Linear Code Equivalence Problem Cryptanalysis

Charles Brion*[1]

[1]University of Rouen – Université de Rouen Normandie – France

Résumé

The Code Equivalence Problem is a set of cryptographic primitives on which are based several submissions to the last NIST call for signatures. Among them we can find LESS, MEDS or PERK. Basically, linear codes are vectors spaces endowed with a metric for which we define isometries. These applications preserve the metric of codes. A problem can be defined for two given codes with the same metric: *find (if exists) an isometry sending one code to the other.* In the case of Hamming metric, isometries are the linear (or monomial) applications which act on the codewords by permuting and scaling the coordinates. Several frameworks led to attacks of this primitive. The two main categories of attacks are the one based on **matches between codewords** of the two codes and the one based on **canonical forms** for generator matrices. Our work is an optimisation of the first type of attacks.

*Intervenant