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] Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized
Date: Tuesday, July 05, 2022 11:32:23 AM ET

Announcement

After careful consideration during the 3rd Round of the NIST PQC Standardization Process, NIST has identified four candidate algorithms for standardization. The primary algorithms NIST recommends be implemented for most use cases areCRYSTALS-KYBER (key-establishment) and CRYSTALS-Dilithium (digital signatures).In addition, the signature schemes Falcon and SPHINCS+ will also be standardized.

Algorithms to be Standardized

Public-Key Encryption/KEMs

CRYSTALS-KYBER

Digital Signatures

CRYSTALS-Dilithium

Falcon

SPHINCS+

CRYSTALS-KYBER (key-establishment) and CRYSTALS-Dilithium (digital signatures) were both selected for their strong security and excellent performance, and NIST expects them to work well in most applications. Falcon will also be standardized by NIST since there may be use cases for which CRYSTALS-Dilithium signatures are too large. Additionally, SPHINCS+ will be standardized to avoid only relying on the security of lattices for signatures. NIST asks for public feedback on a version of SPHINCS+ with a lower number of maximum signatures.

Additionally, the following candidate KEM algorithms will advance to the fourth round:

4th Round Candidates

Public-Key Encryption/KEMs

BIKE

Classic McEliece

HQC

SIKE

Both BIKE and HQC are based on structured codes, and either would be suitable as a general-purpose KEM that is not based on lattices. NIST expects to select at most one of these two candidates for standardization at the conclusion of thefourth round. SIKE remains an attractive candidate for standardization because of its smallkey and ciphertext sizes and will continue to study it in the fourth round. ClassicMcEliece was a finalist but is not being standardized by NIST at this time. Although ClassicMcEliece is widely regarded as secure, NIST does not anticipateit being widely used due to its large public key size. NIST may choose to standardize Classic McEliece at the end of the fourth round.

For the algorithms moving on to the fourth round, NIST will allow the submission teams to provide updated specifications and implementations (“tweaks”). The deadline for these tweaks will be **October 1, 2022**. Any submission team that feels that they may not meet the deadline should contact NIST as soon as possible. NIST will review the proposed modifications and publish the accepted submissions shortly afterwards. As a general guideline, NIST expects any modifications to be relatively minor. The fourth round will proceed similarly to the previous rounds. More detailed information and guidance will be provided in another message.

A detailed description of the decision process and rationale for selection will be included in NIST Interagency or Internal Report (NISTIR) 8413, *Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process,* which will soon be available at https://csrc.nist.gov/publications and on the NIST post-quantum webpage https://nist.gov/pqcrypto. Questions may be directed to pqc-comments@nist.gov.

NIST will create new draft standards for the algorithms to be standardized and will coordinate with the submission teams to ensure that the standards comply with the specifications. As part of the drafting process, NIST will seek input on specific parameter sets to include, particularly for security category 1. When finished, the standards will be posted for public comment. After the close of the comment period, NIST will revise the draft standards as appropriate based on the feedback received. A final review, approval, and promulgation process will then follow.

NIST will hold a 4th NIST PQC Standardization Conference on November 29 – December 1, 2022. The conference details have not yet been finalized. The preliminary Call for Papers will be posted, both on the pqc-forum and the NIST PQC webpage http://nist.gov/pqcrypto.

NIST also plans to issue a new Call for Proposals for public-key (quantum-resistant) digital signature algorithms by the end of summer 2022. NIST is primarily looking to diversify its signature portfolio, so signature schemes that are not based on structured lattices are of greatest interest. NIST would like submissions for signature schemes that have short signatures and fast verification (e.g., UOV). Submissions in response to this call will be due by June 1, 2023. Submitters are encouraged to communicate with NIST ahead of time. NIST will decide which (if any) of the submitted signature algorithms to accept and will initiate a new process for evaluation. NIST expects this process to be much smaller in scope than the current PQC process. The signature schemes accepted to this process will need to be thoroughly analyzed, which will similarly take several years.

NIST would like to thank the community and all of the submission teams for their efforts in this standardization process and hopes that the teams whose schemes were not selected to advance will continue to participate by evaluating and analyzing the remaining cryptosystems alongside the cryptographic community at large. These combined efforts are crucial to the development of NIST's future post-quantum public-key standards.

