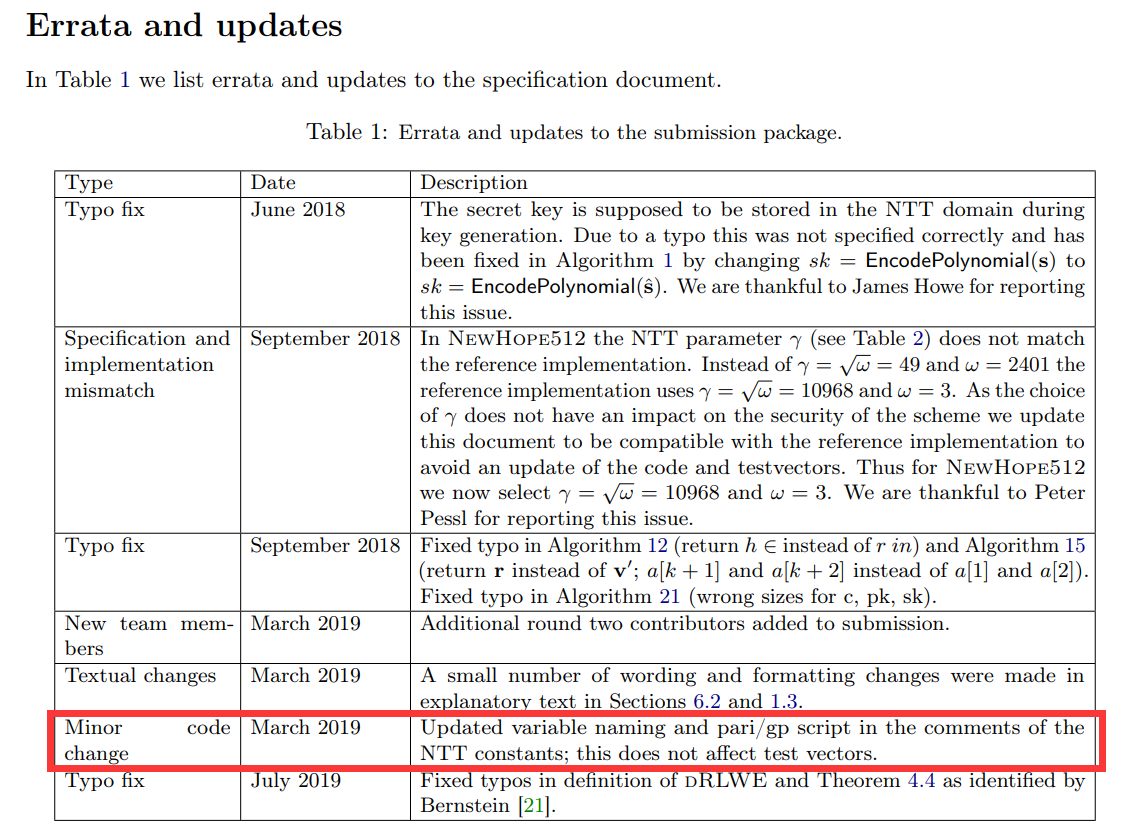
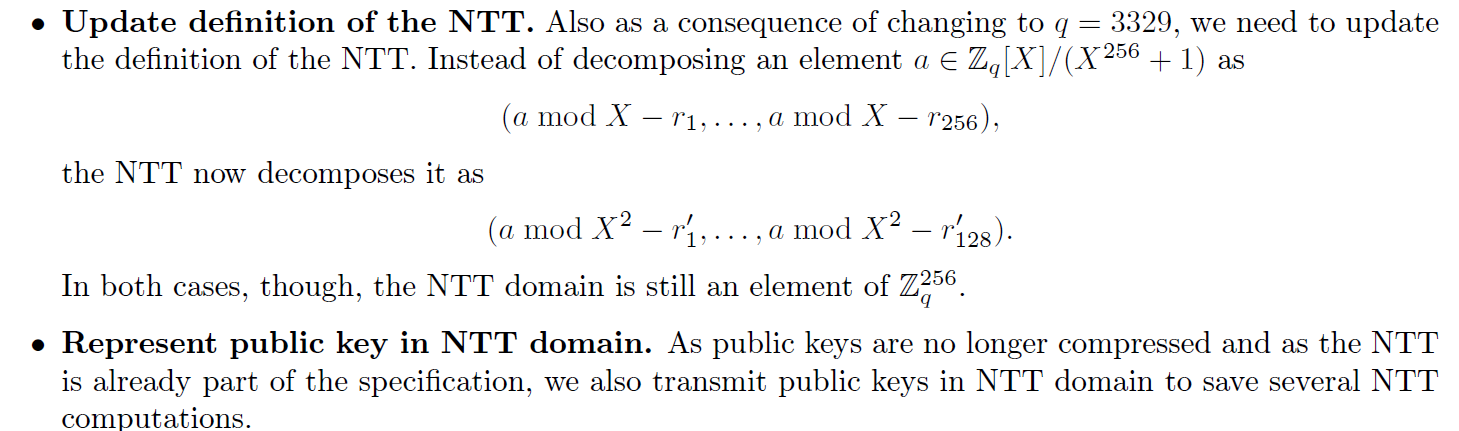
1. In NewHope specification, only mentioned that:Updated variable naming and pari/gp script in the comments of the NTT constants; this does not affect test vectors.



Is this the target we need to confirm?

1. In KYBER specification, the changelog mentioned that:



In my opinion, it just update the expression form, but didn't influence the implementation of NTT?

1. In Dilithium specification, the changelog mentioned that:

The other changes were in the implementation. We made various optimizations in the signing algorithm. The most important optimization is how the rejection condition based on the low part of the vector w and the hint vector is computed. Our AVX2 omptimized implementation now makes more use of vectorization and includes a simpler assembler NTT implementation using macros.

It indeed changed the implementation of the NTT and need to learn.

4. So, in the three update, which would lead to the biggest change of the analysis?

5. I have understood where to inject the fault and the result of injecting this fault. But I haven’t understood that how to perform key recovery clearly. Maybe need more time or explanation.