Constant-time decoding of Gabidulin codes and their generalizations with application to RQC

Anthony Fraga*[1]

[1]Mathématiques Sécurité de l'information – Xlim – France

Résumé

Gabidulin codes are a rank metric analog of Reed-Solomon codes. Although these codes are used indifferent very efficient rank-based cryptosystems like the RQC cryptosystem or the Loidreau cryptosystem, there was no constant-time implementation of Gabidulin codes, when having a constant-time implementation is crucial for real-life development of cryptosystems.

In this paper, we propose the first constant-time decoding algorithm of Augmented Gabidulin (AG) codes, a simple variation on Gabidulin codes where one adds zero columns to Gabidulin codes, and which contains the case of Gabidulin codes. These AG codes are used in practice in the most efficient variations of the RQC cryptosystem.

We prove that AG code decoding can be achieved with quadratic complexity. We further present a constant-time algorithm for the left division of q-polynomials along with a complete description of the AG code decoding procedure. These algorithms are integrated into the RQC-Block-MS-AG scheme, and we evaluate the performance of our implementation through benchmarks. Our results show that our implementation outperforms the original RQC, though it remains approximately four times

*Intervenant

slower than HQC. However, it achieves ciphertexts and key sizes about

four times smaller, highlighting an appealing trade-off between performance and compactness.