The NIST PQC team

From: Deirdre Connolly <durumcrustulum@gmail.com> 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] Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized
Date: Tuesday, July 05, 2022 11:45:12 AM ET

Congratulations and thank you to the NIST team and all the submitters! 🎇

On Tue, Jul 5, 2022, 11:32 AM 'Moody, Dustin (Fed)' via pqc-forum <pqc-forum@list.nist.gov> wrote:

> **Announcement**
>
> After careful consideration during the 3rd Round of the NIST PQC Standardization Process, NIST has identified four candidate algorithms for standardization. The primary algorithms NIST recommends be implemented for most use cases areCRYSTALS-KYBER (key-establishment) and CRYSTALS-Dilithium (digital signatures).In addition, the signature schemes Falcon and SPHINCS+ will also be standardized.
>
> **Algorithms to be Standardized**
>
> Public-Key Encryption/KEMs
>
> CRYSTALS-KYBER
>
> Digital Signatures
>
> CRYSTALS-Dilithium
>
> Falcon
>
> SPHINCS+
>
> CRYSTALS-KYBER (key-establishment) and CRYSTALS-Dilithium (digital signatures) were both selected for their strong security and excellent performance, and NIST expects them to work well in most applications. Falcon will also be standardized by NIST since there may be use cases for which CRYSTALS-Dilithium signatures are too large. Additionally, SPHINCS+ will be standardized to avoid only relying on the security of lattices for

signatures. NIST asks for public feedback on a version of SPHINCS+ with a lower number of maximum signatures.

Additionally, the following candidate KEM algorithms will advance to the fourth round:

4th Round Candidates

Public-Key Encryption/KEMs

BIKE

Classic McEliece

HQC

SIKE

Both BIKE and HQC are based on structured codes, and either would be suitable as a general-purpose KEM that is not based on lattices. NIST expects to select at most one of these two candidates for standardization at the conclusion of thefourth round. SIKE remains an attractive candidate for standardization because of its smallkey and ciphertext sizes and will continue to study it in the fourth round. ClassicMcEliece was a finalist but is not being standardized by NIST at this time. Although ClassicMcEliece is widely regarded as secure, NIST does not anticipateit being widely used due to its large public key size. NIST may choose to standardize Classic McEliece at the end of the fourth round.

For the algorithms moving on to the fourth round, NIST will allow the submission teams to provide updated specifications and implementations (“tweaks”). The deadline for these tweaks will be **October 1, 2022**. Any submission team that feels that they may not meet the deadline should contact NIST as soon as possible. NIST will review the proposed modifications and publish the accepted submissions shortly afterwards. As a general guideline, NIST expects any modifications to be relatively minor. The fourth round will proceed similarly to the previous rounds. More detailed information and guidance will be provided in another message.

A detailed description of the decision process and rationale for selection will be included in NIST Interagency or Internal Report (NISTIR) 8413, *Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process,* which will soon be available at https://csrc.nist.gov/publications and on the NIST post-quantum webpage https://nist.gov/pqcrypto. Questions may be directed to pqc-comments@nist.gov.

> NIST will create new draft standards for the algorithms to be standardized and will coordinate with the submission teams to ensure that the standards comply with the specifications. As part of the drafting process, NIST will seek input on specific parameter sets to include, particularly for security category 1. When finished, the standards will be posted for public comment. After the close of the comment period, NIST will revise the draft standards as appropriate based on the feedback received. A final review, approval, and promulgation process will then follow.
>
> NIST will hold a 4th NIST PQC Standardization Conference on November 29 – December 1, 2022. The conference details have not yet been finalized. The preliminary Call for Papers will be posted, both on the pqc-forum and the NIST PQC webpage http://nist.gov/pqcrypto.
>
> NIST also plans to issue a new Call for Proposals for public-key (quantum-resistant) digital signature algorithms by the end of summer 2022. NIST is primarily looking to diversify its signature portfolio, so signature schemes that are not based on structured lattices are of greatest interest. NIST would like submissions for signature schemes that have short signatures and fast verification (e.g., UOV). Submissions in response to this call will be due by June 1, 2023. Submitters are encouraged to communicate with NIST ahead of time. NIST will decide which (if any) of the submitted signature algorithms to accept and will initiate a new process for evaluation. NIST expects this process to be much smaller in scope than the current PQC process. The signature schemes accepted to this process will need to be thoroughly analyzed, which will similarly take several years.
>
> NIST would like to thank the community and all of the submission teams for their efforts in this standardization process and hopes that the teams whose schemes were not selected to advance will continue to participate by evaluating and analyzing the remaining cryptosystems alongside the cryptographic community at large. These combined efforts are crucial to the development of NIST's future post-quantum public-key standards.
>
> The 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/SA1PR09MB866933A15C3568FC510B4B68E5819%40SA1PR09MB8669.namprd09.prod.outlook.com.

