From: Moody, Dustin (Fed)
To: Perlner, Ray A. (Fed); (b) (6)
Subject: Re: question
Date: Friday, February 17, 2017 11:56:25 AM

We could also shorten the experiments section. We don't have as much data as last time. I tried to say these experiments were just a sanity check. So condensing it would be fine with me.

From: Perlner, Ray (Fed)
Sent: Friday, February 17, 2017 10:06:51 AM
To: Daniel Smith
Cc: Moody, Dustin (Fed)
Subject: RE: question

Can you move the section on completing the key recovery into an appendix?

From: Daniel Smith (b) (6)
Sent: Friday, February 17, 2017 4:32 AM
To: Perlner, Ray (Fed) <ray.perlner@nist.gov>
Cc: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: question

What should we do about the length? The cfp said that submissions had to retain lncs standard margins with no adjustments. When I remove our cheat, we have a couple of pages too much.

On Thu, Feb 16, 2017 at 2:48 PM, Daniel Smith (b) (6) wrote:

> Attached are my edits. Please check that nothing is crazy. I haven't proofread it yet. I'll give it a look soon, but I'm busy for a while.
>
> Cheers,
> Daniel
>
> On Thu, Feb 16, 2017 at 12:22 PM, Perlner, Ray (Fed) <ray.perlner@nist.gov> wrote:
>
>> If you do the same trick of only changing one coordinate of w1 and w2 at a time, I'm pretty sure you can get the search down to s^4, at which point the s^{2\omega} rank calculation is the limiting step.
>>
>> **From:** Daniel Smith (b) (6)
>> **Sent:** Thursday, February 16, 2017 12:20 PM
>> **To:** Perlner, Ray (Fed) <ray.perlner@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>
>> **Subject:** question
>>
>> Dustin brings up again the issue of s^6 vs s^{2\omega} in the context of the quadratic scheme. I recall Ray saying that there is a way to make it s^{2\omega} but I'm not seeing it right now. Don't we have to search a 3-dim space over GF(s^2)? Wouldn't this be s^6?

> > I'm trying to finish a revised intro, outro, but this data is relevant.
> >
> > Cheers!