Error floor prediction with Markov models for QC-MDPC codes

Angela Robinson

National Institute of Standards and Technology, USA

Quasi-cyclic moderate-density parity check (QC-MDPC) code-based encryption schemes under iterative decoders offer highly-competitive performance in the quantum-resistant space of cryptography, but the decoding-failure rate (DFR) of these algorithms are not well-understood. The DFR decreases extremely rapidly as the ratio of code-length to error-bits increases, then decreases much more slowly in regimes known as the waterfall and error-floor, respectively. This work establishes three, successively more detailed probabilistic models of the DFR for iterative decoders for QC-MPDC codes: the simplified model, the refined model for perfect keys, and the refined model for all keys. The models are built upon a Markov model introduced by Sendrier and Vasseur that closely predicts decoding behavior in the waterfall region but does not capture the error floor behavior. The simplified model introduces a modification which captures the dominant contributor to error floor behavior which is convergence to near codewords introduced by Vasseur in his PhD thesis. The refined models give more accurate predictions taking into account certain structural features of specific keys. Our models are based on the step-by-step decoder, which is highly simplified and experimentally displays worse decoding performance than parallel decoders used in practice. Despite the use of the simplified decoder, we obtain an accurate prediction of the DFR in the error floor and demonstrate that the error floor behavior is dominated by convergence to a near codeword during a failed decoding instance. Furthermore, we have run this model for a simplified version of the QC-MDPC code-based cryptosystem BIKE to better ascertain whether the DFR is low enough to achieve IND-CCA2 security. Our model for a modified version of BIKE 1 gives a DFR which is below

MCA 2025 internal code: SS55-T07

$2^{-129.5}$, using a block length $r = 13477$ instead of the BIKE 1 parameter $r = 12323$.

In Special Session 55 on Post-Quantum Cryptography at the Mathematical Congress of the Americas 2025.