From: Moody, Dustin (Fed) <dustin.moody@nist.gov> via pqc-forum <pqc-forum@list.nist.gov>
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: [pqc-forum] Call for Additional Signatures is released
Date: Tuesday, September 06, 2022 04:16:06 PM ET

All,

NIST is calling for additional digital signature proposals to be considered in the PQC standardization process. NIST is primarily interested in additional general-purpose signature schemes that are not based on structured lattices. For certain applications, such as certificate transparency, NIST may also be interested in signature schemes that have short signatures and fast verification. NIST is open to receiving additional submissions based on structured lattices, but is intent on diversifying the post-quantum signature standards. As such, any structured lattice-based signature proposal would need to significantly outperform CRYSTALS-Dilithium and FALCON in relevant applications and/or ensure substantial additional security properties to be considered for standardization.

You can find the Call, as well as instructions and requirements for submissions at:

https://csrc.nist.gov/projects/pqc-dig-sig/standardization/call-for-proposals

Submission packages must be received by NIST by June 1, 2023. Submission packages received before March 1, 2023, will be reviewed for completeness by NIST; the submitters will be notified of any deficiencies by March 31, 2023, allowing time for deficient packages to be amended by the submission deadline. No amendments to packages will be permitted after the submission deadline, except at specified times during the evaluation phase.

Please let us know if you have any questions.

Dustin Moody

NIST PQC team

From: Mike Ounsworth <mike.ounsworth@entrust.com> via pqc-forum <pqc-forum@list.nist.gov>
To: Paul Hoffman <paul.hoffman@icann.org>, pqc-forum <pqc-forum@list.nist.gov>
Subject: RE: [Ext] [pqc-forum] Call for Additional Signatures is released
Date: Tuesday, September 06, 2022 06:23:35 PM ET

---

crt.sh shows that we're in the single-digit-billion certs in the index. If you were to download and integrity-check the entire thing on a regular basis, then I could see short signatures and fast verifications being a big deal.

https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fcrt.sh%2Fcert-populations&data=05%7C01%7Cyi-kai.liu%40nist.gov%7C2ddda533436e40ab631e08da90566f7d%7C2ab5d82fd8fa4797a93e054655c61dec%7C1%7C0%7C637980998156351978%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=rOwDpUaaMXPE4hW1mS4QfA%2BvLk1VpB0Xqlnwj9yz83k%3D&reserved=0

That said, I'm also curious why CT was singled out as *the* motivating use-case in Dustin's announcement.

—
Mike Ounsworth
Software Security Architect, Entrust

-----Original Message-----
From: pqc-forum@list.nist.gov <pqc-forum@list.nist.gov> On Behalf Of Paul Hoffman
Sent: September 6, 2022 4:42 PM
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: [EXTERNAL] Re: [Ext] [pqc-forum] Call for Additional Signatures is released

WARNING: This email originated outside of Entrust.
DO NOT CLICK links or attachments unless you trust the sender and know the content is safe.

On Sep 6, 2022, at 1:15 PM, 'Moody, Dustin (Fed)' via pqc-forum <pqc-forum@list.nist.gov> wrote:

> For certain applications, such as certificate transparency, NIST may also be interested in signature schemes that have short signatures and fast verification.

Can you say more about the motivation here? Are you forcusing on schemes that have possibly-giant keys but short signatures, or are you still hoping for schemes that have a variety of different key/signature size balances? I ask as someone who supports a protocol (DNSSEC) that is concerned with delivering both keys and signatures, so size of each will matter to us.

--Paul Hoffman

--
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/CH0PR11MB5739C43F1F621D7489FFAA349F7E9%40CH0PR11MB5739.namprd11.prod.outlook.com.

From: Bas Westerbaan <bas@cloudflare.com> via pqc-forum <pqc-forum@list.nist.gov>
To: Mike Ounsworth <mike.ounsworth@entrust.com>
CC: Paul Hoffman <paul.hoffman@icann.org>, pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [Ext] [pqc-forum] Call for Additional Signatures is released
Date: Wednesday, September 07, 2022 07:25:42 AM ET

On Wed, Sep 7, 2022 at 12:22 AM 'Mike Ounsworth' via pqc-forum <pqc-forum@list.nist.gov> wrote:

> crt.sh shows that we're in the single-digit-billion certs in the index. If you were to download and integrity-check the entire thing on a regular basis, then I could see short signatures and fast verifications being a big deal.

I'd say having a small-signature&fast-verification scheme is a much bigger deal for the 2+ SCTs that are in every single leaf certificate on the web. Also it's nice for the signature in the intermediate certificate. There are not that many root CAs and CT logs, so having slightly larger public keys for those keypairs could be a worthwhile trade-off.

Best,

Bas

From: Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [Ext] [pqc-forum] Call for Additional Signatures is released
Date: Wednesday, September 07, 2022 07:49:04 AM ET
Attachments: smime.p7m

Having a small-signature && fast-verification is **crucial** for constrained environments (that I'm often dealing with).

I agree that a smaller signature at the cost of slightly larger public key would be a good compromise, at least for my use cases.

Thanks!

--

V/R,

Uri

There are two ways to design a system. One is to make it so simple there are obviously no deficiencies.

The other is to make it so complex there are no obvious deficiencies.

- C. A. R. Hoare

From: 'Bas Westerbaan' via pqc-forum
Reply-To: Bas Westerbaan
Date: Wednesday, September 7, 2022 at 07:25
To: Mike Ounsworth
Cc: Paul Hoffman , pqc-forum
Subject: Re: [Ext] [pqc-forum] Call for Additional Signatures is released

On Wed, Sep 7, 2022 at 12:22 AM 'Mike Ounsworth' via pqc-forum <pqc-forum@list.nist.gov> wrote:

> crt.sh shows that we're in the single-digit-billion certs in the index. If you were to download and integrity-check the entire thing on a regular basis, then I could see short signatures and fast verifications being a big deal.

I'd say having a small-signature&fast-verification scheme is a much bigger deal for the 2+ SCTs that are in every single leaf certificate on the web. Also it's nice for the signature in the intermediate certificate. There are not that many root CAs and CT logs, so having slightly larger public keys for those keypairs could be a worthwhile trade-off.

Best,

Bas

--

--

From: Bo Lin <crypto.sec@outlook.com> via pqc-forum@list.nist.gov
To: Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu>, pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [Ext] [pqc-forum] Call for Additional Signatures is released
Date: Wednesday, September 07, 2022 05:42:30 PM ET

Yes, totally agree! There are many applications that key size overweighs performance

Get Outlook for iOS

From: pqc-forum@list.nist.gov <pqc-forum@list.nist.gov> on behalf of Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu>
Sent: Wednesday, September 7, 2022 12:49 pm
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [Ext] [pqc-forum] Call for Additional Signatures is released

Having a small-signature && fast-verification is **crucial** for constrained environments (that I'm often dealing with).

I agree that a smaller signature at the cost of slightly larger public key would be a good compromise, at least for my use cases.

Thanks!

--

V/R,

Uri

There are two ways to design a system. One is to make it so simple there are obviously no deficiencies.

The other is to make it so complex there are no obvious deficiencies.

- C. A. R. Hoare

> **From:** 'Bas Westerbaan' via pqc-forum <pqc-forum@list.nist.gov>
> **Reply-To:** Bas Westerbaan <bas@cloudflare.com>
> **Date:** Wednesday, September 7, 2022 at 07:25

To: Mike Ounsworth <Mike.Ounsworth@entrust.com>
Cc: Paul Hoffman <paul.hoffman@icann.org>, pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [Ext] [pqc-forum] Call for Additional Signatures is released

On Wed, Sep 7, 2022 at 12:22 AM 'Mike Ounsworth' via pqc-forum <pqc-forum@list.nist.gov> wrote:

> crt.sh shows that we're in the single-digit-billion certs in the index. If you were to download and integrity-check the entire thing on a regular basis, then I could see short signatures and fast verifications being a big deal.

