From: Kathrin Hövelmanns <kathrin.hoevelmanns@gmail.com> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: [pqc-forum] Failing gracefully: Decryption failures and the Fujisaki-Okamoto transform
Date: Friday, March 25, 2022 08:14:41 AM ET

Dear PQC forum,

we have recently posted a preprint on improving the analysis of how correctness errors impact security of FO-transformed schemes. Previous work had the following limitations:
- The correctness term defined in HHK17 is conservative - intuitvely, it assumes the failure-finding attacker to know the secret key. Furthermore, it turns out to be somewhat hard to bound in practice, at least for some of the relevant instantiations. (E.g., asking adversaries to find a bad message-randomness pair, knowing the secret key, disallows to use LWE-type assumptions.)
- Even if the conservative correctness definition would have turned out to be necessary for INDCCA security, the correctness-related part of all of FO's previously known INDCCA bounds looked far more loose in the QROM than in the ROM, and it was not clear whether this loss is meaningful.

We therefore improved on these points: Instead of delta-correctness, our result requires a bound on a game where the adversary has to find failing plaintexts (called FFP), without knowing the secret key. The FFP term in the INDCCA bound only has a linear loss in the number of the attacker's decapsulation queries, regardless of whether the proof is in the ROM or the QROM. We factor the FFP game further into two separate games, yielding the following two additive error terms:
- An error term that depends on the key-independent error probability, i.e., of the maximum failure probability when encryption randomness and key pair are randomly chosen, as well as the corresponding variance, and
- an error term equal to the advantage in a game where the adversary needs to distinguish the use of the secret key corresponding to a given public key from the use of a random secret key via a single decryption query. This game captures the ability of the adversary to use the public key to find a decryption failure.

We hope that the result simplifies dealing with correctness errors. Any feedback would be very welcome.

Cheers,

Kathrin Hövelmanns, Andreas Hülsing and Chris Majenz

--