From:	Chen, Lily (Fed)
To:	Perlner, Ray A. (Fed); Alperin-Sheriff, Jacob (Fed); Moody, Dustin (Fed); internal-pqc
Subject:	RE: About second-round PQC standardization (draft)
Date:	Thursday, January 31, 2019 3:02:48 PM

I think the response is fine.

Lily

From: Perlner, Ray (Fed)
Sent: Thursday, January 31, 2019 9:45 AM
To: Alperin-Sheriff, Jacob (Fed) <jacob.alperin-sheriff@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>; internal-pqc <internal-pqc@nist.gov>
Subject: RE: About second-round PQC standardization (draft)

I like this response

Maybe change “KCL Team” to “Dear KCL Team,” but other than that, this seems good as is.

From: Alperin-Sheriff, Jacob (Fed)
Sent: Thursday, January 31, 2019 9:26 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; internal-pqc <internal-pqc@nist.gov>
Subject: Re: About second-round PQC standardization (draft)

I would strongly suggest that we echo what they’ve said in our response.

KCL Team,

In terms of concrete evaluations of the security and performance of the schemes, NIST utilized a number of sources, including our own performance testing, results reported by the submitters that we made publicly available nearly a year ago on the forum, and the performance testing and security evaluations performed by various third parties, including but not limited to the “Estimate all the {LWE,NTRU} Schemes” of Albrecht et al. https://estimate-all-the-lwe-ntru-schemes.github.io. We were not able to use SUPERCOP [https://bench.cr.yp.to/primitives-kem.html] data in our evaluation of KCL, as it was not submitted to them for evaluation.

As you have alluded to in your email, KCL was indeed extremely similar to several other submissions, and NIST found other extremely similar submissions to be more competitive in implementation quality and in terms of being widely adoptable as a standard. If you have any further questions, please contact us at pqc-comments@nist.gov

---

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Thursday, January 31, 2019 at 8:28 AM
To: pqc-comments <pqc-comments@nist.gov>

Subject: FW: About second-round PQC standardization

We'll need to write up a response for KCL. He is being gracious about it – that's good!

From: 赵运磊 <ylzhao@fudan.edu.cn>
Sent: Thursday, January 31, 2019 12:02 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: About second-round PQC standardization

Dear Dr. Moody:
We just noticed the release of the second-round PQC standardization.
We note that KCL is not in the second round. That is fine, and is not surprised.

We wonder whether there are concrete evaluation report related to KCL, from which we can learn more informatiion about the evaluation and selection.

To be honest, KCL indeed outperforms Newhope and Frodo from a mathematical and technical view. But we guess there might be issues related to patents, and to implementation issues (our implementations of KCL may not be good enough).

In any case, our congratulation for the second-round PQC standardizaiton. We would be much appreciated if we could receive more information about the evaluaiton and selection.

All my best
Yours sincerely
Yunlei

> -----**原始邮件**-----
> **发件人:**"Moody, Dustin (Fed)" <dustin.moody@nist.gov>
> **发送**时间**:**2018-12-11 22:32:55 (**星期二**)
> **收件人:** "赵**运磊**" <ylzhao@fudan.edu.cn>
> **抄送:**
> **主题:** RE: Thanks, and new result on ECC-aided OKCN/AKCN-MLWE-KEM
>
> Yunlei,
> We are not accepting new submissions, which would be what your signature scheme is. So, if KCL makes it to the 2nd round, you are free to describe in your specification that there is an OKCN-base signature, but NIST will not be considering it for standardization, as it was not submitted with all the other digital signature schemes by Nov. 30th of last year.
>
> You can of course update your specification with new analyses, parameter sets, etc. if you make it

to the 2nd round.

Dustin

From: 赵运磊 <ylzhao@fudan.edu.cn>
Sent: Tuesday, December 11, 2018 3:11 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Thanks, and new result on ECC-aided OKCN/AKCN-MLWE-KEM

Dear Dr. Moody:
Thanks sincerely for your kind response and help with the upload of official comment.

In case KCL could move to the second round, we hope we could be allowed to add the OKCN-based signature scheme in our KCL proposal. We suggest it is useful to build both KEM/PKE and signature upon modulue lattice, and moreover, on the same routine of OKCN. This is helpful for simplifying the system complexity of lattice-based crypto.

