Errata for "A Study of Error Floor Behavior in QC-MDPC Codes"

Sarah Arpin[1], Tyler Raven Billingsley[2], Daniel Rayor Hast[3], Jun Bo Lau[4], Ray Perlner[5], and Angela Robinson[5]

[1] Universiteit Leiden, Mathematics Institute
[2] Rose-Hulman Institute of Technology, Department of Mathematics
[3] Boston University, Department of Mathematics & Statistics
[4] University of California San Diego, Department of Mathematics
[5] National Institute of Standards and Technology, Computer Security Division

Abstract. This errata corrects some errors found after publication in the paper "A study of error floor behavior for QC-MDPC codes".

Keywords: BIKE, error-correcting codes, McEliece, PQC, QC-MDPC

1 Introduction

After publication, we discovered an inconsistency between our implementation of the BGF decoder used to analyze decoding failures and the intended BGF decoder. The purpose of this errata is to document this inconsistency and note what implications it has for the results of our paper [3]. (See [2] for the decoder implementation and raw data used in the paper.)

The bit-flipping threshold T used in the BGF decoder is the maximum of two values: $\frac{d+1}{2}$, where d is the column weight of the BIKE secret key H, and the output of an adaptive threshold function, call it T', first defined in [4] and in section 2.5.1 of the BIKE v1.0 specification [1].

While we correctly implemented the adaptive threshold function T', we failed to set the bit-flipping threshold $T = \max(T', \frac{d+1}{2})$. Vasseur notes that "a threshold lower than $\frac{d+1}{2}$ is generally detrimental for decoding" [5, §6.1.3.1]. This lower bound on the threshold was inadvertently omitted from our implementation.

2 Implications

To determine the extent of the impact of this inconsistency on our results, we re-ran our analyses using new data generated by a more highly optimized implementation[6] (written in Rust) that uses the correct lower bound on the threshold. Overall, many of our results do not significantly differ in the reanalysis; however, some did change. The key implications are as follows:

1. The plot of decoding failure rates for non-weak keys with weak key threshold $T = 3$ (corresponding to Figure 1 in [3]) did not change in any significant *qualitative* way; the waterfall region and error floor region are still clearly visible and have roughly the same shape, with nearly quadratic fit for the waterfall region and linear fit for the error floor region.
2. The overall decoding failure rates (DFRs) are slightly smaller: for example, approximately $2^{-20.8}$ instead of $2^{-19.6}$ for $r = 587$. The updated plot is shown in Figure 1 on the left.
3. For *unfiltered* random keys (that is, allowing weak keys), the difference in the DFR is highly significant. In section 3 of our paper, we noted that filtering out fewer weak keys just by increasing the weak key threshold from $T = 3$ to $T = 4$ caused the DFR to "increase enormously", rising to around 2^{-8} for $r = 587$. With the corrected threshold function, this large discrepancy between weak and non-weak keys is not seen; the DFR for unfiltered keys is larger than for non-weak keys, but the difference—while

