

MAYO Round 3 Submission Modifications

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

- **Updated parameters for MAYO₁ and MAYO₂.** We decided to make a minor change to MAYO₁ for the round-3 submission to slightly increase the security against a direct attack, at essentially no cost in performance or sizes (2% increase). In response to the wedge attack which was discovered in the second round we modified the MAYO₂ parameter set to increase the cost of key-recovery attacks.¹ This change resulted in a 28% increase in signature size, a 40% reduction in key size, and improved keygen, signing, and verification performance. Initially, we wanted to change the MAYO₂ parameters to $(n, m, o, k, q) = (82, 64, 13, 5, 16)$. However, days before the submission deadline we were notified privately by Lars Ran and Simon-Philipp Merz of a new key-recovery attack on UOV-like public keys that is more broadly applicable than the Wedge attack. We used $n = 86$ instead of $n = 82$ to push the cost of this new attack above 2^{143} . The new attack will be made public relatively soon. As we are not yet aware of the technical details of this attack, we have not included it in the security analysis section.
- **MDS whipping schedule.** We change the whipping schedule $\{E_{ij}\}_{i \in [k], j \in [k]}$. These matrices correspond to multiplication by powers of z in $\mathbb{F}_q[z]/(f_m(z))$. In the second round submission the order of these matrices was $E_{ij} \leftrightarrow z^{\ell(i,j)}$, where $\ell(i, j) = ik - i(i+1)/2 + j$ for $i \leq j$, and $\ell(i, j) = \ell(j, i)$ otherwise. (This ℓ was implicitly defined by the order in which we loop over (i, j) in the signing algorithm.) However, with this choice, the symmetric matrix $Z := \{z^{\ell(i,j)}\}_{ij}$ has submatrices of unusually low rank, which can be exploited to mildly speed up collision attacks. In the third round submission we have changed the order of the powers of z to make the whipping schedule Z an MDS matrix (i.e., all submatrices have full rank) to eliminate this weakness. This has no impact on the efficiency of the scheme.
- **Adding linear terms to the trapdoor map.** In the second-round submission the public trapdoor map $\mathcal{P}^*$ is a homogeneous quadratic map. We decided to add linear terms to the verification equation, which now becomes $\mathcal{P}^*(s) + L(s) = \text{SHAKE256}(\text{SHAKE256}(M) \parallel \text{salt})$, where the coefficients of the linear map L are determined from the hash of $\text{SHAKE256}(M) \parallel \text{salt}$. The purpose of this modification is to prevent collision attacks. Since both sides of the verification equation depend on M and salt, one can no longer perform a collision search to find forgeries. This is an old idea, proposed already in the original UOV paper in 1999. We have added this modification to the third-round submission, in response to some improvements in claw-finding attacks that were communicated to us privately in August 2026.
- **Improved implementations.** We have made several improvements to our implementations of MAYO, increasing the speed of key-generation, signing, and verification, without the need for changing KAT values. We added an alternative approach to signing which avoids using the L value which is precomputed during MAYO.ExpandSK. This is 20%–30% more efficient when signing using a compact representation of the secret key (because we don't need to compute L), but less efficient when signing a batch of messages (because L can be computed once and used for all of the signatures). We have made the new approach without L the default implementation when signing a message using the compact secret key, while keeping the old approach when signing from a pre-expanded secret key. This approach was suggested to us and implemented by Hiroshi

¹The bit cost of the wedge attack against MAYO₂ was 2^{112} which is lower than the target value of 2^{143} . However, we argue that the attack is much less threatening than the 2^{112} number suggests. The attack requires doing 2^{49} sequential matrix-vector products with a bit cost of 2^{63} each. The sequential nature of the attack limits the amount of parallelization that can be used and forces a long latency of the attack. For example, even if humanity manages to build a machine that does the huge matrix-vector multiplication in 0.02 milliseconds (which is faster than an honest signing or verification operation), the attack would still take 357 years. Simply throwing more hardware at the problem does not bring down the latency. This is reminiscent of the analysis of Grover's algorithm on AES-128. Despite the low gate count, Grover's algorithm is not considered to be a threat against AES-128 in practice, because it requires a very large depth (and thus latency).

Amagasa, who is added to the list of implementers in the third-round submission. Moreover, we have also added an implementation which uses AVX512, GFNI, and VAES instructions, which gives significant speedups on platforms where these are available.

- **Expanded design rationale.** The NIST IR 8610 second round status report mentioned it might be worthwhile to consider odd characteristic parameter sets, and the use of a “salt-UOV” variant of MAYO. We have added the “Choice of finite field.” and “The use of a salt.” paragraphs to section 1 to explain our design choices.
- **Updated security analysis.** We updated the security analysis section with references to the new Wedge attack and improved algorithms for finding solutions to underdetermined systems of quadratic equations. We updated the security proof to include the linear terms in the trapdoor map.