I'd say having a small-signature&fast-verification scheme is a much bigger deal for the 2+ SCTs that are in every single leaf certificate on the web. Also it's nice for the signature in the intermediate certificate. There are not that many root CAs and CT logs, so having slightly larger public keys for those keypairs could be a worthwhile trade-off.

Best,

Bas

From: Sofi Celi <soficeli0@gmail.com> via pqc-forum@list.nist.gov
To: Edoardo Persichetti <epersichetti@fau.edu>
CC: Bo Lin <crypto.sec@outlook.com>, Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu>, pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [Ext] [pqc-forum] Call for Additional Signatures is released
Date: Wednesday, September 07, 2022 07:22:19 PM ET

Dear, Edoardo and all,
For DNSSEC, there is this interesting presentation from Roland van Rijswijk-Deij around which sizes and computational times might work: https://github.com/claucece/PQNet-Workshop/blob/main/slides/PQC%20and%20DNSSEC%202022.pdf (the last set of slides: from 96 onwards).

There is also the master thesis of one of his students on the matter: http://essay.utwente.nl/89509/1/Beernink_MA_EEMCS.pdf and another paper: https://conferences.sigcomm.org/sigcomm/2021/files/papers/3431832.3431838.pdf

For TLS, Douglas Stebila, Goutam Tamvada and Christian Paquin benchmarked some of the PQC algorithms: https://www.douglas.stebila.ca/research/papers/PQCrypto-PaqSteTam20/ , which provides a very nice insight.

Hope this helps,

El mié, 7 sept 2022 a la(s) 22:48, 'Edoardo Persichetti' via pqc-forum (pqc-forum@list.nist.gov) escribió:

> Hi all! I guess, for us designers, it would be great to have a more precise understanding of what are the ballparks and sizes discussed here, with reference for the various use cases, since the terms “large”, “short”, “slightly larger” and similar are very vague. Are we talking about a few bytes, a few kilobytes, a few dozen kilobytes, a few hundred kilobytes (e.g. UOV)...?
> Thanks for your insight.
>
> Best,
>
> Edoardo

On Sep 7, 2022, at 5:42 PM, Bo Lin <crypto.sec@outlook.com> wrote:

> **EXTERNAL EMAIL :**Exercise caution when responding, opening links, or opening attachments.

Yes, totally agree! There are many applications that key size overweighs performance

GetOutlook for iOS

From:pqc-forum@list.nist.gov<pqc-forum@list.nist.gov> on behalf of Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu>
Sent: Wednesday, September 7, 2022 12:49 pm
To:pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [Ext] [pqc-forum] Call for Additional Signatures is released

Having a small-signature && fast-verification is**crucial**for constrained environments (that I'm often dealing with).
I agree that a smaller signature at the cost of slightly larger public key would be a good compromise, at least for my use cases.
Thanks!
--
V/R,
Uri
There are two ways to design a system. One is to make it so simple there are obviously no deficiencies.
The other is to make it so complex there are no obvious deficiencies.
- C. A. R. Hoare

From:'Bas Westerbaan' via pqc-forum <pqc-forum@list.nist.gov>
Reply-To: Bas Westerbaan <bas@cloudflare.com>
Date: Wednesday, September 7, 2022 at 07:25
To: Mike Ounsworth <Mike.Ounsworth@entrust.com>
Cc: Paul Hoffman <paul.hoffman@icann.org>, pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [Ext] [pqc-forum] Call for Additional Signatures is released

On Wed, Sep 7, 2022 at 12:22 AM 'Mike Ounsworth' via pqc-forum <pqc-forum@list.nist.gov> wrote:

> crt.sh shows that we're in the single-digit-billion certs in the index. If you were to download and integrity-check the entire thing on a regular basis, then I could see short signatures and fast verifications being a big deal.

I'd say having a small-signature&fast-verification scheme is a much bigger deal for the 2+ SCTs that are in every single leaf certificate on the web. Also it's nice for the signature in the intermediate certificate. There are not that many root CAs and CT logs, so having slightly larger public keys for those keypairs could be a worthwhile trade-off.

Best,

Bas

--

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 topqc-forum+unsubscribe@list.nist.gov.

To view this discussion on the web visithttps://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/CAMjbhoW%2B2EOTBfcLF0ERATw9GgmkQd-EPJh_-Y0uPnsSatiphA%40mail.gmail.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 topqc-forum+unsubscribe@list.nist.gov.

To view this discussion on the web visithttps://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/3139A267-51A2-402C-BE3D-65FED31B6E89%40ll.mit.edu.

--

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 topqc-forum+unsubscribe@list.nist.gov.

To view this discussion on the web visithttps://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/LO2P123MB36612BE22406EE5C8F3385A484419%40LO2P123MB3661.GBRP123.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/489BEB1A-0041-4425-8E76-E845767A88F0%40fau.edu.

--

Sofía Celi
@claucece
Cryptographic research and implementation at many places, but specially at Brave

Reach me out at: cherenkov@riseup.net
74BE 6517 031D 11CC D233 3FCA 44DF 95B9 E3BC 4369

--

From: Samuel Lavery <sam.lavery@gmail.com> via pqc-forum@list.nist.gov
To: Sofi Celi <soficeli0@gmail.com>
CC: Edoardo Persichetti <epersichetti@fau.edu>, Bo Lin <crypto.sec@outlook.com>, Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu>, pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [Ext] [pqc-forum] Call for Additional Signatures is released
Date: Wednesday, September 07, 2022 08:53:14 PM ET

Hi Sofi and everyone,
I've read a few of these before, but some were new, so thank you. I think I have a reasonable understanding of the impacts and constraints for wired frame based protocols, but I've never been able to find anything about the impacts to wireless protocols. I have very little understanding of how things like LTE and other long range wireless protocols use signatures and what their constraints are. Have you ever come across any similar research for non-avian (RFC1149) over the air protocols? I have some intuition about it, but haven't been able to find any research.

Thanks,

Sam

> On Sep 7, 2022, at 4:21 PM, Sofi Celi <soficeli0@gmail.com> wrote:
>
> Dear, Edoardo and all,
> For DNSSEC, there is this interesting presentation from Roland van Rijswijk-Deij around which sizes and computational times might work: https://github.com/claucece/PQNet-Workshop/blob/main/slides/PQC%20and%20DNSSEC%202022.pdf (the last set of slides: from 96 onwards).
>
> There is also the master thesis of one of his students on the matter: http://essay.utwente.nl/89509/1/Beernink_MA_EEMCS.pdf and another paper: https://conferences.sigcomm.org/sigcomm/2021/files/papers/3431832.3431838.pdf
>
> For TLS, Douglas Stebila, Goutam Tamvada and Christian Paquin benchmarked some of the PQC algorithms: https://www.douglas.stebila.ca/research/papers/PQCrypto-PaqSteTam20/ , which provides a very nice insight.
>
> Hope this helps,

El mié, 7 sept 2022 a la(s) 22:48, 'Edoardo Persichetti' via pqc-forum (pqc-forum@list.nist.gov) escribió:

