From: Sydney Antonov <ska84@protonmail.com> via pqc-forum <pqc-forum@list.nist.gov>
To: pqc-forum@list.nist.gov
Subject: [pqc-forum] Survey: conservative KEMs for long-term secrecy
Date: Tuesday, August 09, 2022 05:09:57 PM ET

Dear forum,

What are your personal opinions on what KEM(s) and parameters should be used when high confidence in long-term secrecy is desired? And do you have any opinions on hybrids with ECC and hybrids with multiple post-quantum KEMs?

Sydney

From: Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu> via pqc-forum@list.nist.gov
To: Sydney Antonov <ska84@protonmail.com>
CC: pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] Survey: conservative KEMs for long-term secrecy
Date: Tuesday, August 09, 2022 05:28:22 PM ET
Attachments: smime.p7m

The only outcome that could justify Hybrid is if all of the following become true:

A. Crypto-Relevant Quantum Computer doesn't materialize; and

B. PQ algorithms selected get broken by Classic (not Quantum!) attacks; and

C. Classic algorithms selected do not get broken by Classic attacks.

I do not consider this possibility likely. Some Classic algorithms turned out broken, some are surviving so far. Some PQ algorithms got broken, some are surviving - Lattice-based approach has been around for more than 25 years already, "mature enough" in my book. ECC was "younger" than that when it was embraced, and nobody insisted that it should be, e.g., "paired with RSA because we aren't 100% sure ECC would hold".

My $0.05.

Regards,
Uri

> On Aug 9, 2022, at 17:10, 'Sydney Antonov' via pqc-forum wrote:
>
> Dear forum,
>
> What are your personal opinions on what KEM(s) and parameters should be used when high confidence in long-term secrecy is desired? And do you have any opinions on hybrids with ECC and hybrids with multiple post-quantum KEMs?
>
> Sydney

> --
> 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/qXiNVwauaRcfw9x2_A4iQcm1zTqjLkw_GkdPyOy-GTkunq0SYu56tqAIlIbnxqy1aF6zrhFHYy-ICntLheWtaAmi98eKhTnXbpEYl5lYSlU%3D%40protonmail.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/5D4E282C-6294-47ED-AB60-F6CC6316E388%40ll.mit.edu.

From: Mike Ounsworth <mike.ounsworth@entrust.com> via pqc-forum <pqc-forum@list.nist.gov>
To: Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu>, Sydney Antonov <ska84@protonmail.com>
CC: pqc-forum@list.nist.gov
Subject: RE: [pqc-forum] Survey: conservative KEMs for long-term secrecy
Date: Tuesday, August 09, 2022 05:39:05 PM ET

Sydney,

“Is hybrid useful?” is probably the most contentious PQ-related issue in this community You have opened this can of worms again. :/

Uri,

Your analysis below ignores the possibility of implementation bugs in the new PQ stuff.

We recently added a section “Value proposition of hybrid / composite schemes” to our composite draft (see github because it’s not up on datatracker yet)

https://github.com/EntrustCorporation/draft-ounsworth-pq-composite-keys/blob/master/draft-ounsworth-pq-composite-keys.txt#L247

I would be interested in your rebuttal to our analysis above.

—
Mike Ounsworth

From: pqc-forum@list.nist.gov <pqc-forum@list.nist.gov> On Behalf Of Blumenthal, Uri - 0553 - MITLL
Sent: August 9, 2022 4:28 PM
To: Sydney Antonov <ska84@protonmail.com>
Cc: pqc-forum@list.nist.gov
Subject: [EXTERNAL] Re: [pqc-forum] Survey: conservative KEMs for long-term secrecy

WARNING: This email originated outside of Entrust.

DO NOT CLICK links or attachments unless you trust the sender and know the content is safe.

The only outcome that could justify Hybrid is if all of the following become true:

A. Crypto-Relevant Quantum Computer doesn’t materialize; and
B. PQ algorithms selected get broken by Classic (not Quantum!) attacks; and
C. Classic algorithms selected do not get broken by Classic attacks.

I do not consider this possibility likely. Some Classic algorithms turned out broken, some are surviving so far. Some PQ algorithms got broken, some are surviving - Lattice-based approach has been around for more than 25 years already, “mature enough” in my book. ECC was “younger” than that when it was embraced, and nobody insisted that it should be, e.g., “paired with RSA because we aren’t 100% sure ECC would hold”.

My $0.05.
Regards,
Uri

On Aug 9, 2022, at 17:10, 'Sydney Antonov' via pqc-forum <mailto:pqc-forum@list.nist.gov> wrote:
Dear forum,

What are your personal opinions on what KEM(s) and parameters should
be used when high confidence in long-term secrecy is desired? And do
you have any opinions on hybrids with ECC and hybrids with multiple
post-quantum KEMs?

Sydney

--
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 mailto: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/qXiNVwauaRcfw9×2_A4iQcm1zTqjLkw_GkdPyOy-GTkunq0SYu56tqAIlIbnxqy1aF6zrhFHYy-ICntLheWtaAmi98eKhTnXbpEYl5lYSlU%3D%40protonmail.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 mailto: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/5D4E282C-6294-47ED-AB60-F6CC6316E388%40ll.mit.edu?utm_medium=email&utm_source=footer.

--

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/CH0PR11MB57390771CADD51C1CC40092B9F629%40CH0PR11MB5739.namprd11.prod.outlook.com.

From: Greg Maxwell <gmaxwell@gmail.com> via pqc-forum@list.nist.gov
To: Sydney Antonov <ska84@protonmail.com>
CC: pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] Survey: conservative KEMs for long-term secrecy
Date: Tuesday, August 09, 2022 06:02:20 PM ET

I think your question is still a bit under-defined-- after all, none of the PQ proposals have an attached "maximum lifetime" requirement so you couldn't say they were unsuitable for long term use.

If I read your question as "What would you use for an application where long term security concerns completely dominated bandwidth and computation considerations?"   I'd use mceliece8192128 + ed448. Ed448 so the security doesn't rest exclusively on a single hard problem which, although long and well studied, could suffer speedups--even mceliece which has the longest history of study of its underlying hard problem. I wouldn't hybridize further since the additional implementations bring their own risks but the greatest gain is from having any assumption diversity at all, and the costs of other PQ schemes as hybrids are considerable.

Hybrid also has the regret minimizing advantage that, assuming reasonable implementation diligence (without which security is impossible at all), deployment of a fancy PQ scheme cannot result in less security than if you had taken a very conventional route. The additional communication cost of ECC is negligible compared to ANY of the proposed PQ schemes (except perhaps SIDH).

I find Uri's response a bit perplexing, considering that we've seen multiple third round candidates (/parameter sets) fall to *pratical* classical attacks. There have also been numerous attacks (e.g. side channels) on PQC implementations as techniques for efficient and secure implementation of these schemes are themselves less mature.

I don't think there is any reasonable grounds to argue that PQ crypto as a field (and particularly the popular lattice schemes) are remotely as mature as ECC and many parties delayed switching from RSA to ECC

for over a decade due to a mixture of maturity and patent risk concerns.

The comparison of adding RSA to ECC isn't really apt as RSA would add at 11x communications overhead to an ECC scheme, but adding ECC to any of the PQ schemes (except SIDH) would cause a relatively tiny communications overhead. Even classic ECC+SIDH would be easy to swallow compared to adding RSA to ECC. There are also fairly tight links between the security assumptions underlying ECC and RSA, so it's very plausible that related new attacks would break both. This is much less true for the combination of ECC and most of the PQ proposals.

In industry I think hybridization is being assumed to just be a default. No one will ever get fired for opting to hybridize a PQ scheme with ECC.

Consider, for example, Thomas Ptacek's recent bombastic public comment that "everybody's position is to combine classical key exchanges with PQC KEMs" (https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fnews.ycombinator.com%2Fitem%3Fid%3D32368313&data=05%7C01%7Cyi-kai.liu%40nist.gov%7C8011ea0813604dca039a08da7a52d3a9%7C2ab5d82fd8fa4797a93e054655c61dec%7C1%7C0%7C637956793401804239%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=azGjU4%2FKSbjrEMQf7ZlAnHUE7L7nPcdtZ4SK5uLNdrQ%3D&reserved=0), of course-- in years past Thomas also famously made similarly bombastic statements that the NSA backdooring of NIST approved Dual_EC_DRBG wasn't a big deal because no one would ever have used it, unaware at the time that NSA had bribed RSA labs to make it a default in BSAFE.

