From: (b) (6)
To: Perlner, Ray A. (Fed)
Subject: Re: Here are my slides so far for SAC (Note I"m planning on ending the presentation at slide 22, but I"m keeping the rest of the slides from my reading club talk just in case.)
Date: Thursday, August 4, 2016 9:43:08 AM

Yes it is. It is a special case of extension field cancellation, too. It can be attacked with a differential invariant attack, with minrank, with Q-rank (same as previous, but justification is different) and with the linearization equations attack. Actually, it can also be attacked with a subspace differential invariant attack, but I think that the answer would come from the differential invariant property and not the subspace differential invariant property.

Of these, the order in terms of complexity (least to greatest) assuming parameters similar to Ding's is:
1) differential invariant/subspace differential invariant;
2) linearization equations;
3) minrank/Q-rank.

Even the last one is going to be quite fast. The minrank search does a lot of rank computations, though, which are costly. The system of equations in the linearization attack is larger, but still should be easier.

Cheers!

On Thu, Aug 4, 2016 at 8:50 AM, Perlner, Ray (Fed) <ray.perlner@nist.gov> wrote:

> Isn’t that a special case of balanced oil and vinegar? (y is oil x is vinegar)
>
> **From:** Daniel [mailto:(b) (6)
> **Sent:** Wednesday, August 03, 2016 8:07 PM
> **To:** Perlner, Ray (Fed) <ray.perlner@nist.gov>
> **Subject:** RE: Here are my slides so far for SAC (Note I'm planning on ending the presentation at slide 22, but I'm keeping the rest of the slides from my reading club talk just in case.)
>
> I had a random thought about extension field cancellation. What if it used A(x)x and B(y)x instead of how it is. It could be two variable to two variable. There would be half rank maps in the span of the public key, but is it easy to break? Decryption is the same.
>
> Sent from my T-Mobile 4G LTE Device
>
> -------- Original message --------
>
> From: "Perlner, Ray (Fed)" <ray.perlner@nist.gov>
>
> Date:08/03/2016 3:45 PM (GMT-05:00)
>
> To: "Daniel Smith ((b) (6) "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
>
> Cc:

> Subject: Here are my slides so far for SAC (Note I'm planning on ending the presentation at slide 22, but I'm keeping the rest of the slides from my reading club talk just in case.)