From: Brandao, Luis (IntlAssoc)
To: Kelsey, John M. (Fed)
Subject: Re: Crypto Reading Club 2021-Nov-03
Date: Thursday, October 28, 2021 11:48:55 AM

Thanks John,

I forgot to ask: do you want your presentation recorded?

If yes, we can then consider to make the video available publicly or only within NIST.

Luís

From: Kelsey, John M. (Fed) <john.kelsey@nist.gov>
Sent: Thursday, October 28, 2021 10:16
To: Brandao, Luis (IntlAssoc) <luis.brandao@nist.gov>
Subject: Re: Crypto Reading Club 2021-Nov-03

We show how to construct a threshold version of stateful hash-based signature schemes like those defined in XMSS and LMS. Our techniques assume a trusted dealer and secure point-to-point communications, and are efficient in terms of communications and computation, but do require at least one party to have a large (but practical) amount of storage, and support n-of-n and k-of-n signatures, and also coalition signatures–we can directly define arbitrary coalitions of trustees who are permitted to sign messages. We propose the addition of an untrusted Helper to manage the large storage required without being given access to any secret information. We prove the security of our schemes in a straightforward way, reducing their strength to that of the underlying hash-based signature scheme. Our schemes are quite practical, and substantially decrease the risk of accidental key reuse.

From: "Brandao, Luis (IntlAssoc)" <luis.brandao@nist.gov>
Date: Wednesday, October 27, 2021 at 17:16
To: "Kelsey, John M. (Fed)" <john.kelsey@nist.gov>
Subject: Re: Crypto Reading Club 2021-Nov-03

Thanks John,

Do you plan to produce an abstract?

If yes soon, I could consider waiting a bit to make the calendar update (which will send a new email to everyone).

Thanks, Luís

From: Kelsey, John M. (Fed) <john.kelsey@nist.gov>
Sent: Wednesday, October 27, 2021 16:38
To: Brandao, Luis (IntlAssoc) <luis.brandao@nist.gov>

Subject: Re: Crypto Reading Club 2021-Nov-03

Luis,

I'll be talking about Threshold Hash-Based Signatures.

Thanks,

--John

From: "Brandao, Luis (IntlAssoc)" <luis.brandao@nist.gov>
Date: Wednesday, October 27, 2021 at 16:36
To: CRYPTO-CLUB <CRYPTO-CLUB@list.nist.gov>
Cc: "Kelsey, John M. (Fed)" <john.kelsey@nist.gov>
Subject: Crypto Reading Club 2021-Nov-03

Crypto Reading Club meeting (virtual) on Wednesday, 2021-Nov-03, 2pm--3pm EST:

Please note the unusual time --- this talk will be in the afternoon 2pm--3pm EST.

Presenter: John Kelsey, NIST.

Title and abstract to be announced.