From: Simon Hoerder <simon@hoerder.net> via pqc-forum@list.nist.gov
To: pqc-forum@list.nist.gov
Subject: [pqc-forum] Round 3 algorithm announcement?
Date: Thursday, June 23, 2022 04:00:39 AM ET

Hi,

I’d like to know when NIST plans to announce its selection of round 3 candidates for standardization. Can NIST say something a little more tangible than “ASAP” on this, please?

Best,
Simon

From: BongHo Kang <bonghokang@gmail.com> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
CC: SH <simon@hoerder.net>
Subject: [pqc-forum] Re: Round 3 algorithm announcement?
Date: Monday, June 27, 2022 10:18:17 PM ET

Thanks Simon for initiating this request.

Hello Dr. Moody and Dr. Chen,
I am also very interested in this topic and would like to know elaborated schedule for selection announcement and standardization.

All the best,
BH.

On Thursday, June 23, 2022 at 5:00:27 PM UTC+9 SH wrote:

> Hi,
>
> I'd like to know when NIST plans to announce its selection of round 3 candidates for standardization. Can NIST say something a little more tangible than "ASAP" on this, please?
>
> Best,
> Simon

--
You received this message because you are subscribed to the Google Groups "pqc-forum" group.
To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.
To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/4be2ba67-fb43-4584-b0d0-f46c55bc7375n%40list.nist.gov.

From: Moody, Dustin (Fed) <dustin.moody@nist.gov> via pqc-forum <pqc-forum@list.nist.gov>
To: BongHo Kang <bonghokang@gmail.com>, pqc-forum <pqc-forum@list.nist.gov>
CC: SH <simon@hoerder.net>
Subject: RE: [pqc-forum] Re: Round 3 algorithm announcement?
Date: Tuesday, June 28, 2022 11:43:02 AM ET

We’ve been asked for an update on where things stand with our announcement.

We know the delay is frustrating, and we are also very eager for it to happen. We want to emphasize that no technical issues are behind the delay in the announcement. There are still some legal and procedural steps being taken care of, and while we remain hopeful that we'll be able to announce very soon, the remaining steps are out of our hands. So, we cannot provide more tangible information on when the announcement will come.

We do have some information we can share. Our next NIST PQC Standardization Conference will be held Nov 29 – Dec 1, 2022. As NIST is not yet welcoming visitors, the conference will be held virtually. We will shortly send out a Call for Papers with more information.

Dustin Moody

NIST PQC team

From: pqc-forum@list.nist.gov <pqc-forum@list.nist.gov> **On Behalf Of** BongHo Kang
Sent: Monday, June 27, 2022 10:18 PM
To: pqc-forum <pqc-forum@list.nist.gov>
Cc: SH <simon@hoerder.net>
Subject: [pqc-forum] Re: Round 3 algorithm announcement?

Thanks Simon for initiating this request.

Hello Dr. Moody and Dr. Chen,
I am also very interested in this topic and would like to know elaborated schedule for selection announcement and standardization.

All the best,
BH.

On Thursday, June 23, 2022 at 5:00:27 PM UTC+9 SH wrote:

> Hi,
>
> I’d like to know when NIST plans to announce its selection of round 3 candidates for standardization. Can NIST say something a little more tangible than “ASAP” on this, please?
>
> Best,
> Simon

From: William Whyte <wwhyte@qti.qualcomm.com> via pqc-forum@list.nist.gov
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>, BongHo Kang <bonghokang@gmail.com>, pqc-forum <pqc-forum@list.nist.gov>
CC: SH <simon@hoerder.net>
Subject: RE: [pqc-forum] Re: Round 3 algorithm announcement?
Date: Tuesday, June 28, 2022 11:51:57 AM ET

Hi Dustin – without revealing the selections, would you be able to provide some specifics about the criteria you used to make the decision? There've been concerns expressed about how the rationales as described in the previous report seemed not to be 100% consistent between candidate algorithms. If you can provide more information on the criteria that would help the audience to understand and agree with the final decision when it's released.

(Obviously revealing the criteria implies the decision, but this can't be helped – if the most desirable candidate by the technical criteria can't be legally cleared, so be it).

Cheers,

William

From: 'Moody, Dustin (Fed)' via pqc-forum <pqc-forum@list.nist.gov>
Sent: Tuesday, June 28, 2022 5:43 PM
To: BongHo Kang <bonghokang@gmail.com>; pqc-forum <pqc-forum@list.nist.gov>
Cc: SH <simon@hoerder.net>
Subject: RE: [pqc-forum] Re: Round 3 algorithm announcement?

WARNING: This email originated from outside of Qualcomm. Please be wary of any links or attachments, and do not enable macros.

We've been asked for an update on where things stand with our announcement.

