From: Chen, Lily (Fed)
To: Gundlach, David (Fed)
Subject: RE: question about quantum cryptography for congressional testimony prep
Date: Friday, October 6, 2017 5:09:00 PM

Hi, David,

How about use “NIST researchers are using their understanding of quantum algorithms to create new classical encryption algorithms, commonly referred to as post-quantum cryptography, that are resistant to quantum computing attacks” to replace the whole second paragraph?

Lily

From: Gundlach, David (Fed)
Sent: Friday, October 06, 2017 4:56 PM
To: Chen, Lily (Fed) <lily.chen@nist.gov>
Subject: RE: question about quantum cryptography for congressional testimony prep

Hi Lily,

Here is what I captured from our talk yesterday –

Quantum Algorithms and Post-Quantum Cryptography
NIST programs on quantum algorithms and post-quantum cryptography further build on our core effort in quantum information theory with a focus on addressing security challenges for when quantum computers are realized. NIST, working with industry, has played a leading role in developing cryptography standards that dates to the 1970’s. Today’s classical computers and computer networks employing Public Key Cryptography are using cryptography standardized by NIST. Unfortunately, these standards are not resistant to attack by quantum computers.

NIST researchers are using quantum algorithms to perform theoretical evaluations of possible attacks made on classical computers and computer networks using a quantum computer to understand vulnerabilities. NIST researchers are also developing post-quantum encryption methods based on classical mathematic techniques that predate quantum information to make systems resistant to such attacks.

Carl’s suggested change for the sentence highlighted above is:

“NIST researchers are using their understanding of quantum algorithms to create new classical encryption algorithms that are resistant to quantum computing attacks”

Would this be correct?

David J. Gundlach

Program Coordination Office
Office of the Under Secretary for Standards & Technology, and NIST Director

National Institute of Standards and Technology (NIST)
100 Bureau Dr. MS-1060
Building 101 / Room A1005
Gaithersburg, MD 20899-1060
Office: 301-975-8085

David.Gundlach@NIST.gov

From: Chen, Lily (Fed)
Sent: Thursday, October 05, 2017 12:37 PM
To: Gundlach, David (Fed) <david.gundlach@nist.gov>
Subject: RE: question about quantum cryptography for congressional testimony prep

Yes. I am and just back to my office. Any time from now on will work.

Lily

From: Gundlach, David (Fed)
Sent: Thursday, October 05, 2017 12:17 PM
To: Chen, Lily (Fed) <lily.chen@nist.gov>
Subject: RE: question about quantum cryptography for congressional testimony prep

Lily, would it be possible to stop over around 12.45? You are in 222/B362 correct?

David J. Gundlach

Program Coordination Office
Office of the Under Secretary for Standards & Technology, and NIST Director

National Institute of Standards and Technology (NIST)
100 Bureau Dr. MS-1060
Building 101 / Room A1005
Gaithersburg, MD 20899-1060
Office: 301-975-8085

David.Gundlach@NIST.gov

From: Chen, Lily (Fed)
Sent: Thursday, October 05, 2017 11:49 AM
To: Gundlach, David (Fed) <david.gundlach@nist.gov>; Scholl, Matthew (Fed) <matthew.scholl@nist.gov>
Cc: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: RE: question about quantum cryptography for congressional testimony prep

Hi, David,

I will be available before 3:00 today. I will be here tomorrow. My schedule tomorrow is pretty open.

Lily

From: Gundlach, David (Fed)
Sent: Thursday, October 05, 2017 11:39 AM
To: Scholl, Matthew (Fed) <matthew.scholl@nist.gov>
Cc: Chen, Lily (Fed) <lily.chen@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: RE: question about quantum cryptography for congressional testimony prep

Hi Matt, Lily, and Dustin,

Thanks for the links and files. 3 is pushing it for me (with deadlines and other meetings). Carl also suggested talking to Lily.

@ Lily – would you have time to meet just briefly. This is really just a matter of hammering out two paragraphs and I think it might be more useful to chat for a few minutes rather than working through too much background information.

David J. Gundlach

Program Coordination Office
Office of the Under Secretary for Standards & Technology, and NIST Director

National Institute of Standards and Technology (NIST)
100 Bureau Dr. MS-1060
Building 101 / Room A1005
Gaithersburg, MD 20899-1060
Office: 301-975-8085

David.Gundlach@NIST.gov

From: Scholl, Matthew (Fed)
Sent: Thursday, October 05, 2017 10:52 AM
To: Gundlach, David (Fed) <david.gundlach@nist.gov>

Cc: Chen, Lily (Fed) <lily.chen@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: question about quantum cryptography for congressional testimony prep

David,
Can do. We have a few slide decks we have used to talk PQC as well as:

PQC Overview Web Page; https://csrc.nist.gov/projects/post-quantum-cryptography
News Pages on PQC: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/news
The IR on the PQC Project: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/publications

Let me know when you want to meet. Today is a bit nutty but I am open about 3. I will see if we can get you some slides in the mean time
Matt

From: "Gundlach, David (Fed)" <david.gundlach@nist.gov>
Date: Thursday, October 5, 2017 at 9:36 AM
To: "Scholl, Matthew (Fed)" <matthew.scholl@nist.gov>
Subject: question about quantum cryptography for congressional testimony prep

Hi Matt,

I am working up testimony for Carl Williams re. quantum computing. Part of that testimony will touch on cryptography. Would you have time to chat today. I need to close the document out soon and I think the crypto side still needs the most help. This should not be an exhaustive list of activities or in too much detail but basically pointing out the significant activities at NIST re. quantum crypto, post quantum crypto, and possibly algorithms and applications.

Thanks,

David J. Gundlach

Program Coordination Office
Office of the Under Secretary for Standards & Technology, and NIST Director

National Institute of Standards and Technology (NIST)
100 Bureau Dr. MS-1060
Building 101 / Room A1005
Gaithersburg, MD 20899-1060
Office: 301-975-8085

David.Gundlach@NIST.gov