On Tue, Aug 9, 2022 at 9:09 PM 'Sydney Antonov' via pqc-forum <pqc-forum@list.nist.gov> wrote:

>

> Dear forum,

>

> What are your personal opinions on what KEM(s) and parameters should
> be used when high confidence in long-term secrecy is desired? And do
> you have any opinions on hybrids with ECC and hybrids with multiple
> post-quantum KEMs?
>
> Sydney
>
> --
> 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/qXiNVwauaRcfw9×2_A4iQcm1zTqjLkw_GkdPyOy-GTkunq0SYu56tqAIlIbnxqy1aF6zrhFHYy-ICntLheWtaAmi98eKhTnXbpEYl5lYSlU%3D%40protonmail.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/CAAS2fgTrtYhwyWVVucMFJ%3Dr4g_k4kfjkrpYVxESR2T_Y2XQ3uQ%40mail.gmail.com.

From: Tony Arcieri <bascule@gmail.com> via pqc-forum@list.nist.gov
To: Greg Maxwell <gmaxwell@gmail.com>
CC: Sydney Antonov <ska84@protonmail.com>, pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] Survey: conservative KEMs for long-term secrecy
Date: Tuesday, August 09, 2022 06:24:14 PM ET

On Tue, Aug 9, 2022 at 4:01 PM Greg Maxwell <gmaxwell@gmail.com> wrote:

> In industry I think hybridization is being assumed to just be a default. No one will ever get fired for opting to hybridize a PQ scheme with ECC.

Question to anyone from NIST who happens to be reading: are standardized hybrid schemes potentially on the horizon?

Especially with the recent failures of Round 3 finalists, I would strongly agree that hybrid KEMs are going to be considered an important belt-and-suspenders defense until enough time passes we can be reasonably assured that other PQ schemes won't suffer a similar fate.

And in that regard, it would be nice if there were standardized well-analyzed hybrid schemes which are FIPS-compliant with test vectors, rather than relegating such schemes to be standardized elsewhere with "some assembly required"

--
Tony Arcieri

From: Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu> via pqc-forum@list.nist.gov
To: Mike Ounsworth <mike.ounsworth@entrust.com>, Sydney Antonov <ska84@protonmail.com>
CC: pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] Survey: conservative KEMs for long-term secrecy
Date: Tuesday, August 09, 2022 06:39:21 PM ET
Attachments: smime.p7m

On 8/9/22, 17:39, "'Mike Ounsworth' via pqc-forum" <pqc-forum@list.nist.gov> wrote:

> Sydney,
>
> “Is hybrid useful?” is probably the most contentious PQ-related issue
> in this community You have opened this can of worms again. :/

That he did. ;-)

> Uri,
>
> Your analysis below ignores the possibility of implementation bugs in the new PQ stuff.

As opposed to implementation (and re-implementation/maintenance) bugs in the older Classic algorithms, plus bugs in the "convergence" code that deals with two independent mechanisms, plus increased attack surface because now you have at least two targets ... ?

> We recently added a section “Value proposition of hybrid / composite schemes”
> to our composite draft (see github because it’s not up on datatracker yet)
> https://github.com/EntrustCorporation/draft-ounsworth-pq-composite-keys/blob/master/draft-ounsworth-pq-composite-keys.txt#L247

As you know, I'm against Composite approach - but I'll take a look, and review - at least for myself (no promise to post comments here).

> I would be interested in your rebuttal to our analysis above.

Understood, thanks. Will read, no further promises.

TNX

From: pqc-forum@list.nist.gov <pqc-forum@list.nist.gov> On Behalf Of Blumenthal, Uri - 0553 - MITLL
Sent: August 9, 2022 4:28 PM
To: Sydney Antonov <ska84@protonmail.com>
Cc: pqc-forum@list.nist.gov
Subject: [EXTERNAL] Re: [pqc-forum] Survey: conservative KEMs for long-term secrecy

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

The only outcome that could justify Hybrid is if all of the following become true:

A. Crypto-Relevant Quantum Computer doesn’t materialize; and
B. PQ algorithms selected get broken by Classic (not Quantum!) attacks; and
C. Classic algorithms selected do not get broken by Classic attacks.

I do not consider this possibility likely. Some Classic algorithms turned out broken, some are surviving so far. Some PQ algorithms got broken, some are surviving - Lattice-based approach has been around for more than 25 years already, “mature enough” in my book. ECC was “younger” than that when it was embraced, and nobody insisted that it should be, e.g., “paired with RSA because we aren’t 100% sure ECC would hold”.

My $0.05.
Regards,
Uri

On Aug 9, 2022, at 17:10, 'Sydney Antonov' via pqc-forum <mailto:pqc-forum@list.nist.gov> wrote:

Dear forum,

What are your personal opinions on what KEM(s) and parameters should be used when high confidence in long-term secrecy is desired? And do you have any opinions on hybrids with ECC and hybrids with multiple post-quantum KEMs?

Sydney

To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/CH0PR11MB57390771CADD51C1CC40092B9F629%40CH0PR11MB5739.namprd11.prod.outlook.com.

--

From: Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu> via pqc-forum@list.nist.gov
To: Greg Maxwell <gmaxwell@gmail.com>, Sydney Antonov <ska84@protonmail.com>
CC: pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] Survey: conservative KEMs for long-term secrecy
Date: Tuesday, August 09, 2022 06:53:15 PM ET
Attachments: smime.p7m

> I find Uri's response a bit perplexing, considering that we've seen
> multiple third round candidates (/parameter sets) fall to *pratical*
> classical attacks. There have also been numerous attacks (e.g. side
> channels) on PQC implementations as techniques for efficient and
> secure implementation of these schemes are themselves less mature.

And I find your reply to my response a bit disingenuous, considering that there were candidates that failed immediately, candidates that failed later on in the process (e.g., SIKE fell only now), AND candidates whose basis appears to have survived decades of analysis - yes, I mean Lattice-based. NTRU was published in 1996, right? What "*practical* classical attacks" have been published against NTRU, Kyber, and Saber? Say, NIST Sec Level 5 parameter sets (which appeared rather late for NTRU, but it finally did, to my pleasure)?

> I don't think there is any reasonable grounds to argue that PQ crypto
> as a field (and particularly the popular lattice schemes) are remotely
> as mature as ECC and many parties delayed switching from RSA to ECC
> for over a decade due to a mixture of maturity and patent risk concerns.

PQ crypto now is more mature than EC crypto was when it was deployed. Many parties delayed switching to ECC because there were standing Certicom patents actively threatening potential vendors (or requiring to pay ransom fee, err, license fee). After those expired, switching jumped up by leaps and bounds.

> The comparison of adding RSA to ECC isn't really apt as RSA would add
> at 11x communications overhead to an ECC scheme, but adding ECC to any
> of the PQ schemes (except SIDH) would cause a relatively tiny
> communications overhead.

Adding ECC to a Lattice-based scheme would be indistinguishable communications-wise, but rather nasty computations-wise, as Kyber concludes on my platforms in microseconds. I would lose the capabilities it offers me by anchoring myself down with ECC.

> Even classic ECC+SIDH would be easy to swallow compared to adding RSA to ECC.

Yeah, if you have a ton of time to wait for SIDH/SIKE to finish ...

> In industry I think hybridization is being assumed to just be a
> default. No one will ever get fired for opting to hybridize a PQ
> scheme with ECC.

Probably.

> Consider, for example, Thomas Ptacek's recent bombastic public
> comment that "everybody's position is to combine classical key
> exchanges with PQC KEMs"

Who's Thomas, and why should I care what he says?

> (https://news.ycombinator.com/item?id=32368313), of course-- in years
> past Thomas also famously made similarly bombastic statements that the
> NSA backdooring of NIST approved Dual_EC_DRBG wasn't a big deal
> because no one would ever have used it, unaware at the time that NSA
> had bribed RSA labs to make it a default in BSAFE.

My opinion is to use CTR_DRBG. In case it matters.

> On Tue, Aug 9, 2022 at 9:09 PM 'Sydney Antonov' via pqc-forum
> <pqc-forum@list.nist.gov> wrote:
> >
> > Dear forum,
> >
> > What are your personal opinions on what KEM(s) and parameters should
> > be used when high confidence in long-term secrecy is desired? And do

> you have any opinions on hybrids with ECC and hybrids with multiple
> post-quantum KEMs?
>
> Sydney
>
> --
> 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/qXiNVwauaRcfw9×2_A4iQcm1zTqjLkw_GkdPyOy-GTkunq0SYu56tqAIlIbnxqy1aF6zrhFHYy-ICntLheWtaAmi98eKhTnXbpEYl5lYSlU%3D%40protonmail.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/CAAS2fgTrtYhwyWVVucMFJ%3Dr4g_k4kfjkrpYVxESR2T_Y2XQ3uQ%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/1E78D30C-5484-4816-B8CA-34D166F35778%40ll.mit.edu.

