From: (b) (6)
To: Perlner, Ray A. (Fed)
Subject: RE: Review Request
Date: Monday, December 11, 2017 6:37:17 PM

Thanks, and, "Sure. Can do."

Sent from my T-Mobile 4G LTE Device

-------- Original message --------
From: "Perlner, Ray (Fed)" <ray.perlner@nist.gov>
Date: 12/11/17 3:13 PM (GMT-05:00)
To: Daniel Smith (b) (6)
Subject: RE: Review Request

Here’s my review:

This paper extends the worst case to average case and search to decision reductions of ring LWE to LWE over tensor products of number fields, claiming motivation from applications of homomorphic encryption to signal processing.

On the plus side, the authors appear to know what they are doing mathematically. Everything I could verify appeared to be technically sound and in keeping with best practices in the subject matter area, although I don’t think I’m enough of an expert to verify everything.

The major drawback is that, what’s actually in the submitted paper is pretty minimal, being only a proof outline. The proofs are not included, and the reader is merely directed to the extended version of the paper on ArXiv. If the main focus was the cryptographic application, and more detail was given regarding the performance and potential usage scenarios of a cryptosystem based on multivariate LWE, such a proof sketch would likely be sufficient for the resulting paper to remain useful, but being that this is essentially a proof paper, it seems odd for it to leave so much of the details to be explained in the extended version.

I think I lean towards weak reject, but I have fairly low confidence.

Cheers,

Ray

P.S. Dustin says I should bug you about your complete & proper reviews. Do you think you’ll have them done by Friday? Thanks!

From: Perlner, Ray (Fed)
Sent: Tuesday, November 28, 2017 3:51 PM
To: 'Daniel Smith' (b) (6)
Subject: RE: Review Request

Sure. Can do.

From: Daniel Smith (b) (6)
Sent: Tuesday, November 28, 2017 3:48 PM
To: Perlner, Ray (Fed) <ray.perlner@nist.gov>
Subject: Review Request

Hi, Ray,

Would you be able to review the following attached paper for PQCRYPTO? "On Ring Learning with Errors over the Tensor Product of Number Fields"

This is a paper I will be paying attention to but that may fool me, so I could use another pair of eyes.

If you can, please give me your review by Dec. 15th. My deadline is Dec 17th and I want to be able to add whatever else I think is significant.

If you can't please let me know so that I can ask around.

Cheers,

Daniel