From: Moody, Dustin (Fed) <dustin.moody@nist.gov> via pqc-forum <pqc-forum@list.nist.gov>
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: [pqc-forum] Request for feedback on Classic McEliece
Date: Wednesday, November 30, 2022 07:30:39 AM ET

All,

NIST is confident in the security of Classic McEliece and would be comfortable standardizing the submitted parameter sets (under a different claimed security strength in some cases). However, it is unclear whether Classic McEliece represents the best option for enough applications to justify standardizing it at this time. For genera lpurpose systems wishing to base their security on codes rather than lattices, BIKE or HQC may represent a more attractive option.

NIST would like feedback on specific use cases for which Classic McEliece would be a good solution.

Thank you,

NIST PQC team

From: Mike Hamburg <mike@shiftleft.org> via pqc-forum@list.nist.gov
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
CC: pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] Request for feedback on Classic McEliece
Date: Wednesday, November 30, 2022 08:55:36 AM ET

Hi Dustin and team,
I propose that virtual private networks are a use case where Classic McEliece may be a good fit. Of course not all VPN deployments are the same, but often the parties deploying a VPN are willing to pay a premium for more confidence in the security of their communications. VPNs connect relatively infrequently, perhaps a few times per day. They are often deployed in places where bandwidth is relatively cheap, such as offices or homes, so large public keys are affordable. Furthermore, VPNs have relatively static client-server relationships, so the public keys can be cached depending on the desired forward secrecy window.

Regards,

— Mike

> On Nov 30, 2022, at 1:30 PM, 'Moody, Dustin (Fed)' via pqc-forum <pqc-forum@list.nist.gov> wrote:
>
> All,
>
> NIST is confident in the security of Classic McEliece and would be comfortable standardizing the submitted parameter sets (under a different claimed security strength in some cases). However, it is unclear whether Classic McEliece represents the best option for enough applications to justify standardizing it at this time. For genera lpurpose systems wishing to base their security on codes rather than lattices, BIKE or HQC may represent a more attractive option.
>
> NIST would like feedback on specific use cases for which Classic McEliece would be a good solution.
>
> Thank you,
>
> NIST PQC team

--

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

To unsubscribe from this group and stop receiving emails from it, send an email topqc-forum+unsubscribe@list.nist.gov.

To view this discussion on the web visithttps://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/SA1PR09MB86692928B933935B57535F57E5159%40SA1PR09MB8669.namprd09.prod.outlook.com.

From: Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu> via pqc-forum@list.nist.gov
To: Mike Hamburg <mike@shiftleft.org>
CC: pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] Request for feedback on Classic McEliece
Date: Wednesday, November 30, 2022 09:52:52 AM ET
Attachments: smime.p7m

Respectfully disagree. I certainly can't afford megabytes-worth of key exchange on my home VPN, and I'm sure my work would frown at the cost as well (especially scaling it up to all the employees, whose keys the work-server-appliance would need to cache). This could work only for pre-provisioned/cached scenarios, and once the cache gets invalidated for whatever reason, the cost becomes prohibitive. Bandwidth can never be this cheap, as laws of physics limit it. Also, even if bandwidth is free – factor in the latency caused by the need to download (and upload) public key of such size...

As I see it, the McEliece use case should fit all of the following:

- Pre-defined or static group of communicating entities – additions to the group must happen rarely; and
    - Or the entities really don't mind exchanging megabytes-worth of public keys – but I can't think of any situation where it's true;
- High tolerance to maintaining/caching large public keys for all the acceptable peers.

Might add "Can't afford larger ciphertexts of Lattice-based KEMs", but in this case all the peers must be pre-provisioned, with no possibility to re-key.

--

Regards,

Uri

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

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

- C. A. R. Hoare

From: on behalf of Mike Hamburg
Date: Wednesday, November 30, 2022 at 08:55
To: Dustin Moody
Cc: pqc-forum
Subject: Re: [pqc-forum] Request for feedback on Classic McEliece

Hi Dustin and team,

I propose that virtual private networks are a use case where Classic McEliece may be a good fit. Of course not all VPN deployments are the same, but often the parties deploying a VPN are willing to pay a premium for more confidence in the security of their communications. VPNs connect relatively infrequently, perhaps a few times per day. They are often deployed in places where bandwidth is relatively cheap, such as offices or homes, so large public keys are affordable. Furthermore, VPNs have relatively static client-server relationships, so the public keys can be cached depending on the desired forward secrecy window.

Regards,

— Mike

> On Nov 30, 2022, at 1:30 PM, 'Moody, Dustin (Fed)' via pqc-forum wrote:
>
> All,
>
> NIST is confident in the security of Classic McEliece and would be comfortable standardizing the submitted parameter sets (under a different claimed security strength in some cases). However, it is unclear whether Classic McEliece represents the best option for enough applications to justify standardizing it at this time. For genera lpurpose systems wishing to base their security on codes rather than lattices, BIKE or HQC may represent a more attractive option.
>
> NIST would like feedback on specific use cases for which Classic McEliece would be a good solution.
>
> Thank you,
>
> NIST PQC team

--

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

To unsubscribe from this group and stop receiving emails from it, send an email topqc-forum+unsubscribe@list.nist.gov.

To view this discussion on the web visithttps://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/SA1PR09MB86692928B933935B57535F57E5159%40SA1PR09MB8669.namprd09.prod.outlook.com.

--

You received this message because you are subscribed to the Google Groups "pqc-forum" group.
To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.
To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/2D692D2D-6763-4216-83CC-4360AEBA5DD9%40shiftleft.org.

--

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/5C91A99E-AF32-45EE-A6A4-F4C8B82AF47C%40ll.mit.edu.

From: Mike Hamburg <mike@shiftleft.org> via pqc-forum@list.nist.gov
To: Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu>
CC: pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] Request for feedback on Classic McEliece
Date: Wednesday, November 30, 2022 12:59:10 PM ET

Hi Uri,
I understand your disagreement, but I will back up my suggestion with some calculations. Let's suppose you're working remotely, connecting to an office VPN 100 times per month (~4-5x per workday, more than the typical once in the morning and maybe once after lunch), with mceliece8192128 (the largest instance, with a 1.36 MB public key) sent by the server to your laptop, which is on your home network. Suppose that the server's public key is never cached for some reason, that the 208-byte ciphertext is negligible for this analysis (anyway it's smaller than Kyber), and that other components of a VPN key exchange are out of scope. I would expect a VPN to use signing client certs (especially if the alternative is McEliece), but I will briefly touch on McEliece client certs later.

Suppose you have mediocre American internet: Comcast XFinity cable internet with 75 Mbps download speed and a 1.2 TB monthly data cap. The price and availability of such internet depends on location, but in San Francisco that's the cheapest tier at $25/mo. With such a connection, downloading the key takes 1.36e6 * 8 bit / (75e6 bit / s) = 127ms at rated speeds, or maybe double that if the network is loaded. Doing this 100 times per month uses 136 MB, which is 0.01% of your data cap. That latency isn't great, but if you have to type your password or use two-factor authentication or even scan a finger, then it takes much longer than a quarter-second to log in.

Suppose the server is on Amazon EC2 in Northern California. I'm choosing this because it's easy to determine pricing; Amazon are not known to be especially cheap. An on-premises server rack with business internet would likely have cheaper bandwidth, but it's complicated to calculate because logins are likely to be bursty. Anyway, outgoing data transfers from that zone cost $0.09 / GB, ignoring bulk discounts as you scale up. At 136 MB / month, this is costing the company about 1.2¢ / month / user. I'm not an accountant, but this seems plenty affordable to me.

For some protocols, it's possible that the client must also upload a McEliece key. That seems unlikely, and more likely to be cacheable since client certs are not regenerated frequently. Typically the dollar cost for uploads is similar to the cost for downloads (actually less on AWS), but the available bandwidth from homes is much lower — perhaps by a factor of 10, leading to a 1.2s - 2.5s increased login latency when the cache is invalid. That's getting pretty inconvenient, but it's not outright unaffordable.

Suppose instead that the company caches the certs server-side. If the company is Microsoft and has 221,000 employees, then this uses 300 GB of storage to cache one key for each employee. Possibly you would need a few keys per employee (cell phone, older keys or whatever) so let's say it takes 1 TB, and the cache must be replicated across several VPN gateways. That's a lot, but you're only reaching this size at Microsoft's scale. Putting 1 TB SSD in each of 100 gateways costs what, $10k? I'm pretty sure Microsoft can afford this as a 1-time capex — and again, I think the likely case is that you're using signatures (I dunno, SPHINCS+?) for client certs, and use McEliece in the other direction.

As a comparison point, Zoom's system requirements page recommends 600 kilobit / second incoming and outgoing bandwidth for "high quality" 1-on-1 video calling. "High quality" is the lowest full-frame video option, with half the bitrate of 720p, and group calls use more bandwidth. At that rate, a 1-hour video Zoom meeting would use 600 kbit * 3600 / 8 = 270 megabytes incoming data, which is about double the above budget for a month of McEliece key exchanges. This is a recommendation for smooth video and not a real usage estimate, so the true value might only be a quarter of this, but even then a month of key exchanges costs the same bandwidth as a couple hours of meetings (downstream, and the meetings also require upstream bandwidth). Remote work is bandwidth intensive: for example, my work laptop has downloaded about 40 GB and uploaded about 7 GB in the past month according to its network statistics.

This is not representative of every user or every company, and surely some will not be able to afford it. The above calculation with cellular tethering — say Google Fi Flexible at $10 / GB — would be much more significant at $1.36 / user / mo with no caching. But for companies using typical remote work tools, the VPN key exchanges will not be a large fraction of their bandwidth budget, and I think some will consider a cents-per-user-per-month cost to be affordable for the increased assurance.

