From: Miller, Carl A. (Fed)
To: Kuo, Paulina S. (Fed)
Cc: Peralta, Rene C. (Fed)
Subject: Re: randomness at the optics teleconference
Date: Sunday, September 25, 2016 1:54:41 PM

Hi Paulina –

Sorry you've had a tough couple of weeks. Hope things are stable and that you're on the mend. I'll definitely keep you in mind for any follow-ups to the meeting -- talk to you later!

-Carl

_____

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

On 9/24/16, 6:50 PM, "Kuo, Paulina (Fed)" <paulina.kuo@nist.gov> wrote:

> Hi Carl and Rene,
>
> I am just getting back from a (kind of major) health issue that led to be to be out sick for the last two weeks. I am only going to be working from home and around NIST part time for the next few weeks. Although I would very much like to, I can not attend the upcoming Tuesday 11:30am meeting.
>
> Please don't reschedule the meeting for me, but do keep me in the loop with your discussions (meeting notes would be great if that is possible).
>
> Thanks for your understanding!
>
> Paulina
>
> -----Original Message-----
> From: Miller, Carl A. (Fed)
> Sent: Friday, September 23, 2016 2:48 PM
> To: Gerrits, Thomas (Assoc) <thomas.gerrits@nist.gov>; Glancy, Scott (Fed) <scott.glancy@nist.gov>; Jordan, Stephen P (Fed) <stephen.jordan@nist.gov>; Kuo, Paulina (Fed) <paulina.kuo@nist.gov>; Peralta, Rene (Fed) <rene.peralta@nist.gov>
> Subject: Re: randomness at the optics teleconference
>
> Hi folks --
>
> I thought I'd check in with you all about our tentative plans for the optics meeting next week. BTW, I think someone else (Adriana Lita) is listed on the Excel calendar for Sept. 27th – or is that for a different event?
>
> So, from my angle, this meeting is a good way to get more deeply involved in the randomness beacon (which is my main interest right now) and to get more introduced to the group. During the meeting I could give a presentation that goes something like this:
>
> 1. Briefly describe a Bell experiment / randomness expansion protocol as I'm used to seeing it (the language might be different, so this just gets us on the same page).

2. Describe the best theoretical security results that have been proved.
3. Run through some of the current research directions that I'm exploring (e.g., new security proofs for variants of the Bell experiments).

(Item 3 is mainly just to get a dialogue going. My real interest is in finding out what new theoretical results could be useful for the randomness beacon.)

Let me know if you have any thoughts (and if anyone else would like to take the lead during the meeting we can coordinate). See you next week!

-Carl

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

On 9/12/16, 6:05 PM, "Miller, Carl A. (Fed)" <carl.miller@nist.gov> wrote:

Ok, great, let's plan on that (11:30am EST on Sept. 27th). (Rene and Paulina: This is for the Fortnightly Tuesday meeting.)

I'll be giving two talks that week about my work on randomness. So I could come to the meeting with my slides from those talks and plan to go through some of them.

One of my biggest interests is to find out how those of us on the theory side can diversify our methods to help out the experimentalists. (Examples: accounting for detector failures, allowing for more complex causal relationships between different devices, etc.) I think the meeting could be a good opportunity to talk about that (and anything else people would like to discuss). See you then!

-Carl

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

On 9/12/16, 5:10 PM, "Gerrits, Thomas (Assoc)" <thomas.gerrits@nist.gov> wrote:

Hi Scott,

I don't think I replied to you yet. Yes, this would be a good topic for the 27th!

Thanks,
Thomas

-----Original Message-----
From: Scott Glancy [mailto:sglancy@nist.gov]
Sent: Thursday, September 08, 2016 3:17 PM
To: Gerrits, Thomas (Assoc) <thomas.gerrits@nist.gov>
Cc: Miller, Carl A. (Fed) <carl.miller@nist.gov>; Jordan, Stephen P (Fed) <stephen.jordan@nist.gov>
Subject: randomness at the optics teleconference

Thomas,

For the optics teleconference on Sep-27, could we discuss randomness theory and the NIST random beacon? The Computer Security Division has hired Carl Miller, a quantum randomness theory expert, and we want to talk with him about his work and how it could be applied to the NIST random beacon and related things.

Also, can you make sure that Carl and Stephen Jordan are on your mailing list for these meetings?

Scott