From: Liu, Yi-Kai (Fed)
To: Perlner, Ray A. (Fed)
Cc: Moody, Dustin (Fed)
Subject: Re: Minimal edits to make quantum security section self consistent.
Date: Friday, May 27, 2016 12:49:50 PM
Attachments: CFP v9.3_RayEditsOn4a.4_YKL-Edits.docx

Hi Ray,

I edited the quantum security section some more.

- I added some simple advice: if you have a quantum algorithm, report both the time and space complexity, and if possible, say what is the tradeoff between them. I tried to keep this separate from the more complicated discussion about how to define quantum bits of security.

- I said that this is preliminary guidance from NIST, and we will discuss with the community as we go forward.

- I said some more about the possibility of defining quantum bits of security with respect to SHA-256 rather than AES-128. (Since we are already doing this in some of our target security strengths.) It is problematic because these two definitions (SHA vs AES) are not equivalent.

What do you think? Sorry I didn't do this sooner, this week has been a bit crazy.

Thanks!

--Yi-Kai

From: Perlner, Ray (Fed)
Sent: Tuesday, May 24, 2016 2:17 PM
To: Liu, Yi-Kai (Fed)
Subject: Minimal edits to make quantum security section self consistent.