Abstract:
In this talk, we explain how the algebraic subfield structure can be exploited to obtain more efficient cryptanalysis in many cryptosystems. Firstly, we describe ”extended tower number field sieve” method (based on my work at Crypto2016 and PKC2017) that leads a significant security loss in pairing-based cryptosystems using subfield structures of finite fields. In addition, we also present that lattice reduction algorithms (e.g. LLL algorithm) can be accelerated when the lattices are defined over a number field that contains a certain subfield (whose ring of integers are Euclidean ring). The later topic is based on my recent work that appeared at IMA conference on Cryptography and Coding.