From:	Chen, Lily (Fed)
To:	Chen, Lily (Fed)
Subject:	FW: Work on your version
Date:	Thursday, February 7, 2019 9:57:38 AM
Attachments:	PQCarticle1.pdf PQCarticle1.tex

From: Dustin Moody <dustin.moody@nist.gov>
Date: Thursday, February 7, 2019 at 9:41 AM
To: Lily Chen <lily.chen@nist.gov>
Subject: RE: Work on your version

Changes made. Here's the .pdf (and .tex)

From: Chen, Lily (Fed)
Sent: Thursday, February 7, 2019 9:38 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: RE: Work on your version

Hi, Dustin,

It does not compile on my machine, can you please change it and send back to me and also change my name to Lidong Chen.

Thanks,

Lily

From: Moody, Dustin (Fed)
Sent: Wednesday, February 06, 2019 2:21 PM
To: Chen, Lily (Fed) <lily.chen@nist.gov>
Subject: Re: Work on your version

Okay, we can change "mathematicians expert in these areas" to "mathematicians and experts in these areas..."

I think we're okay not putting in the LWE/RLWE details. Are there further changes you would like? I am happy with it.

Dustin

From: Chen, Lily (Fed)
Sent: Wednesday, February 6, 2019 2:17:26 PM
To: Moody, Dustin (Fed)
Subject: RE: Work on your version

Hi, Dustin,

I think the added content and questions can lead the readers to explore more, if they are interested. Like you, I do not know how deep we shall go. With the page limit, I do not think we can go too far. Assume the readers are mathematical researchers, they might google the content and find out the relevant details. As you said, may an introduction on LWE and R-LWE problem on page 7 (3rd paragraph) can make the reading easier? I like the example on isogeny of EC.

One sentence at 3rd from the end "Unfortunately, there are not enough mathematicians expert in these areas who are studying the cryptographic implications of their work." May be "mathematicians and experts"?

Lily

From: Moody, Dustin (Fed)
Sent: Wednesday, February 06, 2019 11:18 AM
To: Chen, Lily (Fed) <lily.chen@nist.gov>
Subject: Re: Work on your version

Lily,

I tried to beef up section 5. Let me know what you think. Another possibility would be to add in a few mathematical details, for example, when we discuss LWE and R-LWE we could put in the details of what the actual LWE problem is. I'm not sure if we need to get that technical or not.

Dustin

From: Moody, Dustin (Fed)
Sent: Tuesday, February 5, 2019 2:38:34 PM
To: Chen, Lily (Fed)
Subject: RE: Work on your version

There's always Yi-Kai. Or Jintai himself could be a WERB reader.

From: Chen, Lily (Fed)

Sent: Tuesday, February 5, 2019 2:36 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: RE: Work on your version

We can think about WERB readers so that when we send to Jintai, we can send to readers, Ray and …?

Lily

From: Moody, Dustin (Fed)
Sent: Tuesday, February 05, 2019 2:27 PM
To: Chen, Lily (Fed) <lily.chen@nist.gov>
Subject: RE: Work on your version

Lily,
I've converted it into latex. Sorry – it took a little longer than I thought. I am switching out laptops and the new laptop arrived today and so I had to install latex on it and switch over. I will begin to revise it now.

Dustin

From: Chen, Lily (Fed)
Sent: Tuesday, February 5, 2019 9:41 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: RE: Work on your version

Hi, Dustin,

Thanks a lot for the improvements. This indeed gives ME an opportunity to learn writing even though I have worked on my English writing for a long time. It is my lifetime task. I appreciate every opportunity and help.

I accepted all the changes, except questions on 1 or 2 places and read it through. We have 10 page limit. When converting to latex, it should use less space. Think some math stuff we can add on.

Lily

From: Moody, Dustin (Fed)
Sent: Tuesday, February 05, 2019 8:45 AM
To: Chen, Lily (Fed) <lily.chen@nist.gov>
Subject: RE: Work on your version

Yes. And I'll try to add in more "math-ness".

From: Chen, Lily (Fed)
Sent: Tuesday, February 05, 2019 8:44 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Work on your version

Hi, Dustin,

Thanks for the corrections and modifications. I am working on the version you sent to me. Then I will send to you to convert it to Latex. Is it okay?

Lily