From: John Mattsson <john.mattsson@ericsson.com> via pqc-forum <pqc-forum@list.nist.gov>
To: pqc-forum@list.nist.gov
Subject: [pqc-forum] OFFICIAL COMMENT: CRYSTALS-Dilithium
Date: Thursday, July 07, 2022 07:51:26 AM ET

Dear NIST,

The current specification of CRYSTALS-Dilithium provides two versions. One deterministic and one randomized. I strongly think NIST should also standardize a hedged version where the seed is derived from a random string, a key, and the message. The deterministic version is according to the specification not recommended in scenarios where an adversary can mount side-channel attacks. The randomized version is (I assume) not recommended in scenarios where the PRNG cannot be fully trusted. A hedged version could likely be made to protect against both side-channel attacks and weak PRNGs. The Dual_EC_DRBG story has thought us the importance of not blindly trusting the PRNG. Putting minimal trust in the PRNG and trying to minimize the impact of a compromised PRNG is an essential part of following zero trust principles. Having hedged signature was one of the most requested features in the comments on FIPS 186-5 (Draft).

Best Regards,

John Preuß Mattsson

From: Vadim Lyubashevsky <vadim1980@gmail.com> via pqc-forum@list.nist.gov
To: John Mattsson <john.mattsson@ericsson.com>, pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] OFFICIAL COMMENT: CRYSTALS-Dilithium
Date: Friday, July 08, 2022 05:48:03 AM ET

Hi John, all,

On Thu, 2022-07-07 at 11:50 +0000, 'John Mattsson' via pqc-forum wrote:

> Dear NIST,
>
> The current specification of CRYSTALS-Dilithium provides two versions. One deterministic and one randomized. I strongly think NIST should also standardize a hedged version where the seed is derived from a random string, a key, and the message.

The "hedged" version can simply replace the current randomized version which does not take the key and the message as inputs. Since the key is short and the message is already hashed anyway, including these two things in the seed creation will probably have a negligible performance effect.

If people think it's a good idea, it should be easy to incorporate and I suspect that it's better having just 2 versions of the algorithm instead of 3.

Best,

Vadim

From: Hanno Böck <hanno@hboeck.de> via pqc-forum@list.nist.gov
To: pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] OFFICIAL COMMENT: CRYSTALS-Dilithium
Date: Friday, July 08, 2022 06:38:15 AM ET

On Fri, 08 Jul 2022 11:47:30 +0200
Vadim Lyubashevsky <vadim1980@gmail.com> wrote:

> If people think it's a good idea, it should be easy to incorporate and
> I suspect that it's better having just 2 versions of the algorithm
> instead of 3.

Or just 1.
Please make one the default and don't spec several different versions
of the possibly major crypto algorithm of the future internet. I think
if we've learned one thing from past cryptography standards it's that
excess flexibility is almost always bad.
Provide as few options as possible.

--
Hanno Böck
https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fhboeck.de%2F&data=05%7C01%7Cyi-kai.liu%40nist.gov%7Ce5caecc9b4034239ba8c08da60cdf5b2%7C2ab5d82fd8fa4797a93e054655c61dec%7C1%7C0%7C637928734956225195%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=4Z4RP0WAJFi8pFt6qK8M6zX4Ae2mwHrIomk1bj8ux7M%3D&reserved=0

From: Taylor R Campbell <campbell+nist-pqc-forum@mumble.net> via Taylor R Campbell <campbell@mumble.net>
To: Vadim Lyubashevsky <vadim1980@gmail.com>
CC: John Mattsson <john.mattsson@ericsson.com>, pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] OFFICIAL COMMENT: CRYSTALS-Dilithium
Date: Friday, July 08, 2022 09:05:30 AM ET

> Date: Fri, 08 Jul 2022 11:47:30 +0200
> From: Vadim Lyubashevsky <vadim1980@gmail.com>
>
> On Thu, 2022-07-07 at 11:50 +0000, 'John Mattsson' via pqc-forum wrote:
> > The current specification of CRYSTALS-Dilithium provides two
> > versions. One deterministic and one randomized. I strongly think NIST
> > should also standardize a hedged version where the seed is derived
> > from a random string, a key, and the message.
>
> The "hedged" version can simply replace the current randomized version
> which does not take the key and the message as inputs. Since the key is
> short and the message is already hashed anyway, including these two
> things in the seed creation will probably have a negligible performance
> effect.
>
> If people think it's a good idea, it should be easy to incorporate and
> I suspect that it's better having just 2 versions of the algorithm
> instead of 3.

Don't have two or three versions -- have just one!

Signature creation should be defined to be a deterministic function of

1. secret key,
2. message, and
3. a randomization string.