> Hi all! I guess, for us designers, it would be great to have a more precise understanding of what are the ballparks and sizes discussed here, with reference for the various use cases, since the terms “large”, “short”, “slightly larger” and similar are very vague. Are we talking about a few bytes, a few kilobytes, a few dozen kilobytes, a few hundred kilobytes (e.g. UOV)...?
> Thanks for your insight.
>
> Best,
>
> Edoardo
>
> On Sep 7, 2022, at 5:42 PM, Bo Lin <crypto.sec@outlook.com> wrote:
>
> > **EXTERNAL EMAIL :**Exercise caution when responding, opening links, or opening attachments.
>
> Yes, totally agree! There are many applications that key size overweighs performance
>
> GetOutlook for iOS
>
> ---
>
> **From:**pqc-forum@list.nist.gov<pqc-forum@list.nist.gov> on behalf of Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu>
> **Sent:**Wednesday, September 7, 2022 12:49 pm
> **To:**pqc-forum <pqc-forum@list.nist.gov>
> **Subject:**Re: [Ext] [pqc-forum] Call for Additional Signatures is released
>
> Having a small-signature && fast-verification is**crucial**for constrained environments (that I’m often dealing with).
> I agree that a smaller signature at the cost of slightly larger public key would be a good compromise, at least for my use cases.
> Thanks!
> --
> V/R,
> Uri

There are two ways to design a system. One is to make it so simple there are obviously no deficiencies.
The other is to make it so complex there are no obvious deficiencies.
- C. A. R. Hoare

From:'Bas Westerbaan' via pqc-forum <pqc-forum@list.nist.gov>
Reply-To: Bas Westerbaan <bas@cloudflare.com>
Date: Wednesday, September 7, 2022 at 07:25
To: Mike Ounsworth <Mike.Ounsworth@entrust.com>
Cc: Paul Hoffman <paul.hoffman@icann.org>, pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [Ext] [pqc-forum] Call for Additional Signatures is released

On Wed, Sep 7, 2022 at 12:22 AM 'Mike Ounsworth' via pqc-forum <pqc-forum@list.nist.gov> wrote:

> crt.sh shows that we're in the single-digit-billion certs in the index. If you were to download and integrity-check the entire thing on a regular basis, then I could see short signatures and fast verifications being a big deal.

I'd say having a small-signature&fast-verification scheme is a much bigger deal for the 2+ SCTs that are in every single leaf certificate on the web. Also it's nice for the signature in the intermediate certificate. There are not that many root CAs and CT logs, so having slightly larger public keys for those keypairs could be a worthwhile trade-off.

Best,
Bas

--
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 topqc-forum+unsubscribe@list.nist.gov.
To view this discussion on the web visithttps://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/CAMjbhoW%2B2EOTBfcLF0ERATw9GgmkQd-EPJh_-Y0uPnsSatiphA%40mail.gmail.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 topqc-forum+unsubscribe@list.nist.gov.
> To view this discussion on the web visithttps://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/3139A267-51A2-402C-BE3D-65FED31B6E89%40ll.mit.edu.
>
> --
>
> 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 topqc-forum+unsubscribe@list.nist.gov.
>
> To view this discussion on the web visithttps://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/LO2P123MB36612BE22406EE5C8F3385A484419%40LO2P123MB3661.GBRP123.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/489BEB1A-0041-4425-8E76-E845767A88F0%40fau.edu.

--
Sofía Celi
@claucece
Cryptographic research and implementation at many places, but specially at Brave

Reach me out at: cherenkov@riseup.net
74BE 6517 031D 11CC D233 3FCA 44DF 95B9 E3BC 4369

--
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/CAHy9yixfZfD5Fe8WMzyRNBZJHDnuuhJkEycSKLG3fB3Rt2LFjw%40mail.gmail.com.

From: Brent Kimberley <brent.kimberley@durham.ca> via pqc-forum <pqc-forum@list.nist.gov>
To: Samuel Lavery <sam.lavery@gmail.com>, Sofi Celi <soficeli0@gmail.com>
CC: Edoardo Persichetti <epersichetti@fau.edu>, Bo Lin <crypto.sec@outlook.com>, Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu>, pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [Ext] [pqc-forum] Call for Additional Signatures is released
Date: Wednesday, September 07, 2022 10:11:27 PM ET

Interesting question. Should 4G, 5G, 6G, 7G or "future mobile technologies" align with the CNSA 2.0 roadmap? (Perhaps they already are aligned?)

From: pqc-forum@list.nist.gov <pqc-forum@list.nist.gov> on behalf of Samuel Lavery <sam.lavery@gmail.com>
Sent: Wednesday, September 7, 2022, 8:54 p.m.
To: Sofi Celi <soficeli0@gmail.com>
Cc: Edoardo Persichetti <epersichetti@fau.edu>; Bo Lin <crypto.sec@outlook.com>; Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu>; pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [Ext] [pqc-forum] Call for Additional Signatures is released

Hi Sofi and everyone,
I've read a few of these before, but some were new, so thank you. I think I have a reasonable understanding of the impacts and constraints for wired frame based protocols, but I've never been able to find anything about the impacts to wireless protocols. I have very little understanding of how things like LTE and other long range wireless protocols use signatures and what their constraints are. Have you ever come across any similar research for non-avian (RFC1149) over the air protocols? I have some intuition about it, but haven't been able to find any research.

Thanks,

Sam

> On Sep 7, 2022, at 4:21 PM, Sofi Celi <soficeli0@gmail.com> wrote:
>
> Dear, Edoardo and all,
> For DNSSEC, there is this interesting presentation from Roland van Rijswijk-Deij around which sizes and computational times might work: https://github.com/

claucece/PQNet-Workshop/blob/main/slides/PQC%20and%20DNSSEC%202022.pdf (the last set of slides: from 96 onwards).

There is also the master thesis of one of his students on the matter: http://essay.utwente.nl/89509/1/Beernink_MA_EEMCS.pdf and another paper: https://conferences.sigcomm.org/sigcomm/2021/files/papers/3431832.3431838.pdf

For TLS, Douglas Stebila, Goutam Tamvada and Christian Paquin benchmarked some of the PQC algorithms: https://www.douglas.stebila.ca/research/papers/PQCrypto-PaqSteTam20/ , which provides a very nice insight.

Hope this helps,

El mié, 7 sept 2022 a la(s) 22:48, 'Edoardo Persichetti' via pqc-forum (pqc-forum@list.nist.gov) escribió:

> Hi all! I guess, for us designers, it would be great to have a more precise understanding of what are the ballparks and sizes discussed here, with reference for the various use cases, since the terms “large”, “short”, “slightly larger” and similar are very vague. Are we talking about a few bytes, a few kilobytes, a few dozen kilobytes, a few hundred kilobytes (e.g. UOV)...?
> Thanks for your insight.
>
> Best,
>
> Edoardo
>
> On Sep 7, 2022, at 5:42 PM, Bo Lin <crypto.sec@outlook.com> wrote:
>
> > **EXTERNAL EMAIL :**Exercise caution when responding, opening links, or opening attachments.
>
> Yes, totally agree! There are many applications that key size overweighs performance
>
> GetOutlook for iOS
>
> **From:**pqc-forum@list.nist.gov<pqc-forum@list.nist.gov> on behalf of Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu>

Sent: Wednesday, September 7, 2022 12:49 pm
To:pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [Ext] [pqc-forum] Call for Additional Signatures is released

Having a small-signature && fast-verification is**crucial**for constrained environments (that I'm often dealing with).
I agree that a smaller signature at the cost of slightly larger public key would be a good compromise, at least for my use cases.
Thanks!
--
V/R,
Uri
There are two ways to design a system. One is to make it so simple there are obviously no deficiencies.
The other is to make it so complex there are no obvious deficiencies.
- C. A. R. Hoare

From:'Bas Westerbaan' via pqc-forum <pqc-forum@list.nist.gov>
Reply-To: Bas Westerbaan <bas@cloudflare.com>
Date: Wednesday, September 7, 2022 at 07:25
To: Mike Ounsworth <Mike.Ounsworth@entrust.com>
Cc: Paul Hoffman <paul.hoffman@icann.org>, pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [Ext] [pqc-forum] Call for Additional Signatures is released

On Wed, Sep 7, 2022 at 12:22 AM 'Mike Ounsworth' via pqc-forum <pqc-forum@list.nist.gov> wrote:

> crt.sh shows that we're in the single-digit-billion certs in the index. If you were to download and integrity-check the entire thing on a regular basis, then I could see short signatures and fast verifications being a big deal.