From: Mike Ounsworth <mike.ounsworth@entrust.com> via pqc-forum <pqc-forum@list.nist.gov>
To: Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu>, Sydney Antonov <ska84@protonmail.com>
CC: pqc-forum@list.nist.gov
Subject: RE: [pqc-forum] Survey: conservative KEMs for long-term secrecy
Date: Tuesday, August 09, 2022 06:56:49 PM ET

Uri said:

> As opposed to implementation (and re-implementation/maintenance) bugs in the older Classic algorithms,

Sure, they may still be zero-day bugs lurking in RSA / ECC code. Hybrid would add value and protection to bridge across the required patches.

> plus bugs in the "convergence" code that deals with two independent mechanisms,

At least for signatures, I conjecture that "concatenate" "un-concatenate", and "check that both are valid" is several orders of magnitude easier to implement correctly than, for example, FALCON.

Composite / hybrid KEMs currently have an open research question about how to implement combiners to achieve IND-CCA2 even if one alg is broken, or one shared secret is chosen maliciously, etc. But I conjecture that once we sort that theory out, correctly applying KDFs in the prescribed order will still be an order of magnitude easier to implement correctly than Kyber.

> plus increased attack surface because now you have at least two targets … ?

By this I assume you mean an implementation bug within a cryptographic primitive so bad that it allows for remote code execution (like a fully exploitable buffer overflow). I suppose this is possible, but if a system supports both primitives in isolation, then you are not increasing the attack surface by also offering them in hybrid.

—

Mike Ounsworth

———Original Message———
From: Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu>
Sent: August 9, 2022 5:39 PM
To: Mike Ounsworth <Mike.Ounsworth@entrust.com>; Sydney Antonov <ska84@protonmail.com>
Cc: pqc-forum@list.nist.gov
Subject: [EXTERNAL] Re: [pqc-forum] Survey: conservative KEMs for long-term secrecy

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 8/9/22, 17:39, "'Mike Ounsworth' via pqc-forum" <pqc-forum@list.nist.gov> wrote:

> Sydney,
>
> “Is hybrid useful?” is probably the most contentious PQ-related issue
> in this community You have opened this can of worms again. :/

That he did. ;-)

> Uri,
>
> Your analysis below ignores the possibility of implementation bugs in the new PQ stuff.

As opposed to implementation (and re-implementation/maintenance) bugs in the older Classic algorithms, plus bugs in the "convergence" code that deals with two independent mechanisms, plus increased attack surface because now you have at least two targets … ?

> We recently added a section “Value proposition of hybrid / composite schemes”
> to our composite draft (see github because it’s not up on datatracker yet)
> https://github.com/EntrustCorporation/draft-ounsworth-pq-composite-keys/blob/master/draft-ounsworth-pq-composite-keys.txt#L247

As you know, I'm against Composite approach – but I'll take a look, and review – at least for myself (no promise to post comments here).

> I would be interested in your rebuttal to our analysis above.

Understood, thanks. Will read, no further promises.

TNX

From: pqc-forum@list.nist.gov <pqc-forum@list.nist.gov> On Behalf Of Blumenthal, Uri - 0553 - MITLL
Sent: August 9, 2022 4:28 PM
To: Sydney Antonov <ska84@protonmail.com>
Cc: pqc-forum@list.nist.gov
Subject: [EXTERNAL] Re: [pqc-forum] Survey: conservative KEMs for long-term secrecy

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

The only outcome that could justify Hybrid is if all of the following become true:

A. Crypto-Relevant Quantum Computer doesn’t materialize; and
B. PQ algorithms selected get broken by Classic (not Quantum!) attacks; and
C. Classic algorithms selected do not get broken by Classic attacks.

I do not consider this possibility likely. Some Classic algorithms turned out broken, some are surviving so far. Some PQ algorithms got broken, some are surviving – Lattice-based approach has been around for more than 25 years already, “mature enough” in my book. ECC was “younger” than that when it was embraced, and nobody insisted that it should be, e.g., “paired with RSA because we aren’t 100% sure ECC would hold”.

My $0.05.
Regards,

Uri

On Aug 9, 2022, at 17:10, 'Sydney Antonov' via pqc-forum <mailto:pqc-forum@list.nist.gov> wrote:

Dear forum,

What are your personal opinions on what KEM(s) and parameters should be used when high confidence in long-term secrecy is desired? And do you have any opinions on hybrids with ECC and hybrids with multiple post-quantum KEMs?

Sydney

--

--

--

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/CH0PR11MB57390771CADD51C1CC40092B9F629%40CH0PR11MB5739.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/CH0PR11MB5739F5A202DA63F3841AD3719F629%40CH0PR11MB5739.namprd11.prod.outlook.com.

From: Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu> via pqc-forum@list.nist.gov
To: Mike Ounsworth <mike.ounsworth@entrust.com>
CC: pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] Survey: conservative KEMs for long-term secrecy
Date: Tuesday, August 09, 2022 07:08:10 PM ET
Attachments: smime.p7m

> > Your analysis below ignores the possibility of implementation bugs in the new PQ stuff.
>
> As opposed to implementation (and re-implementation/maintenance) bugs in
> the older Classic algorithms, plus bugs in the "convergence" code that
> deals with two independent mechanisms, plus increased attack surface
> because now you have at least two targets ... ?

It is a bit of apples-to-oranges comparison, but I compared OpenSSL EC source directory (ECDH-related and supporting code only)

```
$ tokei openssl/crypto/ec/ec_*.[ch] openssl/crypto/ec/ecdh*.[ch]  openssl/crypto/ec/ecp_nistp*.[ch]
```

Language	Files	Lines	Code	Comments	Blanks
C	21	18463	13218	3434	1811
C Header	1	773	535	184	54
Total	22	19236	13753	3618	1865

With liboqs Kyber-1024 directory (OQS-OpenSSL uses PQ stuff from liboqs)

```
$ tokei liboqs/src/kem/kyber/*.[ch] liboqs/src/kem/kyber/pqcrystals-kyber_kyber1024_ref/*.[ch]
```

Language	Files	Lines	Code	Comments	Blanks
C	15	2102	1290	591	221
C Header	12	500	385	8	107

Total	27	2602	1675	599	328

Where would you expect to find more potential bugs? ;-)

--

From: Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu> via pqc-forum@list.nist.gov
To: Mike Ounsworth <mike.ounsworth@entrust.com>
CC: pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] Survey: conservative KEMs for long-term secrecy
Date: Tuesday, August 09, 2022 07:15:55 PM ET
Attachments: smime.p7m

> Sure, they may still be zero-day bugs lurking in RSA / ECC code.
> Hybrid would add value and protection to bridge across the required patches.

Code tends to get updated, recompiled on new platforms and with new toolchains, rewritten for various reasons, etc. etc. Doesn't have to be a lurking zero-day.

> At least for signatures, I conjecture that "concatenate" "un-concatenate",
> and "check that both are valid" is several orders of magnitude easier to
> implement correctly than, for example, FALCON.

I'll leave this point alone, and instead would like to talk to you (off-list, probably) about FALCON - what did you find particularly difficult to implement in it. And how much of the FALCON properties, good ones and bad ones, in your opinion "translates" to ZALCON.

> Composite / hybrid KEMs currently have an open research question about how to
> implement combiners to achieve IND-CCA2 even if one alg is broken, or one shared
> secret is chosen maliciously, etc. But I conjecture that once we sort that theory
> out, correctly applying KDFs in the prescribed order will still be an order of
> magnitude easier to implement correctly than Kyber.

I've implemented a couple of Lattice-based KEMs, and found them to be pretty darn straightforward. Mind you, it was not an assembly-accelerated "squeeze every bit of performance and space" implementation, but it worked. (And passed KAT ;).

> > plus increased attack surface because now you have at least two targets ... ?
>
> By this I assume you mean an implementation bug within a cryptographic primitive
> so bad that it allows for remote code execution (like a fully exploitable buffer
> overflow). I suppose this is possible, but if a system supports both primitives

> in isolation, then you are not increasing the attack surface by also offering
> them in hybrid.

IMHO, people who know enough to correctly isolate both primitives, are likely to implement both or either without an exploitable bug. We're talking ballpark 1.5K lines of code for Kyber.