Users can take advantage of this _single_ standard function for many purposes:

- Users can cheaply test implementations as black boxes against
  standard known-answer test vectors to verify that they are
  incorporating all of the inputs.

  Ignoring any one of the inputs in deriving rho' is invisible to
  verifiers, so interoperability tests will fail to detect such
  potentially security-destroying bugs -- even if the hard parts, the
  ring arithmetic and NTT, are formally verified and correct.

  For randomized signatures, even if the RNG you feed into signature
  creation has a broken entropy source (like Sony PlayStation 3), the
  implementation will still thwart cryptanalytic attacks by using a
  secret uniform random function of the message.

- Users can make deterministic signatures by setting the randomization
  string to something fixed in an application like the empty string.

- Users can cheaply mitigate fault attacks (or do anything else
  requiring randomized signatures) by feeding uniform random RNG
  output to signature creation as the randomization string. Everyone
  with access to a crypto API will have access to the RNG it would
  have used internally. No protocol changes are required for
  interoperability like transmitting an IV.

- Users can also _detect_ fault attacks at somewhat higher cost: use a
  randomized signature as above, but pick the randomization string
  once and then run the signature creation function twice with the
  same inputs and verify whether the output is the same.

This keeps the specification simple -- _one_ standard primitive
signature creation function -- and cheaply enables defences against
several different threat models: interoperable implementation bugs
outside the hard parts, cryptanalytic attacks against predictable or
reused per-signature secrets with a broken RNG, fault attacks.

--

From: John Mattsson <john.mattsson@ericsson.com> via pqc-forum <pqc-forum@list.nist.gov>
To: Hanno Böck <hanno@hboeck.de>, pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] OFFICIAL COMMENT: CRYSTALS-Dilithium
Date: Friday, July 08, 2022 12:30:34 PM ET

Vadim Lyubashevsky wrote:

> The "hedged" version can simply replace the current randomized version

I think that is a great idea.

Hanno Böck wrote:

>Please make one the default and don't spec several different versions
>of the possibly major crypto algorithm of the future internet. I think
>if we've learned one thing from past cryptography standards it's that
>excess flexibility is almost always bad.

I think there are strong reasons to have a deterministic implementation option. That enables testing which might otherwise be impossible. If the signature algorithm is implemented in a black box like an HSM, any randomized version (also hedged) implies blind trust in the HSM vendor. A deterministic version allows the user to verify that the HSM follows the specification and does not leak the private key by using bad randomness (I don't know if that is the consequence in Dilithium, but it is in ECDSA). National states have in the past controlled cryptographic hardware manufacturers like the Swiss company Crypto AG and intentionally weakened the products. Putting minimal trust in the HSM manufacturer is an essential part of following zero trust principles.

Note that the "versions" that are discussed would be the same algorithm from a protocol perspective. The verifier stays the same. The "versions" are just implementation choices for the signer.

Cheers,

John

From: pqc-forum@list.nist.gov <pqc-forum@list.nist.gov> on behalf of Hanno Böck <hanno@hboeck.de>
Date: Friday, 8 July 2022 at 12:38

To: pqc-forum@list.nist.gov <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] OFFICIAL COMMENT: CRYSTALS-Dilithium

On Fri, 08 Jul 2022 11:47:30 +0200
Vadim Lyubashevsky <vadim1980@gmail.com> wrote:

> If people think it's a good idea, it should be easy to incorporate and
> I suspect that it's better having just 2 versions of the algorithm
> instead of 3.

Or just 1.
Please make one the default and don't spec several different versions
of the possibly major crypto algorithm of the future internet. I think
if we've learned one thing from past cryptography standards it's that
excess flexibility is almost always bad.
Provide as few options as possible.

--
Hanno Böck
https://protect2.fireeye.com/v1/url?k=31323334-501d5122-313273af-454445555731-92357668b9c0e739&q=1&e=68f2c4c0-896f-42e1-b043-5663c2850e2e&u=https%3A%2F%2Fhboeck.de%2F

From: Scott Fluhrer (sfluhrer) <sfluhrer@cisco.com> via pqc-forum <pqc-forum@list.nist.gov>
To: John Mattsson <john.mattsson@ericsson.com>, Hanno Böck <hanno@hboeck.de>, pqc-forum@list.nist.gov
Subject: RE: [pqc-forum] OFFICIAL COMMENT: CRYSTALS-Dilithium
Date: Friday, July 08, 2022 02:11:36 PM ET

On the other hand, requiring only the 'hedged' version would mean that an implementation must do two passes over the message to be signed. This can be a practical issue; for example, if an HSM is signing a large message, it can't hold the entire message internally, which means it must be fed the message twice.

