From: (b) (6)
To: Perlner, Ray A. (Fed)
Cc: Moody, Dustin (Fed)
Subject: Re: question
Date: Friday, February 17, 2017 3:25:08 PM

I'm not very confident that I know what I meant by that claim, either. I looked at the minors modeling problem for this, and it seems a bit daunting, but this rank property is possible to model that way, as well. For the cubic it would be a sort of hybrid approach. We would randomly pick a vector w and compute \mathbf{H}(\mathcal{E}_i)(w). This would give us s^2 quadratic forms. Then we would solve the MinRank instance here with minors modeling. The complexity should be around q(s^2)^((2s+1)\omega) and is more independent of q. I think the memory requirements are offensive, but that seems like it could kill the schemes for good. Anyway, that's not this paper, though maybe we should do that next.

I agree with you. I think that the scheme is broken for original parameters.

On Fri, Feb 17, 2017 at 1:41 PM, Perlner, Ray (Fed) <ray.perlner@nist.gov> wrote:

> I'm not sure I agree with the claim that the scheme is completely broken. Our attack can be avoided by simply increasing q. This should have only minimal impact on the parameters. I still think that quadratic ABC looks pretty good as far as multivariate encryption goes (which isn't saying all that much, admittedly.)
>
> I'm also still not sure what you mean by the claim that the attack on cubic ABC is actually cheaper than the attack on quadratic ABC. It seems the cost is pretty much the same for the same value of q and s (although the key will be much larger for cubic ABC, of course.)
>
> **From:** Daniel Smith (b) (6)
> **Sent:** Thursday, February 16, 2017 2:49 PM
> **To:** Perlner, Ray (Fed) <ray.perlner@nist.gov>
> **Cc:** Moody, Dustin (Fed) <dustin.moody@nist.gov>
> **Subject:** Re: question
>
> 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!