From: Miller, Carl A. (Fed)
To: Chen, Lily (Fed); (b) (6) Moody, Dustin (Fed)
Cc: Liu, Yi-Kai (Fed)
Subject: Re: Postquantum crypto project
Date: Tuesday, April 18, 2017 7:35:49 PM

Hi all –

Thanks a lot for your comments!

Stephen: That's a good point about the danger of making estimates. I'm currently thinking I'll say something more vague like, "These days large companies are competing to build quantum computers, and quantum cryptographic solutions are being made available to the public." This kind of audience may not care much whether I'm being quantitative. (Thanks in any case for that article – looks very interesting.)

-Carl

———

Carl A. Miller
Mathematician, Computer Security Division
National Institute of Standards and Technology
Gaithersburg, MD

From: "Chen, Lily (Fed)" <lily.chen@nist.gov>
Date: Tuesday, April 18, 2017 at 3:09 PM
To: Stephen Jordan (b) (6), "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Cc: "Miller, Carl A. (Fed)" <carl.miller@nist.gov>, "Liu, Yi-Kai (Fed)" <yi-kai.liu@nist.gov>
Subject: Re: Postquantum crypto project

Hi, Carl:

The write up is very good. I enjoined to read. I think Stephen made good suggestions. Dustin's clarification has good point.

Lily

From: Stephen Jordan (b) (6)
Sent: Tuesday, April 18, 2017 11:18:01 AM
To: Moody, Dustin (Fed)
Cc: Miller, Carl A. (Fed); Chen, Lily (Fed); Liu, Yi-Kai (Fed)

Subject: Re: Postquantum crypto project

"The investments in the field of quantum computing are now at $XXX per year."

This is both fuzzily defined and nontrivial to estimate. I wonder whether NIST wants to be quoted on having made such an estimate. Probably it is safer to cite somebody else's estimate. For example, in this article in the economist:

http://www.economist.com/technology-quarterly/2017-03-09/quantum-devices

it says:

"According to McKinsey, a consulting firm, in 2015 about 7,000 people worldwide, with a combined budget of about $1.5bn, were working on quantum-technology research (see chart)."

This actually answers a different question than you were asking, which is about quantum computing specifically, rather than quantum technologies more broadly. However, I am not aware of a published estimate specifically for R&D on quantum computing.

Best regards,

Stephen

On Tue, Apr 18, 2017 at 10:33 AM, Moody, Dustin (Fed) <dustin.moody@nist.gov> wrote:

> Carl,
> I read the full draft and enjoyed it! I think you've done a good job of explaining some of these concepts to the lay person, as well as sharing your journey through it. A few minor comments:
>
> - When I read "double-edged sword", I was thinking of how quantum can help, such as QKD. But I believe you are talking about certified quantum randomness. You may wish to mention quantum crypto or QKD, but you certainly don't need to.
> - Perhaps change "…would make many of the ways…." To "… and would make some of the ways…" to be a little less alarming?
>
> Dustin
>
> ---
>
> **From:** Miller, Carl A. (Fed)
> **Sent:** Tuesday, April 18, 2017 10:18 AM
> **To:** Moody, Dustin (Fed) <dustin.moody@nist.gov>; Chen, Lily (Fed) <lily.chen@nist.gov>
> **Cc:** Stephen Jordan (b) (6) ; Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>
> **Subject:** Postquantum crypto project
>
> Hi Lily & Dustin:
>
> If you have a minute:
>
> I'm writing an entry for the NIST "Taking Measure" blog (http://nist-takingmeasure.blogs.govdelivery.com) and making some comments about the Postquantum Cryptography Project. Here's what I have right now. What do you think?

"The game-changing effect of quantum physics on cryptography is a double-edged sword. In 1994 Peter Shor invented a quantum algorithm, which, if implemented in a large-scale quantum computer (and we're not close to having one yet) would make many of the ways that we protect information completely insecure. Today I work in the Cryptographic Technologies group at NIST. Here, we create services and standards for the public to help them stay ahead of the game in the ongoing effort to protect information. We lead the postquantum cryptography project, the goal of which is to design next generation cryptography standards that are resistant to quantum computers."

[The full draft is attached, although it's long and I wouldn't expect you to read the whole thing. Comments on that are welcome too.]

The editors and I have been working to write something that is not too alarming, but also accurately calls public attention to PQC. Your input is welcome.

Yi-Kai and Stephen: Your input is also welcome! (You may know more about the background than I do.) And I'm also trying to fill in a figure in the following sentence:

"The investments in the field of quantum computing are now at $XXX per year."

-Carl

Carl A. Miller
Mathematician, Computer Security Division
National Institute of Standards and Technology
Gaithersburg, MD