

From: [Moody, Dustin \(Fed\)](#)
To: [Lichtinger, Jacob T. \(Fed\)](#); [Perlner, Ray A. \(Fed\)](#)
Subject: Re: Kyber Ring Structure
Date: Friday, March 11, 2022 12:00:23 PM

Glad to be of no help!

From: Lichtinger, Jacob T. (Fed) <jacob.lichtinger@nist.gov>
Sent: Friday, March 11, 2022 11:53 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Perlner, Ray A. (Fed) <ray.perlner@nist.gov>
Subject: Re: Kyber Ring Structure

Nevermind, I found the issue.

From: Lichtinger, Jacob T. (Fed)
Sent: Friday, March 11, 2022 11:00 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Perlner, Ray A. (Fed) <ray.perlner@nist.gov>
Subject: Kyber Ring Structure

Hi Dustin and Ray,

In looking at the S-unit information, I started thinking about the Kyber ring structure again. I wrote up an idea for analysis, but I feel like it is too simple to be effective/correct. Do you see somewhere I made a mistake? I wanted someone to double check the idea before bringing it to the group.

Thanks,

Jacob