Second Round Tweaks - MQDSS
(Post-Quantum Cryptography Standardization Process)

The design of MQDSS has not changed significantly from the version submitted to the NIST Post-Quantum cryptography standardization process. Only minor design changes were made that result in improved efficiency in terms of signature size and speed, as well as improved security analysis.

The following small design tweaks were made:

- The commitment functions now take an additional argument - a random string of length $2k$.
  The reason for this change is that with this additional random input it can be shown that the commitment function in MQDSS instantiated using SHAKE256 is computationally hiding - a propery needed to show the EU-CMA security of MQDSS. We use a recent result from [45]. We have updated the algorithms for key generation, signing and verification accordingly to reflect this change (see Chapter 7 and Chapter 9 for details). We have also updated the security analysis (see Chapter10 and Appendix A).
- The number of rounds r has been reduced to half.
  The reason for this change is that the necessary number of rounds r is half of the one given in the initial sumbission (see Chapter 5 for definition of the parameter r, and Chapter 8 for how it is derived).

A consequence of the introduced tweaks is that for all security levels, the signature size is reduced by more than 35%. There is also a reduction in the size of the public and the secret keys (See Chapter 8 for details, and compare to the same chapter in Version 1.0). Furthermore the performance of the reference and the optimized implementation is significantly improved. Namely, in the reference implementation the signing and verification process are 50% faster than the same algorithms in Version 1.0. The improvement in the optimized implementation is not as dramatic, but still around 40%.

Furthermore, a more accurate analysis for the best classical attacks against the $\mathcal{MQ}$ problem was done, and the estimated classical complexity is now given in terms of gates.