kahrobaei, Ph.D.

Professor of Mathematics and Computer Science at the City University of New York, Queens College and the Honorary Chair of Cybersecurity at the University of York

Hosted by Reza Azarderakhsh, Ph.D.

Friday, Feb. 16
11 a.m. – 12 p.m.
Engineering East Building, EE303c, Boca Raton Campus and on Zoom

Unable to join in person? Attend on Zoom
http://tinyurl.com/nhjkntz6

For more information, please contact
Yami Triana at ytriana@fau.edu or (561)-297-2886