I'd say having a small-signature&fast-verification scheme is a much bigger deal for the 2+ SCTs that are in every single leaf certificate on the web. Also it's nice for the signature in the intermediate certificate. There are not that many root CAs and CT logs, so having slightly larger public keys for those keypairs could be a worthwhile trade-off.
Best,
Bas

> --
> 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 topqc-forum+unsubscribe@list.nist.gov.
> To view this discussion on the web visithttps://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/CAMjbhoW%2B2EOTBfcLF0ERATw9GgmkQd-EPJh_-Y0uPnsSatiphA%40mail.gmail.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 topqc-forum+unsubscribe@list.nist.gov.
> To view this discussion on the web visithttps://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/3139A267-51A2-402C-BE3D-65FED31B6E89%40ll.mit.edu.
>
> --
> 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 topqc-forum+unsubscribe@list.nist.gov.
> To view this discussion on the web visithttps://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/LO2P123MB36612BE22406EE5C8F3385A484419%40LO2P123MB3661.GBRP123.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/489BEB1A-0041-4425-8E76-E845767A88F0%40fau.edu.

--
Sofía Celi
@claucece
Cryptographic research and implementation at many places, but specially at Brave

Reach me out at: cherenkov@riseup.net
74BE 6517 031D 11CC D233 3FCA 44DF 95B9 E3BC 4369

--
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/CAHy9yixfZfD5Fe8WMzyRNBZJHDnuuhJkEycSKLG3fB3Rt2LFjw%40mail.gmail.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/50E97BA5-7F89-4652-8ECF-5B5D75853881%40gmail.com.

From: John Mattsson <john.mattsson@ericsson.com> via pqc-forum <pqc-forum@list.nist.gov>
To: Brent Kimberley <brent.kimberley@durham.ca>, Samuel Lavery <sam.lavery@gmail.com>, Sofi Celi <soficeli0@gmail.com>
CC: Edoardo Persichetti <epersichetti@fau.edu>, Bo Lin <crypto.sec@outlook.com>, Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu>, pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [Ext] [pqc-forum] Call for Additional Signatures is released
Date: Thursday, September 08, 2022 12:50:48 AM ET

Just like IETF, 3GPP has had a lot of discussion about PQC. I expect 3GPP to introduce PQC in their specifications as soon as NIST has released final standards and IETF has published updates to TLS 1.3, IKEv2, X.509, and HPKE. 3GPP relies on IETF standards for almost all use of public key cryptography. 3GPP might mandate support of level 1 or 3 and have high security level 5 as should support. This is what current 3GPP documents mostly do regarding P-256/SHA-256 and P-384/SHA-384. I agree with the CNSA 2.0 statement that Kyber and Dilithium should not be used before there are final NIST standards. I think we need to make sure there are NIST and IETF standards before setting timelines for 5G.

3GPP RAN mostly rely on pre-shared keys for authentication and key exchange. 5G introduces the use of ECIES to encrypt identities over the air and there is 2000 bytes reserved to be able to handle PQC KEMs. HPKE with Kyber would likely be a good choice. There is also work on introducing ECDHE in AKA (see EAP-AKA' FS) to provide forward secrecy and align with zero trust principles. Always assuming breach such as key compromise (e.g., in the sim card supply chain) and minimizing the impact of breach are essential zero-trust principles. This should be a main priority for the next 5G releases. Would be good with NIST help to drive zero trust in 5G RAN.

https://www.ericsson.com/en/blog/2022/4/extensible-authentication-protocol-eap-networks

Non-constrained wireless networks will likely be impacted similarly to wired protocols, but it would be good with more research. For very constrained wireless protocols the situation is dire and Kyber and Dilithium do in many cases not work at all. I have written a position paper to the NIST Fourth PQC Standardization Conference about this that I will submit soon.

Cheers,

John

From: 'Brent Kimberley' via pqc-forum <pqc-forum@list.nist.gov>
Date: Thursday, 8 September 2022 at 04:13

To: Samuel Lavery <sam.lavery@gmail.com>, Sofi Celi <soficeli0@gmail.com>
Cc: Edoardo Persichetti <epersichetti@fau.edu>, Bo Lin <crypto.sec@outlook.com>, Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu>, pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [Ext] [pqc-forum] Call for Additional Signatures is released

Interesting question. Should 4G, 5G, 6G, 7G or "future mobile technologies" align with the CNSA 2.0 roadmap? (Perhaps they already are aligned?)

From: pqc-forum@list.nist.gov <pqc-forum@list.nist.gov> on behalf of Samuel Lavery <sam.lavery@gmail.com>
Sent: Wednesday, September 7, 2022, 8:54 p.m.
To: Sofi Celi <soficeli0@gmail.com>
Cc: Edoardo Persichetti <epersichetti@fau.edu>; Bo Lin <crypto.sec@outlook.com>; Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu>; pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [Ext] [pqc-forum] Call for Additional Signatures is released

Hi Sofi and everyone,

I've read a few of these before, but some were new, so thank you. I think I have a reasonable understanding of the impacts and constraints for wired frame based protocols, but I've never been able to find anything about the impacts to wireless protocols. I have very little understanding of how things like LTE and other long range wireless protocols use signatures and what their constraints are. Have you ever come across any similar research for non-avian (RFC1149) over the air protocols? I have some intuition about it, but haven't been able to find any research.

Thanks,

Sam

> On Sep 7, 2022, at 4:21 PM, Sofi Celi <soficeli0@gmail.com> wrote:
>
> Dear, Edoardo and all,
>
> For DNSSEC, there is this interesting presentation from Roland van Rijswijk-Deij around which sizes and computational times might work: https://github.com/claucece/PQNet-Workshop/blob/main/slides/PQC%20and%20DNSSEC%202022.pdf (the last set of slides: from 96 onwards).

There is also the master thesis of one of his students on the matter: http://essay.utwente.nl/89509/1/Beernink_MA_EEMCS.pdf and another paper: https://conferences.sigcomm.org/sigcomm/2021/files/papers/3431832.3431838.pdf

For TLS, Douglas Stebila, Goutam Tamvada and Christian Paquin benchmarked some of the PQC algorithms: https://www.douglas.stebila.ca/research/papers/PQCrypto-PaqSteTam20/ , which provides a very nice insight.

Hope this helps,

El mié, 7 sept 2022 a la(s) 22:48, 'Edoardo Persichetti' via pqc-forum (pqc-forum@list.nist.gov) escribió:

> Hi all! I guess, for us designers, it would be great to have a more precise understanding of what are the ballparks and sizes discussed here, with reference for the various use cases, since the terms “large”, “short”, “slightly larger” and similar are very vague. Are we talking about a few bytes, a few kilobytes, a few dozen kilobytes, a few hundred kilobytes (e.g. UOV)...?
>
> Thanks for your insight.
>
> Best,
>
> Edoardo
>
> > On Sep 7, 2022, at 5:42 PM, Bo Lin <crypto.sec@outlook.com> wrote:
> >
> > **EXTERNAL EMAIL :** Exercise caution when responding, opening links, or opening attachments.
> >
> > Yes, totally agree! There are many applications that key size overweighs performance
> >
> > Get Outlook for iOS
> >
> > **From:**pqc-forum@list.nist.gov <pqc-forum@list.nist.gov> on behalf of Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu>
> >
> > **Sent:** Wednesday, September 7, 2022 12:49 pm
> >
> > **To:** pqc-forum <pqc-forum@list.nist.gov>
> >
> > **Subject:** Re: [Ext] [pqc-forum] Call for Additional Signatures is released

Having a small-signature && fast-verification is **crucial** for constrained environments (that I'm often dealing with).