TNX

-----Original Message-----
From: Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu>
Sent: August 9, 2022 5:39 PM
To: Mike Ounsworth <Mike.Ounsworth@entrust.com>; Sydney Antonov <ska84@protonmail.com>
Cc: pqc-forum@list.nist.gov
Subject: [EXTERNAL] Re: [pqc-forum] Survey: conservative KEMs for long-term secrecy

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 8/9/22, 17:39, "'Mike Ounsworth' via pqc-forum" <pqc-forum@list.nist.gov> wrote:

> Sydney,
>
> “Is hybrid useful?” is probably the most contentious PQ-related issue
> in this community You have opened this can of worms again. :/

That he did. ;-)

> Uri,
>
> Your analysis below ignores the possibility of implementation bugs in the new PQ stuff.

As opposed to implementation (and re-implementation/maintenance) bugs in the older Classic algorithms, plus bugs in the "convergence" code that deals with two independent mechanisms, plus increased attack surface because now you have at least two targets … ?

> We recently added a section “Value proposition of hybrid / composite schemes”
> to our composite draft (see github because it’s not up on datatracker yet)
> https://github.com/EntrustCorporation/draft-ounsworth-pq-composite-keys/blob/master/draft-ounsworth-pq-composite-keys.txt#L247

As you know, I'm against Composite approach - but I'll take a look, and review - at least for myself (no promise to post comments here).

> I would be interested in your rebuttal to our analysis above.

Understood, thanks. Will read, no further promises.

TNX

From: pqc-forum@list.nist.gov <pqc-forum@list.nist.gov> On Behalf Of Blumenthal, Uri - 0553 - MITLL
Sent: August 9, 2022 4:28 PM
To: Sydney Antonov <ska84@protonmail.com>
Cc: pqc-forum@list.nist.gov
Subject: [EXTERNAL] Re: [pqc-forum] Survey: conservative KEMs for long-term secrecy

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

The only outcome that could justify Hybrid is if all of the following become true:

A. Crypto-Relevant Quantum Computer doesn’t materialize; and
B. PQ algorithms selected get broken by Classic (not Quantum!) attacks; and

C. Classic algorithms selected do not get broken by Classic attacks.

I do not consider this possibility likely. Some Classic algorithms turned out broken, some are surviving so far. Some PQ algorithms got broken, some are surviving - Lattice-based approach has been around for more than 25 years already, “mature enough” in my book. ECC was “younger” than that when it was embraced, and nobody insisted that it should be, e.g., “paired with RSA because we aren’t 100% sure ECC would hold”.

My $0.05.
Regards,
Uri

On Aug 9, 2022, at 17:10, 'Sydney Antonov' via pqc-forum <mailto:pqc-forum@list.nist.gov> wrote:

Dear forum,

What are your personal opinions on what KEM(s) and parameters should be used when high confidence in long-term secrecy is desired? And do you have any opinions on hybrids with ECC and hybrids with multiple post-quantum KEMs?

Sydney

--

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 mailto: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/qXiNVwauaRcfw9×2_A4iQcm1zTqjLkw_GkdPyOy-GTkunq0SYu56tqAIlIbnxqy1aF6zrhFHYy-ICntLheWtaAmi98eKhTnXbpEYl5lYSlU%3D%40protonmail.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 mailto: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/5D4E282C-6294-47ED-AB60-F6CC6316E388%40ll.mit.edu?utm_medium=email&utm_source=footer.

--

--

--

From: Sydney Antonov <ska84@protonmail.com> via pqc-forum <pqc-forum@list.nist.gov>
To: Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu>
CC: pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] Survey: conservative KEMs for long-term secrecy
Date: Tuesday, August 09, 2022 07:19:51 PM ET

> The only outcome that could justify Hybrid is if all of the following become true:
> A. Crypto-Relevant Quantum Computer doesn't materialize; and
> B. PQ algorithms selected get broken by Classic (not Quantum!) attacks; and
> C. Classic algorithms selected do not get broken by Classic attacks.

I think it would cause less harm in many cases if secrets remain secret until attackers get CRQCs and if less secrets are exposed due to limited CRQC resources.

And even if a tool is designed for long-term secrecy, some uses may not actually require it.

Sydney

From: Alexandre Augusto <alexandre.a.giron@gmail.com> via pqc-forum@list.nist.gov
To: Sydney Antonov <ska84@protonmail.com>
CC: pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] Survey: conservative KEMs for long-term secrecy
Date: Tuesday, August 09, 2022 07:23:13 PM ET

Dear forum,

I would like to share our paper about hybrid Key Exchange in this discussion. It wraps up the literature and gives insight about the design challenges, performance and security aspects of post-quantum hybrid KEX. It is a Systematic Mapping Study (like a secondary study).

Link: https://link.springer.com/article/10.1007/s13389-022-00288-9

Best regards,

Em ter., 9 de ago. de 2022 às 20:19, 'Sydney Antonov' via pqc-forum <pqc-forum@list.nist.gov> escreveu:

> The only outcome that could justify Hybrid is if all of the following become true:
> A. Crypto-Relevant Quantum Computer doesn't materialize; and
> B. PQ algorithms selected get broken by Classic (not Quantum!) attacks; and
> C. Classic algorithms selected do not get broken by Classic attacks.

I think it would cause less harm in many cases if secrets remain secret
until attackers get CRQCs and if less secrets are exposed due to limited
CRQC resources.

And even if a tool is designed for long-term secrecy, some uses may not
actually require it.

Sydney

--
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/txzh13YAoFS0AskAo7FoAcGQNTW_LYKH-5rIXo_J8NGgUqSfWYdJhinyvh_cd-o3Q7PDpxRU_IIgUpUX5h1mhwxsxUl3aRxk2EM1HYS-ePk%3D%40protonmail.com.

--
Alexandre Augusto Giron

Federal University of Technology - Parana (UTFPR)

PhD Student at Federal University of Santa Catarina (UFSC)

--
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/CABLzjm_0XoDfH5Pmzqz_AFADeg9bwRv2e-3aC_spBWzZ7nzwqQ%40mail.gmail.com.

From: Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu> via pqc-forum@list.nist.gov
To: Sydney Antonov <ska84@protonmail.com>
CC: pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] Survey: conservative KEMs for long-term secrecy
Date: Tuesday, August 09, 2022 09:40:06 PM ET
Attachments: smime.p7m

> And even if a tool is designed for long-term secrecy, some uses may not
> actually require it.

Of course. You don't need PQ security today if your data will lose its value in a few years or sooner. You probably need PQ security if your data will remain valuable for a couple of decades or longer.

From: Doge Protocol <dogeprotocol1@gmail.com> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
CC: u...@ll.mit.edu <uri@ll.mit.edu>, pqc-...@list.nist.gov <pqc-forum@list.nist.gov>, Sydney Antonov <ska84@protonmail.com>
Subject: Re: [pqc-forum] Survey: conservative KEMs for long-term secrecy
Date: Wednesday, August 10, 2022 12:33:52 AM ET

Hybrid is still preferable (pq + ecc). It serves as a temporary hedge against hithereto unknown attacks on currently standardized schemes.
The security conscious may choose to adopt hybrid quicker than pure pq schemes, but may be reluctant to deploy soon with pq only schemes.

That aside, the pq program itself should be a continuing one, not limited to just the ones that are currently in the program. It would be nice if the NIST program is kept open for new pq schemes (for both key establishment as well as digital signatures).

For certain use-cases like blockchains, its important not to rush to adopt pq only digital signature schemes, but rather use hybrid (even though hybrid will have other negative tradeoffs in performance etc.).

On Tuesday, August 9, 2022 at 6:40:00 PM UTC-7 u...@ll.mit.edu wrote:

> > And even if a tool is designed for long-term secrecy, some uses may not
> > actually require it.
>
> Of course. You don't need PQ security today if your data will lose its value in a few years or sooner. You probably need PQ security if your data will remain valuable for a couple of decades or longer.

From: D. J. Bernstein <djb@cr.yp.to> via pqc-forum@list.nist.gov
To: pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] Survey: conservative KEMs for long-term secrecy
Date: Wednesday, August 10, 2022 04:14:28 AM ET
Attachments: smime.p7m

Tony Arcieri writes:
> Question to anyone from NIST who happens to be reading: are standardized
> hybrid schemes potentially on the horizon?

Formally, NIST's current standards already _allow_ hybrids. You aren't violating their ECC standards if you hash in an extra KDF input that comes from Kyber or from SIKE or from whatever else you have in mind.

