From:	Dang, Quynh (Fed)
To:	Chen, Lily (Fed); Moody, Dustin (Fed); Perlner, Ray A. (Fed); Regenscheid, Andrew R. (Fed); Dworkin, Morris J. (Fed); Kelsey, John M. (Fed); Vassilev, Apostol T. (Fed); Barker, Elaine B. (Fed); Keller, Sharon (Fed); Bassham, Lawrence E. (Fed); McKay, Kerry A. (Fed); Roginsky, Allen L. (Fed); Peralta, Rene C. (Fed); Burr, William E. (Assoc); Liu, Yi-Kai (Fed); Daniel C Smith (daniel-c.smith@louisville.edu)
Cc:	Scholl, Matthew A. (Fed)
Subject:	Re: Public key hybrid encryption and signature - for further discussion
Date:	Thursday, March 10, 2016 2:41:28 PM

Hi all,

That is a clever approach. As long as an algorithm does not claim providing cryptographic security, then it does not need to comply with our cryptographic standards and guidelines.

A few questions are below.

1) How much would protocols designers/implementers/users (especially the users and implementers) use the post-quantum algorithms that way knowing that they'll pay some performance cost (could be heavy performance cost) (and IPR fee(s) in some cases) and do not know which one(s) will be adopted by standard bodies such as NIST and/or the IETF (adopted by a standard body implies some level of confidence in the security of the adopted scheme(s)) ?

2) Would we like to be in a world where different post-quantum algorithms are supported in different protocols when we decide what algorithm(s) to standardize?

3) Maybe some algorithm(s) will stand out as popular choice(s) and that might or might not help us in our standardization process. For example, an algorithm is widely supported, but we don't believe it is a good or best choice.

4) Standardized algorithms bring significant interoperability, efficiency and security for the internet. So, I am not sure if all kinds of algorithms being supported or/and used is the best that we are looking for.

Regards,
Quynh.

From: Chen, Lily (Fed)
Sent: Thursday, March 10, 2016 11:07 AM
To: Moody, Dustin (Fed); Perlner, Ray (Fed); Regenscheid, Andrew (Fed); Dworkin, Morris J. (Fed); Kelsey, John M. (Fed); Vassilev, Apostol (Fed); Dang, Quynh (Fed); Barker, Elaine B. (Fed); Keller, Sharon (Fed); Bassham, Lawrence E (Fed); McKay, Kerry A. (Fed); Roginsky, Allen (Fed); Peralta, Rene (Fed); Burr, William E. (Assoc); Liu, Yi-Kai (Fed); Daniel C Smith (daniel-c.smith@louisville.edu)

Cc: Scholl, Matthew (Fed)
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