I agree that a smaller signature at the cost of slightly larger public key would be a good compromise, at least for my use cases.

Thanks!

--

V/R,

Uri

There are two ways to design a system. One is to make it so simple there are obviously no deficiencies.

The other is to make it so complex there are no obvious deficiencies.

- C. A. R. Hoare

From: 'Bas Westerbaan' via pqc-forum <pqc-forum@list.nist.gov>
Reply-To: Bas Westerbaan <bas@cloudflare.com>
Date: Wednesday, September 7, 2022 at 07:25
To: Mike Ounsworth <Mike.Ounsworth@entrust.com>
Cc: Paul Hoffman <paul.hoffman@icann.org>, pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [Ext] [pqc-forum] Call for Additional Signatures is released

On Wed, Sep 7, 2022 at 12:22 AM 'Mike Ounsworth' via pqc-forum <pqc-forum@list.nist.gov> wrote:

> crt.sh shows that we're in the single-digit-billion certs in the index. If you were to download and integrity-check the entire thing on a regular basis, then I could see short signatures and fast verifications being a big deal.

I'd say having a small-signature&fast-verification scheme is a much bigger deal for the 2+ SCTs that are in every single leaf certificate on

the web. Also it's nice for the signature in the intermediate certificate. There are not that many root CAs and CT logs, so having slightly larger public keys for those keypairs could be a worthwhile trade-off.

Best,

Bas

--
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/CAMjbhoW%2B2EOTBfcLF0ERATw9GgmkQd-EPJh_-Y0uPnsSatiphA%40mail.gmail.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/3139A267-51A2-402C-BE3D-65FED31B6E89%40ll.mit.edu.

--
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/LO2P123MB36612BE22406EE5C8F3385A484419%40LO2P123MB3661.GBRP123.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/489BEB1A-0041-4425-8E76-E845767A88F0%40fau.edu.

--

Sofía Celi
@claucece
Cryptographic research and implementation at many places, but specially at Brave

Reach me out at: cherenkov@riseup.net
74BE 6517 031D 11CC D233 3FCA 44DF 95B9 E3BC 4369

--
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/CAHy9yixfZfD5Fe8WMzyRNBZJHDnuuhJkEycSKLG3fB3Rt2LFjw%40mail.gmail.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/50E97BA5-7F89-4652-8ECF-5B5D75853881%40gmail.com.

--

From: Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu> via pqc-forum@list.nist.gov
To: Edoardo Persichetti <epersichetti@fau.edu>
CC: pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [Ext] [pqc-forum] Call for Additional Signatures is released
Date: Thursday, September 08, 2022 05:47:09 PM ET
Attachments: smime.p7m

> Hi all! I guess, for us designers, it would be great to have a more precise understanding of what are the ballparks and sizes discussed here, with reference for the various use cases, since the terms “large”, “short”, “slightly larger” and similar are very vague.

OK, for you designers: my “constrained” use case prefers

- signatures in ballpark of 1 Kbyte or less,
- public keys for KEM – in ballpark of 1.5 KB or less,
- public keys for signature – within a couple of KB, if over-the-air exchange of intermediate CA certificates required – less than 2 KB.

Performance for signature:

- fast verification is a-must,
- fast signing is preferred,
- fast keygen is not that critical.

Performance for KEM: everything must be fast.

Hope this helps.

TNX

> On Sep 7, 2022, at 5:42 PM, Bo Lin <crypto.sec@outlook.com> wrote:
>
> **EXTERNAL EMAIL :**Exercise caution when responding, opening links, or opening attachments.
>
> Yes, totally agree! There are many applications that key size overweighs performance
>
> GetOutlook for iOS

From:pqc-forum@list.nist.gov<pqc-forum@list.nist.gov> on behalf of Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu>

Sent: Wednesday, September 7, 2022 12:49 pm

To:pqc-forum <pqc-forum@list.nist.gov>

Subject: Re: [Ext] [pqc-forum] Call for Additional Signatures is released

Having a small-signature && fast-verification is**crucial**for constrained environments (that I'm often dealing with).

I agree that a smaller signature at the cost of slightly larger public key would be a good compromise, at least for my use cases.

Thanks!

--

V/R,

Uri

There are two ways to design a system. One is to make it so simple there are obviously no deficiencies.

The other is to make it so complex there are no obvious deficiencies.

- C. A. R. Hoare

From:'Bas Westerbaan' via pqc-forum <pqc-forum@list.nist.gov>
Reply-To: Bas Westerbaan <bas@cloudflare.com>
Date: Wednesday, September 7, 2022 at 07:25
To: Mike Ounsworth <Mike.Ounsworth@entrust.com>
Cc: Paul Hoffman <paul.hoffman@icann.org>, pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [Ext] [pqc-forum] Call for Additional Signatures is released

On Wed, Sep 7, 2022 at 12:22 AM 'Mike Ounsworth' via pqc-forum <pqc-forum@list.nist.gov> wrote:

> crt.sh shows that we're in the single-digit-billion certs in the index. If you were to download and integrity-check the entire thing on a

> regular basis, then I could see short signatures and fast verifications being a big deal.

I'd say having a small-signature&fast-verification scheme is a much bigger deal for the 2+ SCTs that are in every single leaf certificate on the web. Also it's nice for the signature in the intermediate certificate. There are not that many root CAs and CT logs, so having slightly larger public keys for those keypairs could be a worthwhile trade-off.

Best,

Bas

From: Bas Westerbaan <bas@cloudflare.com> via pqc-forum <pqc-forum@list.nist.gov>
To: Edoardo Persichetti <epersichetti@fau.edu>
CC: Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu>, pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [Ext] [pqc-forum] Call for Additional Signatures is released
Date: Thursday, September 08, 2022 06:11:41 PM ET

In TLS for the Web there are many different signatures, so I'm afraid I can't give the same simple guidance as Uri. But have a look at https://blog.cloudflare.com/sizing-up-post-quantum-signatures/

On Thu, Sep 8, 2022 at 11:49 PM 'Edoardo Persichetti' via pqc-forum <pqc-forum@list.nist.gov> wrote:

> Thanks Uri, this is very accurate :)
>
> Best,
>
> Edoardo
>
> > On Sep 8, 2022, at 5:46 PM, Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu> wrote:
> >
> > > Hi all! I guess, for us designers, it would be great to have a more precise understanding of what are the ballparks and sizes discussed here, with reference for the various use cases, since the terms “large”, “short”, “slightly larger” and similar are very vague.
> >
> > OK, for you designers: my “constrained” use case prefers
> > - signatures in ballpark of 1 Kbyte or less,
> > - public keys for KEM – in ballpark of 1.5 KB or less,
> > - public keys for signature – within a couple of KB, if over-the-air exchange of intermediate CA certificates required – less than 2 KB.
> >
> > Performance for signature:
> > - fast verification is a-must,
> > - fast signing is preferred,
> > - fast keygen is not that critical.

Performance for KEM: everything must be fast.
Hope this helps.
TNX

On Sep 7, 2022, at 5:42 PM, Bo Lin <crypto.sec@outlook.com> wrote:

> **EXTERNAL EMAIL :**Exercise caution when responding, opening links, or opening attachments.