Also this whole calculation is assuming no client-side caching at all. A realistic deployment would have at least some caching.

Regards,

— Mike

On Nov 30, 2022, at 3:52 PM, Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu> wrote:

Respectfully disagree. I certainly can’t afford megabytes-worth of key exchange on my home VPN, and I’m sure my work would frown at the cost as well (especially scaling it up to all the employees, whose keys the work-server-appliance would need to cache). This could work only for pre-provisioned/cached scenarios, and once the cache gets invalidated for whatever reason, the cost becomes prohibitive. Bandwidth can never bethischeap, as laws of physics limit it. Also, even if bandwidth is free – factor in the latency caused by the need to download (and upload) public key of such size…

As I see it, the McEliece use case should fitallof the following:

- Pre-defined or static group of communicating entities – additions to the group must happen rarely; and
    - Or the entitiesreallydon’t mind exchanging megabytes-worth of public keys – but I can’t think of any situation where it’s true;
- High tolerance to maintaining/caching large public keys for all the acceptable peers.

Might add “Can’t afford larger ciphertexts of Lattice-based KEMs”, but in this case all the peers must be pre-provisioned, with no possibility to re-key.

--

Regards,

Uri

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

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

- C. A. R. Hoare

From:<pqc-forum@list.nist.gov> on behalf of Mike Hamburg <mike@shiftleft.org>

Date: Wednesday, November 30, 2022 at 08:55

To: Dustin Moody <dustin.moody@nist.gov>

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

Subject: Re: [pqc-forum] Request for feedback on Classic McEliece

Hi Dustin and team,

I propose that virtual private networks are a use case where Classic McEliece may be a good fit. Of course not all VPN deployments are the same, but often the parties deploying a VPN are willing to pay a premium for more confidence in the security of their communications. VPNs connect relatively infrequently, perhaps a few times per day. They are often deployed in places where bandwidth is relatively cheap, such as offices or homes, so large public keys are affordable. Furthermore, VPNs have relatively static client-server relationships, so the public keys can be cached depending on the desired forward secrecy window.

Regards,

— Mike

> On Nov 30, 2022, at 1:30 PM, 'Moody, Dustin (Fed)' via pqc-forum <pqc-forum@list.nist.gov> wrote:
>
> All,
>
> NIST is confident in the security of Classic McEliece and would be comfortable standardizing the submitted parameter sets (under a different claimed security strength in some cases). However, it is unclear whether Classic McEliece represents the best option for enough applications to justify standardizing it at this time. For genera lpurpose systems wishing to base their security on codes rather than lattices, BIKE or HQC may represent a more attractive option.
>
> NIST would like feedback on specific use cases for which Classic McEliece would be a good solution.
>
> Thank you,
>
> NIST PQC team
>
> --
>
> You received this message because you are subscribed to the Google Groups "pqc-forum" group.
>
> To unsubscribe from this group and stop receiving emails from it, send an email topqc-forum+unsubscribe@list.nist.gov.
>
> To view this discussion on the web visithttps://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/SA1PR09MB86692928B933935B57535F57E5159%40SA1PR09MB8669.namprd09.prod.outlook.com.

--

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

To unsubscribe from this group and stop receiving emails from it, send an email topqc-forum+unsubscribe@list.nist.gov.

To view this discussion on the web visithttps://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/2D692D2D-6763-4216-83CC-4360AEBA5DD9%40shiftleft.org.

From: Brent Kimberley <brent.kimberley@durham.ca> via pqc-forum <pqc-forum@list.nist.gov>
To: Mike Hamburg <mike@shiftleft.org>, Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu>
CC: pqc-forum <pqc-forum@list.nist.gov>
Subject: RE: [pqc-forum] Request for feedback on Classic McEliece
Date: Wednesday, November 30, 2022 01:06:38 PM ET

>>It appears that we might be building the case for a DPU or HSM capable of storing megabytes-worth of key exchange.

From: pqc-forum@list.nist.gov <pqc-forum@list.nist.gov> **On Behalf Of** Mike Hamburg
Sent: November 30, 2022 12:59 PM
To: Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu>
Cc: pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] Request for feedback on Classic McEliece

Hi Uri,

I understand your disagreement, but I will back up my suggestion with some calculations. Let's suppose you're working remotely, connecting to an office VPN 100 times per month (~4-5x per workday, more than the typical once in the morning and maybe once after lunch), with mceliece8192128 (the largest instance, with a 1.36 MB public key) sent by the server to your laptop, which is on your home network. Suppose that the server's public key is never cached for some reason, that the 208-byte ciphertext is negligible for this analysis (anyway it's smaller than Kyber), and that other components of a VPN key exchange are out of scope. I would expect a VPN to use signing client certs (especially if the alternative is McEliece), but I will briefly touch on McEliece client certs later.

Suppose you have mediocre American internet: Comcast XFinity cable internet with 75 Mbps download speed and a 1.2 TB monthly data cap. The price and availability of such internet depends on location, but in San Francisco that's the cheapest tier at $25/mo. With such a connection, downloading the key takes 1.36e6 * 8 bit / (75e6 bit / s) = 127ms at rated speeds, or maybe double that if the network is loaded. Doing this 100 times per month uses 136 MB, which is 0.01% of your data cap. That latency isn't great, but if you have to type your password or use two-factor authentication or even scan a finger, then it takes much longer than a quarter-second to log in.

Suppose the server is on Amazon EC2 in Northern California. I'm choosing this because it's easy to determine pricing; Amazon are not known to be especially cheap. An on-premises server rack with business internet would likely have cheaper bandwidth, but it's complicated to calculate because logins are likely to be bursty. Anyway, outgoing data transfers from that zone cost $0.09 / GB, ignoring bulk discounts as you scale up. At 136 MB / month, this is costing the company about 1.2¢ / month / user. I'm not an accountant, but this seems plenty affordable to me.

For some protocols, it's possible that the client must also upload a McEliece key. That seems unlikely, and more likely to be cacheable since client certs are not regenerated frequently. Typically the dollar cost for uploads is similar to the cost for downloads (actually less on AWS), but the available bandwidth from homes is much lower — perhaps by a factor of 10, leading to a 1.2s - 2.5s increased login latency when the cache is invalid. That's getting pretty inconvenient, but it's not outright unaffordable.

Suppose instead that the company caches the certs server-side. If the company is Microsoft and has 221,000 employees, then this uses 300 GB of storage to cache one key for each employee. Possibly you would need a few keys per employee (cell phone, older keys or whatever) so let's say it takes 1 TB, and the cache must be replicated across several VPN gateways. That's a lot, but you're only reaching this size at Microsoft's scale. Putting 1 TB SSD in each of 100 gateways costs what, $10k? I'm pretty sure Microsoft can afford this as a 1-time capex — and again, I think the likely case is that you're using signatures (I dunno, SPHINCS+?) for client certs, and use McEliece in the other direction.

As a comparison point, Zoom's system requirements page recommends 600 kilobit / second incoming and outgoing bandwidth for "high quality" 1-on-1 video calling. "High quality" is the lowest full-frame video option, with half the bitrate of 720p, and group calls use more bandwidth. At that rate, a 1-hour video Zoom meeting would use 600 kbit * 3600 / 8 = 270 megabytes incoming data, which is about double the above budget for a month of McEliece key exchanges. This is a recommendation for smooth video and not a real usage estimate, so the true value might only be a quarter of this, but even then a month of key exchanges costs the same bandwidth as a couple hours of meetings (downstream, and the meetings also require upstream bandwidth). Remote work is bandwidth intensive: for example, my work laptop has downloaded about 40 GB and uploaded about 7 GB in the past month according to its network statistics.

This is not representative of every user or every company, and surely some will not be able to afford it. The above calculation with cellular tethering — say Google Fi Flexible at $10 / GB — would be much more significant at $1.36 / user / mo with no caching. But for companies using typical remote work tools, the VPN key exchanges will not be a large fraction of their bandwidth budget, and I think some will consider a cents-per-user-per-month cost to be affordable for the increased assurance.

Also this whole calculation is assuming no client-side caching at all. A realistic deployment would have at least some caching.

Regards,

— Mike

> On Nov 30, 2022, at 3:52 PM, Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu> wrote:
>
> Respectfully disagree. I certainly can't afford megabytes-worth of key exchange on my home VPN, and I'm sure my work would frown at the cost as well (especially scaling it up to all the employees, whose keys the work-server-appliance would need to cache). This could work only for pre-provisioned/cached scenarios, and once the cache gets invalidated for whatever reason, the cost becomes prohibitive. Bandwidth can never bethischeap, as laws of physics limit it. Also, even if bandwidth is free – factor in the latency caused by the need to download (and upload) public key of such size…
>
> As I see it, the McEliece use case should fitallof the following:
>
> - Pre-defined or static group of communicating entities – additions to the group must happen rarely; and
>   - Or the entitiesreallydon't mind exchanging megabytes-worth of public keys – but I can't think of any situation where it's true;
> - High tolerance to maintaining/caching large public keys for all the acceptable peers.
>
> Might add "Can't afford larger ciphertexts of Lattice-based KEMs", but in this case all the peers must be pre-provisioned, with no possibility to re-key.
>
> --
>
> Regards,
>
> Uri

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

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

- C. A. R. Hoare

From:<pqc-forum@list.nist.gov> on behalf of Mike Hamburg <mike@shiftleft.org>
Date: Wednesday, November 30, 2022 at 08:55
To: Dustin Moody <dustin.moody@nist.gov>
Cc:pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] Request for feedback on Classic McEliece

Hi Dustin and team,

I propose that virtual private networks are a use case where Classic McEliece may be a good fit. Of course not all VPN deployments are the same, but often the parties deploying a VPN are willing to pay a premium for more confidence in the security of their communications. VPNs connect relatively infrequently, perhaps a few times per day. They are often deployed in places where bandwidth is relatively cheap, such as offices or homes, so large public keys are affordable. Furthermore, VPNs have relatively static client-server relationships, so the public keys can be cached depending on the desired forward secrecy window.

