MASTER INTERNSHIP PROPOSAL

A. COUVREUR

Title: Cryptanalysis of rank–metric code based systems.

Key words: Rank metric codes, skew polynomials, algebraic codes, cryptanalysis.

Contact: Alain COUVREUR (CR INRIA Saclay) alain.couvreur@inria.fr.

Rank metric codes are spaces of matrices endowed with the following metric: the distance between two matrices is the rank of their difference. This metric is natural for instance when you consider packets failure and losses in networks. On the other hand this metric can be considered in code-based cryptography: in the current NIST call for post quantum cryptosystem, two proposals selected to round 2 are based on rank metric \cite{2,1}.

Among the existing proposals in rank metric, one of them due to Faure and Loidreau \cite{3} relies on the hardness of decoding Gabidulin codes \cite{4} above half the minimum distance. This proposal has been subject to an attack by Gaborit, Otmani and Talé \cite{5} and a recent reparation has been proposed \cite{6}. The objective of this internship are:

— Study the literature on rank metric codes and their applications to cryptography;
— Analyse the security of the proposed reparation of Faure–Loidreau system.

RÉFÉRENCES