Yes, totally agree! There are many applications that key size overweighs performance

GetOutlook for iOS

From:pqc-forum@list.nist.gov<pqc-forum@list.nist.gov> on behalf of Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu>

Sent: Wednesday, September 7, 2022 12:49 pm

To:pqc-forum <pqc-forum@list.nist.gov>

Subject: Re: [Ext] [pqc-forum] Call for Additional Signatures is released

Having a small-signature && fast-verification is**crucial**for constrained environments (that I'm often dealing with).
I agree that a smaller signature at the cost of slightly larger public key would be a good compromise, at least for my use cases.
Thanks!
--
V/R,
Uri
There are two ways to design a system. One is to make it so simple there are obviously no deficiencies.
The other is to make it so complex there are no obvious deficiencies.
- C. A. R. Hoare

From:'Bas Westerbaan' via pqc-forum <pqc-forum@list.nist.gov>
Reply-To: Bas Westerbaan <bas@cloudflare.com>
Date: Wednesday, September 7, 2022 at 07:25
To: Mike Ounsworth <Mike.Ounsworth@entrust.com>
Cc: Paul Hoffman <paul.hoffman@icann.org>, pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [Ext] [pqc-forum] Call for Additional Signatures is released

On Wed, Sep 7, 2022 at 12:22 AM 'Mike Ounsworth' via pqc-forum <pqc-forum@list.nist.gov> wrote:

> crt.sh shows that we're in the single-digit-billion certs in the index. If you were to download and integrity-check the entire thing on a regular basis, then I could see short signatures and fast verifications being a big deal.

I'd say having a small-signature&fast-verification scheme is a much bigger deal for the 2+ SCTs that are in every single leaf certificate on the web. Also it's nice for the signature in the intermediate certificate. There are not that many root CAs and CT logs, so having slightly larger public keys for those keypairs could be a worthwhile trade-off.

Best,

Bas

--

--

--

> LO2P123MB36612BE22406EE5C8F3385A484419%40LO2P123MB3661.GBRP123.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/3199409D-8CFA-4CD3-B27A-511BC647ACA0%40fau.edu.

--
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/CAMjbhoUb4oHSM-cCuWBGr29FnQry8XbKvpjy%3Dk1fS51D8JiFSA%40mail.gmail.com.

From: Brent Kimberley <brent.kimberley@durham.ca> via pqc-forum <pqc-forum@list.nist.gov>
To: John Mattsson <john.mattsson@ericsson.com>, pqc-forum <pqc-forum@list.nist.gov>
CC: Edoardo Persichetti <epersichetti@fau.edu>, Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu>
Subject: RE: [Ext] [pqc-forum] Call for Additional Signatures is released
Date: Monday, September 12, 2022 01:20:34 PM ET

>> Note that static keys..

Please note, an actuary, statistician, or equivalent with operational experience should be involved when making the final determination re risk / contingency-holdback / energy budget / expected operational demand / effective headroom – especially if the systems are life-crit.

From: 'John Mattsson' via pqc-forum <pqc-forum@list.nist.gov>
Sent: September 12, 2022 1:03 PM
To: pqc-forum <pqc-forum@list.nist.gov>
Cc: Edoardo Persichetti <epersichetti@fau.edu>; Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu>
Subject: Re: [Ext] [pqc-forum] Call for Additional Signatures is released

Hi,

Note that there are much more constrained networks than Uri's use case. The world "constrained" can refer to systems with several orders of magniture difference in capabilities. While constrained devices has gotten quite a lot of attention, the radio is often the most constrained part. To reduce overhead and processing in constrained radio networks, IETF has created several working groups and technologies for constrained networks such as 6lo, 6LoWPAN, 6TiSCH, ACE, CBOR, CoRE (CoAP, OSCORE), COSE, LAKE (EDHOC) ROLL (RPL), and LPWAN (SCHC).

Constrained radio networks are characterized by very small frame sizes on the order of tens of bytes transmitted a few times per day at ultra-low speeds, high latency, and severe duty cycles constraints. The number of different constrained radio network technologies is large and growing. Some examples of constrained network technologies are LoRaWAN, NB-IoT, Sigfox, Wi-SUN FAN, Bluetooth Low Energy, and IEEE 802.15.4. IEEE 802.15.4 is used in Zigbee, ISA100.11a, WirelessHART, MiWi, 6LoWPAN, 6TiSCH, Thread and SNAP. Low Power Wide Area Networks (LPWANs) is a huge and very quickly growing market expected to reach over 1000 billion USD globally by 2027.

To work well in constrained radio networks, the message sizes need to align with the tens of bytes transmitted a few times per day that the networks are designed for. Infrequently sending a few hundred bytes is acceptable in many constrained networks but sending a thousand bytes is not

feasible in more constrained networks. Note that static keys often do not need to be sent over constrained links, as they can be provisioned or accessed over non-constrained links. Moreover, signatures can in many cases be replaced by a symmetrical MAC from an Ephemeral-Static or Static-Static key exchange by changing the architecture and protocols, as long as the proving node is online.

As several people asked me offline, here is a copy of the paper we submitted to NIST.

https://drive.google.com/file/d/1Vky_uA8DhJMGM-keHH-ujF23xG6stUXq

Cheers,

John

From: 'Edoardo Persichetti' via pqc-forum <pqc-forum@list.nist.gov>
Date: Thursday, 8 September 2022 at 23:49
To: Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu>
Cc: pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [Ext] [pqc-forum] Call for Additional Signatures is released

Thanks Uri, this is very accurate :)

Best,

Edoardo

> On Sep 8, 2022, at 5:46 PM, Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu> wrote:
>
> > Hi all! I guess, for us designers, it would be great to have a more precise understanding of what are the ballparks and sizes discussed here, with reference for the various use cases, since the terms “large”, “short”, “slightly larger” and similar are very vague.
>
> OK, for you designers: my “constrained” use case prefers
>
> - signatures in ballpark of 1 Kbyte or less,
> - public keys for KEM – in ballpark of 1.5 KB or less,
> - public keys for signature – within a couple of KB, if over-the-air exchange of intermediate CA certificates required – less than 2 KB.
>
> Performance for signature:
>
> - fast verification is a-must,
> - fast signing is preferred,

- fast keygen is not that critical.

Performance for KEM: everything must be fast.

Hope this helps.

TNX

> On Sep 7, 2022, at 5:42 PM, Bo Lin <crypto.sec@outlook.com> wrote:
>
> **EXTERNAL EMAIL :**Exercise caution when responding, opening links, or opening attachments.
>
> Yes, totally agree! There are many applications that key size overweighs performance
>
> GetOutlook for iOS
>
> **From:**pqc-forum@list.nist.gov<pqc-forum@list.nist.gov> on behalf of Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu>
> **Sent:**Wednesday, September 7, 2022 12:49 pm
> **To:**pqc-forum <pqc-forum@list.nist.gov>
> **Subject:**Re: [Ext] [pqc-forum] Call for Additional Signatures is released
>
> Having a small-signature && fast-verification is**crucial**for constrained environments (that I'm often dealing with).
>
> I agree that a smaller signature at the cost of slightly larger public key would be a good compromise, at least for my use cases.
>
> Thanks!
>
> --
>
> V/R,
>
> Uri
>
> *There are two ways to design a system. One is to make it so simple there are obviously no deficiencies.*
>
> *The other is to make it so complex there are no obvious deficiencies.*
>
> *- C. A. R. Hoare*

From:'Bas Westerbaan' via pqc-forum <pqc-forum@list.nist.gov>
Reply-To: Bas Westerbaan <bas@cloudflare.com>
Date: Wednesday, September 7, 2022 at 07:25
To: Mike Ounsworth <Mike.Ounsworth@entrust.com>
Cc: Paul Hoffman <paul.hoffman@icann.org>, pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [Ext] [pqc-forum] Call for Additional Signatures is released

On Wed, Sep 7, 2022 at 12:22 AM 'Mike Ounsworth' via pqc-forum <pqc-forum@list.nist.gov> wrote:

> crt.sh shows that we're in the single-digit-billion certs in the index. If you were to download and integrity-check the entire thing on a regular basis, then I could see short signatures and fast verifications being a big deal.