Regards,

— Mike

> On Nov 30, 2022, at 1:30 PM, 'Moody, Dustin (Fed)' via pqc-forum <pqc-forum@list.nist.gov> wrote:
>
> All,
>
> NIST is confident in the security of Classic McEliece and would be comfortable standardizing the submitted parameter sets (under a different claimed security strength in some cases). However, it is unclear whether Classic McEliece represents the best option for enough applications to justify standardizing it at this time. For genera lpurpose systems wishing to base their security on codes

> > rather than lattices, BIKE or HQC may represent a more attractive option.
> >
> > NIST would like feedback on specific use cases for which Classic McEliece would be a good solution.
> >
> > Thank you,
> >
> > NIST PQC team
> >
> > --
> >
> > You received this message because you are subscribed to the Google Groups "pqc-forum" group.
> > To unsubscribe from this group and stop receiving emails from it, send an email topqc-forum+unsubscribe@list.nist.gov.
> > To view this discussion on the web visithttps://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/SA1PR09MB86692928B933935B57535F57E5159%40SA1PR09MB8669.namprd09.prod.outlook.com.
>
> --
>
> You received this message because you are subscribed to the Google Groups "pqc-forum" group.
> To unsubscribe from this group and stop receiving emails from it, send an email topqc-forum+unsubscribe@list.nist.gov.
> To view this discussion on the web visithttps://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/2D692D2D-6763-4216-83CC-4360AEBA5DD9%40shiftleft.org.

--

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/BABFBE19-1410-4B00-B329-EE8BF2E9C305%40shiftleft.org.

THIS MESSAGE IS FOR THE USE OF THE INTENDED RECIPIENT(S) ONLY AND MAY CONTAIN INFORMATION THAT IS PRIVILEGED, PROPRIETARY, CONFIDENTIAL, AND/OR EXEMPT FROM DISCLOSURE UNDER ANY RELEVANT PRIVACY LEGISLATION. No rights to any privilege have been waived. If you are not the intended recipient, you are hereby notified that any review, re-transmission, dissemination, distribution, copying, conversion to hard copy, taking of action in reliance on or other use of this communication is strictly prohibited. If you are not the intended recipient and have received this message in error, please notify me by return e-mail and delete or destroy all copies of this message.

From: Gustavo Souza Banegas <gustavosouzabanegas@gmail.com> via pqc-forum@list.nist.gov
To: Brent Kimberley <brent.kimberley@durham.ca>
CC: Mike Hamburg <mike@shiftleft.org>, Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu>, pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] Request for feedback on Classic McEliece
Date: Wednesday, November 30, 2022 01:39:15 PM ET

Hi Mike, Hi Uri,
Well, MulladVPN has added an experimental feature in July 2022 that allows users to use McEliece with WireGuard. See [1] for more details.

This is bigger than a private network for sure, I don't think that they showed the results of the number of users and data, but it is still already a change towards something considered "too big".

All the best,

Gustavo

[1] - https://mullvad.net/fr/blog/2022/7/11/experimental-post-quantum-safe-vpn-tunnels/

On Wed, 30 Nov 2022 at 19:06, 'Brent Kimberley' via pqc-forum <pqc-forum@list.nist.gov> wrote:

> >>It appears that we might be building the case for a DPU or HSM capable of storing megabytes-worth of key exchange.
>
> ---
>
> **From:**pqc-forum@list.nist.gov <pqc-forum@list.nist.gov> **On Behalf Of** Mike Hamburg
> **Sent:** November 30, 2022 12:59 PM
> **To:** Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu>
> **Cc:** pqc-forum <pqc-forum@list.nist.gov>
> **Subject:** Re: [pqc-forum] Request for feedback on Classic McEliece
>
> Hi Uri,
>
> I understand your disagreement, but I will back up my suggestion with some calculations. Let's suppose you're working remotely, connecting to an office VPN 100 times per month (~4-5x per workday, more than the typical once in the morning and maybe once after lunch), with mceliece8192128 (the largest instance, with a 1.36 MB public key) sent by the server to your laptop, which is on your home network. Suppose that the server's public key

is never cached for some reason, that the 208-byte ciphertext is negligible for this analysis (anyway it's smaller than Kyber), and that other components of a VPN key exchange are out of scope. I would expect a VPN to use signing client certs (especially if the alternative is McEliece), but I will briefly touch on McEliece client certs later.

Suppose you have mediocre American internet: Comcast XFinity cable internet with 75 Mbps download speed and a 1.2 TB monthly data cap. The price and availability of such internet depends on location, but in San Francisco that's the cheapest tier at $25/mo. With such a connection, downloading the key takes 1.36e6 * 8 bit / (75e6 bit / s) = 127ms at rated speeds, or maybe double that if the network is loaded. Doing this 100 times per month uses 136 MB, which is 0.01% of your data cap. That latency isn't great, but if you have to type your password or use two-factor authentication or even scan a finger, then it takes much longer than a quarter-second to log in.

Suppose the server is on Amazon EC2 in Northern California. I'm choosing this because it's easy to determine pricing; Amazon are not known to be especially cheap. An on-premises server rack with business internet would likely have cheaper bandwidth, but it's complicated to calculate because logins are likely to be bursty. Anyway, outgoing data transfers from that zone cost $0.09 / GB, ignoring bulk discounts as you scale up. At 136 MB / month, this is costing the company about 1.2¢ / month / user. I'm not an accountant, but this seems plenty affordable to me.

For some protocols, it's possible that the client must also upload a McEliece key. That seems unlikely, and more likely to be cacheable since client certs are not regenerated frequently. Typically the dollar cost for uploads is similar to the cost for downloads (actually less on AWS), but the available bandwidth from homes is much lower — perhaps by a factor of 10, leading to a 1.2s - 2.5s increased login latency when the cache is invalid. That's getting pretty inconvenient, but it's not outright unaffordable.

Suppose instead that the company caches the certs server-side. If the company is Microsoft and has 221,000 employees, then this uses 300 GB of storage to cache one key for each employee. Possibly you would need a few keys per employee (cell phone, older keys or whatever) so let's say it takes 1 TB, and the cache must be replicated across several VPN gateways. That's a lot, but you're only reaching this size at Microsoft's scale. Putting 1 TB SSD in each of 100 gateways costs what, $10k? I'm pretty sure Microsoft can afford this as a 1-time capex — and again, I think the likely case is that you're using signatures (I dunno, SPHINCS+?) for client certs, and use McEliece in the other direction.

> As a comparison point, Zoom’s system requirements page recommends 600 kilobit / second incoming and outgoing bandwidth for “high quality” 1-on-1 video calling. “High quality” is the lowest full-frame video option, with half the bitrate of 720p, and group calls use more bandwidth. At that rate, a 1-hour video Zoom meeting would use 600 kbit * 3600 / 8 = 270 megabytes incoming data, which is about double the above budget for a month of McEliece key exchanges. This is a recommendation for smooth video and not a real usage estimate, so the true value might only be a quarter of this, but even then a month of key exchanges costs the same bandwidth as a couple hours of meetings (downstream, and the meetings also require upstream bandwidth). Remote work is bandwidth intensive: for example, my work laptop has downloaded about 40 GB and uploaded about 7 GB in the past month according to its network statistics.
>
> This is not representative of every user or every company, and surely some will not be able to afford it. The above calculation with cellular tethering — say Google Fi Flexible at $10 / GB — would be much more significant at $1.36 / user / mo with no caching. But for companies using typical remote work tools, the VPN key exchanges will not be a large fraction of their bandwidth budget, and I think some will consider a cents-per-user-per-month cost to be affordable for the increased assurance.
>
> Also this whole calculation is assuming no client-side caching at all. A realistic deployment would have at least some caching.
>
> Regards,
>
> — Mike
>
>> On Nov 30, 2022, at 3:52 PM, Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu> wrote:
>>
>> Respectfully disagree. I certainly can’t afford megabytes-worth of key exchange on my home VPN, and I’m sure my work would frown at the cost as well (especially scaling it up to all the employees, whose keys the work-server-appliance would need to cache). This could work only for pre-provisioned/cached scenarios, and once the cache gets invalidated for whatever reason, the cost becomes prohibitive. Bandwidth can never bethischeap, as laws of physics limit it. Also, even if bandwidth is free – factor in the latency caused by the need to download (and upload) public key of such size...

