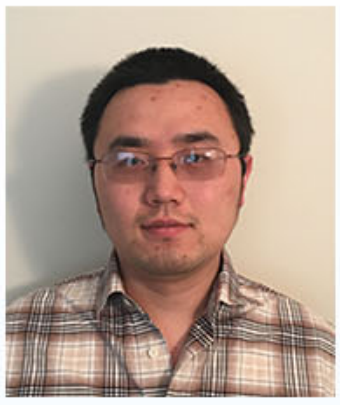
PolyU

THE HONG KONG POLYTECHNIC UNIVERSITY
香港理工大學

Department of Computing
電子計算學系

Research Seminar

A short review of the NTRU cryptosystem



Dr Zhenfei Zhang
Senior Research Scientist
OnBoard Security
USA

Date : 13 July 2017 (Thursday)
Time : 10:30 a.m. – 11:30 a.m.
Venue : Room PQ703, 7/Floor, PQ Core, Mong Man Wai Building,
The Hong Kong Polytechnic University

Abstract

In this talk we will be talking about one of the most promising candidate of quantum-safe cryptography, namely, the NTRU lattice based cryptosystem. In particular, we will be focusing on two candidate schemes: the NTRUEncrypt public key encryption scheme, and the pqNTRUSign signature scheme.
We will start with the basic construction of the NTRU lattice, NTRU trapdoor function, then moving towards the detailed construction of those schemes. We will review the best known attacks in the literature, and show how to derive parameters to thwart those attacks while maintaining practicality. The talk will be conclude with a list of future work/challenges.

About the Speaker

Dr Zhenfei Zhang is a senior research scientist at OnBoard Security, a company that developed NTRU and the related technologies. Before joining OnBoard Security, he was a Ph.D candidate at University of Wollongong, Australia, and received his degree in 2014. His main research interest is quantum-safe cryptography, specifically, lattice-based cryptography. He is also an active member of several quantum-safe standardization groups such as European Telecommunications Standards Institute (ETSI) Industry specification group (ISG) of quantum-safe cryptography and International Organization for Standardization (ISO) cyber-security working group.

All are welcome!

Enquiries:
Professor George Baciu
Email: csgeorge@comp.polyu.edu.hk
Tel : 2766 7295 / 2766 7272

We drive innovation through
SMART COMPUTING