However, NIST has dodged requests to _commit_ to hybrids. It has set evaluation criteria that are actively counterproductive when hybrids are in place, and has dodged objections to those criteria. Examples of such objections and requests (two quotes from me, one from Vadim Lyubashevsky):

* "Scrap the requirement of a pre-quantum security analysis. Users will use cheap ECC hybrids to obtain the pre-quantum security that they want." https://blog.cr.yp.to/20161030-pqnist.html

  (See also the explanation there of the damage that would be caused by having pre-quantum security, without hybrids, as the focus of a post-quantum effort. This was filed before the submission criteria were finalized, and NIST did act on some of my other comments, such as my recommendation to call for IND-CCA2 KEMs.)

* "If we seriously start considering hybrid modes (and I think we should), then I think that this is a game-changer for the standardization process in at least three ways ... if the hybrid mode is the default option and its purpose is exactly to provide classical security, then why should we care about the classical security of our post-quantum algorithms?"
  https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/msRrR13muS4/m/abayy2wNBgAJ

   * "On a related note, it's disturbing to see NSA's continued efforts
     to convince people to _turn off ECC_ in favor of lattices. NIST
     should endorse ANSSI's statement that 'the maturity level of the
     post-quantum algorithms presented to the NIST process should not be
     overestimated' and should join other organizations in recommending
     that post-quantum algorithms be deployed _only_ as a second layer
     of encryption (and/or signatures) together with ECC."
     https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/KFgw5_qCXiI/m/xWpu5ndqAwAJ

When I say "dodged", I don't mean that NIST has been silent; I mean that NIST keeps switching to different questions. Typical NIST response: "nothing NIST is planning to do should PREVENT the use of these diverse hybrid cryptosystems" (emphasis added).

In the end, here's what matters. NSA has direct control over large volumes of U.S. government purchasing, and, preemptively warping the market, has announced that it doesn't plan to approve hybrids:

   https://web.archive.org/web/20220524232249/https://twitter.com/mjos_crypto/status/1433443198534361101/photo/1

NIST has considerable power to fight against this, by committing to having each of its post-quantum standards explicitly require hybrids. Committing to this six years ago would have been much better, but doing it now still has tremendous value.

It would still be possible for NSA to eliminate hybrids for its non-FIPS purchases, such as purchases of Suite A equipment. This doesn't mean that NSA would be trusting lattices for its own use——NSA has already established a program

   https://web.archive.org/web/20220524232250/https://www.nsa.gov/Portals/75/documents/resources/everyone/csfc/threat-prevention.pdf

requiring two independent encryption layers "to mitigate the ability of

an adversary to exploit a single cryptographic implementation to compromise both layers", and the same machinery lets NSA glue together ECC and lattices for itself. Anyway, Suite A is a separate corner of the market; NIST should be setting standards to do the right thing for organizations that are following those standards.

——D. J. Bernstein

From: Dan Brown <danibrown%blackberry.com@gtempaccount.com> via pqc-forum <pqc-forum@list.nist.gov>
To: pqc-forum <pqc-forum@list.nist.gov>
CC: Sydney Antonov <ska84@protonmail.com>, Sydney Antonov <ska84@protonmail.com>
Subject: [pqc-forum] Re: Survey: conservative KEMs for long-term secrecy
Date: Wednesday, August 10, 2022 11:40:29 AM ET

Hybrid should be recommended, non-hybrid should be optional (to accommodate constrained systems).

Supporting this is a simplistic quantified argument that I cited here last year:

https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/OpFVbuMYk8c/m/d4D9H4EEAwAJ

An artificial example from the cited IACR eprint 2021/608 considered 16 possible combinations of ECDH, McEliece, NTRU, and SIKE. The example estimated that ECDH & McEliece & NTRU was the optimal combination, and also ECDH & McEliece would be good enough. (To repeat: this example assumed artificial circumstances that were a bit contrived in order to illustrate workings the 2021/608 method.)

The 2021/608 method can estimate different conclusions under different circumstances (usage costs, data value, attack effort, which are treated as input estimates). For example, suppose that McEliece is deemed to have usage cost much higher than was used in the example above. The method could then estimate that a different combination is optimal, perhaps ECDH+NTRU (if crunching the numbers says so).

When aiming for very long-term forward secrecy, the methods in 2021/608 tend to estimate attack probabilities so high that newer cryptography, e.g. SIKE, tends to be excluded from the hybrid combination, because the usage cost outweighs the relatively small benefit. Nevertheless, my hunch is that hybrid (of not-yet broken KEMs) will help long-term forward secrecy and that better quantified estimation methods can support this.

- Dan

PS1: In the 2021/608 example, I used NTRU, not Kyber. I was not familiar with Kyber, and did not predict NIST picking Kyber. How similar is Kyber to good old NTRU?

PS2: Cryptographers quantify security levels against best-known attacks. Cryptographers seek provable reductions between cryptography security and basic computational problems (or heuristic oracles). Why not try to quantify basic cost-benefit decisions on cryptography?

On Tuesday, August 9, 2022 at 5:09:51 PM UTC-4 Sydney Antonov wrote:

> Dear forum,
>
> What are your personal opinions on what KEM(s) and parameters should be used when high confidence in long-term secrecy is desired? And do you have any opinions on hybrids with ECC and hybrids with multiple post-quantum KEMs?
>
> Sydney

--

From: Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu> via pqc-forum@list.nist.gov
To: pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] Survey: conservative KEMs for long-term secrecy
Date: Wednesday, August 10, 2022 12:03:35 PM ET
Attachments: smime.p7m

> Formally, NIST's current standards already _allow_ hybrids. You aren't
> violating their ECC standards if you hash in an extra KDF input that
> comes from Kyber or from SIKE or from whatever else you have in mind.

So, those who want hybrid, can do it already. And those who don't - can do without.

> However, NIST has dodged requests to _commit_ to hybrids.

Which is good - they tell you how to do what you want to do, not what do to.

> In the end, here's what matters. NSA has direct control over large
> volumes of U.S. government purchasing

Not in the non-military/non-DoD, AFAIK.

> and, preemptively warping the market, has announced that
> it doesn't plan to approve hybrids:
> https://web.archive.org/web/20220524232249/https://twitter.com/mjos_crypto/status/1433443198534361101/photo/1

An interesting presentation. I did not attend that ICMC myself. A colleague told me that she questioned this, and the clarification was that they "don't plan to REQUIRE hybrids". Yes, I can read the slides/screenshots as well as you, but that's what she told me.

I'd expect that if something is not required, a "normal" vendor would not put it in their product - unless that "something" is selling like a hot cake elsewhere.

> NIST has considerable power to fight against this, by committing to
> having each of its post-quantum standards explicitly require hybrids.

Respectfully disagree. Requiring hybrids does not make any more sense than, e.g., REQUIRING (rather than allowing) that you super-encrypt ChaCha-encrypted data with AES or vs. versa. If you want to do that - fine, if you don't - fine too.

> It would still be possible for NSA to eliminate hybrids for its non-FIPS
> purchases, such as purchases of Suite A equipment.

So ... ? And what do we care? You bought or used any Suite A equipment lately?

> This doesn't mean that NSA would be trusting lattices for its own
> use——NSA has already established a program
> https://web.archive.org/web/20220524232250/https://www.nsa.gov/Portals/75/documents/resources/everyone/csfc/threat-prevention.pdf

That program is explicitly about using COMMERCIAL stuff, presumably without the ability to exhaustively analyze it (like, reviewing all the source code and going through it with a fine-tooth comb). So, to avoid any issue with one commercial product, they want two independent implementations.

> requiring two independent encryption layers "to mitigate the ability of
> an adversary to exploit a single cryptographic IMPLEMENTATION to
> compromise both layers",

The word highlighted by me completely explains what the concern is.

Note, that it doesn't seem to require different ALGORITHMS, merely different IMPLEMENTATIONS.

--

From: D. J. Bernstein <djb@cr.yp.to> via pqc-forum@list.nist.gov
To: pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] Survey: conservative KEMs for long-term secrecy
Date: Wednesday, August 10, 2022 03:59:48 PM ET
Attachments: smime.p7m

> A colleague told me that she questioned this, and the clarification
> was that they "don't plan to REQUIRE hybrids".

That's not a clarification; it's a secondhand rumor that's completely
inconsistent with what the NSA slide

   https://web.archive.org/web/20220524232249/https://twitter.com/mjos_crypto/status/1433443198534361101/photo/1

says in considerable detail. Even if there's enough pressure at some
point to force NSA to publicly switch to allowing hybrids, vendors have
already received the memo that NSA doesn't want hybrids. (The slide was
presented at the International Cryptographic Module Conference.)