> As I see it, the McEliece use case should fitallof the following:
>
> - Pre-defined or static group of communicating entities – additions to the group must happen rarely; and
>   - Or the entitiesreallydon't mind exchanging megabytes-worth of public keys – but I can't think of any situation where it's true;
> - High tolerance to maintaining/caching large public keys for all the acceptable peers.
>
> Might add "Can't afford larger ciphertexts of Lattice-based KEMs", but in this case all the peers must be pre-provisioned, with no possibility to re-key.
>
> --
>
> Regards,
>
> Uri
>
> *There are two ways to design a system. One is to make is so simple there are obviously no deficiencies.*
>
> *The other is to make it so complex there are no obvious deficiencies.*
>
> *- C. A. R. Hoare*
>
> **From:**<pqc-forum@list.nist.gov> on behalf of Mike Hamburg <mike@shiftleft.org>
> **Date:**Wednesday, November 30, 2022 at 08:55
> **To:**Dustin Moody <dustin.moody@nist.gov>
> **Cc:**pqc-forum <pqc-forum@list.nist.gov>
> **Subject:**Re: [pqc-forum] Request for feedback on Classic McEliece
>
> Hi Dustin and team,
>
> I propose that virtual private networks are a use case where Classic McEliece may be a good fit. Of course not all VPN deployments are the same, but often the parties deploying a VPN are willing to pay a premium for more confidence in the security of their communications. VPNs connect relatively infrequently, perhaps a few times per day. They are often deployed in places where bandwidth is relatively cheap, such as

offices or homes, so large public keys are affordable. Furthermore, VPNs have relatively static client-server relationships, so the public keys can be cached depending on the desired forward secrecy window.

Regards,

— Mike

> On Nov 30, 2022, at 1:30 PM, 'Moody, Dustin (Fed)' via pqc-forum <pqc-forum@list.nist.gov> wrote:
>
> All,
>
> NIST is confident in the security of Classic McEliece and would be comfortable standardizing the submitted parameter sets (under a different claimed security strength in some cases). However, it is unclear whether Classic McEliece represents the best option for enough applications to justify standardizing it at this time. For genera lpurpose systems wishing to base their security on codes rather than lattices, BIKE or HQC may represent a more attractive option.
>
> NIST would like feedback on specific use cases for which Classic McEliece would be a good solution.
>
> Thank you,
>
> NIST PQC team
>
> --
>
> You received this message because you are subscribed to the Google Groups "pqc-forum" group.
>
> To unsubscribe from this group and stop receiving emails from it, send an email topqc-forum+unsubscribe@list.nist.gov.
>
> To view this discussion on the web visithttps://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/SA1PR09MB86692928B933935B57535F57E5159%40SA1PR09MB8669.namprd09.prod.outlook.com.

--

You received this message because you are subscribed to the Google

>> Groups "pqc-forum" group.
>> To unsubscribe from this group and stop receiving emails from it, send an email topqc-forum+unsubscribe@list.nist.gov.
>> To view this discussion on the web visithttps://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/2D692D2D-6763-4216-83CC-4360AEBA5DD9%40shiftleft.org.
>
> --
> 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/BABFBE19-1410-4B00-B329-EE8BF2E9C305%40shiftleft.org.
>
> THIS MESSAGE IS FOR THE USE OF THE INTENDED RECIPIENT(S) ONLY AND MAY CONTAIN INFORMATION THAT IS PRIVILEGED, PROPRIETARY, CONFIDENTIAL, AND/OR EXEMPT FROM DISCLOSURE UNDER ANY RELEVANT PRIVACY LEGISLATION. No rights to any privilege have been waived. If you are not the intended recipient, you are hereby notified that any review, re-transmission, dissemination, distribution, copying, conversion to hard copy, taking of action in reliance on or other use of this communication is strictly prohibited. If you are not the intended recipient and have received this message in error, please notify me by return e-mail and delete or destroy all copies of this message.
> --
> 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/YT1PR01MB41871B863C44BDA5CC897B92FA159%40YT1PR01MB4187.CANPRD01.PROD.OUTLOOK.COM.

--
Best Regards,
Gustavo Souza Banegas
http://www.cryptme.in/

--
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/CAAWmNLM4uPR3HiETuhHRXxBvE_yUHjjgDwgtN9JAW15q1XsQxA%40mail.gmail.com.

From: Simon Hoerder <simon@hoerder.net> via pqc-forum@list.nist.gov
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
CC: pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] Request for feedback on Classic McEliece
Date: Wednesday, November 30, 2022 01:40:23 PM ET

Hi,
Would ‘BSI compatibility’ be a valid use-case? As far as I understand, Germany’s BSI is sticking to their TR-02202-1 recommendation of Classic McEliece and FrodoKEM and does not intend to follow NISTs example of standardising CRYSTALS-Kyber. My understanding may be wrong though, would be good to hear from BSI itself. It would also be good to know whether BSI will adopt the round 4 version of Classic McEliece or whether they prefer to stay with older versions at the risk of international incompatibility.

Another question that I can’t answer is whether BSI TR-02102-1 will have any impact beyond German NSS.

Best,

Simon
(speaking for myself only)

> On 30 Nov 2022, at 13:30, 'Moody, Dustin (Fed)' via pqc-forum <pqc-forum@list.nist.gov> wrote:
>
> All,
>
> NIST is confident in the security of Classic McEliece and would be comfortable standardizing the submitted parameter sets (under a different claimed security strength in some cases). However, it is unclear whether Classic McEliece represents the best option for enough applications to justify standardizing it at this time. For genera lpurpose systems wishing to base their security on codes rather than lattices, BIKE or HQC may represent a more attractive option.
>
> NIST would like feedback on specific use cases for which Classic McEliece would be a good solution.

Thank you,

NIST PQC team

--
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/SA1PR09MB86692928B933935B57535F57E5159%40SA1PR09MB8669.namprd09.prod.outlook.com.

From: Sofi Celi <soficeli0@gmail.com> via pqc-forum@list.nist.gov
To: Simon Hoerder <simon@hoerder.net>
CC: Moody, Dustin (Fed) <dustin.moody@nist.gov>, pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] Request for feedback on Classic McEliece
Date: Friday, December 02, 2022 01:03:09 PM ET

Dear, all,
Thank you, Dustin, for starting this discussion.

I agree with Mike. The post-quantum Wireguard paper by Hülsing et al. (https://eprint.iacr.org/2020/379.pdf) gives good insight: Classic McEliece with its small ciphertext size can be used for operations in which the transmission of public key material is not constantly needed (static long-term keys, where keys are not rotated so often or somehow they are cached). So VPNs seem like a good candidate.

There is also research on using it in OpenVPN: https://essay.utwente.nl/70677/1/2016-08-09%20MSc%20Thesis%20Simon%20de%20Vries%20final%20color.pdf

Thank you,

El mié, 30 nov 2022 a la(s) 19:40, Simon Hoerder (simon@hoerder.net) escribió:

> Hi,
> Would ‘BSI compatibility’ be a valid use-case? As far as I understand, Germany’s BSI is sticking to their TR-02202-1 recommendation of Classic McEliece and FrodoKEM and does not intend to follow NISTs example of standardising CRYSTALS-Kyber. My understanding may be wrong though, would be good to hear from BSI itself. It would also be good to know whether BSI will adopt the round 4 version of Classic McEliece or whether they prefer to stay with older versions at the risk of international incompatibility.
>
> Another question that I can’t answer is whether BSI TR-02102-1 will have any impact beyond German NSS.
>
> Best,
>
> Simon
> (speaking for myself only)

> > On 30 Nov 2022, at 13:30, 'Moody, Dustin (Fed)' via pqc-forum <pqc-forum@list.nist.gov> wrote:
> >
> > All,
> >
> > NIST is confident in the security of Classic McEliece and would be comfortable standardizing the submitted parameter sets (under a different claimed security strength in some cases). However, it is unclear whether Classic McEliece represents the best option for enough applications to justify standardizing it at this time. For genera lpurpose systems wishing to base their security on codes rather than lattices, BIKE or HQC may represent a more attractive option.
> >
> > NIST would like feedback on specific use cases for which Classic McEliece would be a good solution.
> >
> > Thank you,
> >
> > NIST PQC team
> >
> > --
> > 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/SA1PR09MB86692928B933935B57535F57E5159%40SA1PR09MB8669.namprd09.prod.outlook.com.
>
> --
> You received this message because you are subscribed to the Google Groups "pqc-forum" group.
> To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.
> To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/A91BCBAC-7FB8-46EB-82D4-3BE420066C9B%40hoerder.net.

--

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

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

--
You received this message because you are subscribed to the Google Groups "pqc-forum" group.
To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.
To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/CAHy9yixipf9VFyLbcgV6%2B5-cpxj8zoZzMVVsuZ0up-tBR%3DAyKw%40mail.gmail.com.

From: Kampanakis, Panos <kpanos@amazon.com>
To: pqc-forum <pqc-forum@list.nist.gov>
CC: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: RE: [pqc-forum] Request for feedback on Classic McEliece
Date: Friday, December 02, 2022 03:55:04 PM ET

What happens with a VPN termination point that has to allocate 1GB of memory for a mere 1000 connection sustained DoS attack from a few little Raspberry PIs? I can appreciate the brainstorming nature of this thread, but no one would negotiate ephemeral 1MB McEliece public keys in live transport protocols after carefully considering the pros and cons. Also, it has historically not been good for interop and engineering debt to deploy algorithm X for transport protocol X, algorithm Y for protocol Y, Z for Z etc.

From: pqc-forum@list.nist.gov <pqc-forum@list.nist.gov> **On Behalf Of** Sofi Celi
Sent: Friday, December 2, 2022 1:03 PM
To: Simon Hoerder <simon@hoerder.net>
Cc: Moody, Dustin (Fed) <dustin.moody@nist.gov>; pqc-forum <pqc-forum@list.nist.gov>
Subject: RE: [EXTERNAL][pqc-forum] Request for feedback on Classic McEliece

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you can confirm the sender and know the content is safe.

Dear, all,

Thank you, Dustin, for starting this discussion.

I agree with Mike. The post-quantum Wireguard paper by Hülsing et al. (https://eprint.iacr.org/2020/379.pdf) gives good insight: Classic McEliece with its small ciphertext size can be used for operations in which the transmission of public key material is not constantly needed (static long-term keys, where keys are not rotated so often or somehow they are cached). So VPNs seem like a good candidate.