From: Doge Protocol <dogeprotocol1@gmail.com> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
CC: dustin...@nist.gov <dustin.moody@nist.gov>
Subject: [pqc-forum] Re: Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized
Date: Tuesday, July 05, 2022 12:27:27 PM ET

Thanks NIST team!
>>>NIST would like submissions for signature schemes that have short signatures and fast verification (e.g., UOV).

On this, will having shorter public keys also be a pre-requisite for submissions or only shorter signatures is a pre-req?

Yesterday there was a paper posted that improves on Falcon signature size. Would this and similar improvements in the future also be considered eligible for submission?

On Tuesday, July 5, 2022 at 8:32:17 AM UTC-7 dustin...@nist.gov wrote:

> **Announcement**
>
> After careful consideration during the 3rd Round of the NIST PQC Standardization Process, NIST has identified four candidate algorithms for standardization. The primary algorithms NIST recommends be implemented for most use cases areCRYSTALS-KYBER (key-establishment) and CRYSTALS-Dilithium (digital signatures).In addition, the signature schemes Falcon and SPHINCS+ will also be standardized.
>
> **Algorithms to be Standardized**
>
> Public-Key Encryption/KEMs
>
> CRYSTALS-KYBER
>
> Digital Signatures
>
> CRYSTALS-Dilithium
>
> Falcon
>
> SPHINCS+

> CRYSTALS-KYBER (key-establishment) and CRYSTALS-Dilithium (digital signatures) were both selected for their strong security and excellent performance, and NIST expects them to work well in most applications. Falcon will also be standardized by NIST since there may be use cases for which CRYSTALS-Dilithium signatures are too large. Additionally, SPHINCS+ will be standardized to avoid only relying on the security of lattices for signatures. NIST asks for public feedback on a version of SPHINCS+ with a lower number of maximum signatures.
>
> Additionally, the following candidate KEM algorithms will advance to the fourth round:
>
> **4th Round Candidates**
>
> Public-Key Encryption/KEMs
>
> BIKE
>
> Classic McEliece
>
> HQC
>
> SIKE
>
> Both BIKE and HQC are based on structured codes, and either would be suitable as a general-purpose KEM that is not based on lattices. NIST expects to select at most one of these two candidates for standardization at the conclusion of thefourth round. SIKE remains an attractive candidate for standardization because of its smallkey and ciphertext sizes and will continue to study it in the fourth round. ClassicMcEliece was a finalist but is not being standardized by NIST at this time. Although ClassicMcEliece is widely regarded as secure, NIST does not anticipateit being widely used due to its large public key size. NIST may choose to standardize Classic McEliece at the end of the fourth round.
>
> For the algorithms moving on to the fourth round, NIST will allow the submission teams to provide updated specifications and implementations (“tweaks”). The deadline for these tweaks will be **October 1, 2022**. Any submission team that feels that they may not meet the deadline should contact NIST as soon as possible. NIST will review the proposed modifications and publish the accepted submissions shortly afterwards. As a general guideline, NIST expects any modifications to be relatively minor. The fourth round will proceed similarly to the previous rounds. More detailed information and guidance will be provided in another message.

