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: Allowing 1 level trees.
Date: Thursday, August 15, 2019 7:11:27 AM

Hi all,

The draft currently disallows 1-level trees. We did that because we thought that 1-level trees could not do back-ups without exporting secret keying material.

However, as we discussed the issue thoroughly, 1-level trees can do back-ups just fine without the need to export secret keying material.

The downside of a 1 level tree is key generation time (and doing some input/output from the modules) but that is not a prohibited cost in all situations. Small 1-level trees would do very well in this situation. And, 1 level trees have smaller signature chain sizes which may be desirable in many situations.

My suggestion is that we allow 1-level trees (LMS and XMSS) as long as no secret keying material is exported. We don't have to specify how back-ups can be done with a 1-level tree right now. People who would like to use a 1 level tree would be able to figure out the method that we currently know of very quickly.

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