There is also research on using it in OpenVPN: https://essay.utwente.nl/70677/1/2016-08-09%20MSc%20Thesis%20Simon%20de%20Vries%20final%20color.pdf

Thank you,

El mié, 30 nov 2022 a la(s) 19:40, Simon Hoerder (simon@hoerder.net) escribió:

> Hi,
>
> Would ‘BSI compatibility’ be a valid use-case? As far as I understand, Germany’s BSI is sticking to their TR-02202-1 recommendation of Classic McEliece and FrodoKEM and does not intend to follow NISTs example of standardising CRYSTALS-Kyber. My understanding may be wrong though, would be good to hear from BSI itself. It would also be good to know whether BSI will adopt the round 4 version of Classic McEliece or whether they prefer to stay with older versions at the risk of international incompatibility.
>
> Another question that I can’t answer is whether BSI TR-02102-1 will have any impact beyond German NSS.
>
> Best,
>
> Simon
> (speaking for myself only)
>
>> On 30 Nov 2022, at 13:30, 'Moody, Dustin (Fed)' via pqc-forum <pqc-forum@list.nist.gov> wrote:
>>
>> All,
>>
>> NIST is confident in the security of Classic McEliece and would be comfortable standardizing the submitted parameter sets (under a different claimed security strength in some cases). However, it is unclear whether Classic McEliece represents the best option for enough applications to justify standardizing it at this time. For genera lpurpose systems wishing to base their security on codes rather than lattices, BIKE or HQC may represent a more attractive option.
>>
>> NIST would like feedback on specific use cases for which Classic McEliece would be a good solution.
>>
>> Thank you,
>>
>> NIST PQC team
>>
>> --
>> 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/SA1PR09MB86692928B933935B57535F57E5159%40SA1PR09MB8669.namprd09.prod.outlook.com.
>
> --
> You received this message because you are subscribed to the Google Groups "pqc-forum" group.
> To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.
> To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/A91BCBAC-7FB8-46EB-82D4-3BE420066C9B%40hoerder.net.

--

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

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

--
You received this message because you are subscribed to the Google Groups "pqc-forum" group.
To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.
To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/CAHy9yixipf9VFyLbcgV6%2B5-cpxj8zoZzMVVsuZ0up-tBR%3DAyKw%40mail.gmail.com.

From: Bruno Couillard <bruno@crypto4a.com> via pqc-forum@list.nist.gov
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>, pqc-forum <pqc-forum@list.nist.gov>
Subject: RE: [pqc-forum] Request for feedback on Classic McEliece
Date: Saturday, December 03, 2022 03:22:16 PM ET

Dustin, NIST team,

Thank you for asking the question and allowing the community to participate in this process.

Crypto4A currently uses Classic McEliece in all of its HSMs for three important use cases:

1. To secure the transfer of sensitive items (keys, secrets and other information) between HSMs in “clustered scenario”;

2. To secure the transfer of sensitive information from Crypto4A to its fielded HSMs; and

3. To secure the long term archiving of users' sensitive material.

In all of the above use cases, we use a hybrid approach (ECDH P-384 and McEliece) that offers both FIPS compliance as well as PQC readiness.

We determined a long time ago that the conservative and strong security claims of Classic McEliece would confer our HSM a strong claim of being Quantum Safe by design.

For the same reasons that have driven us to adopt Classic McEliece for its more conservative security properties, we believe that Classic McEliece will find use in other systems where the importance of said systems, or their inherent unsuitableness to support future updates (think of satellite systems and Industrial IoT for instance) are paramount. For those use cases, it is possible to envision a conservative PQC KEM such as Classic McEliece.

We also consider that use-cases such as long term archiving of “petabytes” of data for many decades would also benefit from using a very conservative KEM algorithm such as Classic McEliece.

Without a proper standardisation and ensuing validation process that would come from a proper NIST standardization process, Classic McEliece might not ever be considered by the masses as being a “legitimate” PQC algorithm. It is our belief that for those uses-cases where highly sensitive information is being protected for many decades, or systems that wouldn’t be easy to upgrade once launched/deployed, Classic McEliece is a very strong candidate PQC

KEM, and users will find ways to accommodate the large public key sizes in the interest of security.

We hope that the above sample use-cases and reasoning might favour the standardisation of Classic McEliece in the next round.

Sincerely,

Team Crypto4A

From: 'Moody, Dustin (Fed)' via pqc-forum <pqc-forum@list.nist.gov>
Sent: November 30, 2022 7:30 AM
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: [pqc-forum] Request for feedback on Classic McEliece

All,

NIST is confident in the security of Classic McEliece and would be comfortable standardizing the submitted parameter sets (under a different claimed security strength in some cases). However, it is unclear whether Classic McEliece represents the best option for enough applications to justify standardizing it at this time. For genera lpurpose systems wishing to base their security on codes rather than lattices, BIKE or HQC may represent a more attractive option.

NIST would like feedback on specific use cases for which Classic McEliece would be a good solution.

Thank you,

NIST PQC team

--
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/SA1PR09MB86692928B933935B57535F57E5159%40SA1PR09MB8669.namprd09.prod.outlook.com.

From: Stephan Ehlen <mail@stephanehlen.de> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
CC: SH <simon@hoerder.net>, pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] Request for feedback on Classic McEliece
Date: Friday, December 09, 2022 04:37:19 AM ET

Dear Simon,

dear all,

thank you for pointing out our (BSI's) recommendations.

Indeed, BSI recommends FrodoKEM-976 and FrodoKEM-1344

as well as Level 3 and 5 parameters for Classic McEliece in TR-02102-1

(see https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html).

Even though FrodoKEM is no longer in the NIST process, we intend to keep this recommendation.

We will evaluate draft standards of NIST's selection when they are published and (in principle)

we are open to adding further algorithms to our technical guidelines after conclusion of our evaluation.

Best,

Stephan

Dr. Stephan Ehlen

Referat KM 21 - Vorgaben an und Entwicklung von Kryptoverfahren
Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185-189
53175 Bonn
E-Mail: stephan.ehlen@bsi.bund.de
Internet: www.bsi.bund.de

#DeutschlandDigitalSicherBSI

Alle Informationen zum Umgang mit Ihren personenbezogenen
Daten finden Sie unter bsi.bund.de/datenschutz.

On Wednesday, November 30, 2022 at 7:40:20 PM UTC+1 SH wrote:

> Hi,
> Would ‘BSI compatibility’ be a valid use-case? As far as I understand, Germany’s BSI is sticking to their TR-02202-1 recommendation of Classic McEliece and FrodoKEM and does not intend to follow NISTs example of standardising CRYSTALS-Kyber. My understanding may be wrong though, would be good to hear from BSI itself. It would also be good to know whether BSI will adopt the round 4 version of Classic McEliece or whether they prefer to stay with older versions at the risk of international incompatibility.
>
> Another question that I can’t answer is whether BSI TR-02102-1 will have any impact beyond German NSS.
>
> Best,
>
> Simon
> (speaking for myself only)
>
>> On 30 Nov 2022, at 13:30, 'Moody, Dustin (Fed)' via pqc-forum <pqc-...@list.nist.gov> wrote:
>>
>> All,
>>
>> NIST is confident in the security of Classic McEliece and would be comfortable standardizing the submitted parameter sets (under a different claimed security strength in some cases). However, it is unclear whether Classic McEliece represents the best option for enough applications to justify standardizing it at

> this time. For genera lpurpose systems wishing to base their security on codes rather than lattices, BIKE or HQC may represent a more attractive option.
>
> NIST would like feedback on specific use cases for which Classic McEliece would be a good solution.
>
> Thank you,
>
> NIST PQC team
>
> --
>
> You received this message because you are subscribed to the Google Groups "pqc-forum" group.
> To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+...@list.nist.gov.
> To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/SA1PR09MB86692928B933935B57535F57E5159%40SA1PR09MB8669.namprd09.prod.outlook.com.

--
You received this message because you are subscribed to the Google Groups "pqc-forum" group.
To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.
To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/fb6430c2-ce28-4f36-8481-be7b387ab283n%40list.nist.gov.

From: Wrenna Robson <wren.robson@gmail.com> via pqc-forum@list.nist.gov
To: Stephan Ehlen <mail@stephanehlen.de>
CC: pqc-forum <pqc-forum@list.nist.gov>, SH <simon@hoerder.net>
Subject: Re: [pqc-forum] Request for feedback on Classic McEliece
Date: Friday, December 09, 2022 04:41:37 AM ET

Hi Stephen,
Is there an intention to create a standardised form of FrodoKEM? If so, under whose auspices? If not, what is to be considered the definitive version against which those who wish to follow this recommendation must compare implementations?

Best,

Wrenna

On Fri, 9 Dec 2022, 09:37 Stephan Ehlen, <mail@stephanehlen.de> wrote:

> Dear Simon,
>
> dear all,
>
> thank you for pointing out our (BSI's) recommendations.
>
> Indeed, BSI recommends FrodoKEM-976 and FrodoKEM-1344
>
> as well as Level 3 and 5 parameters for Classic McEliece in TR-02102-1
>
> (see https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html).
>
> Even though FrodoKEM is no longer in the NIST process, we intend to keep this recommendation.
>
> We will evaluate draft standards of NIST's selection when they are published and (in principle)
>
> we are open to adding further algorithms to our technical guidelines after conclusion of our evaluation.

