From:	Kerman, Sara J. (Fed)
To:	Perlner, Ray A. (Fed)
Cc:	Smith-Tone, Daniel C. (Fed); daniel-c.smith@louisville.edu
Subject:	FW: Paper accepted at SAC
Date:	Monday, August 7, 2017 1:53:02 PM

Ray,
You may want to get this paper - **Total Break of the SRP Encryption Scheme -** into NIKE for review (Div Reader and Outside Reader needed) since the conference is next week.

Sara

From: Moody, Dustin (Fed)
Sent: Monday, August 07, 2017 10:28 AM
To: Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Cc: Petzoldt, Albrecht R. (IntlAssoc) <albrecht.petzoldt@nist.gov>; Smith-Tone, Daniel (Fed) <daniel.smith@nist.gov>; Perlner, Ray (Fed) <ray.perlner@nist.gov>
Subject: RE: Paper accepted at SAC

It should be Ray's name – not mine. Albrecht probably accidentally put me in for Ray. I assume Ray or Daniel will do a WERB.

From: Kerman, Sara J. (Fed)
Sent: Monday, August 07, 2017 10:25 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Cc: Petzoldt, Albrecht R. (IntlAssoc) <albrecht.petzoldt@nist.gov>; Smith-Tone, Daniel (Fed) <daniel.smith@nist.gov>
Subject: Paper accepted at SAC

Dustin,
I don't have a record of the paper referenced below in NIKE (accepted at SAC). Which author will be taking care of starting the WERB process?

Sara

From: Petzoldt, Albrecht R. (IntlAssoc)
Sent: Monday, August 07, 2017 8:21 AM
To: Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Subject: RE: Two PQCrypto Papers

Sorry, I forgot to tell you.

The paper was unfortunately not accepted.
However, we have another paper accepted as SAC

Total Break of the SRP Encryption Scheme
By Dustin Moody, Albrecht Petzoldt and Daniel Smith-Tone

Most probably Dustin already told you about that.

Best regards,
Albrecht

From: Kerman, Sara J. (Fed)
Sent: Thursday, August 03, 2017 3:17 PM
To: Petzoldt, Albrecht R. (IntlAssoc) <albrecht.petzoldt@nist.gov>
Subject: RE: Two PQCrypto Papers

Hi Albrecht,

1. I never heard back – was your paper "Revisiting the HFEv- Signature Scheme over Larger Fields" accepted at SAC?

Sara

From: Petzoldt, Albrecht R. (IntlAssoc)
Sent: Thursday, July 06, 2017 3:03 PM
To: Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Subject: RE: Two PQCrypto Papers

Dear Sara,
The second paper was not accepted at PQCrypto. I've sent it to SAC. The Notification is tomorrow. I will tell you what came out of it.

Best regards,
Albrecht

From: Kerman, Sara J. (Fed)
Sent: Thursday, July 06, 2017 12:49 PM
To: Petzoldt, Albrecht R. (IntlAssoc) <albrecht.petzoldt@nist.gov>
Subject: Two PQCrypto Papers

Albrecht,
I published paper #1 (in NIKE/WERB) after finding it in the PQCrypto LNCS Proceedings. Paper #2 was not accepted, correct? Will you try to submit/publish elsewhere?

1. HMFEv - An Efficient Multivariate Signature Scheme
2. Revisiting the HFEv- Signature Scheme over Larger Fields

Thanks,

Sara J. Kerman
NIST
301-975-4634
sara@nist.gov