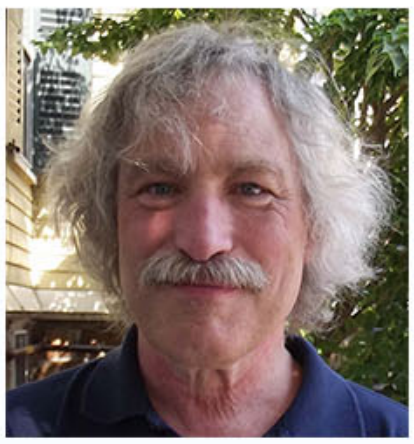
PolyU

THE HONG KONG POLYTECHNIC UNIVERSITY
香港理工大學

Department of Computing
電子計算學系

Research Seminar

The NTRU class of cryptosystems, lattices, and post quantum Cryptography



Prof. Jeffrey Hoffstein

Professor
Mathematics Department
Brown University
USA

Date : 1 August 2017 (Tuesday)
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

I will give a history of the development of the NTRU cryptosystem, and a high level overview of how it works. I will also explain how NTRU influenced the development of cryptography over the past 20 years and why it and other related cryptosystems have become particularly relevant in a future that may include quantum computers. No previous knowledge of cryptography will be assumed.

About the Speaker

Jeffrey Hoffstein is a Professor of Mathematics at Brown University, a co-inventor of the NTRU public key cryptographic system, an ICERM Associate Director and a member of the Board of Directors of Security Innovation Inc and OnBoard Security, inc. He received his PhD in mathematics from MIT in 1978. After holding postdoctoral positions at the Institute for Advanced Study, Cambridge University, and Brown University, Hoffstein was an Assistant and Associate Professor at the University of Rochester. He came to Brown as a Full Professor in 1989. His research interests are number theory, automorphic forms, and cryptography. Hoffstein has written over seventy papers in these fields, co-authored an undergraduate textbook in cryptography, and jointly holds twelve patents for his cryptographic inventions. He was a co-founder of NTRU Cryptosystems, Inc., now merged with Security Innovation, Inc.

All are welcome!

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

We drive innovation through
SMART COMPUTING