MAYO Round 2 Submission Modifications

The following modifications to the MAYO submission were made for the second round of the NIST PQC Additional Digital Signature Schemes process:

- **Different representation of sequences of $\mathbf{m}$ matrices.** Batches of matrices are now stored in nibble-sliced form, rather than bitsliced form. This change allows for significantly faster implementations on AVX2 and Arm NEON platforms by using shuffle instructions, and slightly more efficient implementations on Cortex-M4 platforms using the method of the four Russians. For more information, we refer to [BCC+24].
- **Updated security analysis.** The security analysis section was expanded to keep it up to date with the cryptanalysis of OV-based schemes. A paragraph about the rectangular minrank attack was added, the section about claw-finding attacks was expanded, and the system-solving section was expanded to encompass Hashimoto's algorithm for solving underdetermined systems of multivariate quadratic polynomials.
- **Updated parameters.** New parameter sets are selected satisfying the following criteria:
  - $\mathbf{n} - \mathbf{o} \leq \mathbf{m}$. In the round 1 submission, the parameters satisfied $o > n - m$, which means that the dimension of the variety defined by $\mathcal{P}(\mathbf{x}) = 0$ is larger than $n - m$, the generic dimension of a variety defined by m multivariate quadatic equations in n variables. We are not aware of ways to compute this dimension that are more efficient than known key recovery attacks, so to the best of our knowledge this does not break the Oil and Vinegar assumption, which says that $\mathcal{P}$ is computationally indistinguishable from a randomly chosen sequence of multivariate quadratic equations. Nevertheless, we decided to pick parameters with $o \leq n - m$, so that $\mathcal{P}(\mathbf{x}) = 0$ has dimension $n - m$. Additionally, this blocks the rectangular Minrank attack [FI23], which simplifies the concrete security analysis of MAYO.
  - **Increased security margin against system-solving attacks.** To hedge against improvements in generic system-solving methods, we pick parameters to have at least 10, 15, and 20 bits of security margin, for the NIST security level 1, 3, and 5 parameters respectively.
  - **Higher restart probability.** During the signing procedure, there is a small probability that the SampleSolution subroutine fails, in which case signing restarts. With the round 1 parameters this restart probability was lower than 2^{-36}, which makes it hard to cover the complete implementation with known answer tests. Therefore, for the round 2 parameters, we increased this probability to between 2^{-12} and 2^{-20}, so that the restarting is easier to test, but still low enough so that the average signing time is not affected much.
- **Added more implementations and benchmarks.** We have added an Arm NEON optimized implementation of MAYO to the submission package, and included benchmark results for the Apple M1 and M3 processors. We extended the Cortex-M4 optimized implementation to cover MAYO_3, and added benchmark results.

References

[BCC+24] Ward Beullens, Fabio Campos, Sofía Celi, Basil Hess, and Matthias J. Kannwischer. Nibbling MAYO: Optimized implementations for AVX2 and cortex-M4. *IACR TCHES*, 2024(2):252–275, 2024.

[FI23] Hiroki Furue and Yasuhiko Ikematsu. A new security analysis against MAYO and QR-UOV using rectangular MinRank attack. In Junji Shikata and Hiroki Kuzuno, editors, *IWSEC 23*, volume 14128 of *LNCS*, pages 101–116. Springer, Cham, August 2023.