From: (b) (6)
To: Smith-Tone, Daniel C. (Fed)
Subject: RE: FW: MinRank Paper
Date: Friday, May 19, 2017 6:58:57 PM

Thanks. I will take a look at this tomorrow. Every day is a work day when you have insufficient talent.

Sent from my T-Mobile 4G LTE Device

-------- Original message --------
From: "Smith-Tone, Daniel (Fed)" <daniel.smith@nist.gov>
Date:05/19/2017 5:15 PM (GMT-05:00)
To: (b) (6)
Cc:
Subject: FW: MinRank Paper

From: Perlner, Ray (Fed)
Sent: Friday, May 19, 2017 5:15:06 PM (UTC-05:00) Eastern Time (US & Canada)
To: Smith-Tone, Daniel (Fed)
Subject: RE: MinRank Paper

Here are my edits. I added the requested paragraph. I decided not to duplicate the list of references for examples of MinRank attacks, since such a list appeared earlier in your intro. I did add to the list the attack on TTM (which is similar to the attack used to set parameters for Rainbow.)

I also reworded the last paragraph in section 2 for clarity and I added the word “nonzero’ to definition 1.

From: Smith-Tone, Daniel (Fed)
Sent: Thursday, May 18, 2017 5:29 PM
To: Perlner, Ray (Fed) <ray.perlner@nist.gov>
Subject: MinRank Paper

Here are the files for the MinRank paper. I don’t think that it needs much more. I put a note for a paragraph that maybe you can add about the need for n~m. Maybe you can find a reference or two to make it look solid. Then, please check the math and make sure I’m not crazy. Then we can try to find a reasonable journal in algebraic geometry to send it to.

Cheers,

Daniel