From: Chen, Lily (Fed)
To: Scholl, Matthew A. (Fed); (b) (6)
Subject: RE: transition
Date: Friday, December 13, 2019 10:31:00 AM

In many events, we were asked about QKD. I think people can agree with the following points without too much debating with QKD people.

- We, NIST Crypto team, do not work on QKD because we do not have resource, e.g. equipment, and expertise.
- QKD, as a standalone technology, cannot provide a complete solution to cyber security in the future, because pairwise key establishment through QKD is not scalable for large scale networks like internet.
- However, in the applications where QKD is available in a secure way, the current existing protocols like TLS and IKE with PQC can use QKD as additional security data for key derivation.

Lily

From: Scholl, Matthew A. (Fed) <matthew.scholl@nist.gov>
Sent: Tuesday, December 3, 2019 2:07 PM
To: Timothy Grance (b) (6)
Cc: Chen, Lily (Fed) <lily.chen@nist.gov>
Subject: Re: transition

Yes, it can be done by satalite as well

-------- Original Message --------
From: Timothy Grance (b) (6)
Date: Tue, December 03, 2019 2:04 PM -0500
To: "Scholl, Matthew A. (Fed)" <matthew.scholl@nist.gov>
CC: "Chen, Lily (Fed)" <lily.chen@nist.gov>
Subject: Re: transition

More details when I return.

The presenter asserted his company can do this now.

Tim

Sent from my iPhone

> On Dec 3, 2019, at 2:03 PM, Scholl, Matthew A. (Fed) <matthew.scholl@nist.gov> wrote:
>
> It a technology we are not encouraging right now, at least for us. Lots of a angst

because China is big invested in it but that seems to the the main and mostly only motivator I have heard

-------- Original Message --------
From: Timothy Grance (b) (6)
Date: Tue, December 03, 2019 2:00 PM -0500
To: "Scholl, Matthew A. (Fed)" <matthew.scholl@nist.gov>
CC: "Chen, Lily (Fed)" <lily.chen@nist.gov>
Subject: Re: transition

The last presenter was expressing dismay about that

Tim

Sent from my iPhone

> On Dec 3, 2019, at 1:50 PM, Scholl, Matthew A. (Fed) <matthew.scholl@nist.gov> wrote:
>
> No,. QKD is a topic that Alan Mink at math leads and is something that we think is interesting but not very commercially valuable. It has many security issues still that we are not sure how to remedy at this point
>
> -------- Original Message --------
> From: Timothy Grance (b) (6)
> Date: Tue, December 03, 2019 1:44 PM -0500
> To: "Scholl, Matthew A. (Fed)" <matthew.scholl@nist.gov>, "Chen, Lily (Fed)" <lily.chen@nist.gov>
> Subject: transition
>
> Do we have any plans to produce forward looking guidance on quantum key distribution.
>
> Tim
>
> Sent from my iPhone