From:	Dang, Quynh (Fed)
To:	Cooper, David (Fed); Dworkin, Morris J. (Fed); Miller, Carl A. (Fed); Davidson, Michael S. (Fed); Apon, Daniel C. (Fed)
Subject:	Re: Randomized hashing in HBS and a statement about security in quantum world.
Date:	Thursday, August 15, 2019 12:13:52 PM

Hi all,

I might not have made the point clear in the message below.

The point is that the signer is the only party who can find colliding randomized messages by defeating the collision resistance property of the hash function. Therefore, he or she is responsible for any message with a legitimate signature on it.

Quynh.

From: Dang, Quynh (Fed) <quynh.dang@nist.gov>
Sent: Thursday, August 15, 2019 6:44:36 AM
To: Cooper, David A. (Fed) <david.cooper@nist.gov>; Dworkin, Morris J. (Fed) <morris.dworkin@nist.gov>; Miller, Carl A. (Fed) <carl.miller@nist.gov>; Davidson, Michael S. (Fed) <michael.davidson@nist.gov>; Apon, Daniel C. (Fed) <daniel.apon@nist.gov>
Subject: Randomized hashing in HBS and a statement about security in quantum world.

Hi all,

As we discussed yesterday about randomized hashing in HBS, I would like to restate it here.

When the manufacture/vendor is both the message generator/controller and the message signer, he or she can find 2 colliding messages of his/her choice with 2 different randomization values. In addition, the manufacture/vendor is the only entity who can generate a legitimate signature for a message because only he or she knows the OTS private key. Therefore, he or she is responsible for any message that he or she signs.

Randomized hashing in HBS is to prevent the situation where a message generator and the message signer (such as in certificate signing situation) are 2 different identities. The message generator generates 2 different messages, then asks the signer to sign one of them, but later use that signature on the other message. Randomized hashing stops the attack or makes finding a different message which collides with the message the signer signs become a second preimage attack.

My suggestion to replace this text "and it is believed that the security of hash functions will not be broken by the development of large-scale quantum computers.": is either:

1) "and it is believed that the currently known attacks using quantum computers will not break

the second preimage or preimage resistance of the hash functions specified in this special publication. ", or

2) "and it is believed that the currently known attacks using quantum computers will not break security of the hash functions specified in this special publication. "

The option 1 only talks about the preimage and second preimage that are relevant to the HBS options in our standard.

The option 2 talks about all 3 properties of the hash functions.

Quynh.

From: David A. Cooper <david.cooper@nist.gov>
Sent: Wednesday, August 14, 2019 3:40 PM
To: Dworkin, Morris J. (Fed) <morris.dworkin@nist.gov>; Dang, Quynh (Fed) <quynh.dang@nist.gov>; Miller, Carl A. (Fed) <carl.miller@nist.gov>; Davidson, Michael S. (Fed) <michael.davidson@nist.gov>; Apon, Daniel C. (Fed) <daniel.apon@nist.gov>
Subject: Reference for quantum resistance of hash functions

I did some searching for a reference for the text at the end of Section 1. One possibility would be to reference NISTIR 8105, *Report on Post-Quantum Cryptography* (https://doi.org/10.6028/NIST.IR.8105). It doesn't have much text on the subject, but its probably enough to justify the assertion in our text.

Dave