We know the delay is frustrating, and we are also very eager for it to happen. We want to emphasize that no technical issues are behind the delay in the announcement. There are still some legal and procedural steps being taken care of, and while we remain hopeful that we'll be able to announce very soon, the remaining steps are out of our hands. So, we cannot provide more tangible information on when the announcement will come.

We do have some information we can share. Our next NIST PQC Standardization Conference will be held Nov 29 – Dec 1, 2022. As NIST is not yet welcoming visitors, the conference will be held virtually. We will shortly send out a Call for Papers with more information.

Dustin Moody

NIST PQC team

From:pqc-forum@list.nist.gov <pqc-forum@list.nist.gov> **On Behalf Of** BongHo Kang
Sent: Monday, June 27, 2022 10:18 PM
To: pqc-forum <pqc-forum@list.nist.gov>
Cc: SH <simon@hoerder.net>
Subject: [pqc-forum] Re: Round 3 algorithm announcement?

Thanks Simon for initiating this request.

Hello Dr. Moody and Dr. Chen,
I am also very interested in this topic and would like to know elaborated schedule for selection announcement and standardization.

All the best,
BH.

On Thursday, June 23, 2022 at 5:00:27 PM UTC+9 SH wrote:

> Hi,
>
> I'd like to know when NIST plans to announce its selection of round 3 candidates for standardization. Can NIST say something a little more tangible than "ASAP" on this, please?
>
> Best,
> Simon

--
You received this message because you are subscribed to the Google Groups "pqc-forum" group.
To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.

To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/4be2ba67-fb43-4584-b0d0-f46c55bc7375n%40list.nist.gov.

--

From: Moody, Dustin (Fed) <dustin.moody@nist.gov> via pqc-forum <pqc-forum@list.nist.gov>
To: William Whyte <wwhyte@qti.qualcomm.com>, pqc-forum <pqc-forum@list.nist.gov>
Subject: RE: [pqc-forum] Re: Round 3 algorithm announcement?
Date: Tuesday, June 28, 2022 12:40:57 PM ET

William,

We published the selection criteria in our Call for Proposals:

https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf

In particular, see section 4.

Dustin

From: William Whyte <wwhyte@qti.qualcomm.com>
Sent: Tuesday, June 28, 2022 11:52 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; BongHo Kang <bonghokang@gmail.com>; pqc-forum <pqc-forum@list.nist.gov>
Cc: SH <simon@hoerder.net>
Subject: RE: [pqc-forum] Re: Round 3 algorithm announcement?

Hi Dustin – without revealing the selections, would you be able to provide some specifics about the criteria you used to make the decision? There've been concerns expressed about how the rationales as described in the previous report seemed not to be 100% consistent between candidate algorithms. If you can provide more information on the criteria that would help the audience to understand and agree with the final decision when it's released.

(Obviously revealing the criteria implies the decision, but this can't be helped – if the most desirable candidate by the technical criteria can't be legally cleared, so be it).

Cheers,

William

From: 'Moody, Dustin (Fed)' via pqc-forum <pqc-forum@list.nist.gov>
Sent: Tuesday, June 28, 2022 5:43 PM
To: BongHo Kang <bonghokang@gmail.com>; pqc-forum <pqc-forum@list.nist.gov>

Cc: SH <simon@hoerder.net>
Subject: RE: [pqc-forum] Re: Round 3 algorithm announcement?

WARNING: This email originated from outside of Qualcomm. Please be wary of any links or attachments, and do not enable macros.

We’ve been asked for an update on where things stand with our announcement.

We know the delay is frustrating, and we are also very eager for it to happen. We want to emphasize that no technical issues are behind the delay in the announcement. There are still some legal and procedural steps being taken care of, and while we remain hopeful that we'll be able to announce very soon, the remaining steps are out of our hands. So, we cannot provide more tangible information on when the announcement will come.

We do have some information we can share. Our next NIST PQC Standardization Conference will be held Nov 29 – Dec 1, 2022. As NIST is not yet welcoming visitors, the conference will be held virtually. We will shortly send out a Call for Papers with more information.

Dustin Moody

NIST PQC team

From:pqc-forum@list.nist.gov <pqc-forum@list.nist.gov> **On Behalf Of** BongHo Kang
Sent: Monday, June 27, 2022 10:18 PM
To: pqc-forum <pqc-forum@list.nist.gov>
Cc: SH <simon@hoerder.net>
Subject: [pqc-forum] Re: Round 3 algorithm announcement?

Thanks Simon for initiating this request.

Hello Dr. Moody and Dr. Chen,
I am also very interested in this topic and would like to know elaborated schedule for selection announcement and standardization.

All the best,
BH.

On Thursday, June 23, 2022 at 5:00:27 PM UTC+9 SH wrote:

> Hi,
>
> I'd like to know when NIST plans to announce its selection of round 3 candidates for standardization. Can NIST say something a little more tangible than "ASAP" on this, please?
>
> Best,
> Simon

--
You received this message because you are subscribed to the Google Groups "pqc-forum" group.
To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.
To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/4be2ba67-fb43-4584-b0d0-f46c55bc7375n%40list.nist.gov.

