

From: (b) (6)
To: [Perlner, Ray A. \(Fed\)](#); [Smith-Tone, Daniel C. \(Fed\)](#)
Subject: Re: Our paper
Date: Friday, November 17, 2017 2:52:21 PM

I think this would be better. I missed the term HFE.

Am 11/17/2017 um 2:51 PM schrieb Perlner, Ray (Fed):

> How about "Improved Cryptanalysis of HFEv- via Projection"?

>

> -----Original Message-----

> From: Albrecht Petzoldt (b) (6)

> Sent: Friday, November 17, 2017 2:44 PM

> To: Smith-Tone, Daniel (Fed) <daniel.smith@nist.gov>; Perlner, Ray (Fed) <ray.perlner@nist.gov>

> Subject: Our paper

>

> Hi,

>

> I saw that Daniel has changed the title of our paper in "Improved Cryptanalysis via Projection". So you don't want to mention HFEv- or multivariate?

>

> The deadline is on Sunday, 6am EST (same for the second deadline)

>

> If nobody of you comes first, I will submit our draft by Saturday evening.

>

>

> Best,

>

> Albrecht

>

>