PQC – Known Answer Tests and Test Vectors

Test vectors are to be generated that can be used to determine the correctness of an implementation. These files come in two types: Known Answer Tests (KAT) files and Intermediate files. The KAT files are for general use to determine an implementation's correctness. The Intermediate values are useful for debugging an incorrect implementation. KAT files shall be provided to test different aspects of the algorithm, e.g., key generation, encryption, decryption.

Submitters should use the scripts available at
http://csrc.nist.gov/groups/ST/post-quantum-crypto/example-files.html
to generate their KAT files.

It would helpful to also provide a few examples with several intermediate values for debugging purposes. An example of such an example is in the file Intermediate Values, which can also be found at the url above.