From: (b) (6)
To: Perlner, Ray A. (Fed)
Subject: Re: SRP clone
Date: Tuesday, October 31, 2017 1:24:17 PM

Thanks. That's what I meant. Sort of "Andy and family."

Cheers!

On Tue, Oct 31, 2017 at 11:12 AM, Perlner, Ray (Fed) <ray.perlner@nist.gov> wrote:

> (b) (6)
>
> **From:** Daniel Smith (b) (6)
> **Sent:** Tuesday, October 31, 2017 10:42 AM
> **To:** Perlner, Ray (Fed) <ray.perlner@nist.gov>
> **Subject:** SRP clone
>
> Hi, Ray,
>
> I spoke with Tsuyoshi and I think that he and a post-doc are on board to work on the SRP clone we talked about at Dagstuhl. I was wondering if you could help with making an outline for the paper (like we did for the HFEv- stuff that I still haven't contributed to). At some point I'm going to have to give a note to the post-doc saying what needs to be done in terms of experiments so that we can establish parameters that make the rank attack impotent. Other than that, we will need to discuss the degree of regularity of the scheme. I may be able to say something about that, but the important thing in that direction is experiments. We will also have to say something about the rainbow attack, but the plus will take care of that. I was thinking that we should also say something about the difficulty of separating the plus polynomials. (I can't think of an attack that explicitly affects the plus modifier, actually, it's just orthogonal to the attacks that seem relevant to the HFE part.)
>
> If you don't have time, that's fine too. Just let me know. I have to somehow figure out how I'm going to do what I need for the HFEv- attack and a few other projects that I'm trying to finish.
>
> Cheers,
>
> Daniel

BTW, how is everything going with Andy?