From: Moody, Dustin (Fed)
To: Daniel Smith-Tone
Cc: Perlner, Ray A. (Fed)
Subject: revising our PQC paper
Date: Thursday, April 13, 2017 3:16:00 PM
Attachments: KRACABCSMMES-v2.pdf

Daniel,

The only comments that we possibly need to address came from one reviewer. I talked with Ray about them. He'll be on annual leave after today, so it's up to you and me to finish any revisions we decide to to do. Here's a few thoughts on the comments:

1) "- The authors argue that this approach allows for the same complexity regardless of the characteristic of the field, which notably is the motivation of the paper, and was not the case in [18]. However, very little space is devoted to this important question.
In particular, it is not clear why Eq. 1 has always a single solution over all characteristics except 3. Char. 2 is especially important, and the authors should argue more rigorously why there are no linear dependencies (in a form of a proposition or similar).
This will emphasize the novelty of the approach. Even more, I suggest to discuss the difference compared to [18] in the introduction. "

We don't think we really need to do anything in regard to comment 1, because we think the paper already does a good job at explaining everything. Perhaps this comment was caused by not being able to read [18]. We could do some revision, but we didn't think we really had to.

2) "- The description of the MinRank attack (Sec. 4) is somehow in the wrong order or perhaps a part is missing.
First it should be shown that a tensor H(E)(w) will have a rank 2s provided E is in the band and w is in the band kernel."

We'll add "(see Figure 2)" after "at rank at most 2s" at the top of p7. I think Figure 2 shows pretty simply that the rank of H(E)(w) will be 2s.

3)"- It should be commented briefly on the difference of using the Kipnis-Shamir or minors modeling, and why it was chosen not to."

We defer to you on what (if anything) should be mentioned regarding Kipnis-Shamir or minors modeling.

- The paper should be checked for typos and the use of vector notation.

I'll run a spell checker on it. Not sure of any vector notation problems.

Thanks,

Dustin