Recent results on rank-based cryptography

Philippe Gaborit
Université de Limoges, France

Abstract :

Rank-based cryptography was introduced by Gabidulin et al. in 1991, since then many systems have been proposed. Rank-based cryptography has the inherent good property that the complexity of best known attacks increases faster than for Hamming metric for a given size of key.

In this talk we will review recent results on rank-based cryptography, in particular recent submissions to NIST, based on problems with no masking. We will consider the Ouroboros approach and some advanced encryption schemes.