I'd say having a small-signature&fast-verification scheme is a much bigger deal for the 2+ SCTs that are in every single leaf certificate on the web. Also it's nice for the signature in the intermediate certificate. There are not that many root CAs and CT logs, so having slightly larger public keys for those keypairs could be a worthwhile trade-off.

Best,

Bas

--

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 topqc-forum+unsubscribe@list.nist.gov.

To view this discussion on the web visithttps://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/3139A267-51A2-402C-BE3D-65FED31B6E89%40ll.mit.edu.

--

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 topqc-forum+unsubscribe@list.nist.gov.

To view this discussion on the web visithttps://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/LO2P123MB36612BE22406EE5C8F3385A484419%40LO2P123MB3661.GBRP123.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/3199409D-8CFA-4CD3-B27A-511BC647ACA0%40fau.edu.

--

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/HE1PR0701MB30509C8666E8BABB0DC9B89489449%40HE1PR0701MB3050.eurprd07.prod.outlook.com.

intended recipient and have received this message in error, please notify me by return e-mail and delete or destroy all copies of this message.

From: Brent Kimberley <brent.kimberley@durham.ca> via pqc-forum <pqc-forum@list.nist.gov>
To: John Mattsson <john.mattsson@ericsson.com>, pqc-forum <pqc-forum@list.nist.gov>
CC: Edoardo Persichetti <epersichetti@fau.edu>, Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu>
Subject: RE: [Ext] [pqc-forum] Call for Additional Signatures is released
Date: Monday, September 12, 2022 01:28:19 PM ET

For example bulk electric protection doesn't permit more than one mal event per 40 years.

From: Brent Kimberley
Sent: September 12, 2022 1:20 PM
To: John Mattsson <john.mattsson@ericsson.com>; pqc-forum <pqc-forum@list.nist.gov>
Cc: Edoardo Persichetti <epersichetti@fau.edu>; Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu>
Subject: RE: [Ext] [pqc-forum] Call for Additional Signatures is released

>> Note that static keys..

Please note, an actuary, statistician, or equivalent with operational experience should be involved when making the final determination re risk / contingency-holdback / energy budget / expected operational demand / effective headroom – especially if the systems are life-crit.

From: 'John Mattsson' via pqc-forum <pqc-forum@list.nist.gov>
Sent: September 12, 2022 1:03 PM
To: pqc-forum <pqc-forum@list.nist.gov>
Cc: Edoardo Persichetti <epersichetti@fau.edu>; Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu>
Subject: Re: [Ext] [pqc-forum] Call for Additional Signatures is released

Hi,

Note that there are much more constrained networks than Uri's use case. The world "constrained" can refer to systems with several orders of magniture difference in capabilities. While constrained devices has gotten quite a lot of attention, the radio is often the most constrained part. To reduce overhead and processing in constrained radio networks, IETF has created several working groups and technologies for constrained networks such as 6lo, 6LoWPAN, 6TiSCH, ACE, CBOR, CoRE (CoAP, OSCORE), COSE, LAKE (EDHOC) ROLL (RPL), and LPWAN (SCHC).

Constrained radio networks are characterized by very small frame sizes on the order of tens of bytes transmitted a few times per day at ultra-low speeds, high latency, and severe duty cycles constraints. The number of different constrained radio network technologies is large and growing. Some examples

of constrained network technologies are LoRaWAN, NB-IoT, Sigfox, Wi-SUN FAN, Bluetooth Low Energy, and IEEE 802.15.4. IEEE 802.15.4 is used in Zigbee, ISA100.11a, WirelessHART, MiWi, 6LoWPAN, 6TiSCH, Thread and SNAP. Low Power Wide Area Networks (LPWANs) is a huge and very quickly growing market expected to reach over 1000 billion USD globally by 2027.

To work well in constrained radio networks, the message sizes need to align with the tens of bytes transmitted a few times per day that the networks are designed for. Infrequently sending a few hundred bytes is acceptable in many constrained networks but sending a thousand bytes is not feasible in more constrained networks. Note that static keys often do not need to be sent over constrained links, as they can be provisioned or accessed over non-constrained links. Moreover, signatures can in many cases be replaced by a symmetrical MAC from an Ephemeral-Static or Static-Static key exchange by changing the architecture and protocols, as long as the proving node is online.

As several people asked me offline, here is a copy of the paper we submitted to NIST.

https://drive.google.com/file/d/1Vky_uA8DhJMGM-keHH-ujF23xG6stUXq

Cheers,

John

From: 'Edoardo Persichetti' via pqc-forum <pqc-forum@list.nist.gov>
Date: Thursday, 8 September 2022 at 23:49
To: Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu>
Cc: pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [Ext] [pqc-forum] Call for Additional Signatures is released

Thanks Uri, this is very accurate :)

Best,

Edoardo

> On Sep 8, 2022, at 5:46 PM, Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu> wrote:
>
> > Hi all! I guess, for us designers, it would be great to have a more precise understanding of what are the ballparks and sizes discussed here, with reference for the various use cases, since the terms “large”, “short”, “slightly larger” and similar are very vague.

OK, for you designers: my “constrained” use case prefers

- signatures in ballpark of 1 Kbyte or less,
- public keys for KEM – in ballpark of 1.5 KB or less,
- public keys for signature – within a couple of KB, if over-the-air exchange of intermediate CA certificates required – less than 2 KB.

Performance for signature:

- fast verification is a-must,
- fast signing is preferred,
- fast keygen is not that critical.

Performance for KEM: everything must be fast.

Hope this helps.

TNX

> On Sep 7, 2022, at 5:42 PM, Bo Lin <crypto.sec@outlook.com> wrote:
>
> > **EXTERNAL EMAIL :**Exercise caution when responding, opening links, or opening attachments.
>
> Yes, totally agree! There are many applications that key size overweighs performance
>
> GetOutlook for iOS
>
> **From:**pqc-forum@list.nist.gov<pqc-forum@list.nist.gov> on behalf of Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu>
>
> **Sent:**Wednesday, September 7, 2022 12:49 pm
>
> **To:**pqc-forum <pqc-forum@list.nist.gov>
>
> **Subject:**Re: [Ext] [pqc-forum] Call for Additional Signatures is released
>
> Having a small-signature && fast-verification is**crucial**for constrained environments (that I’m often dealing with).
>
> I agree that a smaller signature at the cost of slightly larger public key would be a good compromise, at least for my use cases.
>
> Thanks!

--

V/R,

Uri

There are two ways to design a system. One is to make it so simple there are obviously no deficiencies.

The other is to make it so complex there are no obvious deficiencies.

- C. A. R. Hoare

From:'Bas Westerbaan' via pqc-forum <pqc-forum@list.nist.gov>
Reply-To: Bas Westerbaan <bas@cloudflare.com>
Date: Wednesday, September 7, 2022 at 07:25
To: Mike Ounsworth <Mike.Ounsworth@entrust.com>
Cc: Paul Hoffman <paul.hoffman@icann.org>, pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [Ext] [pqc-forum] Call for Additional Signatures is released

On Wed, Sep 7, 2022 at 12:22 AM 'Mike Ounsworth' via pqc-forum <pqc-forum@list.nist.gov> wrote:

> crt.sh shows that we're in the single-digit-billion certs in the index. If you were to download and integrity-check the entire thing on a regular basis, then I could see short signatures and fast verifications being a big deal.

I'd say having a small-signature&fast-verification scheme is a much bigger deal for the 2+ SCTs that are in every single leaf certificate on the web. Also it's nice for the signature in the intermediate certificate. There are not that many root CAs and CT logs, so having slightly larger public keys for those keypairs could be a worthwhile trade-off.