> Best,
>
> Stephan
>
> Dr. Stephan Ehlen
>
> ---
>
> Referat KM 21 - Vorgaben an und Entwicklung von Kryptoverfahren
> Bundesamt für Sicherheit in der Informationstechnik
>
> Godesberger Allee 185-189
> 53175 Bonn
> E-Mail: stephan.ehlen@bsi.bund.de
> Internet: www.bsi.bund.de
>
> #DeutschlandDigitalSicherBSI
>
> Alle Informationen zum Umgang mit Ihren personenbezogenen
> Daten finden Sie unter bsi.bund.de/datenschutz.
>
> On Wednesday, November 30, 2022 at 7:40:20 PM UTC+1 SH wrote:
>
>> Hi,
>> Would ‘BSI compatibility’ be a valid use-case? As far as I understand, Germany’s BSI is sticking to their TR-02202-1 recommendation of Classic McEliece and FrodoKEM and does not intend to follow NISTs example of standardising CRYSTALS-Kyber. My understanding may be wrong though, would be good to hear from BSI itself. It would also be good to know whether BSI will adopt the round 4 version of Classic McEliece or whether they prefer to stay with older versions at the risk of international incompatibility.
>>
>> Another question that I can’t answer is whether BSI TR-02102-1 will have any impact beyond German NSS.
>>
>> Best,
>>
>> Simon
>> (speaking for myself only)

> > On 30 Nov 2022, at 13:30, 'Moody, Dustin (Fed)' via pqc-forum <pqc-...@list.nist.gov> wrote:
> >
> > All,
> >
> > NIST is confident in the security of Classic McEliece and would be comfortable standardizing the submitted parameter sets (under a different claimed security strength in some cases). However, it is unclear whether Classic McEliece represents the best option for enough applications to justify standardizing it at this time. For genera lpurpose systems wishing to base their security on codes rather than lattices, BIKE or HQC may represent a more attractive option.
> >
> > NIST would like feedback on specific use cases for which Classic McEliece would be a good solution.
> >
> > Thank you,
> >
> > NIST PQC team
> >
> > --
> >
> > You received this message because you are subscribed to the Google Groups "pqc-forum" group.
> > To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+...@list.nist.gov.
> > To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/SA1PR09MB86692928B933935B57535F57E5159%40SA1PR09MB8669.namprd09.prod.outlook.com.
>
> --
> You received this message because you are subscribed to the Google Groups "pqc-forum" group.
> To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.

> To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/fb6430c2-ce28-4f36-8481-be7b387ab283n%40list.nist.gov.

--
You received this message because you are subscribed to the Google Groups "pqc-forum" group.
To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.
To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/CANuKc3iMNAr6QNCHXWboZmXkYY_F9rD1B2%3DreWO9kw1z%3DbB3wA%40mail.gmail.com.

From: Stephan Ehlen <stephan.ehlen@bsi.bund.de> via pqc-forum <pqc-forum@list.nist.gov>
To: pqc-forum <pqc-forum@list.nist.gov>
CC: wren....@gmail.com <wren.robson@gmail.com>, pqc-forum <pqc-forum@list.nist.gov>, SH <simon@hoerder.net>, Stephan Ehlen <mail@stephanehlen.de>
Subject: Re: [pqc-forum] Request for feedback on Classic McEliece
Date: Tuesday, December 13, 2022 11:21:32 AM ET

Hi Wrenna,

at BSI, we support international standardization of FrodoKEM and Classic McEliece.

For instance, there are now some standardization efforts at ISO for PQC and
we hope that our two conservative recommendations will be part of these efforts.

Best,

Stephan

Dr. Stephan Ehlen

Referat KM 21 - Vorgaben an und Entwicklung von Kryptoverfahren
Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185-189
53175 Bonn
E-Mail: stephan.ehlen@bsi.bund.de
Internet: www.bsi.bund.de

#DeutschlandDigitalSicherBSI

Alle Informationen zum Umgang mit Ihren personenbezogenen
Daten finden Sie unter bsi.bund.de/datenschutz.

wren....@gmail.com schrieb am Freitag, 9. Dezember 2022 um 10:41:25 UTC+1:

> Hi Stephen,

> Is there an intention to create a standardised form of FrodoKEM? If so, under whose auspices? If not, what is to be considered the definitive version against which those who wish to follow this recommendation must compare implementations?
>
> Best,
>
> Wrenna
>
> On Fri, 9 Dec 2022, 09:37 Stephan Ehlen, <ma...@stephanehlen.de> wrote:
>
> > Dear Simon,
> >
> > dear all,
> >
> > thank you for pointing out our (BSI's) recommendations.
> >
> > Indeed, BSI recommends FrodoKEM-976 and FrodoKEM-1344
> >
> > as well as Level 3 and 5 parameters for Classic McEliece in TR-02102-1
> >
> > (see https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html).
> >
> > Even though FrodoKEM is no longer in the NIST process, we intend to keep this recommendation.
> >
> > We will evaluate draft standards of NIST's selection when they are published and (in principle)
> >
> > we are open to adding further algorithms to our technical guidelines after conclusion of our evaluation.
> >
> > Best,
> >
> > Stephan
> >
> > Dr. Stephan Ehlen
> >
> > ———————————————————
> >
> > Referat KM 21 - Vorgaben an und Entwicklung von Kryptoverfahren
> > Bundesamt für Sicherheit in der Informationstechnik

> > Godesberger Allee 185-189
> > 53175 Bonn
> > E-Mail: stepha...@bsi.bund.de
> > Internet: www.bsi.bund.de
> >
> > #DeutschlandDigitalSicherBSI
> >
> > Alle Informationen zum Umgang mit Ihren personenbezogenen
> > Daten finden Sie unter bsi.bund.de/datenschutz.
> >
> > On Wednesday, November 30, 2022 at 7:40:20 PM UTC+1 SH wrote:
> >
> > > Hi,
> > > Would 'BSI compatibility' be a valid use-case? As far as I understand, Germany's BSI is sticking to their TR-02202-1 recommendation of Classic McEliece and FrodoKEM and does not intend to follow NISTs example of standardising CRYSTALS-Kyber. My understanding may be wrong though, would be good to hear from BSI itself. It would also be good to know whether BSI will adopt the round 4 version of Classic McEliece or whether they prefer to stay with older versions at the risk of international incompatibility.
> > >
> > > Another question that I can't answer is whether BSI TR-02102-1 will have any impact beyond German NSS.
> > >
> > > Best,
> > >
> > > Simon
> > > (speaking for myself only)
> > >
> > > > On 30 Nov 2022, at 13:30, 'Moody, Dustin (Fed)' via pqc-forum
> > > > <pqc-...@list.nist.gov> wrote:
> > > >
> > > > All,

> > > NIST is confident in the security of Classic McEliece and would be comfortable standardizing the submitted parameter sets (under a different claimed security strength in some cases). However, it is unclear whether Classic McEliece represents the best option for enough applications to justify standardizing it at this time. For genera lpurpose systems wishing to base their security on codes rather than lattices, BIKE or HQC may represent a more attractive option.
> > >
> > > NIST would like feedback on specific use cases for which Classic McEliece would be a good solution.
> > >
> > > Thank you,
> > >
> > > NIST PQC team
> > >
> > > --
> > >
> > > You received this message because you are subscribed to the Google Groups "pqc-forum" group.
> > > To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+...@list.nist.gov.
> > > To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/SA1PR09MB86692928B933935B57535F57E5159%40SA1PR09MB8669.namprd09.prod.outlook.com.
> >
> > --
> > You received this message because you are subscribed to the Google Groups "pqc-forum" group.
> > To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+...@list.nist.gov.
> > To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/fb6430c2-ce28-4f36-8481-be7b387ab283n%40list.nist.gov.

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

To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/09daede0-fc41-493c-99a8-cfd91188a6a4n%40list.nist.gov.

From: John Mattsson <john.mattsson@ericsson.com> via pqc-forum <pqc-forum@list.nist.gov>
To: Stephan Ehlen <stephan.ehlen@bsi.bund.de>, pqc-forum <pqc-forum@list.nist.gov>
CC: wren....@gmail.com <wren.robson@gmail.com>, pqc-forum <pqc-forum@list.nist.gov>, SH <simon@hoerder.net>, Stephan Ehlen <mail@stephanehlen.de>
Subject: Re: [pqc-forum] Request for feedback on Classic McEliece
Date: Tuesday, December 13, 2022 02:01:20 PM ET

Dear Stephan Ehlen,

If BSI wants to use FrodoKEM and Classic McEliece and NIST do not publish them, Ithink BSIshouldapproach IRTF CFRG and publish the algorithms there, alternatively publish them as BSI documents. AsEricsson wrote in our comments on FIPS 186-5 we think it is grat that NIST is specifying ECDSA in FIPS186-5 instead of relying on references behind paywalls. We do not think that cryptographic algorithmspecifications behind paywalls are acceptable. Open access is very important for security specificationsas history has showed over and over again that lack of analysis often lead to serious weaknesses.

Best Regards,

John Preuß Mattsson

From: 'Stephan Ehlen' via pqc-forum <pqc-forum@list.nist.gov>
Date: Tuesday, 13 December 2022 at 17:21
To: pqc-forum <pqc-forum@list.nist.gov>
Cc: wren....@gmail.com <wren.robson@gmail.com>, pqc-forum <pqc-forum@list.nist.gov>, SH <simon@hoerder.net>, Stephan Ehlen <mail@stephanehlen.de>
Subject: Re: [pqc-forum] Request for feedback on Classic McEliece

Hi Wrenna,

at BSI, we support international standardization of FrodoKEM and Classic McEliece.

For instance, there are now some standardization efforts at ISO for PQC and

we hope that our two conservative recommendations will be part of these efforts.