--
You received this message because you are subscribed to the Google Groups "pqc-forum" group.
To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.
To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/SA1PR09MB866935423A7040E49AC13C88E5B89%40SA1PR09MB8669.namprd09.prod.outlook.com.

From: William Whyte <wwhyte@qti.qualcomm.com> via pqc-forum@list.nist.gov
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>, pqc-forum <pqc-forum@list.nist.gov>
Subject: RE: [pqc-forum] Re: Round 3 algorithm announcement?
Date: Tuesday, June 28, 2022 12:45:39 PM ET

I think the discussion since then has pointed out various places where those are incomplete, e.g. around the existence of proofs that apply to the actual parameters used, around memory access costs, etc. Can you provide more specificity on those?

Cheers,

William

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Tuesday, June 28, 2022 6:41 PM
To: William Whyte <wwhyte@qti.qualcomm.com>; pqc-forum <pqc-forum@list.nist.gov>
Subject: RE: [pqc-forum] Re: Round 3 algorithm announcement?

WARNING: This email originated from outside of Qualcomm. Please be wary of any links or attachments, and do not enable macros.

William,

We published the selection criteria in our Call for Proposals:

https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf

In particular, see section 4.

Dustin

From: William Whyte <wwhyte@qti.qualcomm.com>
Sent: Tuesday, June 28, 2022 11:52 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; BongHo Kang <bonghokang@gmail.com>; pqc-forum <pqc-forum@list.nist.gov>
Cc: SH <simon@hoerder.net>
Subject: RE: [pqc-forum] Re: Round 3 algorithm announcement?

Hi Dustin – without revealing the selections, would you be able to provide some specifics about the criteria you used to make the decision? There've been concerns expressed about how the rationales as described in the previous report seemed not to be 100% consistent between candidate algorithms. If you can provide more information on the criteria that would help the audience to understand and agree with the final decision when it's released.

(Obviously revealing the criteria implies the decision, but this can't be helped – if the most desirable candidate by the technical criteria can't be legally cleared, so be it).

Cheers,

William

From: 'Moody, Dustin (Fed)' via pqc-forum <pqc-forum@list.nist.gov>
Sent: Tuesday, June 28, 2022 5:43 PM
To: BongHo Kang <bonghokang@gmail.com>; pqc-forum <pqc-forum@list.nist.gov>
Cc: SH <simon@hoerder.net>
Subject: RE: [pqc-forum] Re: Round 3 algorithm announcement?

WARNING: This email originated from outside of Qualcomm. Please be wary of any links or attachments, and do not enable macros.

We've been asked for an update on where things stand with our announcement.

We know the delay is frustrating, and we are also very eager for it to happen. We want to emphasize that no technical issues are behind the delay in the announcement. There are still some legal and procedural steps being taken care of, and while we remain hopeful that we'll be able to announce very soon, the remaining steps are out of our hands. So, we cannot provide more tangible information on when the announcement will come.

We do have some information we can share. Our next NIST PQC Standardization Conference will be held Nov 29 – Dec 1, 2022. As NIST is not yet welcoming visitors, the conference will be held virtually. We will shortly send out a Call for Papers with more information.

Dustin Moody

NIST PQC team

From:pqc-forum@list.nist.gov <pqc-forum@list.nist.gov> **On Behalf Of** BongHo Kang
Sent: Monday, June 27, 2022 10:18 PM
To: pqc-forum <pqc-forum@list.nist.gov>

Cc: SH <simon@hoerder.net>
Subject: [pqc-forum] Re: Round 3 algorithm announcement?

Thanks Simon for initiating this request.

Hello Dr. Moody and Dr. Chen,
I am also very interested in this topic and would like to know elaborated schedule for selection announcement and standardization.

All the best,
BH.

On Thursday, June 23, 2022 at 5:00:27 PM UTC+9 SH wrote:

> Hi,
>
> I'd like to know when NIST plans to announce its selection of round 3 candidates for standardization. Can NIST say something a little more tangible than "ASAP" on this, please?
>
> Best,
> Simon

--
You received this message because you are subscribed to the Google Groups "pqc-forum" group.
To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.
To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/4be2ba67-fb43-4584-b0d0-f46c55bc7375n%40list.nist.gov.

--
You received this message because you are subscribed to the Google Groups "pqc-forum" group.
To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.
To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/SA1PR09MB866935423A7040E49AC13C88E5B89%40SA1PR09MB8669.namprd09.prod.outlook.com.

From: Simon Hoerder <simon@hoerder.net> via pqc-forum@list.nist.gov
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
CC: pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] Re: Round 3 algorithm announcement?
Date: Wednesday, June 29, 2022 08:56:42 AM ET

Hi,
Thanks for the reply. It's not quite what I was hoping for but at least it does clarify that the cause for the delay hasn't changed.

