Improving the decryption failure rate analysis for the HQC cryptosystem

Nicolas Aragon[*]
Joint work with Philippe Gaborit and Gilles Zémor

Abstract

The Hamming Quasi-Cyclic (HQC) cryptosystem [1] is one of the two code-based cryptosystems selected as alternate candidate for the third round of the NIST standardization process, along with BIKE. The key feature of HQC is the security reduction to the syndrome decoding problem for structured codes: there is no need for an assumption about indistinguishability of the family of codes used in this scheme.

The decryption procedure in HQC uses an efficient decoding algorithm for a public code, which is chosen as a tensor product code of BCH and repetition codes in the original HQC description. As the weight of the error that needs to be decoded is not constant in this scheme, some errors of unusually large Hamming weight can make the decoding algorithm fail, making the choice of the public code particularly important for studying the decryption failure rate (DFR) of the cryptosystem.

The contribution of this work is twofold:

1. We provide a better analysis of the weight distribution of the HQC error vectors. We approximate the HQC error vectors by vectors for which the coordinates follow a binomial distribution, and give theoretical arguments as well as experimental results showing that the two distributions are close. This approximation allows for an easier and more precise analysis of the decoding errors.

2. We propose to use concatenated Reed-Muller and Reed-Solomon codes instead of BCH and repetition codes, and we derive an upper bound for the decoding failure probability of this family of codes against binary symmetric channels.

These two improvements combined together yield an improvement of the HQC parameter sizes of approximately 20%: as an example for 256 bits of security, this allows to reduce the size of the public key from 8.9kB to 7.2kB.

A preprint of this work is already available [2].

References

[1] Carlos Aguilar-Melchor et al. "Efficient encryption from random quasi-cyclic codes". In: *IEEE Transactions on Information Theory* 64.5 (2018), pp. 3927–3943.

[2] Nicolas Aragon, Philippe Gaborit, and Gilles Zémor. "HQC-RMRS, an instantiation of the HQC encryption framework with a more efficient auxiliary error-correcting code". In: *arXiv preprint arXiv:2005.10741* (2020).

[*] Univ Rennes, CNRS, Inria, IRISA