Best,

Stephan

Dr. Stephan Ehlen

Referat KM 21 - Vorgaben an und Entwicklung von Kryptoverfahren
Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185-189
53175 Bonn
E-Mail: stephan.ehlen@bsi.bund.de
Internet: www.bsi.bund.de

#DeutschlandDigitalSicherBSI

Alle Informationen zum Umgang mit Ihren personenbezogenen
Daten finden Sie unter bsi.bund.de/datenschutz.

wren....@gmail.com schrieb am Freitag, 9. Dezember 2022 um 10:41:25 UTC+1:

> Hi Stephen,
>
> Is there an intention to create a standardised form of FrodoKEM? If so, under whose auspices? If not, what is to be considered the definitive version against which those who wish to follow this recommendation must compare implementations?
>
> Best,
>
> Wrenna
>
> On Fri, 9 Dec 2022, 09:37 Stephan Ehlen, <ma...@stephanehlen.de> wrote:
>
> > Dear Simon,
> >
> > dear all,
> >
> > thank you for pointing out our (BSI's) recommendations.
> >
> > Indeed, BSI recommends FrodoKEM-976 and FrodoKEM-1344
> >
> > as well as Level 3 and 5 parameters for Classic McEliece in TR-02102-1
> >
> > (see https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html).

>> Even though FrodoKEM is no longer in the NIST process, we intend to keep this recommendation.
>>
>> We will evaluate draft standards of NIST's selection when they are published and (in principle)
>>
>> we are open to adding further algorithms to our technical guidelines after conclusion of our evaluation.
>>
>> Best,
>>
>> Stephan
>>
>> Dr. Stephan Ehlen
>>
>> ______________________________
>>
>> Referat KM 21 - Vorgaben an und Entwicklung von Kryptoverfahren
>> Bundesamt für Sicherheit in der Informationstechnik
>>
>> Godesberger Allee 185-189
>> 53175 Bonn
>> E-Mail: stepha...@bsi.bund.de
>> Internet: www.bsi.bund.de
>>
>> #DeutschlandDigitalSicherBSI
>>
>> Alle Informationen zum Umgang mit Ihren personenbezogenen
>> Daten finden Sie unter bsi.bund.de/datenschutz.
>>
>> On Wednesday, November 30, 2022 at 7:40:20 PM UTC+1 SH wrote:
>>
>>> Hi,
>>>
>>> Would ‘BSI compatibility’ be a valid use-case? As far as I understand, Germany’s BSI is sticking to their TR-02202-1 recommendation of Classic McEliece and FrodoKEM and does not intend to follow NISTs example of standardising CRYSTALS-Kyber. My understanding may be wrong though, would be good to hear from BSI itself. It would also be good to know whether BSI will adopt the round 4 version of Classic McEliece or whether they prefer to stay with older versions at the risk of international incompatibility.
>>>
>>> Another question that I can’t answer is whether BSI TR-02102-1 will have any impact beyond German NSS.
>>>
>>> Best,

> > > Simon
> > > (speaking for myself only)
> > >
> > > > On 30 Nov 2022, at 13:30, 'Moody, Dustin (Fed)' via pqc-forum <pqc-...@list.nist.gov> wrote:
> > > >
> > > > All,
> > > >
> > > > NIST is confident in the security of Classic McEliece and would be comfortable standardizing the submitted parameter sets (under a different claimed security strength in some cases). However, it is unclear whether Classic McEliece represents the best option for enough applications to justify standardizing it at this time. For genera lpurpose systems wishing to base their security on codes rather than lattices, BIKE or HQC may represent a more attractive option.
> > > >
> > > > NIST would like feedback on specific use cases for which Classic McEliece would be a good solution.
> > > >
> > > > Thank you,
> > > >
> > > > NIST PQC team
> > > >
> > > > --
> > > >
> > > > You received this message because you are subscribed to the Google Groups "pqc-forum" group.
> > > > To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+...@list.nist.gov.
> > > > To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/SA1PR09MB86692928B933935B57535F57E5159%40SA1PR09MB8669.namprd09.prod.outlook.com.
> >
> > --
> > You received this message because you are subscribed to the Google Groups "pqc-forum" group.
> > To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+...@list.nist.gov.

> > To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/fb6430c2-ce28-4f36-8481-be7b387ab283n%40list.nist.gov.

--

You received this message because you are subscribed to the Google Groups "pqc-forum" group.
To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.
To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/09daede0-fc41-493c-99a8-cfd91188a6a4n%40list.nist.gov.

From: Simon Hoerder <simon@hoerder.net> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] Request for feedback on Classic McEliece
Date: Wednesday, December 14, 2022 02:57:32 AM ET

Dear Stephan, dear John, dear all,

Thank you for the information, Stephan. I fully agree with John that paywalled standards such as produced by ISO are undesirable. Putting a standard behind a paywall will not just increase security risks but also hinder adoption. IETF standards, NIST FIPS and SP800 standards and BSI’s own AIS standards are successful because of they are available to be scrutinized and implemented by everyone. Everyone can decide whether to trust them, everyone can deploy them once they do trust.

Best regards,

Simon

(speaking only for myself)

> On 13 Dec 2022, at 20:01, John Mattsson <john.mattsson@ericsson.com> wrote:
>
> Dear Stephan Ehlen,
>
> If BSI wants to use FrodoKEM and Classic McEliece and NIST do not publish them, Ithink BSIshouldapproach IRTF CFRG and publish the algorithms there, alternatively publish them as BSI documents. AsEricsson wrote in our comments on FIPS 186-5 we think it is grat that NIST is specifying ECDSA in FIPS186-5 instead of relying on references behind paywalls. We do not think that cryptographic algorithmspecifications behind paywalls are acceptable. Open access is very important for security specificationsas history has showed over and over again that lack of analysis often lead to serious weaknesses.
>
> Best Regards,
>
> John Preuß Mattsson

From: 'Stephan Ehlen' via pqc-forum <pqc-forum@list.nist.gov>
Date: Tuesday, 13 December 2022 at 17:21
To: pqc-forum <pqc-forum@list.nist.gov>
Cc: wren....@gmail.com <wren.robson@gmail.com>, pqc-forum <pqc-forum@list.nist.gov>, SH <simon@hoerder.net>, Stephan Ehlen <mail@stephanehlen.de>
Subject: Re: [pqc-forum] Request for feedback on Classic McEliece

Hi Wrenna,

at BSI, we support international standardization of FrodoKEM and Classic McEliece.

For instance, there are now some standardization efforts at ISO for PQC and

we hope that our two conservative recommendations will be part of these efforts.

Best,

Stephan

Dr. Stephan Ehlen

___

Referat KM 21 - Vorgaben an und Entwicklung von Kryptoverfahren
Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185-189
53175 Bonn
E-Mail: stephan.ehlen@bsi.bund.de
Internet: www.bsi.bund.de

#DeutschlandDigitalSicherBSI

Alle Informationen zum Umgang mit Ihren personenbezogenen
Daten finden Sie unter bsi.bund.de/datenschutz.

wren....@gmail.com schrieb am Freitag, 9. Dezember 2022 um 10:41:25 UTC+1:

> Hi Stephen,

> Is there an intention to create a standardised form of FrodoKEM? If so, under whose auspices? If not, what is to be considered the definitive version against which those who wish to follow this recommendation must compare implementations?
>
> Best,
>
> Wrenna
>
> On Fri, 9 Dec 2022, 09:37 Stephan Ehlen, <ma...@stephanehlen.de> wrote:
>
> > Dear Simon,
> >
> > dear all,
> >
> > thank you for pointing out our (BSI's) recommendations.
> >
> > Indeed, BSI recommends FrodoKEM-976 and FrodoKEM-1344
> >
> > as well as Level 3 and 5 parameters for Classic McEliece in TR-02102-1
> >
> > (see https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html).
> >
> > Even though FrodoKEM is no longer in the NIST process, we intend to keep this recommendation.
> >
> > We will evaluate draft standards of NIST's selection when they are published and (in principle)
> >
> > we are open to adding further algorithms to our technical guidelines after conclusion of our evaluation.
> >
> > Best,
> >
> > Stephan
> >
> > Dr. Stephan Ehlen
> >
> > ________________________________
> >
> > Referat KM 21 - Vorgaben an und Entwicklung von Kryptoverfahren
> > Bundesamt für Sicherheit in der Informationstechnik
> >
> > Godesberger Allee 185-189

> > 53175 Bonn
> > E-Mail: stepha...@bsi.bund.de
> > Internet: www.bsi.bund.de
> >
> > #DeutschlandDigitalSicherBSI
> >
> > Alle Informationen zum Umgang mit Ihren personenbezogenen
> > Daten finden Sie unter bsi.bund.de/datenschutz.
> >
> > On Wednesday, November 30, 2022 at 7:40:20 PM UTC+1 SH wrote:
> >
> > > Hi,
> > >
> > > Would ‘BSI compatibility’ be a valid use-case? As far as I understand, Germany’s BSI is sticking to their TR-02202-1 recommendation of Classic McEliece and FrodoKEM and does not intend to follow NISTs example of standardising CRYSTALS-Kyber. My understanding may be wrong though, would be good to hear from BSI itself. It would also be good to know whether BSI will adopt the round 4 version of Classic McEliece or whether they prefer to stay with older versions at the risk of international incompatibility.
> > >
> > > Another question that I can’t answer is whether BSI TR-02102-1 will have any impact beyond German NSS.
> > >
> > > Best,
> > >
> > > Simon
> > > (speaking for myself only)
> > >
> > > > On 30 Nov 2022, at 13:30, 'Moody, Dustin (Fed)' via pqc-forum <pqc-...@list.nist.gov> wrote:
> > > >
> > > > All,
> > > >
> > > > NIST is confident in the security of Classic McEliece and would be comfortable standardizing the submitted parameter sets (under a different claimed security strength in some cases). However, it is unclear whether Classic McEliece represents the best option for enough applications to justify standardizing it at this time. For

>>> genera lpurpose systems wishing to base their security on codes rather than lattices, BIKE or HQC may represent a more attractive option.
>>>
>>> NIST would like feedback on specific use cases for which Classic McEliece would be a good solution.
>>>
>>> Thank you,
>>>
>>> NIST PQC team
>>>
>>> --
>>>
>>> You received this message because you are subscribed to the Google Groups "pqc-forum" group.
>>> To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+...@list.nist.gov.
>>> To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/SA1PR09MB86692928B933935B57535F57E5159%40SA1PR09MB8669.namprd09.prod.outlook.com.
>>
>> --
>> You received this message because you are subscribed to the Google Groups "pqc-forum" group.
>> To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+...@list.nist.gov.
>
>> To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/fb6430c2-ce28-4f36-8481-be7b387ab283n%40list.nist.gov.

