

Seminar Talk

Tran Viet Xuan Phuong, Ph.D.
Post Doc Research Associate
Center for Cybersecurity of Education and Research
Old Dominion University

Tuesday, November 07, 2017
3:00 p.m. KH 224

Title: Functional Encryption and Its Application

Abstract:

Access control plays an important role in many information systems. Embedding policy-based access control into modern encryption schemes is an interesting but challenging task that has been intensively studied by the cryptographic research community in recent years. Furthermore, most of encryption schemes require not only the guarantee of security, but also the efficiency in terms of computational and communication cost when producing ciphertext and secret key. In this talk, I will present a next generation of public key encryption called Functional Encryption comprising its sub-classes such as Attribute Based Encryption, Hidden Vector Encryption, and Inner Product Encryption. We boost the advantage of these encryption schemes by improving their performance, which is critical for real applications. We also consider the user anonymity in these encryption systems in order to protect user privacy, which is very important nowadays.

Bio:

Dr. Tran Viet Xuan Phuong received the Bachelor degree in Vietnam National University - University of Science in 2010, M.S. degree in Japan Advanced Institute Science Technology in 2012, Ph.D. degree with the School of Computing and Information Technology, University of Wollongong, Wollongong, Australia in 2016. Currently, she is a Postdoc Research Associate in the Center Cybersecurity of Education and Research, Old Dominion University. Her main research interest is applied cryptography, network security and IoT cybersecurity.