For MLWE-based KEM schemes based on OKCN and AKCN presented in our KCL proposal, we made some new analysis and have some new recommendations regarding them. Specifically, we note that we can use single error correction (SEC) developed in our proposal to further improve the performance. With our new analysis, we may recommend ECC-aided OKCN/AKCN-MLWE. With ECC-aided AKCN-MLWE as an example, we now recommend to use ECC-aided AKCN-MLWE-PKE-1 listed in our KCL proposal. This way, the bandwidth is reduced from 2272 bytes to 1984 bytes. For this ECC-aided AKCN-MLWE-PKC-1 protocol, its quantum security is at least 147, and the error probability is less than 2^{-147}.

All my best
Sincerely yours
Yunlei

-----**原始**邮**件**-----
发件人:"Moody, Dustin (Fed)" <dustin.moody@nist.gov>
发送时间**:**2018-12-11 03:43:48 (**星期二**)
收件人: "赵**运磊**" <ylzhao@fudan.edu.cn>
抄送:
主题: RE: New applications of OKCN to lattice-based signature, and related official comment

Yunlei,
We did see your official comment – it made it through fine. We have read your paper and will take it into account as we continue to determine the submissions which will move on. The comment will be added shortly.

Dustin

From: 赵运磊 <ylzhao@fudan.edu.cn>
Sent: Saturday, December 08, 2018 6:05 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: New applications of OKCN to lattice-based signature, and related official comment

Dear Dr. Moody:
On 6 Dec, I submitted an official comment on my KCL submission. Please kindly find for the details. Unfortunately, I just noticed that this mail may not correctly reach pqc-comments@nist.gov. Please kindly help check the situation, and also please kindly help update the comment with our KCL submission.

Specifically, recently we generalized and optimized Dilithium (one of the most promissing lattice-based signature proposals to NIST). This is enabled by our OKCN developed for KCL (specifically, the dterminisitc version of OKCN with $e=0$). This further justifies and highlights the desirability and priority of OKCN-KEM (i.e., Diffie-Hellman analog) over AKCN-KEM (i.e., ElGamal analog). In my official comment, I tried to briefly summarize the preferrability of OKCN-KEM over El Gamal KEM.

With our new results on lattice-based signatures, Dilithium is actually outperformed by our OKCN-based signature scheme. It might be remarkable to find that the same routine of OKCN can be used both for KEM/PKE and signature. I may suggest it might deserve your kind attention. For your kind reference, the paper is also attached with this mail.
All my best
Yours sincerely
Yunlei

> -----**原始**邮**件**-----
> **发件人:**"Moody, Dustin (Fed)" <dustin.moody@nist.gov>
> **发送**时间**:**2018-06-14 23:20:24 (**星期四**)
> **收件人:** "赵运磊" <ylzhao@fudan.edu.cn>
> **抄送:**
> **主题:** RE: RE: A Note on key exchange vs. key transport for TLS1.3
>
> Thank you.
>
> **From:** 赵运磊 [mailto:ylzhao@fudan.edu.cn]
> **Sent:** Thursday, June 14, 2018 11:15 AM
> **To:** Moody, Dustin (Fed) <dustin.moody@nist.gov>
> **Subject:** Re: RE: A Note on key exchange vs. key transport for TLS1.3
>
> Dear Dr. Moody:
> Thanks for your information. I suggest it should depend upon the situations:
>
> (1) If both the competitive proposal and our proposal are selected, we are open-minded for merging the proposals to form a joint one. And as we promised, we'll give up patents.

(2) If the competitive proposal (being covered with our patents) is selected while ours is not, we may have to protect us.

Thanks!
All my best
Yunlei

-----**原始**邮**件**-----
发件人:"Moody, Dustin (Fed)" <dustin.moody@nist.gov>
发送时间**:**2018-06-13 21:41:15 (**星期三**)
收件人: "**赵运磊**" <ylzhao@fudan.edu.cn>
抄送:
主题: RE: A Note on key exchange vs. key transport for TLS1.3

Yunlei,
Hello, I hope all is well. We appreciated your response to our question, and wanted to ask a follow up question.

If a submission (not yours) were to be selected for standardization which might be covered by your patent, what would your reaction be? We are just trying to understand the patent situation as best as we can. We understand you might not or may not wish to comment, but we would appreciate anything you can tell us.

Dustin

From: **赵运磊** [mailto:ylzhao@fudan.edu.cn]
Sent: Wednesday, April 18, 2018 8:31 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: A Note on key exchange vs. key transport for TLS1.3

Dear Dr. Moody:
I notice tht, for most KEM proposals to NIST based on lattice (particularly those based on LWE and its variants), they are actually key transport protocols based on asymmetric key consensus (AKC) as defined in our KCL proposal.