You can, of course, get around this by hashing the message first (possibly external to the HSM), and then Dilithium signing the hash; however, that is obviously not transparent to the verifier; would it be appropriate to mandate that? The answer may be "yes"; I'm just pointing out the question…

> **From:** 'John Mattsson' via pqc-forum <pqc-forum@list.nist.gov>
> **Sent:** Friday, July 8, 2022 12:30 PM
> **To:** Hanno Böck <hanno@hboeck.de>; pqc-forum@list.nist.gov
> **Subject:** Re: [pqc-forum] OFFICIAL COMMENT: CRYSTALS-Dilithium
>
> Vadim Lyubashevsky wrote:
>
> > The "hedged" version can simply replace the current randomized version
>
> I think that is a great idea.
>
> Hanno Böck wrote:
>
> >Please make one the default and don't spec several different versions
> >of the possibly major crypto algorithm of the future internet. I think
> >if we've learned one thing from past cryptography standards it's that
> >excess flexibility is almost always bad.
>
> I think there are strong reasons to have a deterministic implementation option. That enables testing which might otherwise be impossible. If the signature algorithm is implemented in a black box like an HSM, any randomized version (also hedged) implies blind trust in the HSM vendor. A deterministic version allows the user to verify that the HSM follows the specification and does not leak the private key by using bad

randomness (I don't know if that is the consequence in Dilithium, but it is in ECDSA). National states have in the past controlled cryptographic hardware manufacturers like the Swiss company Crypto AG and intentionally weakened the products. Putting minimal trust in the HSM manufacturer is an essential part of following zero trust principles.

Note that the ”versions” that are discussed would be the same algorithm from a protocol perspective. The verifier stays the same. The “versions” are just implementation choices for the signer.

Cheers,

John

From: pqc-forum@list.nist.gov <pqc-forum@list.nist.gov> on behalf of Hanno Böck <hanno@hboeck.de>
Date: Friday, 8 July 2022 at 12:38
To: pqc-forum@list.nist.gov <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] OFFICIAL COMMENT: CRYSTALS-Dilithium

On Fri, 08 Jul 2022 11:47:30 +0200
Vadim Lyubashevsky <vadim1980@gmail.com> wrote:

> If people think it's a good idea, it should be easy to incorporate and
> I suspect that it's better having just 2 versions of the algorithm
> instead of 3.

Or just 1.
Please make one the default and don't spec several different versions
of the possibly major crypto algorithm of the future internet. I think
if we've learned one thing from past cryptography standards it's that
excess flexibility is almost always bad.
Provide as few options as possible.

--
Hanno Böck
https://protect2.fireeye.com/v1/url?k=31323334-501d5122-313273af-454445555731-92357668b9c0e739&q=1&e=68f2c4c0-896f-42e1-b043-5663c2850e2e&u=https%3A%2F%2Fhboeck.de%2F

--
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://protect2.fireeye.com/v1/url?k=31323334-501d5122-313273af-454445555731-286a1b795108b884&q=1&e=68f2c4c0-896f-42e1-b043-5663c2850e2e&u=https%3A%2F%2Fgroups.google.com%2Fa%2Flist.nist.gov%2Fd%2Fmsgid%2Fpqc-forum%2F20220708123712.47fa7569%2540computer.

--
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/DB6PR0701MB3047E7AE2489938E5048CDD689829%40DB6PR0701MB3047.eurprd07.prod.outlook.com.

From: Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu> via pqc-forum@list.nist.gov
To: Scott Fluhrer (sfluhrer) <sfluhrer@cisco.com>, pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] OFFICIAL COMMENT: CRYSTALS-Dilithium
Date: Friday, July 08, 2022 02:30:50 PM ET
Attachments: smime.p7m

> On the other hand, requiring only the 'hedged' version would mean that an implementation

> must do two passes over the message to be signed.

I'm not sure it's true, considering that every sane email or document signer (that I'm aware of) signs the hash, rather than the document itself.

> This can be a practical issue; for example, if an HSM is signing a large message, it

> can't hold the entire message internally, which means it must be fed the message twice.

>

> You can, of course, get around this by hashing the message first (possibly external to the HSM),

> and then Dilithium signing the hash; however, that is obviously not transparent to the verifier;

> would it be appropriate to mandate that? The answer may be "yes"; I'm just pointing out the question...

In my understanding, this has been de-facto standard for a long time. Thus, IMHO, it is perfectly appropriate to (explicitly) mandate it.

Thanks!

From: 'John Mattsson' via pqc-forum
Sent: Friday, July 8, 2022 12:30 PM
To: Hanno Böck ; pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] OFFICIAL COMMENT: CRYSTALS-Dilithium

Vadim Lyubashevsky wrote:

> The "hedged" version can simply replace the current randomized version

I think that is a great idea.

