From:	Moody, Dustin (Fed)
To:	Chen, Lily (Fed); Jordan, Stephen P (Fed)
Subject:	RE: Re: seminars
Date:	Monday, June 13, 2016 8:12:00 AM

Yes, I'll take care of the room. Thanks.

From: Chen, Lily (Fed)
Sent: Monday, June 13, 2016 8:11 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Jordan, Stephen P (Fed) <stephen.jordan@nist.gov>
Subject: RE: Re: seminars

Shall we get a conference room?
Lily

From: Moody, Dustin (Fed)
Sent: Monday, June 13, 2016 7:08 AM
To: Jordan, Stephen P (Fed) <stephen.jordan@nist.gov>; Chen, Lily (Fed) <lily.chen@nist.gov>
Subject: RE: Re: seminars

Stephen,

Yes, we can schedule Gorjan to talk on the 21st. I will be out of town that week, but I assume everyone else can make it. Thanks!
Dustin

From: Stephen Jordan [mailto:stephen.jordan@nist.gov]
Sent: Friday, June 10, 2016 10:31 AM
To: Chen, Lily (Fed) <lily.chen@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Fwd: Re: seminars

Dear Lily and Dustin,

Gorjan Alagic will be visiting NIST and QuICS the week of June 20. He has volunteered to give a talk at NIST about quantum attacks on symmetric-key cryptography. Title and abstract are below. Could we do this for the PQC seminar on June 21?

-Stephen

-------- Forwarded Message --------
Subject: Re: seminars
Date: Fri, 10 Jun 2016 09:37:17 +0200
From: Gorjan Alagic <galagic@gmail.com>
To: Stephen Jordan <stephen.jordan@nist.gov>

Hi Stephen,
Here is the title and abstract for NIST.
Hidden shifts and quantum attacks on symmetric-key cryptography
---
It is well-known that large-scale quantum computers would devastate the current public-key cryptography infrastructure. Symmetric-key systems, on the other hand, are widely believed to

be quantum-secure. However, this belief is predicated on various assumptions about the security model, some of which may be too strong. Kuwakado and Morii showed that, under a certain notion of ``quantum CPA,'' many classically-secure symmetric-key schemes can be completely broken by a simple quantum adversary. The broken schemes include the 3-round Feistel cipher, the Even-Mansour cipher, the Encrypted-CBC-MAC, and many others. In this talk, we will begin by describing these attacks and the underlying security model. We will then propose a generic adaptation, which can be applied to all of the broken schemes, and which is likely to provide quantum security even in the ``quantum CPA'' model. In particular, we will show that breaking some of the adapted schemes would imply efficient quantum algorithms for the Hidden Shift Problem. Based on joint work with Alex Russell.
Best,
Gorjan
On Thu, Jun 9, 2016 at 10:30 PM, Stephen Jordan <stephen.jordan@nist.gov> wrote:

> That would be excellent.
>
> -Stephen
>
> On 06/09/2016 04:25 PM, Gorjan Alagic wrote:
>
> > Hi Stephen,
> > Sure, that sounds fine. Have the NIST guys seen a talk about the Simon's algorithm attacks on symmetric-key crypto? I'll send you a title and abstract for my talk there tomorrow.
> > I already sent Javiera the title and abstract for the QuICS seminar. It looks like it's up on your webpage. I hope the topic is appropriate.
> > Best,
> > Gorjan
> > On Thu, Jun 9, 2016 at 9:22 PM, Stephen Jordan <stephen.jordan@nist.gov> wrote:
> >
> > > Hi Gorjan,
> > >
> > > Would you be happy to give a seminar at NIST on Tuesday, June 21 at 10am? The audience will include a lot of post-quantum crypto people. Your seminar at QuICS, which is for a QIP-style audience, is scheduled for Wednesday, June 22 at 11am. I'm looking forward to your visit.
> > >
> > > Best regards,
> > >
> > > Stephen
> >
> > --
> > Gorjan Alagic
> > Department of Mathematical Sciences
> > University of Copenhagen

--
Gorjan Alagic

Department of Mathematical Sciences
University of Copenhagen