Best,

Simon

> On 28 Jun 2022, at 17:42, 'Moody, Dustin (Fed)' via pqc-forum <pqc-forum@list.nist.gov> wrote:
>
> We've been asked for an update on where things stand with our announcement.
>
> We know the delay is frustrating, and we are also very eager for it to happen. We want to emphasize that no technical issues are behind the delay in the announcement. There are still some legal and procedural steps being taken care of, and while we remain hopeful that we'll be able to announce very soon, the remaining steps are out of our hands. So, we cannot provide more tangible information on when the announcement will come.
>
> We do have some information we can share. Our next NIST PQC Standardization Conference will be held Nov 29 – Dec 1, 2022. As NIST is not yet welcoming visitors, the conference will be held virtually. We will shortly send out a Call for Papers with more information.
>
> Dustin Moody
>
> NIST PQC team
>
> **From:** pqc-forum@list.nist.gov <pqc-forum@list.nist.gov> **On Behalf Of** BongHo Kang

Sent: Monday, June 27, 2022 10:18 PM
To: pqc-forum <pqc-forum@list.nist.gov>
Cc: SH <simon@hoerder.net>
Subject: [pqc-forum] Re: Round 3 algorithm announcement?

Thanks Simon for initiating this request.

Hello Dr. Moody and Dr. Chen,
I am also very interested in this topic and would like to know elaborated schedule for selection announcement and standardization.

All the best,
BH.

On Thursday, June 23, 2022 at 5:00:27 PM UTC+9 SH wrote:

> Hi,
>
> I’d like to know when NIST plans to announce its selection of round 3 candidates for standardization. Can NIST say something a little more tangible than “ASAP” on this, please?
>
> Best,
> Simon

--
You received this message because you are subscribed to the Google Groups "pqc-forum" group.
To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.
To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/4be2ba67-fb43-4584-b0d0-f46c55bc7375n%40list.nist.gov.

--
You received this message because you are subscribed to the Google Groups "pqc-forum" group.
To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.
To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/

msgid/pqc-forum/SA1PR09MB866935423A7040E49AC13C88E5B89%40SA1PR09MB8669.namprd09.prod.outlook.com.

From: andy yi <hy8196695@gmail.com> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
CC: SH <simon@hoerder.net>, pqc-forum <pqc-forum@list.nist.gov>, dustin...@nist.gov <dustin.moody@nist.gov>
Subject: Re: [pqc-forum] Re: Round 3 algorithm announcement?
Date: Wednesday, June 29, 2022 08:42:41 PM ET

I have been paying close attention to the progress of this matter, and I found that the selection results may have risen to the national strategy, so a series of strategic layouts need to be carried out, such as:
The G7 will also commit to new cooperation to deploy quantum resistant cryptography with the goal of ensuring secure interoperability between ICT systems and fostering growth in the digital economy.
source:
https://www.consilium.europa.eu/en/press/press-releases/2022/06/28/g7-leaders-communique/

https://www.whitehouse.gov/briefing-room/statements-releases/2022/06/28/fact-sheet-the-united-states-continues-to-strengthen-cooperation-with-g7-on-21st-century-challenges-including-those-posed-by-the-peoples-republic-of-china-prc/

在2022年6月29日星期三 UTC+8 20:56:37<SH> 写道：

> Hi,
> Thanks for the reply. It’s not quite what I was hoping for but at least it does clarify that the cause for the delay hasn’t changed.
>
> Best,
>
> Simon
>
> > On 28 Jun 2022, at 17:42, 'Moody, Dustin (Fed)' via pqc-forum <pqc-...@list.nist.gov> wrote:
> >
> > We’ve been asked for an update on where things stand with our announcement.

> We know the delay is frustrating, and we are also very eager for it to happen. We want to emphasize that no technical issues are behind the delay in the announcement. There are still some legal and procedural steps being taken care of, and while we remain hopeful that we'll be able to announce very soon, the remaining steps are out of our hands. So, we cannot provide more tangible information on when the announcement will come.
>
> We do have some information we can share. Our next NIST PQC Standardization Conference will be held Nov 29 – Dec 1, 2022. As NIST is not yet welcoming visitors, the conference will be held virtually. We will shortly send out a Call for Papers with more information.
>
> Dustin Moody
>
> NIST PQC team
>
> ---
>
> **From:**pqc-...@list.nist.gov <pqc-...@list.nist.gov> **On Behalf Of** BongHo Kang
> **Sent:** Monday, June 27, 2022 10:18 PM
> **To:** pqc-forum <pqc-...@list.nist.gov>
> **Cc:** SH <si...@hoerder.net>
> **Subject:** [pqc-forum] Re: Round 3 algorithm announcement?
>
> Thanks Simon for initiating this request.
>
> Hello Dr. Moody and Dr. Chen,
> I am also very interested in this topic and would like to know elaborated schedule for selection announcement and standardization.
>
> All the best,
> BH.
>
> On Thursday, June 23, 2022 at 5:00:27 PM UTC+9 SH wrote:
>
>> Hi,
>>
>> I'd like to know when NIST plans to announce its selection of round 3 candidates for standardization. Can NIST say something a little more tangible than "ASAP" on this, please?