Hanno Böck wrote:

>Please make one the default and don't spec several different versions
>of the possibly major crypto algorithm of the future internet. I think
>if we've learned one thing from past cryptography standards it's that
>excess flexibility is almost always bad.

I think there are strong reasons to have a deterministic implementation option. That enables testing which might otherwise be impossible. If the signature algorithm is implemented in a black box like an HSM, any randomized version (also hedged) implies blind trust in the HSM vendor. A deterministic version allows the user to verify that the HSM follows the specification and does not leak the private key by using bad randomness (I don't know if that is the consequence in Dilithium, but it is in ECDSA). National states have in the past controlled cryptographic hardware manufacturers like the Swiss company Crypto AG and intentionally weakened the products. Putting minimal trust in the HSM manufacturer is an essential part of following zero trust principles.

Note that the "versions" that are discussed would be the same algorithm from a protocol perspective. The verifier stays the same. The "versions" are just implementation choices for the signer.

Cheers,

John

From: pqc-forum@list.nist.gov <pqc-forum@list.nist.gov> on behalf of Hanno Böck <hanno@hboeck.de>
Date: Friday, 8 July 2022 at 12:38
To: pqc-forum@list.nist.gov <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] OFFICIAL COMMENT: CRYSTALS-Dilithium

On Fri, 08 Jul 2022 11:47:30 +0200
Vadim Lyubashevsky <vadim1980@gmail.com> wrote:

> If people think it's a good idea, it should be easy to incorporate and
> I suspect that it's better having just 2 versions of the algorithm
> instead of 3.

Or just 1.
Please make one the default and don't spec several different versions of the possibly major crypto algorithm of the future internet. I think if we've learned one thing from past cryptography standards it's that excess flexibility is almost always bad.
Provide as few options as possible.

--
Hanno Böck
https://protect2.fireeye.com/v1/url?k=31323334-501d5122-313273af-454445555731-92357668b9c0e739&q=1&e=68f2c4c0-896f-42e1-b043-5663c2850e2e&u=https%3A%2F%2Fhboeck.de%2F

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/CH0PR11MB54441756530D08538099094AC1829%40CH0PR11MB5444.namprd11.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/806BC870-E868-4A0B-AEEA-0CF912E530F1%40ll.mit.edu.

From: Vadim Lyubashevsky <vadim.lyubash@gmail.com> via pqc-forum@list.nist.gov
To: Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu>
CC: Scott Fluhrer (sfluhrer) <sfluhrer@cisco.com>, pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] OFFICIAL COMMENT: CRYSTALS-Dilithium
Date: Friday, July 08, 2022 02:38:13 PM ET

On Fri, Jul 8, 2022 at 8:30 PM Blumenthal, Uri - 0553 - MITLL
<uri@ll.mit.edu> wrote:
>
> > On the other hand, requiring only the ‘hedged’ version would mean that an
implementation
>
> > must do two passes over the message to be signed.
>
>
>
> I’m not sure it’s true, considering that every sane email or document signer (that
I’m aware of) signs the hash, rather than the document itself.

And even if it is not hashed, the Dilithium signing algorithm hashes
the message right away and then never touches the actual message
again. So I am not seeing why one would go over the message twice in
any scenario. Just to be clear, the "hedged" mode would replace line
12 of Figure 4 in the dilithium spec with rho'=H(K | seed | mu) where
seed is either "" in the deterministic case or a random 512-bit
string in the randomized one.

Best,
Vadim

>
>
>
> > This can be a practical issue; for example, if an HSM is signing a large message,
it
>

> > can’t hold the entire message internally, which means it must be fed the message twice.
>
> >
>
> > You can, of course, get around this by hashing the message first (possibly external to the HSM),
>
> > and then Dilithium signing the hash; however, that is obviously not transparent to the verifier;
>
> > would it be appropriate to mandate that? The answer may be “yes”; I’m just pointing out the question…
>
>
>
> In my understanding, this has been de-facto standard for a long time. Thus, IMHO, it is perfectly appropriate to (explicitly) mandate it.
>
>
>
> Thanks!
>
>
>
>
>
> From: 'John Mattsson' via pqc-forum <pqc-forum@list.nist.gov>
> Sent: Friday, July 8, 2022 12:30 PM
> To: Hanno Böck <hanno@hboeck.de>; pqc-forum@list.nist.gov
> Subject: Re: [pqc-forum] OFFICIAL COMMENT: CRYSTALS-Dilithium
>
>
>
> Vadim Lyubashevsky wrote:
>
> > The "hedged" version can simply replace the current randomized version
>

