

**From:** [Moody, Dustin \(Fed\)](#)  
**To:** [Robinson, Angela Y. \(Fed\)](#)  
**Subject:** Re: PQC Round 3 Report - typo  
**Date:** Thursday, May 12, 2022 7:24:07 AM

---

Thanks for noticing, Angela.

Dustin

---

**From:** Robinson, Angela Y. (Fed) <[angela.robinson@nist.gov](mailto:angela.robinson@nist.gov)>  
**Sent:** Wednesday, May 11, 2022 12:56 PM  
**To:** Kerman, Sara J. (Fed) <[sara.kerman@nist.gov](mailto:sara.kerman@nist.gov)>; Foti, James (Fed) <[james.foti@nist.gov](mailto:james.foti@nist.gov)>  
**Cc:** Chen, Lily (Fed) <[lily.chen@nist.gov](mailto:lily.chen@nist.gov)>; Moody, Dustin (Fed) <[dustin.moody@nist.gov](mailto:dustin.moody@nist.gov)>; Perlner, Ray A. (Fed) <[ray.perlner@nist.gov](mailto:ray.perlner@nist.gov)>  
**Subject:** RE: PQC Round 3 Report - typo

\*page 30, section 4.2.1

---

**From:** Robinson, Angela Y. (Fed)  
**Sent:** Wednesday, May 11, 2022 12:54 PM  
**To:** Kerman, Sara J. (Fed) <[sara.kerman@nist.gov](mailto:sara.kerman@nist.gov)>; Foti, James (Fed) <[james.foti@nist.gov](mailto:james.foti@nist.gov)>  
**Cc:** Chen, Lily (Fed) <[lily.chen@nist.gov](mailto:lily.chen@nist.gov)>; Moody, Dustin (Fed) <[dustin.moody@nist.gov](mailto:dustin.moody@nist.gov)>; Perlner, Ray A. (Fed) <[ray.perlner@nist.gov](mailto:ray.perlner@nist.gov)>  
**Subject:** FW: PQC Round 3 Report - typo

Dear Sarah/Jim,

There was a typo in an important equation on page 33 of the NIST PQC Round 3 report. The typo has now been corrected. Here is the updated report as of today, May 11.

Kind regards,  
Angela

---

**From:** Chen, Lily (Fed) <[lily.chen@nist.gov](mailto:lily.chen@nist.gov)>  
**Sent:** Wednesday, May 11, 2022 12:48 PM  
**To:** Robinson, Angela Y. (Fed) <[angela.robinson@nist.gov](mailto:angela.robinson@nist.gov)>; Moody, Dustin (Fed) <[dustin.moody@nist.gov](mailto:dustin.moody@nist.gov)>  
**Cc:** Perlner, Ray A. (Fed) <[ray.perlner@nist.gov](mailto:ray.perlner@nist.gov)>  
**Subject:** RE: PQC Round 3 Report - typo

Hi, Angela,

I am glad that you caught it. I think a new PDF version should be sent to Sara/Jim. Just make sure that Dustin is involved since he is the one who has handled the interface with publication team.

Lily

---

**From:** Robinson, Angela Y. (Fed) <[angela.robinson@nist.gov](mailto:angela.robinson@nist.gov)>

**Sent:** Wednesday, May 11, 2022 12:41 PM

**To:** Chen, Lily (Fed) <[lily.chen@nist.gov](mailto:lily.chen@nist.gov)>; Moody, Dustin (Fed) <[dustin.moody@nist.gov](mailto:dustin.moody@nist.gov)>

**Cc:** Perlner, Ray A. (Fed) <[ray.perlner@nist.gov](mailto:ray.perlner@nist.gov)>

**Subject:** PQC Round 3 Report - typo

Hi Dustin/Lily,

There was a typo I made in the BIKE summary of the Round 3 report. It has been corrected now. Do I need to send a new PDF version of the report to Sara/Jim?

Thanks,  
Angela