From: Apon, Daniel C. (Fed)
To: Kelsey, John M. (Fed)
Subject: Re: As a now-pseudo-biased observer of hash-based signatures...
Date: Monday, December 10, 2018 1:18:12 PM

Week of 10-14

Monday: Hey what it be like, my dude?
Tuesday is definitely too quick, I think.. //our 'final' Round 1 PQC meeting is at 10am
Wednesday is an "early" option.. //let me know..
Thursday is DC Area Crypto Day at UMD (all day) //you should go if you can! https://dcareacryptoday.wordpress.com/
//Btw, I'm the "host" for the next DC Area Crypto Day, at NIST, sometime this upcoming Spring
Friday, I have a 9-10 meeting, (b) (6) [redacted]

Week of 17-21

Monday: I think I'm totally free
Tuesday: I think I'm totally free
Wednesday: I am presenting a "Light Intro to Oblivious RAM" (scheduled in the hope you, in particular, will be available!) at NIST's Crypto Reading Group; otherwise, I am free on Wednesday
Thursday: I think I'm totally free
(b) (6) [redacted]

From: Kelsey, John M. (Fed)
Sent: Monday, December 10, 2018 1:06:42 PM
To: Apon, Daniel C. (Fed)
Subject: Re: As a now-pseudo-biased observer of hash-based signatures...

That sounds great to me! Maybe later this week?

--John

> **From:** "Apon, Daniel C. (Fed)" <daniel.apon@nist.gov>
> **Date:** Monday, December 10, 2018 at 10:19 AM
> **To:** "Kelsey, John M. (Fed)" <john.kelsey@nist.gov>
> **Subject:** Re: As a now-pseudo-biased observer of hash-based signatures...
>
> Actually, I haven't gone through the details of Picnic in depth myself..
>
> If you're interested, I could read through the spec (and theory, etc), and you and I could plan some time to sit in front of a whiteboard and work through it..

(I'd find it fun :-))

Want to?
--Daniel

From: Kelsey, John M. (Fed)
Sent: Monday, December 10, 2018 9:43:02 AM
To: Apon, Daniel C. (Fed)
Subject: Re: As a now-pseudo-biased observer of hash-based signatures...

Daniel,

This makes sense. I think stateful hash based signatures are pretty practical in a lot of places (though they might eventually be edged out everywhere by better alternatives), but the stateless ones have the dancing bear property (the surprising thing is that the bear dances at all).

I don't feel like I really understand Picnic all that well yet. Hopefully I can remedy that when I get a few spare hours….

--John

From: "Apon, Daniel C. (Fed)" <daniel.apon@nist.gov>
Date: Friday, December 7, 2018 at 4:01 PM
To: "Kelsey, John M. (Fed)" <john.kelsey@nist.gov>
Subject: As a now-pseudo-biased observer of hash-based signatures...

Hi John,

https://groups.google.com/a/list.nist.gov/forum/#!topic/pqc-forum/zLkDEgbRjRw
As I've worked.. somewhat closely.. with Jonathan Katz and Xiao Wang, I should state that I'm no longer a totally-objective observer of Picnic.
That said, my understanding is that the Picnic Team's intent is to replace Sphincs in terms of state-of-the-art hash-based signatures.

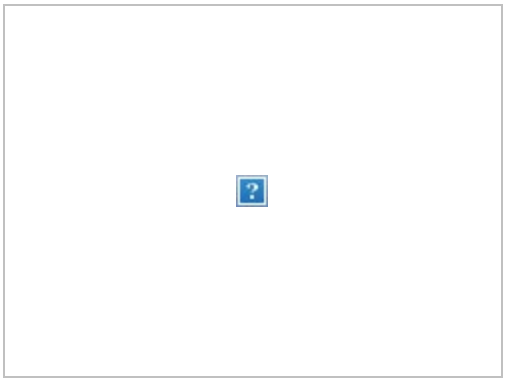
The brand-new Picnic spec deserves some serious consideration, imo.
Whereas I do not personally, truly see Sphincs surviving the extent of the PQC-Sig gauntlet against competing lattice and multivariate signatures,
just as I do not need McEliece surviving its similar PQC-KEM gauntlet against competing lattice and code-based key transport schemes..
..it may be the case that the new Picnic is a "not-1960s, not-1970s, not-1980s, etc." type of scheme that is actually competitive against e.g. lattice signatures.

In particular, whereas Sphincs appears to be 'mostly tapped out' in terms of optimizations, one would have to similarly 'tap out' every type of MPC-

optimization
in order to similarly 'block' the Picnic scheme, imo.

Conclusion/decision TO BE DETERMINED, very much based on your view.
Let me know if you're like to discuss any parts though..
--Daniel

P.S. Naturally, a relevant song: https://www.youtube.com/watch?v=c9cZSLfh7Xw



STARFORCE - Age of Nano

www.youtube.com

New Retro Wave + STARFORCE Stay R
and Subscribe: http://bit.ly/1tmU0Dk
Support: http://bitly.com/1aIGam7 Also
Support: http://bit.ly/1zudbOi Get Your
Retro Wear Here:
http://www.akadewear.com STAR FOR
comes back with an OUTSTANDING rec
Listen up! Stream Here:
https://soundcloud.com/starforce/starf
age-of-nano Picture Source: http ...