>
>
> I think that is a great idea.
>
>
>
> Hanno Böck wrote:
>
> >Please make one the default and don't spec several different versions
> >of the possibly major crypto algorithm of the future internet. I think
> >if we've learned one thing from past cryptography standards it's that
> >excess flexibility is almost always bad.
>
>
>
> I think there are strong reasons to have a deterministic implementation option. That enables testing which might otherwise be impossible. If the signature algorithm is implemented in a black box like an HSM, any randomized version (also hedged) implies blind trust in the HSM vendor. A deterministic version allows the user to verify that the HSM follows the specification and does not leak the private key by using bad randomness (I don’t know if that is the consequence in Dilithium, but it is in ECDSA). National states have in the past controlled cryptographic hardware manufacturers like the Swiss company Crypto AG and intentionally weakened the products. Putting minimal trust in the HSM manufacturer is an essential part of following zero trust principles.
>
>
>
> Note that the ”versions” that are discussed would be the same algorithm from a protocol perspective. The verifier stays the same. The “versions” are just implementation choices for the signer.
>
>
>
> Cheers,
>
> John
>

>
>
> From: pqc-forum@list.nist.gov <pqc-forum@list.nist.gov> on behalf of Hanno Böck <hanno@hboeck.de>
> Date: Friday, 8 July 2022 at 12:38
> To: pqc-forum@list.nist.gov <pqc-forum@list.nist.gov>
> Subject: Re: [pqc-forum] OFFICIAL COMMENT: CRYSTALS-Dilithium
>
> On Fri, 08 Jul 2022 11:47:30 +0200
> Vadim Lyubashevsky <vadim1980@gmail.com> wrote:
>
> > If people think it's a good idea, it should be easy to incorporate and
> > I suspect that it's better having just 2 versions of the algorithm
> > instead of 3.
>
> Or just 1.
> Please make one the default and don't spec several different versions
> of the possibly major crypto algorithm of the future internet. I think
> if we've learned one thing from past cryptography standards it's that
> excess flexibility is almost always bad.
> Provide as few options as possible.
>
> --
> Hanno Böck
> https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fprotect2.fireeye.com%2Fv1%2Furl%3Fk%3D31323334-501d5122-313273af-454445555731-92357668b9c0e739%26q%3D1%26e%3D68f2c4c0-896f-42e1-b043-5663c2850e2e%26u%3Dhttps%253A%252F%252Fhboeck.de%252F&data=05%7C01%7Cyi-kai.liu%40nist.gov%7C8f7706a9f985446608d308da6111022a%7C2ab5d82fd8fa4797a93e054655c61dec%7C1%7C0%7C637929022929564345%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=PrsaZZ6eR4GVMzRcbvOTnUSh2oxgAzW9n8m%2Be6xggBg%3D&reserved=0
>
> --
> 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://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fprotect2.fireeye.com%2Fv1%2Furl%3Fk%3D31323334-501d5122-313273af-454445555731-286a1b795108b884%26q%3D1%26e%3D68f2c4c0-896f-42e1-b043-5663c2850e2e%26u%3Dhttps%253A%252F%252Fgroups.google.com%252Fa%252Flist.nist.gov%252Fd%252Fmsgid%252Fpqc-forum%252F20220708123712.47fa7569%252540computer&data=05%7C01%7Cyi-kai.liu%40nist.gov%7C8f7706a9f985446608d308da6111022a%7C2ab5d82fd8fa4797a93e054655c61dec%7C1%7C0%7C637929022929564345%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=dODgayak%2F57jsjWOGU6UE%2BtZof4YGuIu7qvL8AmljrQ%3D&reserved=0.
>
> --
> 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/DB6PR0701MB3047E7AE2489938E5048CDD689829%40DB6PR0701MB3047.eurprd07.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/CH0PR11MB54441756530D08538099094AC1829%40CH0PR11MB5444.namprd11.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/806BC870-E868-4A0B-AEEA-0CF912E530F1%40ll.mit.edu.

--

From: Scott Fluhrer (sfluhrer) <sfluhrer@cisco.com> via pqc-forum <pqc-forum@list.nist.gov>
To: Vadim Lyubashevsky <vadim.lyubash@gmail.com>, Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu>
CC: pqc-forum@list.nist.gov
Subject: RE: [pqc-forum] OFFICIAL COMMENT: CRYSTALS-Dilithium
Date: Friday, July 08, 2022 02:44:13 PM ET

Hmmm, sorry, I believe I misunderstood what the 'hedged' proposal was -- nevermind...

-----Original Message-----
From: pqc-forum@list.nist.gov <pqc-forum@list.nist.gov> On Behalf Of Vadim Lyubashevsky
Sent: Friday, July 8, 2022 2:37 PM
To: Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu>
Cc: Scott Fluhrer (sfluhrer) <sfluhrer@cisco.com>; pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] OFFICIAL COMMENT: CRYSTALS-Dilithium

On Fri, Jul 8, 2022 at 8:30 PM Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu> wrote:
>
> > On the other hand, requiring only the ‘hedged’ version would mean
> > that an implementation
>
> > must do two passes over the message to be signed.
>
>
>
> I’m not sure it’s true, considering that every sane email or document signer (that I’m aware of) signs the hash, rather than the document itself.

