From: Liu, Yi-Kai (Fed)
To: Moody, Dustin (Fed)
Subject: Re: Suggestion- we should meet sometime over the new CLZ21 paper
Date: Tuesday, October 5, 2021 10:16:20 AM

Thanks! Much appreciated!

--Yi-Kai

_____
From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Tuesday, October 5, 2021 10:03 AM
To: Liu, Yi-Kai (Fed)
Subject: Re: Suggestion- we should meet sometime over the new CLZ21 paper

Yi-Kai,

(b) (6) Of course, we'll postpone to a later time.

Dustin

_____
From: Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>
Sent: Tuesday, October 5, 2021 9:49 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: Suggestion- we should meet sometime over the new CLZ21 paper

Hi Dustin,

I'm sorry but can I postpone my talk on Tuesday Oct. 12 on torsion-point attacks on SIKE?

(b) (6)

Maybe I can combine this with my third-round talks on SIKE and NTRUprime?

Thanks, and sorry about this...

--Yi-Kai

_____
From: Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>
Sent: Wednesday, September 1, 2021 11:05 AM
To: Moody, Dustin (Fed); Apon, Daniel C. (Fed); Alagic, Gorjan (Assoc)
Subject: Re: Suggestion- we should meet sometime over the new CLZ21 paper

Sounds good!

--Yi-Kai

_____
From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Wednesday, September 1, 2021 11:04 AM
To: Liu, Yi-Kai (Fed); Apon, Daniel C. (Fed); Alagic, Gorjan (Assoc)
Subject: Re: Suggestion- we should meet sometime over the new CLZ21 paper

Let's go for the 12th. Earlier the better!

Thanks.

_____
From: Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>
Sent: Wednesday, September 1, 2021 11:04 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Apon, Daniel C. (Fed) <daniel.apon@nist.gov>; Alagic, Gorjan (Assoc) <gorjan.alagic@nist.gov>
Subject: Re: Suggestion- we should meet sometime over the new CLZ21 paper

Hi Dustin,

If it helps, I could probably talk earlier, say Oct. 15 or 12. Let me know... thanks!

--Yi-Kai

_____
From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Wednesday, September 1, 2021 10:58 AM
To: Liu, Yi-Kai (Fed); Apon, Daniel C. (Fed); Alagic, Gorjan (Assoc)
Subject: Re: Suggestion- we should meet sometime over the new CLZ21 paper

Yi-Kai, Oct 19th would probably be okay. I want to start doing our review process right about then. But I imagine we could do your talk and another talk the same day if needed.

Dustin

_____
From: Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>
Sent: Wednesday, September 1, 2021 10:57 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Apon, Daniel C. (Fed) <daniel.apon@nist.gov>; Alagic, Gorjan (Assoc) <gorjan.alagic@nist.gov>
Subject: Re: Suggestion- we should meet sometime over the new CLZ21 paper

Actually, could I talk a bit later, say in October? I'll probably need some time to prepare. Maybe Tuesday Oct. 19?

That paper on SIDH proofs of knowledge looks interesting!

--Yi-Kai

_____
From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Wednesday, September 1, 2021 8:23 AM
To: Apon, Daniel C. (Fed); Liu, Yi-Kai (Fed); Alagic, Gorjan (Assoc)
Subject: Re: Suggestion- we should meet sometime over the new CLZ21 paper

We can do any paper that you guys deem relevant.

When would you each like to talk? They can be the same day, but do not need to be on the same day.

Dustin

P.S. Yi-Kai, I'm glad you are on an isogeny kick! A paper I've been looking at is
https://eprint.iacr.org/2021/1023.pdf
SIDH Proof of Knowledge - eprint.iacr.org<https://eprint.iacr.org/2021/1023.pdf>
SIDH Proof of Knowledge Luca De Feo1, Samuel Dobson 2, Steven D. Galbraith , and Lukas Zobernig2 1IBM Research Europe. luca@defeo.lu 2Mathematics Department, University of Auckland, New Zealand. samuel.dobson.nz@gmail.com, s.galbraith@auckland.ac.nz, lukas.zobernig@auckland.ac.nz August 24, 2021

Abstract
eprint.iacr.org

From: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>
Sent: Wednesday, September 1, 2021 1:34 AM
To: Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>; Alagic, Gorjan (Assoc) <gorjan.alagic@nist.gov>
Subject: Re: Suggestion- we should meet sometime over the new CLZ21 paper

Maybe we could do both.

Jacob Lichtinger + Ray Perlner + I went through https://eprint.iacr.org/2021/1093.pdf in a lot of detail today; I could lead a discussion over it for 30min-1hr (with the other two chiming in)

The earlier or latter part of the meeting could be over Yi-Kai's suggestion?

--Daniel

From: Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>
Sent: Tuesday, August 31, 2021 3:46 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Alagic, Gorjan (Assoc) <gorjan.alagic@nist.gov>
Cc: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>
Subject: Re: Suggestion- we should meet sometime over the new CLZ21 paper

Hi Dustin,

Actually, can I volunteer to present/discuss this paper instead? I've been on an isogeny kick lately.

Improved torsion-point attacks on SIDH variants
(from CRYPTO 2021)
https://eprint.iacr.org/2020/633

--Yi-Kai

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Tuesday, August 31, 2021 2:15 PM
To: Liu, Yi-Kai (Fed); Alagic, Gorjan (Assoc)
Cc: Apon, Daniel C. (Fed)
Subject: Re: Suggestion- we should meet sometime over the new CLZ21 paper

Gorjan, Yi-Kai, Daniel,

Anyway interested in leading a presentation/discussion on this paper? No rush of course...

Dustin

From: Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>
Sent: Monday, August 30, 2021 3:24 PM
To: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>
Cc: internal-pqc <internal-pqc@nist.gov>
Subject: Re: Suggestion- we should meet sometime over the new CLZ21 paper

I'd like to second this. I think Gorjan is interested in this paper too.

--Yi-Kai

_____
From: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>
Sent: Monday, August 30, 2021 12:24 PM
To: Moody, Dustin (Fed)
Cc: internal-pqc
Subject: Suggestion- we should meet sometime over the new CLZ21 paper

https://eprint.iacr.org/2021/1093.pdf

It doesn't impact candidates, but you get the feeling that they took their shot at Dilithium and only just missed.

It's not obvious that it will quickly extend to a serious quantum attack against Dilithium (because it's using Arora-Ge as a subroutine, and inherits all of the limitations related to #samples), but it seems worth understanding the techniques well enough to stay informed about where things are.

Bonus points for this paper: They make big claims, and immediately provide verifiable analysis to support those claims. (I know that's been in short supply lately.)

--Daniel