In this environment, it's critical to know whether NIST's post-quantum
standards will require hybrids. All evidence available so far is that
NIST is on a path to a "no" answer——which is very different from other
organizations saying that _of course_ ECC has to be there too.

> > NSA has direct control over large volumes of U.S. government purchasing
> Not in the non-military/non-DoD, AFAIK.

https://en.wikipedia.org/wiki/Military_budget_of_the_United_States says
"the FY2023 defense budget request will exceed $773 billion".

Cryptography is only one component of that, but "large volumes" is a
fair description of a small slice of the world's largest pie.

——D. J. Bernstein

--

From: Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu> via pqc-forum@list.nist.gov
To: D. J. Bernstein <djb@cr.yp.to>, pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] Survey: conservative KEMs for long-term secrecy
Date: Wednesday, August 10, 2022 04:57:20 PM ET
Attachments: smime.p7m

> > A colleague told me that she questioned this, and the clarification
> > was that they "don't plan to REQUIRE hybrids".
>
> That's not a clarification; it's a secondhand rumor that's completely
> inconsistent with what the NSA slide
> https://web.archive.org/web/20220524232249/https://twitter.com/mjos_crypto/status/1433443198534361101/photo/1

I'm not arguing - I'm simply sharing what I was told when I asked, because that slide surprised me too.

Of course, in any case, it would only apply and matter to those who seek NSA approval or certification of their products, which in turn is only relevant to stuff that protects Classified data (for DoD and such).

> Even if there's enough pressure at some
> point to force NSA to publicly switch to allowing hybrids, vendors have
> already received the memo that NSA doesn't want hybrids. (The slide was
> presented at the International Cryptographic Module Conference.)

If what I've been told is correct - and I've no reason to assume otherwise - hybrids *can* be approved by NSA, i.e., already *are* allowed, just not "encouraged". I understand that me sharing what I've heard may not be sufficient - is there a way to get an official answer from NSA on this?

But, frankly, I don't see why vendors would implement hybrid in the first place in the products that require NSA approval, if NSA doesn't require it. And the fact that NSA does not like hybrids and won't require them is incontestable (unless they change their opinion in the future, which I doubt).

> In this environment, it's critical to know whether NIST's post-quantum
> standards will require hybrids.

I think NIST standards are orthogonal to use of hybrids, and it won't make any sense for NIST to require them. NIST standardizes KEMs. You want to combine/concatenate several of the standardized KEMs, and maybe add ECC and/or RSA to the mix? Fine, just don't try to force me to do the same.

> > > NSA has direct control over large volumes of U.S. government purchasing
> > Not in the non-military/non-DoD, AFAIK.
>
> https://en.wikipedia.org/wiki/Military_budget_of_the_United_States says
> "the FY2023 defense budget request will exceed $773 billion".

DoD used to be the biggest and the most influential customer of companies like Microsoft. It does not seem to be so anymore. I assume NSA would be in the same category. And, as you know, US government is a lot more than DoD.

> Cryptography is only one component of that, but "large volumes" is a
> fair description of a small slice of the world's largest pie.

I agree, but see above. In the early days (as I heard), DoD could tell Microsoft what they wanted to see implemented. It doesn't appear that way now.

--

From: Daniel Apon <dapon.crypto@gmail.com> via pqc-forum@list.nist.gov
To: pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] Survey: conservative KEMs for long-term secrecy
Date: Wednesday, August 10, 2022 06:43:46 PM ET

"Even if there's enough pressure at some

point to force NSA to publicly switch to allowing hybrids"

NSA will do what NSA wants to do. They're responsible for *their* own systems, just like anyone is responsible for *their* own systems. The very idea of you "pressuring NSA" to do X, Y, or Z with *their own systems* is ludicrous simply on the face of things.

"In this environment, it's critical to know whether NIST's post-quantum standards will require hybrids. All evidence available so far is that NIST is on a path to a "no" answer---which is very different from other organizations saying that _of course_ ECC has to be there too."

I am *overwhelmingly thrilled* to be able to introduce you to NIST standards-document nomenclature, which includes a delineation between the words "Shall," "Shall Not," vs. "Should," and "Should Not," etc.

Here is a sample example of the usual boilerplate text for your edification:

"The terms "**shall**" and "**shall not**" indicate requirements to be followed strictly in order to conform to the publication and from which no deviation is permitted.

The terms "**should**" and "**should not**" indicate that, among several possibilities, one is recommended as particularly suitable without mentioning or excluding others, that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is discouraged but not prohibited.

The terms "**may**" and "**need not**" indicate a course of action permissible within the limits of the publication.

The terms "**can**" and "**cannot**" indicate a possibility and capability, whether material, physical,

or causal."

If Organization X, which you favor and decide to abide by, requires A, and NIST allows for A or B, then (A and (A or B)) = A is acceptable to you -- no??

Cheers,
--Daniel

On Wed, Aug 10, 2022 at 3:59 PM D. J. Bernstein <djb@cr.yp.to> wrote:

> A colleague told me that she questioned this, and the clarification
> was that they "don't plan to REQUIRE hybrids".

That's not a clarification; it's a secondhand rumor that's completely
inconsistent with what the NSA slide

https://web.archive.org/web/20220524232249/https://twitter.com/mjos_crypto/status/1433443198534361101/photo/1

says in considerable detail. Even if there's enough pressure at some
point to force NSA to publicly switch to allowing hybrids, vendors have
already received the memo that NSA doesn't want hybrids. (The slide was
presented at the International Cryptographic Module Conference.)

In this environment, it's critical to know whether NIST's post-quantum
standards will require hybrids. All evidence available so far is that
NIST is on a path to a "no" answer---which is very different from other
organizations saying that _of course_ ECC has to be there too.

> > NSA has direct control over large volumes of U.S. government purchasing
> Not in the non-military/non-DoD, AFAIK.

https://en.wikipedia.org/wiki/Military_budget_of_the_United_States says
"the FY2023 defense budget request will exceed $773 billion".

> Cryptography is only one component of that, but "large volumes" is a
> fair description of a small slice of the world's largest pie.
>
> ---D. J. Bernstein
>
> --
> 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/20220810195932.1504047.qmail%40cr.yp.to.

--
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/CAPxHsSLFUR7fFpbimemRQF3z-W_bQ24xcPH5RZeh3gEqN3t9cg%40mail.gmail.com.

From: John Mattsson <john.mattsson@ericsson.com> via pqc-forum <pqc-forum@list.nist.gov>
To: Mike Hamburg <mike@shiftleft.org>
CC: pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] Survey: conservative KEMs for long-term secrecy
Date: Thursday, August 11, 2022 09:30:48 AM ET

Mike Hamburg <mike@shiftleft.org> wrote:

>but just to make sure things are clear: please do not assume that NSA is making this recommendation honestly. Your assumption might be right, or it could be entirely the opposite, that NSA is promoting weak crypto because they can break some or all of the proposed lattice systems, at least at certain key strengths.

>This isn’t an argument in favor of hybrids. It's just a reminder that NSA is not to be trusted.

I think you need to be quite skeptical in general and assume that any party might have a hidden agenda. Signal intelligence agencies are also well-known to often operate behind other government agencies, private companies, and individual persons. You never know which suggestions that are coming from a signal intelligence agency. One of the most influential persons and companies in the history of cryptography Boris Hagelin and Crypto AG did e.g., turn out to be completely controlled by signal intelligence agencies.

I don't want to defend NSA too much, but I think there are quite strong reasons to assume that NSA wants to produce a strong CNSA 2.0 which like Suite B and the CNSA suite will be used by US government to protect TOP SECRET information. I don't think there is any indication that NSA has ever tried to weaken any NIST standards so that other parties could break them (except maybe old standards that had to comply with 40- and 56- bit export control regulation). Doing so would be very bad for US companies, the US economy, and US national security. NSA has designed quite good public standards like SHA-1, SHA-2, the P-curves, and ECDSA. Dual_EC_DRBG was very carefully designed to not be weak to anybody else than the party with the backdoor key. It is quite problematic when NSA suggest changes to algorithms without any public motivation, but in the case of DES it turned out to be an excellent suggestion that significantly increased the security. I think there is often a bit too much focus on NSA, there are a lot of other signal intelligence agencies in the world. Snowden and others have described some of the European agencies as much worse than NSA. There are also a lot of agencies in non-democratic countries.