And even if it is not hashed, the Dilithium signing algorithm hashes the message right away and then never touches the actual message again. So I am not seeing why one would go over the message twice in any scenario. Just to be clear, the "hedged" mode would replace line
12 of Figure 4 in the dilithium spec with rho'=H(K | seed | mu) where seed is either "" in the deterministic case or a random 512-bit string in the randomized one.

Best,
Vadim

>
>
>
> > This can be a practical issue; for example, if an HSM is signing a
> > large message, it
>
> > can’t hold the entire message internally, which means it must be fed the message twice.
>
> >
>
> > You can, of course, get around this by hashing the message first
> > (possibly external to the HSM),
>
> > and then Dilithium signing the hash; however, that is obviously not
> > transparent to the verifier;
>
> > would it be appropriate to mandate that? The answer may be “yes”;
> > I’m just pointing out the question…
>
>
>
> In my understanding, this has been de-facto standard for a long time. Thus, IMHO, it is perfectly appropriate to (explicitly) mandate it.
>
>
>
> Thanks!
>
>
>
>
>
> From: 'John Mattsson' via pqc-forum <pqc-forum@list.nist.gov>

> Sent: Friday, July 8, 2022 12:30 PM
> To: Hanno Böck <hanno@hboeck.de>; pqc-forum@list.nist.gov
> Subject: Re: [pqc-forum] OFFICIAL COMMENT: CRYSTALS-Dilithium
>
>
>
> Vadim Lyubashevsky wrote:
>
> > The "hedged" version can simply replace the current randomized
> > version
>
>
>
> I think that is a great idea.
>
>
>
> Hanno Böck wrote:
>
> >Please make one the default and don't spec several different versions
> >of the possibly major crypto algorithm of the future internet. I
> >think if we've learned one thing from past cryptography standards
> >it's that excess flexibility is almost always bad.
>
>
>
> I think there are strong reasons to have a deterministic implementation option. That enables testing which might otherwise be impossible. If the signature algorithm is implemented in a black box like an HSM, any randomized version (also hedged) implies blind trust in the HSM vendor. A deterministic version allows the user to verify that the HSM follows the specification and does not leak the private key by using bad randomness (I don’t know if that is the consequence in Dilithium, but it is in ECDSA). National states have in the past controlled cryptographic hardware manufacturers like the Swiss company Crypto AG and intentionally weakened the products. Putting minimal trust in the HSM manufacturer is an essential part of following zero trust principles.
>
>

>
> Note that the ”versions” that are discussed would be the same algorithm from a protocol perspective. The verifier stays the same. The “versions” are just implementation choices for the signer.
>
>
>
> Cheers,
>
> John
>
>
>
> From: pqc-forum@list.nist.gov <pqc-forum@list.nist.gov> on behalf of
> Hanno Böck <hanno@hboeck.de>
> Date: Friday, 8 July 2022 at 12:38
> To: pqc-forum@list.nist.gov <pqc-forum@list.nist.gov>
> Subject: Re: [pqc-forum] OFFICIAL COMMENT: CRYSTALS-Dilithium
>
> On Fri, 08 Jul 2022 11:47:30 +0200
> Vadim Lyubashevsky <vadim1980@gmail.com> wrote:
>
> > > If people think it's a good idea, it should be easy to incorporate
> > > and I suspect that it's better having just 2 versions of the
> > > algorithm instead of 3.
>
> Or just 1.
> Please make one the default and don't spec several different versions
> of the possibly major crypto algorithm of the future internet. I think
> if we've learned one thing from past cryptography standards it's that
> excess flexibility is almost always bad.
> Provide as few options as possible.
>
> --
> Hanno Böck