Note that key transport has already been abandoned with TLS1.3 (though key transport is still with TLS1.2). If the NIST KEM standards aim for complying with TLS1.3, then key exchange based on key consensus (KC) as defined in our KCL proposal should be more desirable. As explaied in my presentation slides, KC-based corresponds to Diffie-Hellman, while AKC based corresponds to El Gamal.

This is just for your kind reference, as I couldn't well understand the underlying reason why

most lattice-based KEM proposals only concentrate key transport (but not the seemingly more important key exchange protocol).

All my best
Yours sincerely
Yunlei

-----**原始邮件**-----
发件人:"Moody, Dustin (Fed)" <dustin.moody@nist.gov>
发送时间:2018-04-18 21:13:51 (**星期三**)
收件人: "**赵运磊**" <ylzhao@fudan.edu.cn>
抄送:
主题: RE: RE: Re: Presentation slides of KCL Re: DEADLINE TOMORROW - NIST PQC Presentations Due

Yunlei,
Thanks for this. We're trying to understand the patent issues. We wondered if you had any comment on how you see your patents in regards to other submissions.

Dustin

From: **赵运磊** [mailto:ylzhao@fudan.edu.cn]
Sent: Tuesday, April 17, 2018 7:57 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: RE: Re: Presentation slides of KCL Re: DEADLINE TOMORROW - NIST PQC Presentations Due

Dear Dr. Moody:
If needed, I can sign a separate document to promise to give up/abandon all the patents related to KCL if it could be selected as standard. That is, there will be no patent issues related KCL for standardization consideration. I can send such signed statement to NIST, or hand to NIST at a later stage.

All my best
Yours sincerely
Yunlei

-----**原始邮件**-----
发件人:"Moody, Dustin (Fed)" <dustin.moody@nist.gov>
发送时间:2018-04-17 22:28:04 (**星期二**)
收件人: "'**赵运磊**'" <ylzhao@fudan.edu.cn>
抄送:

主题: RE: Re: Presentation slides of KCL Re: DEADLINE TOMORROW - NIST PQC Presentations Due

Yunlei,
One more question. In your statement 2.D.2, we wanted to confirm that you selected the "without compensation" option. Is that correct? Recall the two options were:

1. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination, OR
2. under reasonable terms and conditions that are demonstrably free of any unfair discrimination

Please let me know. Thanks,

Dustin

From: Moody, Dustin (Fed)
Sent: Tuesday, April 17, 2018 8:27 AM
To: '赵运磊' <ylzhao@fudan.edu.cn>
Subject: RE: Re: Presentation slides of KCL Re: DEADLINE TOMORROW - NIST PQC Presentations Due

Yunlei,
This is an acknowledgement that we have received your signed IP statements, and there is nothing missing. Thank you,

Dustin Moody

From: 赵运磊 [mailto:ylzhao@fudan.edu.cn]
Sent: Wednesday, April 11, 2018 11:31 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: Re: Presentation slides of KCL Re: DEADLINE TOMORROW - NIST PQC Presentations Due

Dear Dr. Moody:
Thanks sincerely for understanding and for warm encouragement! It was indeed sad with the incapability in getting VISA in time, and was almost desparate when finding emails being blocked.

I am full of gratitude for all your kind helps, and particularly your support to help showing my presentation vedio at the workshop. I do sincerely hope for having future chances to meet with you to express my great thanks in person.

My best wishes to you for a great PQC Standardization Conference!

All my best
Yours sincerely
Yunlei

-----**原始**邮**件**-----
发件人:"Moody, Dustin (Fed)" <dustin.moody@nist.gov>
发送时间**:**2018-04-11 22:34:27 (**星期三**)
收件人: "**赵运磊**" <ylzhao@fudan.edu.cn>
抄送:
主题: Re: Presentation slides of KCL Re: DEADLINE TOMORROW - NIST PQC Presentations Due

Yunlei,

I am sorry that you were not able to get your VISA and attend the workshop. We hopefully will be able to meet some other time. We should be able to show your presentation that you sent us. Thank you,

Dustin

From: 赵运磊 <ylzhao@fudan.edu.cn>
Sent: Wednesday, April 11, 2018 8:16:34 AM
To: 赵运磊
Cc: Kerman, Sara J. (Fed); Moody, Dustin (Fed); ily.chen@nist.gov
Subject: Presentation slides of KCL Re: DEADLINE TOMORROW - NIST PQC Presentations Due

Dear Dr. Kerman, Dr. Moody and Dr. Chen:
I feel really regretful that I couldn't get my VISA in time. I start applying for US VISA arounding 1st March, and recently the Foreign Affair Department of our university informed me that I couldn't get the VIDA in time. The lesson learnt is that I should start my VISA application as early as possible.