Best,

Bas

--

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 topqc-forum+unsubscribe@list.nist.gov.
To view this discussion on the web visithttps://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/CAMjbhoW%2B2EOTBfcLF0ERATw9GgmkQd-EPJh_-Y0uPnsSatiphA%40mail.gmail.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 topqc-forum+unsubscribe@list.nist.gov.
To view this discussion on the web visithttps://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/3139A267-51A2-402C-BE3D-65FED31B6E89%40ll.mit.edu.

--

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 topqc-forum+unsubscribe@list.nist.gov.
To view this discussion on the web visithttps://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/LO2P123MB36612BE22406EE5C8F3385A484419%40LO2P123MB3661.GBRP123.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/3199409D-8CFA-4CD3-B27A-511BC647ACA0%40fau.edu.

--

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/HE1PR0701MB30509C8666E8BABB0DC9B89489449%40HE1PR0701MB3050.eurprd07.prod.outlook.com.

From: Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu> via pqc-forum@list.nist.gov
To: John Mattsson <john.mattsson@ericsson.com>, pqc-forum <pqc-forum@list.nist.gov>
CC: Edoardo Persichetti <epersichetti@fau.edu>
Subject: Re: [Ext] [pqc-forum] Call for Additional Signatures is released
Date: Monday, September 12, 2022 01:54:16 PM ET
Attachments: smime.p7m

> Note that there are much more constrained networks than Uri's use case.

Please note that I've only listed my use case constraints, fully understanding that there are other more constrained applications.

> The world "constrained" can refer to systems with several orders of magniture difference in capabilities. While constrained devices has gotten quite a lot of attention, the radio is often the most constrained part.

Yes.

> Constrained radio networks are characterized by very small frame sizes on the order of tens of bytes transmitted a few times per day at ultra-low speeds, high latency, and severe duty cycles constraints. The number of different constrained radio network technologies is large and growing. Some examples of constrained network technologies are LoRaWAN, NB-IoT, Sigfox, Wi-SUN FAN, Bluetooth Low Energy, and IEEE 802.15.4. IEEE 802.15.4 is used in Zigbee, ISA100.11a, WirelessHART, MiWi, 6LoWPAN, 6TiSCH, Thread and SNAP. Low Power Wide Area Networks (LPWANs) is a huge and very quickly growing market expected to reach over 1000 billion USD globally by 2027.
>
> To work well in constrained radio networks, the message sizes need to align with the tens of bytes transmitted a few times per day that the networks are designed for. Infrequently sending a few hundred bytes is acceptable in many constrained networks but sending a thousand bytes is not feasible in more constrained networks.

I concur, and wonder what would be the PQ solution for those.

> Note that static keys often do not need to be sent over constrained links, as they can be provisioned or accessed over non-constrained links.

I disagree. **In some cases** the above is true. In others, like mine – decidedly not so. The only reasonable pre-provisioning in my case is for the known-in-advance CA certs.

I understand that there are others who can pre-provision static keys, in which case McEliece doesn't sound all that bad. 😉 \

Just don't start thinking that it's the "usual" case.

> Moreover, signatures can in many cases be replaced by a symmetrical MAC from an Ephemeral-Static or Static-Static key exchange by changing the architecture and protocols, as long as the proving node is online.

Yes. Tradeoff between how much to send, how often, and who to (including how many entities to talk with during this process).

> As several people asked me offline, here is a copy of the paper we submitted to NIST.
>
> https://drive.google.com/file/d/1Vky_uA8DhJMGM-keHH-ujF23xG6stUXq

Thank you! Let me read it and get back with questions, if any.

TNX

From: 'Edoardo Persichetti' via pqc-forum
Date: Thursday, 8 September 2022 at 23:49
To: Blumenthal, Uri - 0553 - MITLL
Cc: pqc-forum
Subject: Re: [Ext] [pqc-forum] Call for Additional Signatures is released

Thanks Uri, this is very accurate :)

Best,

Edoardo

> On Sep 8, 2022, at 5:46 PM, Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu> wrote:
>
> > Hi all! I guess, for us designers, it would be great to have a more precise understanding of what are the ballparks and sizes discussed here, with reference for the various use cases, since the terms "large", "short", "slightly larger" and similar are very vague.
>
> OK, for you designers: my "constrained" use case prefers
>
> ·signatures in ballpark of 1 Kbyte or less,
> ·public keys for KEM – in ballpark of 1.5 KB or less,

- public keys for signature – within a couple of KB, if over-the-air exchange of intermediate CA certificates required – less than 2 KB.

Performance for signature:

- fast verification is a-must,
- fast signing is preferred,
- fast keygen is not that critical.

Performance for KEM: everything must be fast.

Hope this helps.

TNX

> On Sep 7, 2022, at 5:42 PM, Bo Lin <crypto.sec@outlook.com> wrote:
>
> > **EXTERNAL EMAIL :**Exercise caution when responding, opening links, or opening attachments.
>
> Yes, totally agree! There are many applications that key size overweighs performance
>
> GetOutlook for iOS
>
> **From:**pqc-forum@list.nist.gov<pqc-forum@list.nist.gov> on behalf of Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu>
> **Sent:**Wednesday, September 7, 2022 12:49 pm
> **To:**pqc-forum <pqc-forum@list.nist.gov>
> **Subject:**Re: [Ext] [pqc-forum] Call for Additional Signatures is released
>
> Having a small-signature && fast-verification is**crucial**for constrained environments (that I'm often dealing with).
>
> I agree that a smaller signature at the cost of slightly larger public key would be a good compromise, at least for my use cases.
>
> Thanks!
>
> --
>
> V/R,

Uri

There are two ways to design a system. One is to make it so simple there are obviously no deficiencies.

The other is to make it so complex there are no obvious deficiencies.

- C. A. R. Hoare

From:'Bas Westerbaan' via pqc-forum <pqc-forum@list.nist.gov>
Reply-To: Bas Westerbaan <bas@cloudflare.com>
Date: Wednesday, September 7, 2022 at 07:25
To: Mike Ounsworth <Mike.Ounsworth@entrust.com>
Cc: Paul Hoffman <paul.hoffman@icann.org>, pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [Ext] [pqc-forum] Call for Additional Signatures is released

On Wed, Sep 7, 2022 at 12:22 AM 'Mike Ounsworth' via pqc-forum <pqc-forum@list.nist.gov> wrote:

> crt.sh shows that we're in the single-digit-billion certs in the index. If you were to download and integrity-check the entire thing on a regular basis, then I could see short signatures and fast verifications being a big deal.

I'd say having a small-signature&fast-verification scheme is a much bigger deal for the 2+ SCTs that are in every single leaf certificate on the web. Also it's nice for the signature in the intermediate certificate. There are not that many root CAs and CT logs, so having slightly larger public keys for those keypairs could be a worthwhile trade-off.

Best,

Bas

--
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 topqc-forum+unsubscribe@list.nist.gov.
> To view this discussion on the web visithttps://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/CAMjbhoW%2B2EOTBfcLF0ERATw9GgmkQd-EPJh_-Y0uPnsSatiphA%40mail.gmail.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 topqc-forum+unsubscribe@list.nist.gov.
> To view this discussion on the web visithttps://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/3139A267-51A2-402C-BE3D-65FED31B6E89%40ll.mit.edu.
>
> --
> 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 topqc-forum+unsubscribe@list.nist.gov.
> To view this discussion on the web visithttps://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/LO2P123MB36612BE22406EE5C8F3385A484419%40LO2P123MB3661.GBRP123.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/3199409D-8CFA-4CD3-B27A-511BC647ACA0%40fau.edu.

--
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/HE1PR0701MB30509C8666E8BABB0DC9B89489449%40HE1PR0701MB3050.eurprd07.prod.outlook.com.

--