From: Moody, Dustin (Fed)
To: Daniel Smith; Perlner, Ray A. (Fed)
Subject: RE: flu
Date: Wednesday, April 12, 2017 3:33:21 PM

The only review that offered suggestions said to focus on:

- The authors argue that this approach allows for the same complexity regardless of the characteristic of the field, which notably is the motivation of the paper, and was not the case in [18]. However, very little space is devoted to this important question.
In particular, it is not clear why Eq. 1 has always a single solution over all characteristics except 3.

- Char. 2 is especially important, and the authors should argue more rigorously why there are no linear dependencies (in a form of a proposition or similar).
This will emphasize the novelty of the approach. Even more, I suggest to discuss the difference compared to [18] in the introduction.

- The description of the MinRank attack (Sec. 4) is somehow in the wrong order or perhaps a part is missing.
First it should be shown that a tensor H(E)(w) will have a rank 2s provided E is in the band and w is in the band kernel.

- It should be commented briefly on the difference of using the Kipnis-Shamir or minors modeling, and why it was chosen not to.

- The paper should be checked for typos and the use of vector notation.

Any comments on any of that?

From: Daniel Smith [mailto:dcs.xmr@gmail.com]
Sent: Wednesday, April 12, 2017 3:30 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Perlner, Ray (Fed) <ray.perlner@nist.gov>
B6 [redacted]

B6

B6 [redacted]

B6