> > Best,
> > Simon
>
> --
> You received this message because you are subscribed to the Google Groups "pqc-forum" group.
> To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+...@list.nist.gov.
> To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/4be2ba67-fb43-4584-b0d0-f46c55bc7375n%40list.nist.gov.
>
> --
> You received this message because you are subscribed to the Google Groups "pqc-forum" group.
> To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+...@list.nist.gov.
>
> To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/SA1PR09MB866935423A7040E49AC13C88E5B89%40SA1PR09MB8669.namprd09.prod.outlook.com.

--
You received this message because you are subscribed to the Google Groups "pqc-forum" group.
To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.
To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/17f1b973-f087-447e-9665-47c6031f0cb8n%40list.nist.gov.

From: Moody, Dustin (Fed) <dustin.moody@nist.gov> via pqc-forum <pqc-forum@list.nist.gov>
To: Simon Hoerder <simon@hoerder.net>
CC: pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] Re: Round 3 algorithm announcement?
Date: Friday, July 01, 2022 05:18:37 PM ET

Good news finally!

Things have been falling into place, and we are getting ready to make the announcement. We plan on making it on Tuesday, July 5th. Watch for a pqc-forum post, in addition to some press releases that NIST will put out. The announcement will specify which algorithms we plan to standardize, along with which algorithms will move into the 4th round for further analysis. We will also publish our report which explains the rationale behind our decisions.

Thanks for everybody's patience.

Dustin Moody

NIST PQC team

From: Simon Hoerder <simon@hoerder.net>
Sent: Wednesday, June 29, 2022 8:56 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Cc: pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] Re: Round 3 algorithm announcement?

Hi,
Thanks for the reply. It’s not quite what I was hoping for but at least it does clarify that the cause for the delay hasn’t changed.

Best,

Simon

> On 28 Jun 2022, at 17:42, 'Moody, Dustin (Fed)' via pqc-forum <pqc-forum@list.nist.gov> wrote:

We’ve been asked for an update on where things stand with our announcement.
We know the delay is frustrating, and we are also very eager for it to happen. We want to emphasize that no technical issues are behind the delay in the announcement. There are still some legal and procedural steps being taken care of, and while we remain hopeful that we'll be able to announce very soon, the remaining steps are out of our hands. So, we cannot provide more tangible information on when the announcement will come.
We do have some information we can share. Our next NIST PQC Standardization Conference will be held Nov 29 – Dec 1, 2022. As NIST is not yet welcoming visitors, the conference will be held virtually. We will shortly send out a Call for Papers with more information.
Dustin Moody
NIST PQC team

From: pqc-forum@list.nist.gov <pqc-forum@list.nist.gov> **On Behalf Of** BongHo Kang
Sent: Monday, June 27, 2022 10:18 PM
To: pqc-forum <pqc-forum@list.nist.gov>
Cc: SH <simon@hoerder.net>
Subject: [pqc-forum] Re: Round 3 algorithm announcement?
Thanks Simon for initiating this request.

Hello Dr. Moody and Dr. Chen,
I am also very interested in this topic and would like to know elaborated schedule for selection announcement and standardization.
All the best,
BH.
On Thursday, June 23, 2022 at 5:00:27 PM UTC+9 SH wrote:

> Hi,
>
> I’d like to know when NIST plans to announce its selection of round 3 candidates for standardization. Can NIST say something a little more tangible than “ASAP” on this, please?
>
> Best,
> Simon

--
You received this message because you are subscribed to the Google Groups "pqc-forum" group.
To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.

From: John Mattsson <john.mattsson@ericsson.com> via pqc-forum <pqc-forum@list.nist.gov>
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>, Simon Hoerder <simon@hoerder.net>
CC: pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] Re: Round 3 algorithm announcement?
Date: Saturday, July 02, 2022 07:39:55 AM ET

Great news!

Thanks for all the hard work from the NIST PQC team!

- I assume that the broad timeline given in the PKC 2022 presentation is still accurate.

https://csrc.nist.gov/csrc/media/Presentations/2022/the-beginning-of-the-end-the-first-nist-pqc-standa/images-media/pkc2022-march2022-moody.pdf

- Is NIST planning to make any official statements on the security of symmetric cryptography against quantum computers and maybe formalize the 5 security levels defined in the PQC call for proposals? I think it would be good if NIST included this in some publication. People still seem unreasonably worried about Grover's algorithm. Using the reasonable NIST assumption of 2^40 serial logical quantum gates per year any practical attack on AES-128 becomes completely ridiculous like one million years of uninterrupted computation by one billion CRQCs to find a single AES-128 key [1].

