

From: [Moody, Dustin \(Fed\)](#)
To: [Chen, Lily \(Fed\)](#)
Subject: RE: Draft article for Advances in Mathematics of Communications (AMC)
Date: Monday, February 4, 2019 3:22:35 PM

Yes, tomorrow I will work on that aspect.

From: Chen, Lily (Fed)
Sent: Monday, February 04, 2019 3:22 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: RE: Draft article for Advances in Mathematics of Communications (AMC)

Dustin,

Thanks. It will be on a special edition of “Advances in Mathematics of Communications (AMC)” dedicated to post-quantum cryptography. I know very little about this journal. You can see some articles at <http://www.aims sciences.org/journal/1930-5346>

Can you think some more examples?

Lily

From: Moody, Dustin (Fed)
Sent: Monday, February 04, 2019 3:15 PM
To: Chen, Lily (Fed) <lily.chen@nist.gov>
Subject: RE: Draft article for Advances in Mathematics of Communications (AMC)

Lily,

I have read through and revised the article. Overall, I think it is very well laid out. I think the approach is good, although I agree with you that it might be thin on math. Where is this being published again?

Dustin

From: Chen, Lily (Fed)
Sent: Monday, February 04, 2019 8:24 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Draft article for Advances in Mathematics of Communications (AMC)

Hi, Dustin,

During shutdown, I initiated the attached article, you and I co-authoring, and made some changes during the weekend. Please continue to work on it.

1. I told Jintai that we cannot submit at the end of Jan. because of the shutdown. We may submit by the end of this week.

2. Jintai said that limit is 10 pages.
3. Please check
 - a. Do you think this is a right way to introduce our PQC to math community? You may suggest a different way and start to navigate through.
 - b. Is it too much on background? If too much, see what we can remove?
 - c. Anything I stated is wrong? Please correct.
4. I think it is too thin in math to get everyone interested, Maybe you can think more examples and problems.
5. References need to be checked. I did not make reference to the major categories in PQC. (I did not link references as well, see item 6 below.)
6. I do not know format yet. But it should not be hard to convert it to tex or Latex.

If it were not shutdown, I should have discussed with you before I started. Hope you do not mind. Remember, nothing is determined, we still have time to change.

Lily