From: Moody, Dustin (Fed)
To: Apon, Daniel C. (Fed)
Subject: Re: Suggestion- we should meet sometime over the new CLZ21 paper
Date: Friday, September 3, 2021 9:03:55 AM

Sure, we can do it without slides.

If you're prepared for Tuesday, we'll likely have time for it. Might depend on how long discussion on other topics goes.

Thanks

From: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>
Sent: Thursday, September 2, 2021 9:48 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: Suggestion- we should meet sometime over the new CLZ21 paper

Um-- I am happy to put together some slides if you think that would be helpful

Another option (which I did with Ray + Jacob) would be just to open the paper up and talk through it some

I don't think we believe the exact technical details are super crucial for this one -- you can get a sense of what's going on by reading through the high-level at the beginning.

Which would you prefer though? If slides, then I would need to find some time to write them; if not slides, I could talk through the ideas at the next meeting (with Ray/Jacob chiming in)

--Daniel

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Thursday, September 2, 2021 10:41 AM
To: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>
Subject: Re: Suggestion- we should meet sometime over the new CLZ21 paper

Daniel,

When would you like to do this?

Dustin

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