> A detailed description of the decision process and rationale for selection will be included in NIST Interagency or Internal Report (NISTIR) 8413, *Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process*, which will soon be available at https://csrc.nist.gov/publications and on the NIST post-quantum webpage https://nist.gov/pqcrypto. Questions may be directed to pqc-co...@nist.gov.
>
> NIST will create new draft standards for the algorithms to be standardized and will coordinate with the submission teams to ensure that the standards comply with the specifications. As part of the drafting process, NIST will seek input on specific parameter sets to include, particularly for security category 1. When finished, the standards will be posted for public comment. After the close of the comment period, NIST will revise the draft standards as appropriate based on the feedback received. A final review, approval, and promulgation process will then follow.
>
> NIST will hold a 4th NIST PQC Standardization Conference on November 29 – December 1, 2022. The conference details have not yet been finalized. The preliminary Call for Papers will be posted, both on the pqc-forum and the NIST PQC webpage http://nist.gov/pqcrypto.
>
> NIST also plans to issue a new Call for Proposals for public-key (quantum-resistant) digital signature algorithms by the end of summer 2022. NIST is primarily looking to diversify its signature portfolio, so signature schemes that are not based on structured lattices are of greatest interest. NIST would like submissions for signature schemes that have short signatures and fast verification (e.g., UOV). Submissions in response to this call will be due by June 1, 2023. Submitters are encouraged to communicate with NIST ahead of time. NIST will decide which (if any) of the submitted signature algorithms to accept and will initiate a new process for evaluation. NIST expects this process to be much smaller in scope than the current PQC process. The signature schemes accepted to this process will need to be thoroughly analyzed, which will similarly take several years.
>
> NIST would like to thank the community and all of the submission teams for their efforts in this standardization process and hopes that the teams whose schemes were not selected to advance will continue to participate by evaluating and analyzing the remaining cryptosystems alongside the cryptographic community at large. These combined efforts are crucial to the development of NIST’s future post-quantum public-key standards.
>
> The NIST PQC team

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] RE: Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized
Date: Tuesday, July 05, 2022 01:34:36 PM ET

Guidelines for submitting tweaks for Fourth Round Candidates

Deadline: October 1, 2022

Candidate teams must meet the same submission requirements and minimum acceptability criteria stated in the original Call for Proposals. Submissions must be submitted to NIST at pqc-submissions@nist.gov by October 1, 2022. Submissions should include a cover sheet, algorithm specifications (and other supporting documentation), and optical/digital media (e.g., implementations, known-answer test files, etc.) as described in Section 2 of the original Call For Proposals. In addition, NIST requires a short document outlining the modifications introduced in the new submission. This document should be included in the supporting documentation folder of the submission (see Section 2.C.4 of the CFP). NIST will review the proposed changes to determine whether they meet the submission requirements and minimum acceptability requirements, as well as whether they significantly affect the design of the algorithm and require a major reevaluation. As a general guideline, NIST expects any modifications to be relatively minor. It would be helpful if submission teams provided NIST with a summary of their expected changes prior to the deadline. If the deadline will pose a problem for any submission team, they should contact NIST in advance.

NIST does NOT need new signed IP statements unless new submission team members have

been added or the status of intellectual property for the submission has changed. If either of

these cases apply, NIST will need new signed IP statements (see Section 2.D of the CFP). These

statements must be actual hard copies – not digital scans – and must be provided to NIST by the 4th NIST PQC Standardization Conference (December 1, 2022).

NIST is aware that some submission packages may be large in size. The email system for pqc-submissions@nist.gov can only accept files up to 25MB. For larger files, candidate teams may upload submission packages at a location of their choosing and send NIST the download link. If that option is not suitable, NIST has a file transfer system that can be used (please email pqc-comments@nist.gov for more details). NIST will review the submitted packages as quickly as possible and post the candidate submission packages that are complete and proper on www.nist.gov/pqcrypto. Teams are encouraged to submit early. General questions may be asked on the pqc-forum. For more specific questions, please email pqc-comments@nist.gov.

The NIST PQC team

From: 'Moody, Dustin (Fed)' via pqc-forum <pqc-forum@list.nist.gov>
Sent: Tuesday, July 5, 2022 11:32 AM
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: [pqc-forum] Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized

Announcement

After careful consideration during the 3rd Round of the NIST PQC Standardization Process, NIST has identified four candidate algorithms for standardization. The primary algorithms NIST recommends be implemented for most use cases areCRYSTALS-KYBER (key-establishment) and CRYSTALS-Dilithium (digital signatures).In addition, the signature schemes Falcon and SPHINCS+ will also be standardized.

Algorithms to be Standardized

Public-Key Encryption/KEMs

CRYSTALS-KYBER

Digital Signatures

CRYSTALS-Dilithium

Falcon

SPHINCS+

CRYSTALS-KYBER (key-establishment) and CRYSTALS-Dilithium (digital signatures) were both selected for their strong security and excellent performance, and NIST expects them to work well in most applications. Falcon will also be standardized by NIST since there may be use cases for which CRYSTALS-Dilithium signatures are too large. Additionally, SPHINCS+

will be standardized to avoid only relying on the security of lattices for signatures. NIST asks for public feedback on a version of SPHINCS+ with a lower number of maximum signatures.

