From: (b) (6)
To: Perlner, Ray A. (Fed)
Subject: Re: the invariant attack
Date: Monday, November 20, 2017 9:09:34 PM

Thanks. I haven't taken a look yet, but I will try tonight or tomorrow morning.

On Mon, Nov 20, 2017 at 11:34 AM Perlner, Ray (Fed) <ray.perlner@nist.gov> wrote:

> Ok. I uploaded my section. Let me know if you have any comments
>
> Cheers!
>
> Ray
>
> **From:** Daniel Smith (b) (6)
>
> **Sent:** Friday, November 17, 2017 5:54 PM
>
> **To:** Perlner, Ray (Fed) <ray.perlner@nist.gov>
>
> **Subject:** Re: the invariant attack
>
> Thanks. I will ask Jeremy to go ahead and submit with this tomorrow and we can work on cleaning it up next week.
>
> Cheers!
>
> On Fri, Nov 17, 2017 at 5:35 PM, Perlner, Ray (Fed) <ray.perlner@nist.gov> wrote:
>
> > Well, it looks like I didn't finish my part today. Here's what I have so far. I'll try to finish it Monday.
> >
> > Cheers!
> >
> > ---
> >
> > **From:** Perlner, Ray (Fed)
> > **Sent:** Friday, November 17, 2017 3:42 PM
> > **To:** 'Daniel Smith' (b) (6)

Subject: RE: the invariant attack

Yes. That is what I was saying. I'm writing up the invariant attack section with the l dimensional projection and extra r rainbow equations, though, since that's how it's presented in our paper as written.

Cheers!

From: Daniel Smith (b) (6)
Sent: Friday, November 17, 2017 3:38 PM
To: Perlner, Ray (Fed) <ray.perlner@nist.gov>
Subject: the invariant attack

Hi, Ray,

Just a thought. We proved in our SRP attack that the scheme is equivalent to a scheme with l=0, but we didn't say what the consequence of that identification is. Considering the scheme to have l=0 is exactly the same as forcing the rainbow component to be imbalanced by l.

I'm wondering if this is what you were saying. Specifically, if we have a scheme with l>0 and a ``balanced'' rainbow component F_R with o+d inputs with o=d, it is equivalent to a scheme with l=0 where the rainbow component has o+d inputs with o=d-l.

Cheers!