From: Robinson, Angela Y. (Fed)
To: Moody, Dustin (Fed)
Cc: Perlner, Ray A. (Fed); Alperin-Sheriff, Jacob (Fed)
Subject: Re: Round 5 spec
Date: Friday, April 26, 2019 2:52:32 PM

Please clarify some details of Algorithm 1 related to the creation of S and B. We believe a paragraph about deterministic function f_S would be helpful to include in section 2.4.3, similar to that of deterministic function f_R. We are also trying to reconcile the creation of B, using the rounding function as defined in section 2.2, in both the ring and non-ring cases.

We referred to section 2.11.6, core function "create_S_T" for more information. The description of this core function states that dimension of S^T is \bar{n} x d, so the dimensions of S are d x \bar{n}. In the ring case, it seems that B is created by taking the matrix product AS, reducing each entry mod \Phi_{n+1}, then adding rational number h_1. Please clarify what is meant by the sum of a matrix with h_1. In the non-ring case, does S^T still have dimensions \bar{n} x d?

Thanks,
Angela

From: Moody, Dustin (Fed)
Sent: Friday, April 26, 2019 6:36:07 AM
To: Robinson, Angela Y. (Fed)
Cc: Perlner, Ray (Fed); Alperin-Sheriff, Jacob (Fed)
Subject: Re: Round 5 spec

Angela,
Sounds good. Can you write up a request to the Round 5 team, and then bounce it around Ray, Jacob, Daniel(s), and I? Then we'll send it to Round5. Thanks,

Dustin

From: Robinson, Angela Y. (Fed)
Sent: Thursday, April 25, 2019 2:30 PM
To: Moody, Dustin (Fed)
Cc: Perlner, Ray (Fed); Alperin-Sheriff, Jacob (Fed)
Subject: Round 5 spec

Hi Dustin,

More clarification is needed from the Round5 team on details relating to section 2.4.3 Algorithm 1, step 5. The process to generate B is not clear.

A is either a d x d square matrix (in the non-Ring case) or A is a single polynomial (in the Ring case). In either case, A is multiplied by S. We request some information about the deterministic function f_S, similar to the paragraph found in section 2.4.3 about the deterministic function f_R. This information should include the dimensions of the output S.

The rounding function R_{a \rightarrow b, h} is defined explicitly in section 2.2. By this definition, Algorithm 1, step 5 includes some operation of the form (<AS>_\Phi + h_1). Because we do not know the dimensions of S, it is not clear whether AS will be a vector or a matrix, but in either case it is not clear how to add h_1 to AS. In the case that AS is a square matrix, does this mean to add h_1*Identity?

I talked to Ray and Jacob and they agree that more clarification is needed, but maybe this request should be ironed out before sending to the team?

Thanks,
Angela