From: Chen, Lily (Fed)
To: Smith-Tone, Daniel C. (Fed); Dworkin, Morris J. (Fed)
Cc: (b) (6)
Subject: Re: update
Date: Monday, August 2, 2021 9:58:48 AM

Hi, Daniel,

Nice to hear you. Thanks for the update. The research certainly will increase our confidence. It seems that there are some uncertainties for onramp signatures, which I have concerns. The advanced work will be a great help.

Lily

From: "Smith-Tone, Daniel C. (Fed)" <daniel.smith@nist.gov>
Date: Monday, August 2, 2021 at 9:21 AM
To: Lily Chen <lily.chen@nist.gov>, Morris Dworkin <morris.dworkin@nist.gov>
Cc: (b) (6)
Subject: update

Hi, Lily and Morrie,

I haven't sent you an update on what I'm doing in a while, so I figure it is time to do so.

I'm working on breaking a multivariate scheme that uses the structure of an extension ring instead of an extension field to define the nonlinear component of the map. I don't think that the scheme directly impacts our standards process, but I am using new techniques to break it, so it should advance the science. So far I have broken a related scheme (a homogeneous version), and I am trying to work through the nontrivial details of extending that attack to the full scheme.

I also recently reviewed an ASIACrypt submission that seems as though it might be accepted. It is a new approach to UOV that is similar to a proposal by Barreto in 2012 that Ray and I immediately broke (so it was never published), that Beullens rediscovered a couple of years ago, and was then broken again by a new method last year. This scheme changes what made the attack on the last year work, but doesn't seem to change what made the attacks Ray and I discovered fail (at least obviously). I suspect that there is something that we can do there, but I'm not sure if it is an outright break… probably not. I started looking at this scheme last week also, and I'll continue for a while (since I think that it would be an obvious candidate for submission to our onramp, so breaking it ahead of time might be better).

I am also hoping that we can have a meeting soon to review what impressions we got from PQCrypto a couple of weeks ago. I'm going to try to rewatch some of the talks and see what is worth looking into deeper.

Cheers,

Daniel