NTS-KEM

Second round submission

Changes from the first round submission

There have been no major changes to NTS-KEM for this second round submission aside from replacing explicit rejection of invalid ciphertexts with implicit rejection. As a result of that change, there are updates to the reference, optimized, and additional implementations, performance numbers and security analysis. In particular on performance numbers, we include the average number of CPU cycles required for the various steps in key-generation, encapsulation and decapsulation, for Intel Haswell processor microarchitecture. There are also new KATs and intermediate values.

Implicit rejection utilises a 32-byte value $\mathbf{z}$ which is included as part of the private key and which is randomly selected during key generation. As a consequence, the private key is increased in size by 32 bytes and the key generation procedure has been updated. For invalid ciphertexts the decapsulation procedure now outputs $\mathbf{k}_r = H_\ell(\mathbf{z} \mid \mathbf{1}_a \mid \mathbf{c}^*) \in \mathbb{F}_2^\ell$ rather than $\perp$ as in the first round submission. As before, the encapsulated key $\mathbf{k}_r = H_\ell(\mathbf{k}_e \mid \mathbf{e}) \in \mathbb{F}_2^\ell$ is returned for properly formed ciphertexts. This approach has been implemented in constant time. The security analysis of NTS-KEM has been updated to reflect the use of implicit rejection; the changes required to obtain our new analysis are small.

The performance changes in the NTS-KEM reference implementation due to implicit rejection are small. There are some changes to the performance numbers that we now report for NTS-KEM, mostly improvements, but these are attributable to further compiler optimisations since round 1.

Two of our team members are founders of PQ Solutions Limited. PQ Solutions Limited has abandoned a UK patent and a US patent application for an invention embodied in part of NTS-KEM. PQ Solutions Limited, its officers and related persons, and the individual members of the NTS-KEM submission team, do not hold (directly or indirectly) any interests in any patents, patent applications, or rights to apply for patents, for inventions embodied in the NTS-KEM methodology.