For Favour of posting

The Hong Kong University of Science and Technology

Department of Mathematics

Seminar on Pure Mathematics

Cryptanalysis and Repair of The MI Family of Multivariate Public Key Schemes

By

Prof. Lei HU

State Key Lab of Information Security, CAS

Abstract

Post-quantum cryptography is public key cryptography which is thought to be secure against attacks by quantum computers. This is in response to the progress of quantum computer researches and is currently a hot research topic. Multivariate public key cryptography with the intractability of solving multivariate nonlinear equations as security basis is one particular class of post-quantum cryptography and Matsumoto-Imai (MI) schemes are the earliest and remains an important family in this class. Its original form was broken by linearization equation attack, and thus several variants were proposed and continue to be studied. In this talk, we will review some of the variants and their weakness, and then report some analysis and repair results of the MI Family. In the end we will propose a related finite field problem.

Date: **Wednesday, 28 March 2018**

Time: **5:00p.m. - 6:00p.m.**

Venue: **Room 4475, Academic Building (near Lifts 25 & 26), HKUST**

All are welcome!