From: Kelsey, John M. (Fed)
To: Calik, Cagdas (IntlAssoc)
Subject: Re: Pyramid signature scheme
Date: Friday, December 20, 2019 11:08:28 AM

Cagdas,

I'm around next week—(b) (6)

I think the first thing I'm interested in here is getting details nailed down enough for an implementation, and then figuring out what kind of performance we can get. Also, if you can think of ways to make the signatures either faster or smaller, that would be very interesting. Stateless hash based signatures tend to be so big that they're not really all that useful, and Pyramid continues that tradition.

Thanks,

--John

From: "Calik, Cagdas (IntlAssoc)" <cagdas.calik@nist.gov>
Date: Wednesday, December 18, 2019 at 13:57
To: "Kelsey, John M. (Fed)" <john.kelsey@nist.gov>
Subject: RE: Pyramid signature scheme

Thanks John, I'll take a look into this. Are you around next week, let's schedule a meeting?

Cagdas

From: Kelsey, John M. (Fed) <john.kelsey@nist.gov>
Sent: Wednesday, December 18, 2019 1:55 PM
To: Calik, Cagdas (IntlAssoc) <cagdas.calik@nist.gov>
Subject: Pyramid signature scheme

Cagdas,

Here's the presentation I gave internally about Pyramid. I think this explains the idea pretty well, but let me know if you have questions. I'm working on writing this up for publication, but the paper I have so far is basically just the slides plus some introductory material at the beginning.

Thanks,
--John