> https://gcc02.safelinks.protection.outlook.com/?
url=https%3A%2F%2Fprotect2.fireeye.com%2Fv1%2Furl%3Fk%3D31323334-501d5122-313273af-45
444&data=05%7C01%7Cyi-
kai.liu%40nist.gov%7C9a76f6b3d9aa4c53df1c08da6111d8d1%7C2ab5d82fd8fa4797a93e054655c61
dec%7C1%7C0%7C637929026531798396%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoi
V2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=bZsM0lnfcTYVa9neWReo
Wik47MUPwjaJ%2FXtmfX%2BAa1I%3D&reserved=0
> 5555731-92357668b9c0e739&q=1&e=68f2c4c0-896f-42e1-b043-5663c2850e2e&u=
> https%3A%2F%2Fhboeck.de%2F
>
> --
> 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://
gcc02.safelinks.protection.outlook.com/?
url=https%3A%2F%2Fprotect2.fireeye.com%2Fv1%2Furl%3Fk%3D31323334-501d5122-313273af-45
4445555731-286a1b795108b884%26q%3D1%26e%3D68f2c4c0-896f-42e1-
b043-5663c2850e2e%26u%3Dhttps%253A%252F%252Fgroups.google.com%252Fa%252Flist.nist.gov
%252Fd%252Fmsgid%252Fpqc-
forum%252F20220708123712.47fa7569%252540computer&data=05%7C01%7Cyi-
kai.liu%40nist.gov%7C9a76f6b3d9aa4c53df1c08da6111d8d1%7C2ab5d82fd8fa4797a93e054655c61
dec%7C1%7C0%7C637929026531798396%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoi
V2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=OB5FBFDdWlwrQoHfUz9H
qrKUgakGKYPiULecaulO4qU%3D&reserved=0.
>
> --
> 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/
DB6PR0701MB3047E7AE2489938E5048CDD689829%40DB6PR0701MB3047.eurprd07.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/CH0PR11MB54441756530D08538099094AC1829%40CH0PR11MB5444.namprd11.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/806BC870-E868-4A0B-AEEA-0CF912E530F1%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/CAE158z-09Kw06nufY_iOJm%3D2XCAudGyyi-3fkOB6bONd-AHGeg%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/CH0PR11MB5444251D54984DBC3FC0236BC1829%40CH0PR11MB5444.namprd11.prod.outlook.com.

From: John Mattsson <john.mattsson@ericsson.com> via pqc-forum <pqc-forum@list.nist.gov>
To: Vadim Lyubashevsky <vadim.lyubash@gmail.com>, Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu>
CC: Scott Fluhrer (sfluhrer) <sfluhrer@cisco.com>, pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] OFFICIAL COMMENT: CRYSTALS-Dilithium
Date: Friday, July 08, 2022 03:18:01 PM ET

>Just to be clear, the "hedged" mode would replace line
>12 of Figure 4 in the dilithium spec with rho'=H(K | seed | mu) where
>seed is either "" in the deterministic case or a random 512-bit
>string in the randomized one.

Another benefit with this construction is that it decreases the chance for implementation mistakes like the infamous PS3 bug where the software signing used ECDSA with a fixed number instead of a per-message random number.

John

From: pqc-forum@list.nist.gov <pqc-forum@list.nist.gov> on behalf of Vadim Lyubashevsky <vadim.lyubash@gmail.com>
Date: Friday, 8 July 2022 at 20:38
To: Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu>
Cc: Scott Fluhrer (sfluhrer) <sfluhrer@cisco.com>, pqc-forum@list.nist.gov <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] OFFICIAL COMMENT: CRYSTALS-Dilithium

On Fri, Jul 8, 2022 at 8:30 PM Blumenthal, Uri - 0553 - MITLL
<uri@ll.mit.edu> wrote:
>
> > On the other hand, requiring only the ‘hedged’ version would mean that an implementation
>
> > must do two passes over the message to be signed.
>
>
>
> I’m not sure it’s true, considering that every sane email or document signer (that I’m aware of) signs the hash, rather than the document itself.

And even if it is not hashed, the Dilithium signing algorithm hashes the message right away and then never touches the actual message again. So I am not seeing why one would go over the message twice in any scenario. Just to be clear, the "hedged" mode would replace line 12 of Figure 4 in the dilithium spec with rho'=H(K | seed | mu) where seed is either "" in the deterministic case or a random 512-bit string in the randomized one.

Best,
Vadim

>
>
>
> > This can be a practical issue; for example, if an HSM is signing a large message, it
>
> > can’t hold the entire message internally, which means it must be fed the message twice.
>
> >
>
> > You can, of course, get around this by hashing the message first (possibly external to the HSM),
>
> > and then Dilithium signing the hash; however, that is obviously not transparent to the verifier;
>
> > would it be appropriate to mandate that? The answer may be “yes”; I’m just pointing out the question…
>
>
>
> In my understanding, this has been de-facto standard for a long time. Thus, IMHO, it is perfectly appropriate to (explicitly) mandate it.
>
>
>
> Thanks!

