From: Peralta, Rene (Fed)
To: (b) (6)
Subject: Fw: Key Establishment for PQC algorithms
Date: Friday, October 28, 2016 11:30:32 AM

From: pqc-forum-bounces@nist.gov <pqc-forum-bounces@nist.gov> on behalf of Moody, Dustin (Fed) <dustin.moody@nist.gov>

Sent: Friday, October 28, 2016 11:27 AM

To: pqc-forum

Subject: [Pqc-forum] Key Establishment for PQC algorithms

NIST received several comments regarding our request for a key-exchange algorithm. As a result, we are clarifying what exactly we are looking for. In our revised call, instead of using the term key-exchange we will be asking for Key Encapsulation Mechanisms (KEMs). While the term KEM has been widely used in academic literature, previous NIST publications have tended to describe KEMs using the term "key agreement" (also known as key exchange). KEM schemes consist of algorithms for key generation, encapsulation, and decapsulation.

One important application is using public-key cryptography to securely establish a key to be used for symmetric encryption. NIST intends to standardize one or more schemes that enable semantically secure encryption or key encapsulation with respect to adaptive chosen ciphertext attack (IND-CCA2), for general use. This security definition is substantially similar to what we had in our original draft Call.

As a result of comments received, we are adding another option. While chosen ciphertext security is necessary for many existing applications, it is possible to implement a purely ephemeral key exchange protocol in such a way that only passive security is required from the encryption or KEM primitive. For these applications, NIST will consider standardizing an encryption or KEM scheme which provides semantic security with respect to chosen plaintext attack (IND-CPA).

As the KEM and public key encryption functionalities can generally be interconverted, unless the submitter specifies otherwise, NIST will apply standard conversion techniques to convert between schemes if necessary.

We would like your feedback.

Does this approach seem sound?

What (if any) changes would you suggest?

Dustin Moody

NIST