From:	Alperin-Sheriff, Jacob (Fed)
To:	(b) (6) ; Liu, Yi-Kai (Fed)
Cc:	Perlner, Ray A. (Fed); Peralta, Rene C. (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: Slides for RWC talk
Date:	Friday, March 17, 2017 2:11:28 PM

This is a very old email I never commented on but it came up when I was searching for something else in my past e-mails, but I figured I would point out that it's obviously not known whether NP=EXPTIME, as by the various time-hierarchy theorems we have that P is a proper subset of EXPTIME, meaning that resolving NP?=EXPTIME would mean resolving P?=NP.

From: Daniel Smith (b) (6)
Date: Tuesday, January 3, 2017 at 3:12 PM
To: "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>, "Peralta, Rene (Fed)" <rene.peralta@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: Re: Slides for RWC talk

I thought that it isn't known whether NP=EXPTIME, so to say that "a lot of problems like that are NP-complete" is maybe a bit misleading. Any problem in EXPTIME with known satisfaction of a completeness criterion is actually NP-complete.

With that said, NP is clearly in EXPTIME, but maybe one could solve a non-EXPTIME-hard problem in polynomial time with a quantum computer without any implication about NP. It's not clear that these concepts are so closely tied together.

On Tue, Jan 3, 2017 at 2:28 PM, Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov> wrote:

> I think it's probably not a coincidence. I tend to think that if a problem has a polynomial-time quantum algorithm, then it has quite a lot of special structure, which makes it likely that the problem also has a nontrivial classical algorithm (i.e., some classical algorithm that is faster than exponential-time).
>
> One piece of evidence for this belief is from quantum query complexity: in this black-box setting, one can get super-polynomial quantum speedups for evaluating partial functions, but not for evaluating total functions. (In this picture, partial functions have the extra structure that is missing from total functions.)
>
> You can also ask this question a different way: Why aren't there polynomial-time quantum algorithms that solve problems where the best classical algorithm is exponential-time?
>
> One answer is that a lot of problems like that (where the best classical algorithm is exponential-time) are NP-complete. So if a quantum computer could solve ANY of those

problems in polynomial time, then it could solve ALL of them in polynomial time. Since it appears that a quantum computer CAN'T solve those problems in polynomial time, quantum computers are left to fight over problems that also have subexponential-time classical algorithms.

Cheers,

--Yi-Kai

From: Alperin-Sheriff, Jacob (Fed)
Sent: Tuesday, January 3, 2017 1:07:30 PM
To: Liu, Yi-Kai (Fed); Daniel Smith; Perlner, Ray (Fed)
Cc: Peralta, Rene (Fed); Bassham, Lawrence E (Fed); Chen, Lily (Fed); Jordan, Stephen P (Fed); Miller, Carl A. (Fed); Moody, Dustin (Fed); Smith-Tone, Daniel (Fed); Regenscheid, Andrew (Fed)
Subject: Re: Slides for RWC talk

Taking a tangent on the quantum subject, is it a total coincidence that a lot of these problems with polynomial-time quantum algorithms have known subexponential classical algorithms as well?

On 1/3/17, 12:12 PM, "Liu, Yi-Kai (Fed)" <yi-kai.liu@nist.gov> wrote:

Hi Rene,

I think the slides look pretty good. How much time do you have for your talk? If you have extra time, here are a couple more things you could mention:

- Intellectual property issues?
- Possible strategies for how PQC will be deployed, e.g., hybrid modes?
- Coordination with other standards, e.g., TLS, IPSec, and IETF's work on hash-based signatures?
- Quantum cryptanalysis? (There aren't many people who work on both classical crypto and quantum computation. The quantum attack on Soliloquy is a good example of the kind of expertise that we need to develop.)

I also like the emphasis on asking for a broader "impact assessment," since making PQC work well will also require attention from lower-level hardware engineers and higher-level protocol designers.

Cheers,

--Yi-Kai

From: Daniel Smith (b) (6)
Sent: Tuesday, January 3, 2017 11:42:08 AM
To: Perlner, Ray (Fed)

Cc: Peralta, Rene (Fed); Alperin-Sheriff, Jacob (Fed); Bassham, Lawrence E (Fed); Chen, Lily (Fed); Jordan, Stephen P (Fed); Liu, Yi-Kai (Fed); Miller, Carl A. (Fed); Moody, Dustin (Fed); Smith-Tone, Daniel (Fed); Regenscheid, Andrew (Fed)
Subject: Re: Slides for RWC talk

I agree with point 1. I'm not an expert on the code-based stuff, but I think that the code-based signatures have a better foundation than multivariate encryption, so if only one is to be listed, it should be the other way around. I think that if it is not too inconvenient, both should be listed. Efficient and secure schemes within both frameworks are entirely plausible, even if we are very unlikely to develop sufficient trust in them within our timeline.

On Tue, Jan 3, 2017 at 11:14 AM, Perlner, Ray (Fed) <ray.perlner@nist.gov<mailto:ray.perlner@nist.gov>> wrote:
I have two nitpicks. Not sure either is worth changing though.

1) You have Multivariate listed for both signature and PKE, but code-based is only listed for PKE. The way I'd describe the current situation is that code-based is mostly for PKE and multivariate is mostly for signature, but each has some plausible proposals for obtaining the other functionality. I wouldn't necessarily say that code-based signature proposals are any worse than multivariate encryption proposals, so it seems a little odd to list one but not the other. That said, it's really a judgement call.

2) On slides 3 and 7, you use the following terms: "key agreement" "key establishment" and "PKC" (On slide 3: you probably mean PKE here.) The CFP primarily uses PKE and KEM, which have standard security and correctness definitions, although KEM may be unfamiliar to your audience. Each is then allowed to be submitted for ephemeral-ephemeral only, or for both ephemeral-ephemeral and static-ephemeral. You probably at least want to change PKC to PKE on slide 3. Not sure you care about being ultra-precise with the rest of your terminology, though.

From: Peralta, Rene (Fed)
Sent: Tuesday, January 03, 2017 8:17 AM
To: Alperin-Sheriff, Jacob (Fed) <jacob.alperin-sheriff@nist.gov<mailto:jacob.alperin-sheriff@nist.gov>>; Daniel Smith (b) (6) ; Bassham, Lawrence E (Fed) <lawrence.bassham@nist.gov<mailto:lawrence.bassham@nist.gov>>; Chen, Lily (Fed) <lily.chen@nist.gov<mailto:lily.chen@nist.gov>>; Jordan, Stephen P (Fed) <stephen.jordan@nist.gov<mailto:stephen.jordan@nist.gov>>; Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov<mailto:yi-kai.liu@nist.gov>>; Miller, Carl A. (Fed) <carl.miller@nist.gov<mailto:carl.miller@nist.gov>>; Moody, Dustin (Fed) <dustin.moody@nist.gov<mailto:dustin.moody@nist.gov>>; Perlner, Ray (Fed) <ray.perlner@nist.gov<mailto:ray.perlner@nist.gov>>; Smith-Tone, Daniel (Fed) <daniel.smith@nist.gov<mailto:daniel.smith@nist.gov>>
Cc: Regenscheid, Andrew (Fed) <andrew.regenscheid@nist.gov<mailto:andrew.regenscheid@nist.gov>>; Peralta, Rene (Fed) <rene.peralta@nist.gov<mailto:rene.peralta@nist.gov>>
Subject: Slides for RWC talk

Dear all,

I managed to delete all copies of my talk in Hanoi, so I made a new set of slides for tomorrow's talk at RWC (attached).

Any comments are most welcome.

Happy New Year, Rene.