- I saw that NIST cited [2]. It's great that there is a survey, but my understanding is that all the experts in that survey are personally working on quantum computing. My personal experience is that researchers personally involved in quantum computing are MUCH more optimistic (especially researchers associated with a company) than prominent researchers specializing in other fields on research. It might of course be that researcher working on quantum computing make correct estimates, but history has shown that researchers are often too optimistic on when their research will have commercial implications. For the last 70 years, fusion researchers have estimated that commercial fusion power is 20 years away. I think the consensus study report [3] from the US National Academies of Sciences, Engineering, and Medicine was very good. The talk by Professor Scott Aronsson [4] is also very good with conclusions like "claims about near-term quantum speedups are >95% BS".

[1] https://arxiv.org/ftp/arxiv/papers/2112/2112.00399.pdf

[2] https://globalriskinstitute.org/publications/2021-quantum-threat-timeline-report/

[3] https://nap.nationalacademies.org/read/25196/

[4] https://www.youtube.com/watch?v=QnLmGfNKCLU&t=2710s

Cheers,

John Preuß Mattsson

From: 'Moody, Dustin (Fed)' via pqc-forum <pqc-forum@list.nist.gov>
Date: Friday, 1 July 2022 at 23:18
To: Simon Hoerder <simon@hoerder.net>
Cc: pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] Re: Round 3 algorithm announcement?

Good news finally!

Things have been falling into place, and we are getting ready to make the announcement. We plan on making it on Tuesday, July 5th. Watch for a pqc-forum post, in addition to some press releases that NIST will put out. The announcement will specify which algorithms we plan to standardize, along with which algorithms will move into the 4th round for further analysis. We will also publish our report which explains the rationale behind our decisions.

Thanks for everybody's patience.

Dustin Moody

NIST PQC team

From: Simon Hoerder <simon@hoerder.net>
Sent: Wednesday, June 29, 2022 8:56 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Cc: pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] Re: Round 3 algorithm announcement?

Hi,

Thanks for the reply. It’s not quite what I was hoping for but at least it does clarify that the cause for the delay hasn’t changed.

Best,

Simon

On 28 Jun 2022, at 17:42, 'Moody, Dustin (Fed)' via pqc-forum <pqc-forum@list.nist.gov> wrote:

We’ve been asked for an update on where things stand with our announcement.

We know the delay is frustrating, and we are also very eager for it to happen. We want to emphasize that no technical issues are behind the delay in the announcement. There are still some legal and procedural steps being taken care of, and while we remain hopeful that we'll be able to announce very soon, the remaining steps are out of our hands. So, we cannot provide more tangible information on when the announcement will come.

We do have some information we can share. Our next NIST PQC Standardization Conference will be held Nov 29 – Dec 1, 2022. As NIST is not yet welcoming visitors, the conference will be held virtually. We will shortly send out a Call for Papers with more information.

Dustin Moody

NIST PQC team

From: pqc-forum@list.nist.gov <pqc-forum@list.nist.gov> **On Behalf Of** BongHo Kang
Sent: Monday, June 27, 2022 10:18 PM
To: pqc-forum <pqc-forum@list.nist.gov>
Cc: SH <simon@hoerder.net>
Subject: [pqc-forum] Re: Round 3 algorithm announcement?

Thanks Simon for initiating this request.

Hello Dr. Moody and Dr. Chen,
I am also very interested in this topic and would like to know elaborated schedule for selection announcement and standardization.

All the best,
BH.

On Thursday, June 23, 2022 at 5:00:27 PM UTC+9 SH wrote:

> > Hi,
> >
> > I’d like to know when NIST plans to announce its selection of round 3 candidates for standardization. Can NIST say something a little more tangible than “ASAP” on this, please?
> >
> > Best,
> > Simon
>
> --
> You received this message because you are subscribed to the Google Groups "pqc-forum" group.
> To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.
> To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/4be2ba67-fb43-4584-b0d0-f46c55bc7375n%40list.nist.gov.
>
> --
> You received this message because you are subscribed to the Google Groups "pqc-forum" group.
> To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.
> To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/SA1PR09MB866935423A7040E49AC13C88E5B89%40SA1PR09MB8669.namprd09.prod.outlook.com.

--
You received this message because you are subscribed to the Google Groups "pqc-forum" group.
To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.
To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/SA1PR09MB8669090C4E11F63DA6C0A5F5E5BD9%40SA1PR09MB8669.namprd09.prod.outlook.com.

From: Simon Hoerder <simon@hoerder.net> via pqc-forum@list.nist.gov
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
CC: pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] Re: Round 3 algorithm announcement?
Date: Monday, July 04, 2022 03:58:50 AM ET

Hi Dustin,
that is excellent news indeed! Thanks for the good work.

