**From:** Moody, Dustin (Fed)
**To:** Perlner, Ray A. (Fed)
**Subject:** RE: ERB review request
**Date:** Monday, May 23, 2022 12:21:31 PM

---

Here's my comments. I'll approve it in the system.

Abstract

- You use PK, consider just saying "public key"
- Maybe mention in the abstract if this works on all security categories (or not). Especially when saying you used 200,000 core hours.

Introduction

- To save on acronyms, you probably don't need one for CRQC. It's only used twice in one paragraph.
- May want to be more specific that a quantum computer threatens public-key, not all of crypto
- "The only counter…." What about QKD? They'd argue it is a counter
- "with 5 of the 7 finalists are", the word 'are' sounds a bit awkward being used here. Maybe 'being'?
- Classic McEliece may disagree that FrodoKEM is the most conservative
- Seems strange to center justify the questions at the end of the intro before 1.1
- A reader may be curious why FrodoKEM was selected to target over the finalist algorithms

1.1
- (applies to earlier as well). Consider the first time you use KeyGen to spell out that it is Key Generation, which you'll abbreviate KeyGen

1.2
- DFR is only used one time. So perhaps you don't need to give it an abbreviation.
- in the first paragraph I'd move the citations [6,18,19,48] to the end of the sentence or before the word 'later'
- several abbreviations being used without defining what they are (IND, OW, CPA, CCA, SVP etc)
- may want to explain why "feng shui" is used as the name for memory massaging.
- "couple minutes" -> "couple of minutes" [right before 1.3]

1.4
- What about Section 7? Not mentioned.

- Appendix 7? What about appendix 1-6? Or are section and appendix mixed up here?

2.2
- definition 2.1 and 2.2 are italicized. In the next subsection 2.3 the definition is bolded and starts counting at Definition 1. Use consistent format

2.3
- When you first mention learning with errors you should define LWE. The abbreviation shows up after learning with errors is first brought up
- capitalize Algorithm 1 (shortly after definition 5)
- "Frodo specification" perhaps should be FrodoKEM specification. Frodo appears solo 10 times in the paper.
- "search script in Frodo submission" -> "search script in the FrodoKEM submission"
- "the NIST level 1" isn't how we'd probably word this. Maybe something like NIST security category 1? Also, you may want to mention you're focusing on category 1 earlier in the paper somewhere.

2.4
- aggressor row doesn't have quotes, but victim row does. Be consistent
- the word poison is used several times. Maybe it should be explained precisely what poisoning a key means

4

- Including hobbit in the section title is a bit odd. Not everybody knows Frodo & hobbits
- It feels like the attack has been described several times now. It may not need to be described again here.
- No idea what ASLR is, and its not described

7

- There is a new paragraph started that isn't meant to be a new paragraph (it starts mid-sentence)

A.
- It isn't really mentioned what will be covered in the appendix. I think one reference is given earlier, but it doesn't capture what is all there

---

**From:** Perlner, Ray A. (Fed) <ray.perlner@nist.gov>
**Sent:** Tuesday, May 17, 2022 3:08 PM
**To:** Moody, Dustin (Fed) <dustin.moody@nist.gov>; Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>

**Subject:** ERB review request

Hi Dustin and Yi-Kai.

Can you review the attached paper submitted to ACM Conference on Computer and Communications Security (CCS) (ACM CCS 2022). I left it anonymous since when I tried to deanonymize it in overleaf, it threw up some error messages I didn't feel like investigating, but the author list is:

Michael Fahr Jr. (University of Arkansas);
Hunter Kippen (University of Maryland, College Park);
Andrew Kwong (University of Michigan);
Thinh Dang (George Washington University and The National Institute of Standards and Technology);
Jacob Lichtinger (National Institute of Standards and Technology);
Dana Dachman-Soled (University of Maryland, College Park);
Daniel Genkin (Georgia Tech);
Alexander H. Nelson (University of Arkansas);
Ray Perlner (National Institute of Standards and Technology);
Arkady Yerukhimovich (George Washington University);
Daniel Apon (The MITRE Corporation)

Thanks,
Ray