Manhattan Algebra Day

Ludovic Perret

Universite Pierre et Marie Curie

On the Design of Multivariate Schemes

Friday, December 8, 2017
CUNY Graduate Center, Science Center

Abstract:
The purpose of multivariate cryptography is to design schemes whose security is related to the problem of solving a system of non-linear equations. Multivariate cryptography is a classical candidates for post-quantum cryptography. The current NISTs standardization process on post-quantum cryptography renewed the interest in the design of multivariate cryptosystems. The goal of this talk is to present an overview of the most recent results in this field; with a particular focus on signature schemes.