A post-quantum encryption scheme based on linearized Reed-Solomon codes

Kayodé Epiphane Nouetowa*[1]

[1]Institut de Recherche Mathématique de Rennes – Université de Rennes I – France

Résumé

Designing a McEliece-type scheme is often challenging because the secret codes involved are structured codes that are difficult to hide effectively while still achieving a secure scheme with small key sizes.
For Gabidulin codes, Overbeck's distinguisher is the main tool used to attack schemes based on this family of codes. Linearized Reed–Solomon codes generalize Gabidulin codes. However, to the best of our knowledge, no polynomial-time analogue of Overbeck's distinguisher exists for this family of codes. Therefore, using linearized Reed–Solomon codes provides better protection against structural attacks compared to Gabidulin codes.
In this presentation, I will discuss a new McEliece-type scheme based on linearized Reed–Solomon codes in the sum-rank metric, in which the scrambler matrix is a block-diagonal matrix whose block entries generate a subspace of small dimension. We will see that the resulting key sizes are competitive with those of other well-known schemes.

*Intervenant