Complexity analysis of the Support-Minors modeling of the MinRank problem

Alban Gilard*[1]

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

Résumé

The MinRank problem is a linear algebra problem, largely used in cryptography : given matrices with coefficients in a field, find a non trivial linear combination of the matrices that has a small rank. It is at the core of the Mirath signature scheme which is currently in the second round of the NIST competition for additional signature schemes. Studying the complexity of this problem allows to adjust precisely the parameters for the signature scheme or to estimate the complexity of an attack using the MinRank problem.
There are several algebraic modelings of the problem. The main ones are: the Kipnis-Shamir modeling, the Minors modeling and the Support-Minors modeling. The Minors modeling has been studied by Faugère et al. (2010), where the authors provide an analysis of the complexity of computing a Gröbner basis of the modeling, through the computation of the exact Hilbert Series for a generic instance. The Support-Minors modeling has been introduced by Bardet et al. (2020) and its complexity has previously been investigated by us through the computation of its Hilbert series. Here, we use these previous results to study asymptotically the complexity of computing a Gröbner basis of the Support-Minors modeling or the Minors modeling for generic instances. We then examine the impact of adding field equations to the Support-Minors system, when the field is finite.
This work allows to compare the Minors and Support Minors modeling, and better understand the Support-Minors modeling of a generic MinRank instance. This is a collaboration with Magali Bardet.

*Intervenant