--
You received this message because you are subscribed to the Google Groups "pqc-forum" group.
To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.
To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/09daede0-fc41-493c-99a8-cfd91188a6a4n%40list.nist.gov.

From: Tobias Fehenberger <fehenberger@gmail.com> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
CC: SH <simon@hoerder.net>
Subject: Re: [pqc-forum] Request for feedback on Classic McEliece
Date: Thursday, December 15, 2022 04:52:34 AM ET

Dear NIST team, PQC community,

applications with a high bandwidth can benefit from the security of Classic McEliece. This includes high-speed optical networks where terabits of data are transmitted every second.

Since these systems are usually equipped with specialized and often low-clocked processors, the costly key generation can be avoided by reusing the public key for an appropriate number of ciphertexts as recommended by the Classic McEliece team. Furthermore, the fast encapsulation and decapsulation enables possible key update rates even below one second, which might be of interest for very high data rates.

Our real-world use-case are
1) Encrypted layer 1 optical transport solutions (OTNsec) with 10-400 Gbit/s including BSI approval

Possible future use cases are
2) MACsec using a FIPS-approved (hybrid) key agreement scheme where the Classic McEliece public key is associated to an ethernet port and can be used for multiple secure associations. This results in a very efficient post-quantum-secure key establishment.

The trade-off to be made is between (quantum) perfect forward secrecy and reusing the KEM key pair.

ADVA / Adva Network Security
SH schrieb am Mittwoch, 14. Dezember 2022 um 08:57:21 UTC+1:

> Dear Stephan, dear John, dear all,
>
> Thank you for the information, Stephan. I fully agree with John that paywalled standards such as produced by ISO are undesirable. Putting a standard behind a paywall will not just increase security risks but also hinder adoption. IETF standards, NIST FIPS and SP800 standards and BSI’s own AIS standards are successful because of they are available to be

> scrutinized and implemented by everyone. Everyone can decide whether to trust them, everyone can deploy them once they do trust.
>
> Best regards,
>
> Simon
>
> (speaking only for myself)
>
>> On 13 Dec 2022, at 20:01, John Mattsson <john.m...@ericsson.com> wrote:
>>
>> Dear Stephan Ehlen,
>>
>> If BSI wants to use FrodoKEM and Classic McEliece and NIST do not publish them, Ithink BSIshouldapproach IRTF CFRG and publish the algorithms there, alternatively publish them as BSI documents. AsEricsson wrote in our comments on FIPS 186-5 we think it is grat that NIST is specifying ECDSA in FIPS186-5 instead of relying on references behind paywalls. We do not think that cryptographic algorithmspecifications behind paywalls are acceptable. Open access is very important for security specificationsas history has showed over and over again that lack of analysis often lead to serious weaknesses.
>>
>> Best Regards,
>>
>> John Preuß Mattsson
>>
>> ---
>>
>> **From:** 'Stephan Ehlen' via pqc-forum <pqc-...@list.nist.gov>
>> **Date:** Tuesday, 13 December 2022 at 17:21
>> **To:** pqc-forum <pqc-...@list.nist.gov>
>> **Cc:** wren....@gmail.com <wren....@gmail.com>, pqc-forum <pqc-...@list.nist.gov>, SH <si...@hoerder.net>, Stephan Ehlen <ma...@stephanehlen.de>
>> **Subject:** Re: [pqc-forum] Request for feedback on Classic McEliece
>>
>> Hi Wrenna,
>>
>> at BSI, we support international standardization of FrodoKEM and Classic McEliece.
>>
>> For instance, there are now some standardization efforts at ISO for PQC and

> we hope that our two conservative recommendations will be part of these efforts.
>
> Best,
>
> Stephan
>
> Dr. Stephan Ehlen
>
> ________________________________
>
> Referat KM 21 - Vorgaben an und Entwicklung von Kryptoverfahren
> Bundesamt für Sicherheit in der Informationstechnik
>
> Godesberger Allee 185-189
> 53175 Bonn
> E-Mail: stephan.ehlen@bsi.bund.de
> Internet: www.bsi.bund.de
>
> #DeutschlandDigitalSicherBSI
>
> Alle Informationen zum Umgang mit Ihren personenbezogenen
> Daten finden Sie unter bsi.bund.de/datenschutz.
>
> wren....@gmail.com schrieb am Freitag, 9. Dezember 2022 um 10:41:25 UTC+1:
>
>> Hi Stephen,
>>
>> Is there an intention to create a standardised form of FrodoKEM? If so, under whose auspices? If not, what is to be considered the definitive version against which those who wish to follow this recommendation must compare implementations?
>>
>> Best,
>>
>> Wrenna
>>
>> On Fri, 9 Dec 2022, 09:37 Stephan Ehlen, <ma...@stephanehlen.de> wrote:
>>
>>> Dear Simon,
>>>
>>> dear all,
>>>
>>> thank you for pointing out our (BSI's) recommendations.
>>>
>>> Indeed, BSI recommends FrodoKEM-976 and FrodoKEM-1344

> > > as well as Level 3 and 5 parameters for Classic McEliece in TR-02102-1
> > >
> > > (see https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html).
> > >
> > > Even though FrodoKEM is no longer in the NIST process, we intend to keep this recommendation.
> > >
> > > We will evaluate draft standards of NIST's selection when they are published and (in principle)
> > >
> > > we are open to adding further algorithms to our technical guidelines after conclusion of our evaluation.
> > >
> > > Best,
> > >
> > > Stephan
> > >
> > > Dr. Stephan Ehlen
> > >
> > > ---
> > >
> > > Referat KM 21 - Vorgaben an und Entwicklung von Kryptoverfahren
> > > Bundesamt für Sicherheit in der Informationstechnik
> > >
> > > Godesberger Allee 185-189
> > > 53175 Bonn
> > > E-Mail: stepha...@bsi.bund.de
> > > Internet: www.bsi.bund.de
> > >
> > > #DeutschlandDigitalSicherBSI
> > >
> > > Alle Informationen zum Umgang mit Ihren personenbezogenen
> > > Daten finden Sie unter bsi.bund.de/datenschutz.
> > >
> > > On Wednesday, November 30, 2022 at 7:40:20 PM UTC+1 SH wrote:
> > >
> > > > Hi,
> > > >
> > > > Would ‘BSI compatibility’ be a valid use-case? As far as I understand, Germany’s BSI is sticking to their TR-02202-1 recommendation of Classic McEliece and FrodoKEM and does not intend to follow NISTs example of standardising

> > > CRYSTALS-Kyber. My understanding may be wrong though, would be good to hear from BSI itself. It would also be good to know whether BSI will adopt the round 4 version of Classic McEliece or whether they prefer to stay with older versions at the risk of international incompatibility.
> > >
> > > Another question that I can’t answer is whether BSI TR-02102-1 will have any impact beyond German NSS.
> > >
> > > Best,
> > >
> > > Simon
> > > (speaking for myself only)
> > >
> > > > On 30 Nov 2022, at 13:30, 'Moody, Dustin (Fed)' via pqc-forum <pqc-...@list.nist.gov> wrote:
> > > >
> > > > All,
> > > >
> > > > NIST is confident in the security of Classic McEliece and would be comfortable standardizing the submitted parameter sets (under a different claimed security strength in some cases). However, it is unclear whether Classic McEliece represents the best option for enough applications to justify standardizing it at this time. For genera lpurpose systems wishing to base their security on codes rather than lattices, BIKE or HQC may represent a more attractive option.
> > > >
> > > > NIST would like feedback on specific use cases for which Classic McEliece would be a good solution.
> > > >
> > > > Thank you,
> > > >
> > > > NIST PQC team
> > > >
> > > > --
> > > >
> > > > You received this message because you are subscribed to the Google Groups "pqc-forum" group.
> > > > To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+...@list.nist.gov.

> > > > To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/SA1PR09MB86692928B933935B57535F57E5159%40SA1PR09MB8669.namprd09.prod.outlook.com.
> > >
> > > --
> > > You received this message because you are subscribed to the Google Groups "pqc-forum" group.
> > > To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+...@list.nist.gov.
> >
> > > To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/fb6430c2-ce28-4f36-8481-be7b387ab283n%40list.nist.gov.
>
> --
> You received this message because you are subscribed to the Google Groups "pqc-forum" group.
> To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+...@list.nist.gov.
> To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/09daede0-fc41-493c-99a8-cfd91188a6a4n%40list.nist.gov.

--
You received this message because you are subscribed to the Google Groups "pqc-forum" group.
To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.
To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/88c31e0c-017a-41d5-a3ad-85105d8ef0a3n%40list.nist.gov.