From:	Alperin-Sheriff, Jacob (Fed)
To:	Peralta, Rene C. (Fed); (b) (6) ; Liu, Yi-Kai (Fed)
Cc:	Perlner, Ray A. (Fed); Bassham, Lawrence E. (Fed); Chen, Lily (Fed); Jordan, Stephen P (Fed); Miller, Carl A. (Fed); Moody, Dustin (Fed); Smith-Tone, Daniel C. (Fed); Regenscheid, Andrew R. (Fed)
Subject:	Re: Hash-based signatures
Date:	Wednesday, January 4, 2017 2:50:37 PM

A look through the CFP indicates that we didn't address stateful vs. stateless, so looks like you're not a liar!

But I had thought the problems with stateful signatures go well beyond the size of the private keys …

From: "Peralta, Rene (Fed)" <rene.peralta@nist.gov>
Date: Wednesday, January 4, 2017 at 2:47 PM
To: Daniel Smith (b) (6) , "Liu, Yi-Kai (Fed)" <yi-kai.liu@nist.gov>
Cc: "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>, "Perlner, Ray (Fed)" <ray.perlner@nist.gov>, "Bassham, Lawrence E (Fed)" <lawrence.bassham@nist.gov>, "Chen, Lily (Fed)" <lily.chen@nist.gov>, "Jordan, Stephen P (Fed)" <stephen.jordan@nist.gov>, "Miller, Carl A. (Fed)" <carl.miller@nist.gov>, "Moody, Dustin (Fed)" <dustin.moody@nist.gov>, "Smith-Tone, Daniel (Fed)" <daniel.smith@nist.gov>, "Regenscheid, Andrew (Fed)" <andrew.regenscheid@nist.gov>
Subject: Hash-based signatures

Somebody asked whether I was contradicting the statement that "NIST is not interested in hash-based signatures". I said "yes", hash-based signatures are in scope. Then Dan Boneh asked whether that included stateful hash-based signatures. I answered that we are open to someone making the case that these are useful despite the size of the private keys.

Don't make a liar out of me.

Rene.