>
>
>
>
>
> From: 'John Mattsson' via pqc-forum <pqc-forum@list.nist.gov>
> Sent: Friday, July 8, 2022 12:30 PM
> To: Hanno Böck <hanno@hboeck.de>; pqc-forum@list.nist.gov
> Subject: Re: [pqc-forum] OFFICIAL COMMENT: CRYSTALS-Dilithium
>
>
>
> Vadim Lyubashevsky wrote:
>
> > The "hedged" version can simply replace the current randomized version
>
>
>
> I think that is a great idea.
>
>
>
> Hanno Böck wrote:
>
> >Please make one the default and don't spec several different versions
> >of the possibly major crypto algorithm of the future internet. I think
> >if we've learned one thing from past cryptography standards it's that
> >excess flexibility is almost always bad.
>
>
>
> I think there are strong reasons to have a deterministic implementation option. That enables testing which might otherwise be impossible. If the signature algorithm is implemented in a black box like an HSM, any randomized version (also hedged) implies blind trust in the HSM vendor. A deterministic version allows the user to verify that the HSM follows the specification and does not leak the private key by using bad randomness (I don’t know if that is the consequence in Dilithium, but it is in ECDSA). National states have in the past controlled cryptographic hardware manufacturers like the Swiss

company Crypto AG and intentionally weakened the products. Putting minimal trust in the HSM manufacturer is an essential part of following zero trust principles.

>
>
>
> Note that the ”versions” that are discussed would be the same algorithm from a protocol perspective. The verifier stays the same. The “versions” are just implementation choices for the signer.
>
>
>
> Cheers,
>
> John
>
>
>
> From: pqc-forum@list.nist.gov <pqc-forum@list.nist.gov> on behalf of Hanno Böck <hanno@hboeck.de>
> Date: Friday, 8 July 2022 at 12:38
> To: pqc-forum@list.nist.gov <pqc-forum@list.nist.gov>
> Subject: Re: [pqc-forum] OFFICIAL COMMENT: CRYSTALS-Dilithium
>
> On Fri, 08 Jul 2022 11:47:30 +0200
> Vadim Lyubashevsky <vadim1980@gmail.com> wrote:
>
> > > If people think it's a good idea, it should be easy to incorporate and
> > > I suspect that it's better having just 2 versions of the algorithm
> > > instead of 3.
>
> Or just 1.
> Please make one the default and don't spec several different versions
> of the possibly major crypto algorithm of the future internet. I think
> if we've learned one thing from past cryptography standards it's that
> excess flexibility is almost always bad.
> Provide as few options as possible.
>
> --

> Hanno Böck
> https://protect2.fireeye.com/v1/url?k=31323334-501d5122-313273af-454445555731-92357668b9c0e739&q=1&e=68f2c4c0-896f-42e1-b043-5663c2850e2e&u=https%3A%2F%2Fhboeck.de%2F
>
> --
> 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://protect2.fireeye.com/v1/url?k=31323334-501d5122-313273af-454445555731-286a1b795108b884&q=1&e=68f2c4c0-896f-42e1-b043-5663c2850e2e&u=https%3A%2F%2Fgroups.google.com%2Fa%2Flist.nist.gov%2Fd%2Fmsgid%2Fpqc-forum%2F20220708123712.47fa7569%2540computer.
>
> --
> 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://protect2.fireeye.com/v1/url?k=31323334-501cfaf3-313273af-454445554331-5cfaa1bc14fcaf0c&q=1&e=7d54690e-fff4-4895-a827-251fec8e42c2&u=https%3A%2F%2Fgroups.google.com%2Fa%2Flist.nist.gov%2Fd%2Fmsgid%2Fpqc-forum%2FDB6PR0701MB3047E7AE2489938E5048CDD689829%2540DB6PR0701MB3047.eurprd07.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://protect2.fireeye.com/v1/url?k=31323334-501cfaf3-313273af-454445554331-6e2b4d92811927c0&q=1&e=7d54690e-fff4-4895-a827-251fec8e42c2&u=https%3A%2F%2Fgroups.google.com%2Fa%2Flist.nist.gov%2Fd%2Fmsgid%2Fpqc-forum%2FCH0PR11MB54441756530D08538099094AC1829%2540CH0PR11MB5444.namprd11.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://protect2.fireeye.com/v1/url?k=31323334-501cfaf3-313273af-454445554331-7ee4af837dd02ec3&q=1&e=7d54690e-fff4-4895-a827-251fec8e42c2&u=https%3A%2F%2Fgroups.google.com%2Fa%2Flist.nist.gov%2Fd%2Fmsgid%2Fpqc-forum%2F806BC870-E868-4A0B-AEEA-0CF912E530F1%2540ll.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://protect2.fireeye.com/v1/url?k=31323334-501cfaf3-313273af-454445554331-6d736be5ec352407&q=1&e=7d54690e-fff4-4895-a827-251fec8e42c2&u=https%3A%2F%2Fgroups.google.com%2Fa%2Flist.nist.gov%2Fd%2Fmsgid%2Fpqc-forum%2FCAE158z-09Kw06nufY_iOJm%253D2XCAudGyyi-3fkOB6bONd-AHGeg%2540mail.gmail.com.