From: Dang, Thinh H. (Fed)
To: (b) (6)
Subject: Fw: Draft emails to SIKE, HQC, Frodo
Date: Tuesday, August 17, 2021 2:52:00 PM

From: Perlner, Ray A. (Fed) <ray.perlner@nist.gov>
Sent: Tuesday, August 17, 2021 1:45 PM
To: internal-pqc <internal-pqc@nist.gov>
Subject: Draft emails to SIKE, HQC, Frodo

Dear SIKE team,

It is our understanding that in SIKE's category 1 KEM, the ciphertext is generated deterministically from a 128-bit seed, thus allowing a straightforward multi-ciphertext attack that allows an attacker to recover the shared secret for one out of N ciphertexts at a cost of 2^128/N. While this does not contradict the claim of category 1 IND-CCA security for this parameter set of SIKE, it is an undesirable property, and it seems it can be eliminated at negligible cost by simply using a larger seed. Similar considerations apply at category 3 and category 5. (We're generally more concerned about multi-target attacks at the lower security levels.)

As an Alternate, it is likely that the SIKE team will have the opportunity to submit an official tweak. We encourage you to consider a low cost fix to get rid of multi-target attacks.

--NIST PQC Team

Dear FrodoKEM team,

It is our understanding that in Frodo's category 1 KEM, the ciphertext is generated deterministically from a 128-bit seed, thus allowing a straightforward multi-ciphertext attack that allows an attacker to recover the shared secret for one out of N ciphertexts at a cost of 2^128/N. While this does not contradict the claim of category 1 IND-CCA security for this parameter set of Frodo, it is an undesirable property. We think that this multi-ciphertext attack can be eliminated at negligible cost by incorporating a public salt value into the ciphertext, and using that salt combined with the 128-bit seed to generate the rest of the ciphertext. Similar considerations apply at category 3 and 5. (We're generally more concerned about multi-target attacks at the lower security levels.)

As an Alternate, it is likely that the FrodoKEM team will have the opportunity to submit an official tweak. We encourage you to consider a low cost fix to get rid of multi-target attacks.

--NIST PQC Team

Dear HQC team,

It is our understanding that in HQCs category 1 KEM, the ciphertext is generated deterministically from a 128-bit seed, thus allowing a straightforward multi-ciphertext attack that allows an attacker to recover the shared secret for one out of N ciphertexts at a cost of 2^128/N. While this does not contradict the claim of category 1 IND-CCA security for this parameter set of HQC, it is an undesirable property. We think that this multi-ciphertext attack can be eliminated at negligible cost by incorporating a public salt value into the ciphertext, and using that salt combined with the 128-bit seed to generate the rest of the ciphertext. While this will not eliminate all multi-target attacks, due to the existence of the DOOM attack, it will significantly improve the multi-key security of HQC. Similar considerations apply at category 3 and 5. (We're generally more concerned about multi-target attacks at the lower security levels.)

As an Alternate, it is likely that the HQC team will have the opportunity to submit an official tweak. We encourage you to consider a low cost fix to increase security against multi-target attacks.

--NIST PQC Team