From: Apon, Daniel C. (Fed)
To: Kelsey, John M. (Fed)
Subject: Re: About hash-based blind signatures
Date: Sunday, December 2, 2018 5:18:10 PM

John,

I'd be very interested to hear about your threshold signature scheme!

Blind signatures are interesting, but threshold signatures are more interesting to me.
In fact, I may begin looking into "semi-efficient" lattice-based threshold signatures very soon..

From lattices, there are either early results that don't quite achieve the full notion of threshold signatures,
or there is https://eprint.iacr.org/2017/251.pdf -- which achieves threshold signatures from LWE (but somehow overshoots)..
..in that it works only if you are willing to homomorphically compute a homomorphic computation of a homomorphic computation of the signature scheme's algorithms. (Yikes.)

--Daniel

From: Kelsey, John M. (Fed)
Sent: Thursday, November 29, 2018 5:36:15 PM
To: Apon, Daniel C. (Fed)
Subject: Re: About hash-based blind signatures

Daniel,

That makes sense. I have something very close to hash based blind signatures now--it's a threshold signature scheme where we can get a blind signature as long as at least one trustee doesn't betray the user. I'm going to try to put this together into a talk sometime soon....

--John

From: Apon, Daniel C. (Fed)
Sent: Thursday, November 29, 2018 5:19 PM
To: Kelsey, John M. (Fed)
Subject: About hash-based blind signatures

Hey John,

I was speaking with Jon Katz, and the question of hash-based blind signatures came up. (I remember you asked me about this at one point.)

The belated answer to your question “Do they exist?” is..
1) from things like Sphincs? No. They cannot. http://www.cs.umd.edu/~jkatz/papers/blind-sigs-

impos.pdf
2) from things like Picnic? Perhaps, but this is not known yet either way.

Basically, there cannot be a black-box construction of blind signatures from one-way functions.
For a construction to be ‘non-black-box,’ it has to use the description of some circuit in a non-trivial, cryptographic way.
And since Picnic does MPC-in-the-head of some particular circuit (written out as gates and wires..), there is at least a chance that general approach could eventually lead to blind signatures.

--Daniel