A MinRank-based encryption scheme à la Alekhnovich-Regev

Romaric Neveu*[1]

[1]XLIM – Université de Limoges, Centre National de la Recherche Scientifique – France

Résumé

Introduced in 2003 and 2005, Alekhnovich and Regev's schemes were the first public-key encryption schemes whose security is based solely on the average hardness of decoding random linear codes and LWE, without other security assumptions.
Such security guarantees made them very popular, being at the origin of the now-standardized HQC or Kyber.
However, other metrics (other than Hamming or Euclidean) can be considered. In particular, this talk will focus on matrix codes, using the rank metric.
In this talk, I will present an adaptation of Alekhnovich and Regev's encryption scheme whose security is only based on the hardness of a slight variation of decoding random matrix codes: the stationary-MinRank problem.
We succeeded in reaching this strong security guarantee by showing that stationary-MinRank benefits from a search-to-decision reduction.
Our scheme therefore brings a partial answer to the long-standing open question of building an encryption scheme whose security relies solely on the hardness of decoding random matrix codes.
I will first present the historical background and the motivations of this work, followed by the scheme and its security reduction.
Collaboration avec Thomas Debris-Alazard, Philippe Gaborit, et Olivier Ruatta

*Intervenant