Looking forward to tomorrow,

Simon

Sent from my iPhone

> On 1 Jul 2022, at 23:18, Moody, Dustin (Fed) <dustin.moody@nist.gov> wrote:
>
> Good news finally!
>
> Things have been falling into place, and we are getting ready to make the announcement. We plan on making it on Tuesday, July 5th. Watch for a pqc-forum post, in addition to some press releases that NIST will put out. The announcement will specify which algorithms we plan to standardize, along with which algorithms will move into the 4th round for further analysis. We will also publish our report which explains the rationale behind our decisions.
>
> Thanks for everybody's patience.
>
> Dustin Moody
>
> NIST PQC team
>
> ---
>
> **From:** Simon Hoerder <simon@hoerder.net>
> **Sent:** Wednesday, June 29, 2022 8:56 AM
> **To:** Moody, Dustin (Fed) <dustin.moody@nist.gov>

Cc: pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] Re: Round 3 algorithm announcement?

Hi,
Thanks for the reply. It's not quite what I was hoping for but at least it does clarify that the cause for the delay hasn't changed.

Best,

Simon

> On 28 Jun 2022, at 17:42, 'Moody, Dustin (Fed)' via pqc-forum <pqc-forum@list.nist.gov> wrote:
>
> We've been asked for an update on where things stand with our announcement.
> We know the delay is frustrating, and we are also very eager for it to happen. We want to emphasize that no technical issues are behind the delay in the announcement. There are still some legal and procedural steps being taken care of, and while we remain hopeful that we'll be able to announce very soon, the remaining steps are out of our hands. So, we cannot provide more tangible information on when the announcement will come.
> We do have some information we can share. Our next NIST PQC Standardization Conference will be held Nov 29 – Dec 1, 2022. As NIST is not yet welcoming visitors, the conference will be held virtually. We will shortly send out a Call for Papers with more information.
> Dustin Moody
> NIST PQC team
>
> **From:** pqc-forum@list.nist.gov <pqc-forum@list.nist.gov> **On Behalf Of** BongHo Kang
> **Sent:** Monday, June 27, 2022 10:18 PM
> **To:** pqc-forum <pqc-forum@list.nist.gov>
> **Cc:** SH <simon@hoerder.net>
> **Subject:** [pqc-forum] Re: Round 3 algorithm announcement?
> Thanks Simon for initiating this request.
>
> Hello Dr. Moody and Dr. Chen,

I am also very interested in this topic and would like to know elaborated schedule for selection announcement and standardization.
All the best,
BH.
On Thursday, June 23, 2022 at 5:00:27 PM UTC+9 SH wrote:

> Hi,
>
> I'd like to know when NIST plans to announce its selection of round 3 candidates for standardization. Can NIST say something a little more tangible than "ASAP" on this, please?
>
> Best,
> Simon

--
You received this message because you are subscribed to the Google Groups "pqc-forum" group.
To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.
To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/4be2ba67-fb43-4584-b0d0-f46c55bc7375n%40list.nist.gov.
--
You received this message because you are subscribed to the Google Groups "pqc-forum" group.
To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.
To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/SA1PR09MB866935423A7040E49AC13C88E5B89%40SA1PR09MB8669.namprd09.prod.outlook.com.

From: Moody, Dustin (Fed) <dustin.moody@nist.gov> via pqc-forum <pqc-forum@list.nist.gov>
To: John Mattsson <john.mattsson@ericsson.com>
CC: pqc-forum <pqc-forum@list.nist.gov>
Subject: RE: [pqc-forum] Re: Round 3 algorithm announcement?
Date: Thursday, July 07, 2022 01:45:05 PM ET

John,

Thank you.

Yes, we expect that our overall project timeline is accurate. That is, we are aiming to complete the initial PQC standards by around 2024.

The FAQ still gives an accurate view of what NIST thinks in regard to the impact of quantum computers on AES.

Note the last paragraph: "Based on such understanding, current applications can continue to use AES with key sizes 128, 192, or 256 bits. NIST will issue guidance regarding any transitions of symmetric key algorithms and hash functions to protect against threats from quantum computers when we can foresee a transition need. Until then, users should follow the recommendations and guidelines NIST has already issued. In particular, anything with less than 112 bits of classical security should not be used."

Dustin

From: John Mattsson <john.mattsson@ericsson.com>
Sent: Saturday, July 2, 2022 7:39 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Simon Hoerder <simon@hoerder.net>
Cc: pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] Re: Round 3 algorithm announcement?

Great news!

Thanks for all the hard work from the NIST PQC team!

