From:	Moody, Dustin (Fed)
To:	Daniel Smith
Cc:	Perlner, Ray (Fed)
Subject:	RE: revising our PQC paper
Date:	Monday, April 17, 2017 3:40:00 PM

Yep, I can submit it. Thanks!

From: Daniel Smith [mailto:dcs.xmr@gmail.com]
Sent: Monday, April 17, 2017 3:39 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Cc: Perlner, Ray (Fed) <ray.perlner@nist.gov>
Subject: Re: revising our PQC paper

I've tweaked it again, to correct a reference and to fix a typo. I think that it is good to submit now. Could you do it Dustin? I'll be doing this for a couple more shortly. Please don't forget the data file requested. Thanks a bunch and congratulations, guys.

Cheers,
Daniel

On Mon, Apr 17, 2017 at 2:28 PM, Moody, Dustin (Fed) <dustin.moody@nist.gov> wrote:

> Looks good to me. I believe Ray is out this week. Do you want me to submit or you to submit?
>
> Dustin
>
> **From:** Daniel Smith [mailto:dcs.xmr@gmail.com]
> **Sent:** Monday, April 17, 2017 12:00 PM
> **To:** Moody, Dustin (Fed) <dustin.moody@nist.gov>
> **Cc:** Perlner, Ray (Fed) <ray.perlner@nist.gov>
>
> **Subject:** Re: revising our PQC paper
>
> Hi, guys,
>
> Here are my revisions. Please take a look.
>
> Cheers,
> Daniel
>
> On Fri, Apr 14, 2017 at 8:28 AM, Moody, Dustin (Fed) <dustin.moody@nist.gov> wrote:
>
> > Daniel,
> >
> > I've attached the files for you to add to.

I'd be up for exploring the ideas you mentioned about the break even point. It'd be really good to involve Albrecht as well. Hope you are feeling better.

Dustin

From: Daniel Smith <dcs.xmr@gmail.com>
Sent: Thursday, April 13, 2017 5:27:10 PM
To: Moody, Dustin (Fed)
Cc: Perlner, Ray (Fed)
Subject: Re: revising our PQC paper

Hi, Dustin,

Can you make the changes you mentioned and send me the revised source? I can address 3 fairly well by simply adding a paragraph on why minors modeling doesn't work. The reviewer doesn't know what s/he is talking about though, because KS makes no sense here. I do think, however, that there are many in the intended audience who would be interested in a comparison between the linear algebra technique here and the minors modeling minrank approach. It is interesting to see why the minors modeling approach is so much worse in this case.

On the other hand, finding the break-even point on linear algebra search versus minors modeling is itself a very interesting question that we should study for another paper (independent of any particular scheme). Let's work on this for another submission this year... say SAC again? The idea is this, we take systems of formulae with a low minrank and attack it with linear algebra search and minors modeling and determine the complexity. Then we vary things like number of variables/equations, the minrank, or the field size. (My understanding is that the French team says that minors is always more efficient for these cases.) Then we study the case of differential invariants with interlaced kernels and vary along the same parameters. We already know that the linear algebra search is better for the parameters we attack, but as q increases there will be a breakeven point. As the minrank increases there is likely a breakeven point as well. This could be important work for the establishment of parameters for small field multivariate schemes in the future, so it's definitely worth a try. Let's bring Albrecht on board with this project as well.

Cheers,
Daniel

On Thu, Apr 13, 2017 at 3:15 PM, Moody, Dustin (Fed) <dustin.moody@nist.gov> wrote:

> 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