[6] Available at https://github.com/HastD/rust_bike_decoder

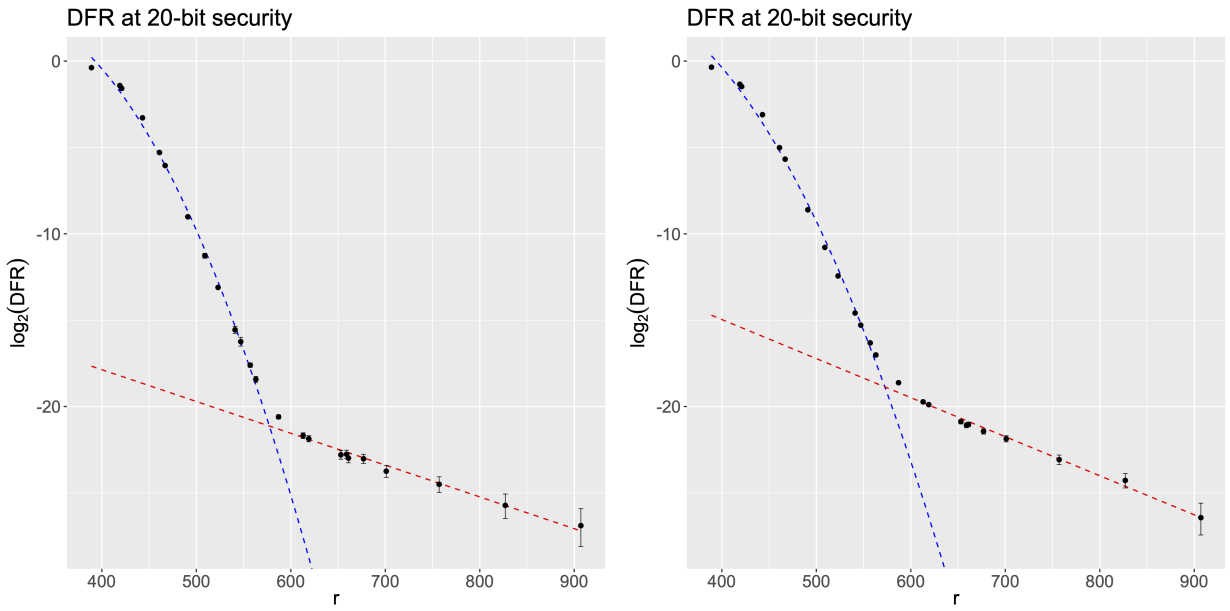

Fig. 1: Semi-log plot of decoding failure rates for non-weak keys ($T = 3$, left) and for unfiltered random keys (right). For all data points, the number of trials was at least 10 times those used in the paper.

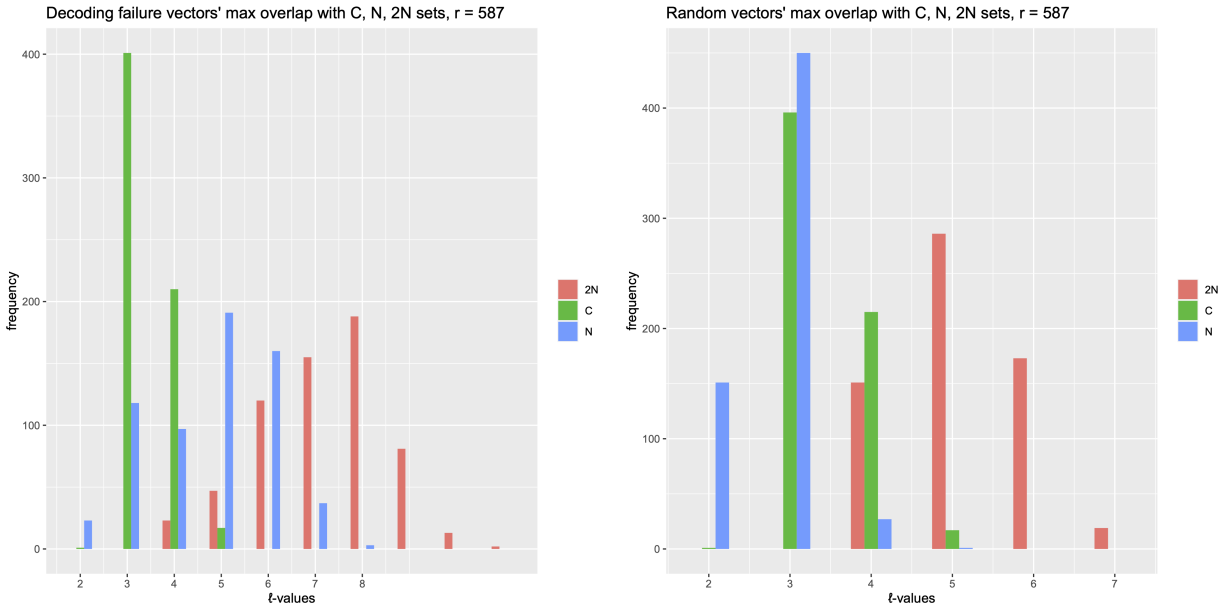

Fig. 2: Distribution of maximum overlaps of decoding failure vectors (left) or random vectors (right) with the sets $\mathcal{C}$, $\mathcal{N}$, and $2\mathcal{N}$ for $r = 587$, using a weak key threshold of $T = 3$ to generate keys.

