From: Chen, Lily (Fed)
To: Moody, Dustin (Fed); Perlner, Ray A. (Fed); (b) (6)
Subject: FW: hybrid mode - ICMC16
Date: Monday, March 14, 2016 4:14:01 PM

The following e-mail is to the people who will attend ICMC16.

Lily

From: Chen, Lily
Sent: Monday, March 14, 2016 4:11 PM
To: Roginsky, Allen; Keller, Sharon; Cooper, Michael Joseph; Keller, Sharon; Scholl, Matthew
Subject: hybrid mode - ICMC16

I looked at ICMC 16 program. William Whyte will give a talk titled "Quantum Safety In Certified Cryptographic Modules (A21c)". Based on the abstract, he will talk about the hybrid mode in TLS. Basically, this is a decision which shall be made by the applications. If IETF community can accept the burden of two "encryptions" (or two signatures), then we will find a way to approve it as long as one share is established by a currently approved method.

As I said in my e-mail below, we do not "disapprove" such mode. But for key agreement, we might need to change the key derivation to allow including "two" shares, where one of them is not generated by the currently approved method. We can also consider the "share" generated by PQC part as additional private information.

Lily

From: Chen, Lily
Sent: Thursday, March 10, 2016 11:08 AM
To: Moody, Dustin (dustin.moody@nist.gov); Perlner, Ray (ray.perlner@nist.gov); Regenscheid, Andrew; Dworkin, Morris J.; Kelsey, John M. (john.kelsey@nist.gov); Vassilev, Apostol; Dang, Quynh (quynh.dang@nist.gov); Barker, Elaine B. (elaine.barker@nist.gov); Keller, Sharon; Bassham, Lawrence E; McKay, Kerry A.; Roginsky, Allen; Peralta, Rene (rene.peralta@nist.gov); Burr, William E.; Liu, Yi-Kai (yi-kai.liu@nist.gov); Daniel C Smith (daniel-c.smith@louisville.edu)
Cc: Scholl, Matthew
Subject: Public key hybrid encryption and signature - for further discussion

This is a heads up. We will need further discussion.

At PQCrypto 2016, we received inquiries and suggestions about NIST to approve "hybrid" mode. Let me first explain what they mean by hybrid mode.

1. For encryption, a message or a key K (because public key encryption is often used for key transport) is randomly split to two shares K = K1 Xor K2. K1 is encrypted by a current approved algorithm and K2 is encrypted by a post quantum crypto method, say NTRU. The receiver will decrypt both shares and recover K.
2. For signature, a message M is signed by two signature schemes, one is currently approved algorithm Sig_1, say ECDSA and another is a post quantum signature, say hash based Sig_2. Then the signature of M is Sig_1(M) and Sig_2(M). It is a valid signature if and only if both Sig_1(M) and Sig_2(M) are valid signatures.

As far as we can tell, there is no security concern as long as one of them is secure. The reason for doing so is to ease the transition to post quantum cryptography.

In fact, currently NIST does not disprove such approach. In the case of encryption, we can consider the second share is sent in plaintext. For signature, we may consider Sig_2 as a dummy signature.

On the other hand, at this stage, no standard bodies have standardized such "hybrid mode". It is not clear whether the applications can accept this approach for the reason of performance. There is one ietf draft https://tools.ietf.org/html/draft-whyte-qsh-tls13-01 to include hybrid ciphersuite to TLS for

handshake with NTRU. It is on its second version, expiring March 20, 2016. The hybrid signature is explained for OS update in Dan Bernstein's PQCrypto 2016 talk.
One –way to handle it is to include it in the IG. But since there is no existing standard or implementation of this mode, it is not clear whether it is proper to include it in the IG.
Please note that the inquiries and suggestions are from the research community. We surely need to see how the real world respond to this.
Lily