

From: [Miller, Carl A. \(Fed\)](#)
To: [Esser, Mark D. \(Fed\)](#)
Subject: Re: Esser, Mark (Fed) has shared "Quantum information Changing the rules of the game"
Date: Monday, April 24, 2017 11:01:01 AM
Attachments: [image002.png](#)

Ok. I'm working on it now, and I'll have something for you later today.

-Carl

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

From: "Esser, Mark (Fed)" <mark.esser@nist.gov>
Date: Monday, April 24, 2017 at 11:00 AM
To: "Miller, Carl A. (Fed)" <carl.miller@nist.gov>
Subject: RE: Esser, Mark (Fed) has shared 'Quantum information Changing the rules of the game'

Whenever you can get around to it is fine. It's likely it won't go out for Math and Statistics Awareness Month, but maybe we could have it ready for World Password Day, which is May 4.

From: Miller, Carl A. (Fed)
Sent: Thursday, April 20, 2017 7:48 PM
To: Esser, Mark (Fed) <mark.esser@nist.gov>
Subject: Re: Esser, Mark (Fed) has shared 'Quantum information Changing the rules of the game'

Hi Mark –

Sorry for the delay – I've been working on some conference submissions. I got some helpful feedback from colleagues in the postquantum crypto project. Would it be ok if I finish the revision by Thursday next week?

-Carl

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

From: "Esser, Mark (Fed)" <mark.esser@nist.gov>

Date: Thursday, April 20, 2017 at 2:54 PM

To: "Miller, Carl A. (Fed)" <carl.miller@nist.gov>

Subject: RE: Esser, Mark (Fed) has shared 'Quantum information Changing the rules of the game'

Hi Carl,

Hope you're doing well. I was just wondering how things were coming along.

From: Miller, Carl A. (Fed)

Sent: Tuesday, April 11, 2017 6:59 PM

To: Esser, Mark (Fed) <mark.esser@nist.gov>; Stein, Ben (Fed) <benjamin.stein@nist.gov>; Huergo, Jennifer (Fed) <jennifer.huergo@nist.gov>

Subject: Re: Esser, Mark (Fed) has shared 'Quantum information Changing the rules of the game'

Ok, that all sounds good -- I'll work on a new draft. (I may ask some colleagues about how to best describe the quantum threat to crypto. ☺)

-Carl

Carl A. Miller

Mathematician, Computer Security Division

National Institute of Standards and Technology

Gaithersburg, MD

From: "Esser, Mark (Fed)" <mark.esser@nist.gov>

Date: Monday, April 10, 2017 at 6:17 PM

To: "Miller, Carl A. (Fed)" <carl.miller@nist.gov>, "Stein, Ben (Fed)" <benjamin.stein@nist.gov>, "Huergo, Jennifer (Fed)" <jennifer.huergo@nist.gov>

Subject: RE: Esser, Mark (Fed) has shared 'Quantum information Changing the rules of the game'

Hi Carl,

Regarding Andrea, I think that was more of a habitual reaction on my part. You just don't see that done very often, but it's not exactly wrong. I would still leave her last name off for privacy reasons. That is, unless the cats also have last names, then I would include all of them.

We'll go with whatever you all are comfortable with.

I think for the second one we were going for succinctness, but you're right, it does lose a little of the urgency. What about?

"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) could break every code we have in a matter of weeks, if not days."

Now it might be too strong, and possibly untrue. Or we could split the difference.

"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 much of our information completely insecure."

And certainly we can link to that resource.

Hope this helps.

From: Miller, Carl A. (Fed)

Sent: Monday, April 10, 2017 5:42 PM

To: Esser, Mark (Fed) <mark.esser@nist.gov>; Stein, Ben (Fed) <benjamin.stein@nist.gov>; Huergo, Jennifer (Fed) <jennifer.huergo@nist.gov>

Subject: Re: Esser, Mark (Fed) has shared 'Quantum information Changing the rules of the game'

Hi all –

Thanks a lot for your comments – I think they help make it a little more fun to read and also clarify some things.

I'm working on a revised draft. Some questions:

- I wrote:

"In 1994 Peter Shor invented a [quantum algorithm](#) which puts in jeopardy most of the secure communication systems available today. It means that if a large-scale quantum computer is built (and we're not there yet) then much of our information will be completely insecure."

This was changed to:

"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 secure information obsolete."

Am I right that this softer statement is to avoid creating public uncertainty? ☺ The upside of making a stronger statement is that we increase public awareness of the need to study postquantum cryptography.

(We could include a link on this topic, e.g., <http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf> .)

- Why do we prefer not to name my partner Andrea? (If it's a privacy thing, we could consider just giving her first name.)

-Carl

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

From: "Esser, Mark (Fed)" <no-reply@sharepointonline.com>

Reply-To: "Esser, Mark (Fed)" <mark.esser@nist.gov>

Date: Thursday, April 6, 2017 at 1:03 PM

To: "Stein, Ben (Fed)" <benjamin.stein@nist.gov>, "Miller, Carl A. (Fed)" <carl.miller@nist.gov>, "Huergo, Jennifer (Fed)" <jennifer.huergo@nist.gov>

Cc: "Esser, Mark (Fed)" <mark.esser@nist.gov>

Subject: Esser, Mark (Fed) has shared 'Quantum information Changing the rules of the game'

Carl,

Please see the text at the link below. We tried to make the text a little clearer in places and we noted some areas where we thought you could add some explanation or detail. Please also correct anything we may have misconstrued.



If you have any trouble accessing Sharepoint, let me know and I'll send you the document in an email.

Thanks!

Open **Quantum information Changing the**

rules of the game.docx

See more related to [Esser, Mark \(Fed\)](#) in Delve.

Get the OneDrive mobile app! Available for  |  | 