Cheers,

John

From: Mike Hamburg <mike@shiftleft.org>
Date: Thursday, 11 August 2022 at 12:58
To: John Mattsson <john.mattsson@ericsson.com>
Cc: pqc-forum@list.nist.gov <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] Survey: conservative KEMs for long-term secrecy

Hi all,

> On Aug 11, 2022, at 10:24 AM, 'John Mattsson' via pqc-forum <pqc-forum@list.nist.gov> wrote:
>
> Uri Blumenthal wrote
> >I think NIST standards are orthogonal to use of hybrids, and it won't make any sense for NIST to require them. NIST standardizes KEMs. You want to combine/concatenate several of the standardized KEMs, and maybe add ECC and/or RSA to the mix? Fine, just don't try to force me to do the same.
>
> I very much agree with Uri here. I assume the different opinions from NSA and ANSSI might have to do with that NSA has spent muchmore time analyzing lattice-based cryptography and therefore have more trust inits security.

Assuming that something *might* be the case doesn’t mean much, but just to make sure things are clear: please do not assume that NSA is making this recommendation honestly. Your assumption might be right, or it could be entirely the opposite, that NSA is promoting weak crypto because they can break some or all of the proposed lattice systems, at least at certain key strengths.

This isn’t an argument in favor of hybrids. It's just a reminder that NSA is not to be trusted.

> I do not have a strong opinion on whether toactuallyuse hybrids or not. But I think NIST should standardize standalone PQC KEMs and allow them to be used in hybrid construction. Irrespectively of what people will use in the next decade, hybrids are likely not the long-term solution.

I agree, but I do think hybrid is prudent in the short term — not that it should be required, but I personally would encourage it. It seems likely to me that Kyber’s security will hold up against practical attack, but not so likely that I wouldn’t bolt on ECC for five years while folks study it more. Also, ECC has better-established countermeasures against power and EM side-channel attacks: while it’s surely feasible to protect Kyber, the FO transform in particular is a giant pain to defend.

> In addition to allowingnon-hybrid PQCandPQC-ECC hybrids. I think there is a strong need to allow systems to continue to use non-hybrid ECC until the threat from CRQCs is more imminent. This is the approach chosen byICANN forDNSSEC. It will also be the approach chosen by many contrained IoT systems as the current PQC algorithms aresimplynot practically usable in the most constrained IoT systems.

Yes, but keep in mind that the deployment time (especially for IoT) is generally longer than people expect. Encouraging systems that at least support PQC, even with a firmware upgrade, is an important part of crypto strategy. Maybe LoRaWAN hardware will take longer due to bandwidth constraints, but most embedded systems can afford PQC.

I also wanted to chip in on Uri's apples-to-oranges comparison of ECC to Kyber. OpenSSL's implementation of ECC is quite complicated, has architecture-specific optimizations and so on. If you want to compare simple, reference implementations of ciphers, you should consider that tweetnacl.c is 808 lines long (without comments though!). It implements SHA512, Salsa20, Poly1305 MAC, x25519 key exchange, Ed25519 signatures and some higher-level "box" constructs combining these operations. Furthermore, sections of it have been formally verified: see eg https://eprint.iacr.org/2021/428.pdf.

Kyber's reference code implements Keccak of course, and the 2602 lines you counted include headers, boilerplate and comments, and aren't optimized for tweeting. But I don't think there's a strong argument that Kyber is generally simpler and thus more likely to be bug-free than ECC key exchange. The math isn't really simpler, there's the FO transform to deal with, and there aren't necessarily fewer corner cases.

Regards,

— Mike

From: Mike Hamburg <mike@shiftleft.org> via pqc-forum@list.nist.gov
To: John Mattsson <john.mattsson@ericsson.com>
CC: pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] Survey: conservative KEMs for long-term secrecy
Date: Thursday, August 11, 2022 05:27:57 PM ET

Hi all,

> On Aug 11, 2022, at 10:24 AM, 'John Mattsson' via pqc-forum <pqc-forum@list.nist.gov> wrote:

> Uri Blumenthal wrote
> >I think NIST standards are orthogonal to use of hybrids, and it won't make any sense for NIST to require them. NIST standardizes KEMs. You want to combine/concatenate several of the standardized KEMs, and maybe add ECC and/or RSA to the mix? Fine, just don't try to force me to do the same.
>
> I very much agree with Uri here. I assume the different opinions from NSA and ANSSI might have to do with that NSA has spent muchmore time analyzing lattice-based cryptography and therefore have more trust inits security.

Assuming that something *might* be the case doesn’t mean much, but just to make sure things are clear: please do not assume that NSA is making this recommendation honestly. Your assumption might be right, or it could be entirely the opposite, that NSA is promoting weak crypto because they can break some or all of the proposed lattice systems, at least at certain key strengths.

This isn’t an argument in favor of hybrids. It's just a reminder that NSA is not to be trusted.

> I do not have a strong opinion on whether toactuallyuse hybrids or not. But I think NIST should standardize standalone PQC KEMs and allow them to be used in hybrid construction. Irrespectively of what people will use in the next decade, hybrids are likely not the long-term solution.

I agree, but I do think hybrid is prudent in the short term — not that it should be required, but I personally would encourage it. It seems likely to me that Kyber's security will hold up against practical attack, but not so likely that I wouldn't bolt on ECC for five years while folks study it more. Also, ECC has better-established countermeasures against power and EM side-channel attacks: while it's surely feasible to protect Kyber, the FO transform in particular is a giant pain to defend.

> In addition to allowingnon-hybrid PQCandPQC-ECC hybrids. I think there is a strong need to allow systems to continue to use non-hybrid ECC until the threat from CRQCs is more imminent. This is the approach chosen byICANN forDNSSEC. It will also be the approach chosen by many contrained IoT systems as the current PQC algorithms aresimplynot practically usable in the most constrained IoT systems.

Yes, but keep in mind that the deployment time (especially for IoT) is generally longer than people expect. Encouraging systems that at least support PQC, even with a firmware upgrade, is an important part of crypto strategy. Maybe LoRaWAN hardware will take longer due to bandwidth constraints, but most embedded systems can afford PQC.

I also wanted to chip in on Uri's apples-to-oranges comparison of ECC to Kyber. OpenSSL's implementation of ECC is quite complicated, has architecture-specific optimizations and so on. If you want to compare simple, reference implementations of ciphers, you should consider that tweetnacl.c is 808 lines long (without comments though!). It implements SHA512, Salsa20, Poly1305 MAC, x25519 key exchange, Ed25519 signatures and some higher-level "box" constructs combining these operations. Furthermore, sections of it have been formally verified: see eg https://eprint.iacr.org/2021/428.pdf.

Kyber's reference code implements Keccak of course, and the 2602 lines you counted include headers, boilerplate and comments, and aren't optimized for tweeting. But I don't think there's a strong argument that Kyber is generally simpler and thus more likely to be bug-free than ECC key exchange. The math isn't really simpler, there's the FO transform to deal with, and there aren't necessarily fewer corner cases.

Regards,

— Mike

From: Tanja Lange <tanja@hyperelliptic.org> via pqc-forum@list.nist.gov
To: pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] Survey: conservative KEMs for long-term secrecy
Date: Friday, August 12, 2022 03:28:32 PM ET

Dear Uri, dear all

I think it's clearer to look at what NSA posts online (and which was the basis for the talk)

https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fmedia.defense.gov%2F2021%2FAug%2F04%2F2002821837%2F-1%2F-1%2F1%2FQuantum_FAQs_20210804.PDF&data=05%7C01%7Cyi-kai.liu%40nist.gov%7Cb2e2747cc83549d8af9c08da7c98d613%7C2ab5d82fd8fa4797a93e054655c61dec%7C1%7C0%7C637959293122462739%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=9hGB7aA%2B1XoVg%2BU03PmGIAlh3ExDlxAA05LpIyetKCI%3D&reserved=0
or
https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.nsa.gov%2FCybersecurity%2FPost-Quantum-Cybersecurity-Resources%2F&data=05%7C01%7Cyi-kai.liu%40nist.gov%7Cb2e2747cc83549d8af9c08da7c98d613%7C2ab5d82fd8fa4797a93e054655c61dec%7C1%7C0%7C637959293122462739%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=wcyAowVlJgXnE3nzTeV7qAaqctybAPRwrb0BE85ra%2B4%3D&reserved=0

" When will CNSA be updated to quantum-resistant algorithms?

