From: Dang, Quynh H. (Fed)
To: Moody, Dustin (Fed); internal-pqc
Subject: Re: kyber"s public key.
Date: Thursday, March 17, 2022 9:31:45 AM

The question is clearly a legitimate security question.

The security analysis and coreSVP estimates were for attacking the encryption, not attacking the public key to figure out the secret key.

Quynh.

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Thursday, March 17, 2022 9:26 AM
To: Dang, Quynh H. (Fed) <quynh.dang@nist.gov>; internal-pqc <internal-pqc@nist.gov>
Subject: Re: kyber's public key.

Quynh,

Dan has asked lots of questions that haven't been answered. He's been asked questions that he hasn't answered. If we want to say something about it then we can, but I don't think there is a need to do so.

Dustin

From: Dang, Quynh H. (Fed) <quynh.dang@nist.gov>
Sent: Thursday, March 17, 2022 8:58 AM
To: internal-pqc <internal-pqc@nist.gov>
Subject: kyber's public key.

Hi Dustin and all,

One thing I forgot: DJB asked about Kyber's public key's security level because it does not have the additional hardness from rounding.

As far as I know, Kyber's team has not responded to that question.

I think we need to address that question in our report.

What do you think ?

Quynh.