From: Robinson, Angela Y. (Fed)
To: Brandao, Luis (IntlAssoc); Peralta, Rene C. (Fed)
Subject: RE: ACCESS Seminar Reminder - Tuesday, Sep 21
Date: Tuesday, September 21, 2021 11:00:29 AM

Platform (b) (6)
[redacted]
Meeting ID: (b) (6)
Passcode: (b) (6)

Sent from Mail for Windows

From: Brandao, Luis (IntlAssoc) <luis.brandao@nist.gov>
Sent: Tuesday, September 21, 2021 10:58:16 AM
To: Robinson, Angela Y. (Fed) <angela.robinson@nist.gov>; Peralta, Rene C. (Fed) <rene.peralta@nist.gov>
Subject: Re: ACCESS Seminar Reminder - Tuesday, Sep 21

Couldn't find any link to video-conference

From: Brandao, Luis (IntlAssoc) <luis.brandao@nist.gov>
Sent: Wednesday, September 15, 2021 10:57
To: Robinson, Angela Y. (Fed) <angela.robinson@nist.gov>; Peralta, Rene C. (Fed) <rene.peralta@nist.gov>
Subject: Re: ACCESS Seminar Reminder - Tuesday, Sep 21

Thanks Angela,

I'll try to attend. I didn't know Alessandra was working on this.

Regards, Luís

From: Robinson, Angela Y. (Fed) <angela.robinson@nist.gov>
Sent: Wednesday, September 15, 2021 10:49
To: Peralta, Rene C. (Fed) <rene.peralta@nist.gov>; Brandao, Luis (IntlAssoc) <luis.brandao@nist.gov>
Subject: FW: ACCESS Seminar Reminder - Tuesday, Sep 21

In case you are free on Tuesday at 11.

Angela

From: ACCESS Organizing Committee
Sent: Tuesday, September 14, 2021 10:36 PM
To: Robinson, Angela Y. (Fed)
Subject: ACCESS Seminar Reminder - Tuesday, Sep 21

Dear Angela,
It is a pleasure to announce the next seminar of the ACCESS - Algebraic Coding and Cryptography on the East coast Seminar Series.
Date: Tuesday, Sep 21, 2021
Time: 11:00 AM EST
Speaker: **Alessandra Scafuro** - North Carolina State University
Title: *One-time Traceable Ring Signatures*

Abstract: A ring signature allows a party to sign messages anonymously on behalf of a group, which is called ring. Traceable ring signatures are a variant of ring signatures that limits the anonymity guarantees, enforcing that a member can sign anonymously at most one message per tag. Namely, if a party signs two different messages for the same tag, it will be de-anomymized. This property is very useful in decentralized platforms to allow members to anonymously endorse statements in a controlled manner. In this talk we introduce one-time traceable ring signatures, where a member can sign anonymously only one message. We show that this natural variant, while sufficient in many applications for which traceable ring signatures are useful, enables us to design a scheme that only requires a few hash evaluations and outperforms existing (not one-time) schemes. We show a very simple one-time traceable ring signature scheme that is fast, is post-quantum resistant, and is the first anonymous signature scheme based on a black-box access to a symmetric-key primitive.
Platform (zoom.us)
If you are interested in the slides of previous talks, the material made available to us by the speakers is available on the archive page of the seminar website.
Felice Manganiello (Clemson University),
Gretchen Matthews (Virginia Tech), and
Edoardo Persichetti (Florida Atlantic University)