    The intention is to update CNSA to remove quantum-vulnerable algorithms and replace them with a subset of the quantum-resistant algorithms selected by NIST at the end of the third round of the NIST post-quantum effort – NIST determines the timeline for each round. See the Future Cryptography section of this FAQ for more information."

and

" Is there a quantum-resistant public-key algorithm that commercial vendors should adopt today?

[..] CNSSP-15 will be updated with a timeline for required use of the post-quantum algorithms and disuse of the quantum-vulnerable portion of the current CNSA Suite of algorithms. [...]"

both sound like a swap, not like an overlapping period.

Also, I was at that ICMC (remotely). The NSA speaker, William Layton, made a point against hybrids saying it's complicated and arguing that when there is a standard, the standard should be implemented.

I see this as a strong argument for NIST to include hybrids in the standards. This will provide clear guidance of how to safely combine two systems and will remove the argument that the standard doesn't cover hybrids.

Regards
Tanja

On Wed, Aug 10, 2022 at 08:56:09PM +0000, Blumenthal, Uri - 0553 - MITLL wrote:
> > > A colleague told me that she questioned this, and the clarification
> > > was that they "don't plan to REQUIRE hybrids".
> >
> > That's not a clarification; it's a secondhand rumor that's completely
> > inconsistent with what the NSA slide
> > https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fweb.archive.org%2Fweb%2F20220524232249%2Fhttps%3A%2F%2Ftwitter.com%2Fmjos_crypto%2Fstatus%2F1433443198534361101%2Fphoto%2F1&data=05%7C01%7Cyi-kai.liu%40nist.gov%7Cb2e2747cc83549d8af9c08da7c98d613%7C2ab5d82fd8fa4797a93e054655c61dec%7C1%7C0%7C637959293122462739%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=l3XKqUA06jNGvlr2O%2Fkq%2Bd4GUnLwDKbULEpNWmQDlXM%3D&reserved=0
>
> I'm not arguing - I'm simply sharing what I was told when I asked, because that slide surprised me too.
>

> Of course, in any case, it would only apply and matter to those who seek NSA approval or certification of their products, which in turn is only relevant to stuff that protects Classified data (for DoD and such).
>
> > Even if there's enough pressure at some
> > point to force NSA to publicly switch to allowing hybrids, vendors have
> > already received the memo that NSA doesn't want hybrids. (The slide was
> > presented at the International Cryptographic Module Conference.)
>
> If what I've been told is correct - and I've no reason to assume otherwise - hybrids *can* be approved by NSA, i.e., already *are* allowed, just not "encouraged". I understand that me sharing what I've heard may not be sufficient - is there a way to get an official answer from NSA on this?
>
> But, frankly, I don't see why vendors would implement hybrid in the first place in the products that require NSA approval, if NSA doesn't require it. And the fact that NSA does not like hybrids and won't require them is incontestable (unless they change their opinion in the future, which I doubt).
>
> > In this environment, it's critical to know whether NIST's post-quantum
> > standards will require hybrids.
>
> I think NIST standards are orthogonal to use of hybrids, and it won't make any sense for NIST to require them. NIST standardizes KEMs. You want to combine/ concatenate several of the standardized KEMs, and maybe add ECC and/or RSA to the mix? Fine, just don't try to force me to do the same.
>
>
> > > > NSA has direct control over large volumes of U.S. government purchasing
> > > Not in the non-military/non-DoD, AFAIK.
> >
> > https://gcc02.safelinks.protection.outlook.com/?
url=https%3A%2F%2Fen.wikipedia.org%2Fwiki%2FMilitary_budget_of_the_United_States&
data=05%7C01%7Cyi-
kai.liu%40nist.gov%7Cb2e2747cc83549d8af9c08da7c98d613%7C2ab5d82fd8fa4797a93e054655c61
dec%7C1%7C0%7C637959293122462739%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoi
V2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=rgt4ga4P8YZQ84C0BrV%
2FGk9cIYUoUUfEC10aunghsEM%3D&reserved=0 says

> > "the FY2023 defense budget request will exceed $773 billion".
>
> DoD used to be the biggest and the most influential customer of companies like Microsoft. It does not seem to be so anymore. I assume NSA would be in the same category. And, as you know, US government is a lot more than DoD.
>
> > Cryptography is only one component of that, but "large volumes" is a
> > fair description of a small slice of the world's largest pie.
>
> I agree, but see above. In the early days (as I heard), DoD could tell Microsoft what they wanted to see implemented. It doesn't appear that way now.
>
> --
> 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/EE46FF7D-DBB3-481E-952F-8462A50C125F%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/20220812192654.GN17864%40ein.win.tue.nl.

From: Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu> via pqc-forum@list.nist.gov
To: pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] Survey: conservative KEMs for long-term secrecy
Date: Friday, August 12, 2022 06:49:16 PM ET
Attachments: smime.p7m

> I think it's clearer to look at what NSA posts online (and

> which was the basis for the talk)

>

> [from NSA FAQ] The intention is to update CNSA to remove

> quantum-vulnerable algorithms and replace them with a subset

> of the quantum-resistant algorithms selected by NIST . . .

>

> [..] CNSSP-15 will be updated with a timeline for required

> use of the post-quantum algorithms and disuse of the

> quantum-vulnerable portion of the current CNSA Suite

>

> both sound like a swap, not like an overlapping period.

Of course! What else is news?

NSA controls CNSA (the suite that you don't have to use, BTW), and they

explicitly stated (more than once) that hybrids aren't in their plans.

I think the following is the succinct summary of this long exchange:

> . . . The NSA speaker . . . made a point against

> hybrids . . .

>

> I see this as a strong argument for NIST to include hybrids in the

> standards.

I see this as a strong argument that

- NIST should standardize good algorithms,
- NSA should choose what they think best for protecting US National Security Systems, and
- We (the community, mostly IETF – as that's where my experience is) should use whatever in whatever combination that cryptographers consider strong, most likely from the NIST standards.

So, if you want to see **protocols** include hybrid – then IETF, and not NIST, is where it's being discussed.

You might be happy to learn that the majority at IETF leans that way – to use NIST algorithms in a hybrid protocol.

Now, a funny bit. I was against hybrid, and did not plan to use it. Now my design uses hybrid protocol. For reasons that have nothing to do with security of PQ KEMs.

On Wed, Aug 10, 2022 at 08:56:09PM +0000, Blumenthal, Uri - 0553 - MITLL wrote:

> > > A colleague told me that she questioned this, and the clarification

> > > was that they "don't plan to REQUIRE hybrids".

> >

> > That's not a clarification; it's a secondhand rumor that's completely

> > inconsistent with what the NSA slide

> > https://web.archive.org/web/20220524232249/https://twitter.com/mjos_crypto/status/1433443198534361101/photo/1

>

> I'm not arguing - I'm simply sharing what I was told when I asked, because that slide surprised me too.

>

> Of course, in any case, it would only apply and matter to those who seek NSA approval or certification of their products, which in turn is only relevant to stuff that protects Classified data (for DoD and such).

>

> > Even if there's enough pressure at some

> > point to force NSA to publicly switch to allowing hybrids, vendors have

> > already received the memo that NSA doesn't want hybrids. (The slide was

> > presented at the International Cryptographic Module Conference.)

>

> If what I've been told is correct - and I've no reason to assume otherwise - hybrids *can* be approved by NSA, i.e., already *are* allowed, just not "encouraged". I understand that me sharing what I've heard may not be sufficient - is there a way to get an official answer from NSA on this?

>

> But, frankly, I don't see why vendors would implement hybrid in the first place in the products that require NSA approval, if NSA doesn't require it. And the fact that NSA does not like hybrids and won't require them is incontestable (unless they change their opinion in the future, which I doubt).

>

> > In this environment, it's critical to know whether NIST's post-quantum

> > standards will require hybrids.

>

> I think NIST standards are orthogonal to use of hybrids, and it won't make any sense for NIST to require them. NIST standardizes KEMs. You want to combine/concatenate several of the standardized KEMs, and maybe add ECC and/or RSA to the mix? Fine, just don't try to force me to do the same.

>

>

> > > > NSA has direct control over large volumes of U.S. government purchasing

> > > Not in the non-military/non-DoD, AFAIK.

> >

> > https://en.wikipedia.org/wiki/Military_budget_of_the_United_States says

> > "the FY2023 defense budget request will exceed $773 billion".

>

> DoD used to be the biggest and the most influential customer of companies like Microsoft. It does not seem to be so anymore. I assume NSA would be in the same category. And, as you know, US government is a lot more than DoD.

--