- I assume that the broad timeline given in the PKC 2022 presentation is still accurate.

https://csrc.nist.gov/csrc/media/Presentations/2022/the-beginning-of-the-end-the-first-nist-pqc-standa/images-media/pkc2022-march2022-moody.pdf

- Is NIST planning to make any official statements on the security of symmetric cryptography against quantum computers and maybe formalize the 5 security levels defined in the PQC call for proposals? I think it would be good if NIST included this in some publication. People still seem unreasonably worried about Grover's algorithm. Using the reasonable NIST assumption of 2^40 serial logical quantum gates per year any practical attack on AES-128 becomes completely ridiculous like one million years of uninterrupted computation by one billion CRQCs to find a single AES-128 key [1].

- I saw that NIST cited [2]. It's great that there is a survey, but my understanding is that all the experts in that survey are personally working on quantum computing. My personal experience is that researchers personally involved in quantum computing are MUCH more optimistic (especially researchers associated with a company) than prominent researchers specializing in other fields on research. It might of course be that researcher working on quantum computing make correct estimates, but history has shown that researchers are often too optimistic on when their research will have commercial implications. For the last 70 years, fusion researchers have estimated that commercial fusion power is 20 years away. I think the consensus study report [3] from the US National Academies of Sciences, Engineering, and Medicine was very good. The talk by Professor Scott Aronsson [4] is also very good with conclusions like "claims about near-term quantum speedups are >95% BS".

[1] https://arxiv.org/ftp/arxiv/papers/2112/2112.00399.pdf

[2] https://globalriskinstitute.org/publications/2021-quantum-threat-timeline-report/

[3] https://nap.nationalacademies.org/read/25196/

[4] https://www.youtube.com/watch?v=QnLmGfNKCLU&t=2710s

Cheers,

John Preuß Mattsson

From: 'Moody, Dustin (Fed)' via pqc-forum <pqc-forum@list.nist.gov>
Date: Friday, 1 July 2022 at 23:18
To: Simon Hoerder <simon@hoerder.net>
Cc: pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] Re: Round 3 algorithm announcement?

Good news finally!

Things have been falling into place, and we are getting ready to make the announcement. We plan on making it on Tuesday, July 5th. Watch for a pqc-forum post, in addition to some press releases that NIST will put out. The announcement will specify which algorithms we plan to standardize, along with which algorithms will move into the 4th round for further analysis. We will also publish our report which explains the rationale behind our decisions.

Thanks for everybody's patience.

Dustin Moody

NIST PQC team

From: Simon Hoerder <simon@hoerder.net>
Sent: Wednesday, June 29, 2022 8:56 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Cc: pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] Re: Round 3 algorithm announcement?

Hi,

Thanks for the reply. It’s not quite what I was hoping for but at least it does clarify that the cause for the delay hasn’t changed.

Best,

Simon

> On 28 Jun 2022, at 17:42, 'Moody, Dustin (Fed)' via pqc-forum <pqc-forum@list.nist.gov> wrote:
>
> We’ve been asked for an update on where things stand with our announcement.
>
> We know the delay is frustrating, and we are also very eager for it to happen. We want to emphasize that no technical issues are behind the delay in the announcement. There are still some legal and procedural steps being taken care of, and while we remain hopeful that we'll be able to announce very soon, the remaining steps are out of our hands. So, we cannot provide more tangible information on when the announcement will come.

We do have some information we can share. Our next NIST PQC Standardization Conference will be held Nov 29 – Dec 1, 2022. As NIST is not yet welcoming visitors, the conference will be held virtually. We will shortly send out a Call for Papers with more information.

Dustin Moody

NIST PQC team

From:pqc-forum@list.nist.gov <pqc-forum@list.nist.gov> **On Behalf Of** BongHo Kang
Sent: Monday, June 27, 2022 10:18 PM
To: pqc-forum <pqc-forum@list.nist.gov>
Cc: SH <simon@hoerder.net>
Subject: [pqc-forum] Re: Round 3 algorithm announcement?

Thanks Simon for initiating this request.

Hello Dr. Moody and Dr. Chen,
I am also very interested in this topic and would like to know elaborated schedule for selection announcement and standardization.

All the best,
BH.

On Thursday, June 23, 2022 at 5:00:27 PM UTC+9 SH wrote:

> Hi,
>
> I'd like to know when NIST plans to announce its selection of round 3 candidates for standardization. Can NIST say something a little more tangible than "ASAP" on this, please?
>
> Best,
> Simon

--
You received this message because you are subscribed to the Google Groups "pqc-forum" group.

> To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.
> To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/4be2ba67-fb43-4584-b0d0-f46c55bc7375n%40list.nist.gov.
>
> --
> You received this message because you are subscribed to the Google Groups "pqc-forum" group.
> To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.
> To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/SA1PR09MB866935423A7040E49AC13C88E5B89%40SA1PR09MB8669.namprd09.prod.outlook.com.

--
You received this message because you are subscribed to the Google Groups "pqc-forum" group.
To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.
To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/SA1PR09MB8669090C4E11F63DA6C0A5F5E5BD9%40SA1PR09MB8669.namprd09.prod.outlook.com.