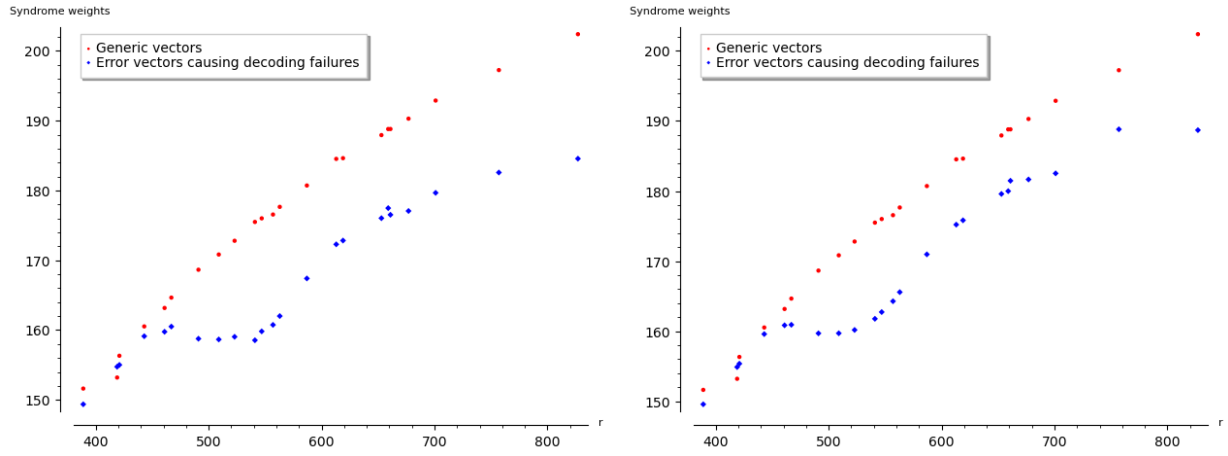

Fig. 3: Distribution of syndrome weights for random error vectors (red) versus error vectors causing decoding failures (blue). The left plot is for non-weak keys (with threshold $T = 3$); the right plot is for unfiltered random keys.

statistically significant—is much smaller, with a DFR of $2^{-18.9}$ for unfiltered keys. The corresponding DFR plot for unfiltered random keys is shown in Figure 1 on the right. Results for non-weak keys with $T = 4$ were in an intermediate range between those of the two figures.

4. The distribution of overlaps of decoding failure vectors with vectors in the sets $\mathcal{N}$ and $2\mathcal{N}$ (but not $\mathcal{C}$), analyzed in figures 3, 4, and 5 of our original paper, shifted by a statistically significant amount in the new data. In particular, while in the older data there does not appear to be a significant difference between the distribution for random error vectors and error vectors that cause decoding failures, the distributions of overlaps with $\mathcal{N}$ and $2\mathcal{N}$ are clearly distinct in the new data. See Figure 2.
   This suggests that some proportion of decoding failures are explained by proximity to $\mathcal{N}$ or $2\mathcal{N}$. However, it is also the case that a significant portion of decoding failure vectors do not have more overlap with these sets than typical random vectors; it will require further analysis to determine what proportion of decoding failures are explained by this proximity.
5. Our conclusion that vectors causing decoding failures have significantly lower syndrome weights than random error vectors is unchanged. In fact, with the larger number of trials, this result is even more clearly visible in the data; see Figure 3 (corresponding to Figure 7 in [3]).

References

1. Nicolas Aragon, Paulo Barreto, Slim Bettaieb, Loïc Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Shay Gueron, Tim Güneysu, Carlos Aguilar Melchor, Rafael Misoczki, Edoardo Persichetti, Nicolas Sendrier, Jean-Pierre Tillich, and Gilles Zémor. BIKE: Bit flipping key encapsulation - spec v1.0. https://bikesuite.org/files/BIKE.2017.11.30.pdf, 2017.
2. Sarah Arpin, Tyler Raven Billingsley, Daniel Rayor Hast, Jun Bo Lau, Ray Perlner, and Angela Robinson. Raw data for the paper "A study of error floor behavior in QC-MDPC codes". https://github.com/HastD/BIKE-error-floor. Accessed: 2022-05-23.
3. Sarah Arpin, Tyler Raven Billingsley, Daniel Rayor Hast, Jun Bo Lau, Ray Perlner, and Angela Robinson. A study of error floor behavior in QC-MDPC codes. In Jung Hee Cheon and Thomas Johansson, editors, *Post-Quantum Cryptography*, pages 89–103, Cham, 2022. Springer International Publishing.
4. Julia Chaulet. *Etude de cryptosystèmes à clé publique basés sur les codes MDPC quasi-cycliques*. Theses, Université Pierre et Marie Curie - Paris VI, March 2017.
5. Valentin Vasseur. *Post-quantum cryptography: a study of the decoding of QC-MDPC codes*. PhD thesis, Université de Paris, Mar 2021.