

Changelog (Round 2 → Round 3)

- **Revised signature generation and verification algorithms:** To prevent an excessive increase in the signature-generation time, we restrict signature generation to cases where the coefficient matrix L of the linear system in the oil variables has rank at least $m - \Delta$. Here, m is the dimension of the square matrix L , and Δ is an additional parameter. When the rank of L is low, the expected number of retries in signature generation grows exponentially. We therefore choose Δ as small as possible, subject to the condition that, for a realistic upper bound on the number of signatures generated, the probability of encountering a matrix L with rank less than $m - \Delta$ remains below $1/2$ for the security proof. This choice balances the signature-generation time against the requirement that the rank threshold not affect the security proof.

In addition, to prevent a trivial forgery against the SUF-CMA (strong existential unforgeability against chosen-message attack) security that affects the previous versions, the algorithm compares the two signature candidates $\mathbf{s}$ and $-\mathbf{s}$ in lexicographic order and outputs the smaller one. Indeed, given a valid signature $\mathbf{s}$ on a queried message, an adversary can obtain another valid signature $-\mathbf{s}$ on the same message, thereby producing a fresh message-signature pair as a trivial forgery against SUF-CMA security. Accordingly, the verification algorithm checks that the received signature is the lexicographically smaller of $\mathbf{s}$ and $-\mathbf{s}$.

- **Parameters:** To provide a more refined selection of parameter sets suited to different implementation requirements, we provide two proposed parameter sets for each security level with $(q, \ell) = (127, 3)$ and $(q, \ell) = (127, 10)$. We retain the main parameter sets with $(q, \ell) = (127, 3)$ from the second-round specification and newly add those with $(q, \ell) = (127, 10)$. We select $q = 127$ for its implementation efficiency; the parameter sets with $\ell = 3$ are intended to provide balanced performance, whereas those with $\ell = 10$ offer relatively small public keys. The remaining parameter sets from the second-round specification are provided as additional parameters in the appendix.
- **Implementations:** We improve the QR-UOV implementations through algorithm-level optimizations and SIMD-based acceleration using AVX2, thereby improving overall performance.
- **Security analysis against key recovery attacks:** We added security analyses of QR-UOV against recent key-recovery attacks, including the wedge product attack, the symmetric algebra attack, and the truncated polynomial ring attack, and confirmed that the proposed parameter sets maintain the claimed security levels against these attacks.
- **Security analysis against timing attacks:** The NIST status report on the second-round candidates raised concerns about the cost of protecting

QR-UOV signature generation against timing side-channel attacks. The signing procedure is not constant time specifically because the number of iterations required to sample a salt for which the linear system in the oil variables is solvable depends on the rank of the coefficient matrix L . Since making the signature-generation time independent of $\text{rank}(L)$ would incur substantial performance overhead, we do not attempt to conceal this timing dependence. Instead, we analyze the security impact of leaking this rank information, and our analysis shows no reduction in the estimated complexity of the known key-recovery attacks considered. We also consider an implementation strategy in which the remaining secret-dependent operations are executed in constant time, and evaluate and compare its performance.