I gave the signed covered letter, the signed statements (2D1,2D2,2D3) to Prof. Yu Yu (who is the author of Lepton and will come to make presentation). Prof. Yu will hand the signed documents to you on site (maybe to Dr.Chen when Dr. Chen after the openning remark of the conference).

Attached please kindly find my presentation files: one is named ``KCL-Audio.mp4" that is the audio file for presentation at the confernece, while the KCL-TextOnly file can be used to be posted on the website.

Sorry for the absense which is a great loss and regret of mine. I would like to express my great gratitude to all of you again for all the great helps and supports! Any further suggestions and instructions please also kindly let me know.

All my best
Yours sincerely
Yunlei

> -----**原始邮件**-----
> **发件人:**"**赵运磊**" <ylzhao@fudan.edu.cn>
> **发送**时间**:**2018-04-11 14:07:05 (**星期三**)
> **收件人:** "Kerman, Sara J. (Fed)" <sara.kerman@nist.gov>
> **抄送:** dustin.moody@nist.gov, ily.chen@nist.gov
> **主题:** Re: DEADLINE TOMORROW - NIST PQC Presentations Due
>
> Dear Dr. Kerman, Dr. Moody and Dr. Chen:
> I feel really regretful that I couldn't get my VISA in time. I start applying for US VISA arounding 1st March, and recently the Foreign Affair Department of our university informed me that I couldn't get the VIDA in time. The lesson learnt is that I should start my VISA application as early as possible.
>
> I gave the signed covered letter, the signed statements (2D1,2D2,2D3) to Prof. Yu Yu (who is the author of Lepton and will come to make presentation). Prof. Yu will hand the signed documents to you on site (maybe to Dr.Chen when Dr. Chen after the openning remark of the conference).
>
> Attached please kindly find my presentation files: one is named ``KCL-Audio.mp4'' that is the audio file for presentation at the confernece, while the KCL-TextOnly file can be used to be posted on the website. As an alternative, you can also download the mp4-file (but not the TextOnly) file via Google drive link:
> https://drive.google.com/open?id=1GkbdDSTImr5q9pj9zVNqjU96nSJXixB5
>
> Sorry for the absense which is a great loss and regret of mine. I would like to express my great gratitude to all of you again for all the great helps and supports! Any further suggestions and instructions please also kindly let me know.
>
> All my best
> Yours sincerely
> Yunlei
>
> > -----**原始邮件**-----
> > **发件人:**"Kerman, Sara J. (Fed)" <sara.kerman@nist.gov>
> > 发送时间**:**2018-04-09 20:52:53 (**星期一**)
> > **收件人:** "ylzhao@fudan.edu.cn" <ylzhao@fudan.edu.cn>
> > **抄送:**
> > **主题:** DEADLINE TOMORROW - NIST PQC Presentations Due

REMINDER – Please submit your NIST PQC Conference presentation by **COB, Tuesday, April 10.** Send to pqc2018@nist.gov

Projector Ratio: 16:9 Widescreen

==========

March 23, 2018

NIST PQC Presenter

We are looking forward to your algorithm presentation at the First PQC Standardization Conference which will be held April 11-13, 2018 at the Pier 66 Hotel and Marina in Fort Lauderdale. The meeting location will be in **The Panorama Ballroom**.

All algorithm presenters will have about 10-15 minutes (including Q&A) for their presentations (please see agenda for your specific time limit). ***We have a very tight program and expect all presenters to adhere to the allotted speaking times provided.*** Please consider the timing when preparing your slides.

Besides summarizing your algorithm, NIST also requests that you address what's special about your algorithm, i.e., what sets it apart from the playing field? What are its advantages (and disadvantages)?

To help maintain the schedule, all presentations will be pre-loaded to a main presentation laptop (if use of your own device is required, please let us know in advance and we can set up a test time during breaks). The laptop will be pre-loaded with

Windows 10

MS 2016 Office (Powerpoint)

Acrobat Reader

Please send your slides to pqc2018@nist.gov by **COB, April 10.**

Unless specifically requested not to, slides (pdf format) will be posted on the NIST PQC Event page ***after*** being presented.

Please let me know if you have any questions.

Sincerely,

Sara Kerman

On behalf of the NIST PQC Standardization team

https://csrc.nist.gov/Events/2018/First-PQC-Standardization-Conference