Abstract:
A multivariate public key cryptosystem (MPKC) is a public key cryptosystem whose public key is a set of multivariate quadratic forms over a finite field. It has been considered to be one of candidates of Post Quantum Cryptographies. From 1980s to now, various MPKCs have been proposed and some of them were already broken. In this talk, we give a survey on MPKCs.