Additionally, the following candidate KEM algorithms will advance to the fourth round:

4th Round Candidates

Public-Key Encryption/KEMs

BIKE

Classic McEliece

HQC

SIKE

Both BIKE and HQC are based on structured codes, and either would be suitable as a general-purpose KEM that is not based on lattices. NIST expects to select at most one of these two candidates for standardization at the conclusion of thefourth round. SIKE remains an attractive candidate for standardization because of its smallkey and ciphertext sizes and will continue to study it in the fourth round. ClassicMcEliece was a finalist but is not being standardized by NIST at this time. Although ClassicMcEliece is widely regarded as secure, NIST does not anticipateit being widely used due to its large public key size. NIST may choose to standardize Classic McEliece at the end of the fourth round.

For the algorithms moving on to the fourth round, NIST will allow the submission teams to provide updated specifications and implementations ("tweaks"). The deadline for these tweaks will be **October 1, 2022**. Any submission team that feels that they may not meet the deadline should contact NIST as soon as possible. NIST will review the proposed modifications and publish the accepted submissions shortly afterwards. As a general guideline, NIST expects any modifications to be relatively minor. The fourth round will proceed similarly to the previous rounds. More detailed information and guidance will be provided in another message.

A detailed description of the decision process and rationale for selection will be included in NIST Interagency or Internal Report (NISTIR) 8413, *Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process,* which will soon be available at https://csrc.nist.gov/publications and on the NIST post-quantum webpage https://nist.gov/pqcrypto. Questions may be directed to pqc-comments@nist.gov.

NIST will create new draft standards for the algorithms to be standardized and will coordinate with the submission teams to ensure that the standards comply with the specifications. As part of the drafting process, NIST will seek input on specific parameter sets to include, particularly for security category 1. When finished, the standards will be posted for public comment. After the close of the comment period, NIST will revise the draft standards as appropriate based on the feedback received. A final review, approval, and promulgation process will then follow.

NIST will hold a 4th NIST PQC Standardization Conference on November 29 – December 1, 2022. The conference details have not yet been finalized. The preliminary Call for Papers will be posted, both on the pqc-forum and the NIST PQC webpage http://nist.gov/pqcrypto.

NIST also plans to issue a new Call for Proposals for public-key (quantum-resistant) digital signature algorithms by the end of summer 2022. NIST is primarily looking to diversify its signature portfolio, so signature schemes that are not based on structured lattices are of greatest interest. NIST would like submissions for signature schemes that have short signatures and fast verification (e.g., UOV). Submissions in response to this call will be due by June 1, 2023. Submitters are encouraged to communicate with NIST ahead of time. NIST will decide which (if any) of the submitted signature algorithms to accept and will initiate a new process for evaluation. NIST expects this process to be much smaller in scope than the current PQC process. The signature schemes accepted to this process will need to be thoroughly analyzed, which will similarly take several years.

NIST would like to thank the community and all of the submission teams for their efforts in this standardization process and hopes that the teams whose schemes were not selected to advance will continue to participate by evaluating and analyzing the remaining cryptosystems alongside the cryptographic community at large. These combined efforts are crucial to the development of NIST's future post-quantum public-key standards.

The NIST PQC team

--

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] RE: Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized
Date:	Tuesday, July 05, 2022 01:35:04 PM ET

During PQC Standardization, the United States Department of Commerce's National Institute of Standards and Technology (NIST) has worked on selecting a cryptographic key encapsulation algorithm that would protect information from attacks by classical and quantum computers. In furtherance of NIST's PQC Standardization efforts, NIST and Dr. Jintai Ding announce intentions to enter into a patent license agreement, wherein a patent owned by Dr. Ding's Ohio-based company, Algo Consulting, would be licensed to NIST. As a result of this patent license agreement, implementers and end users of NIST's PQC standard, which will be based on the selected cryptographic key encapsulation algorithm, will not need a separate license from Algo Consulting, Inc. This will promote the timely and widespread adoption of NIST's PQC standard, a shared goal of NIST and Dr. Ding.

NIST appreciates Dr. Ding's efforts and cooperation and will announce its selection of the cryptographic key encapsulation algorithm as soon as reasonably possible.

The NIST PQC team

Dr. Jintai Ding, owner Algo Consulting, Inc.

From: 'Moody, Dustin (Fed)' via pqc-forum <pqc-forum@list.nist.gov>

Sent: Tuesday, July 5, 2022 11:32 AM

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

Subject: [pqc-forum] Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized

Announcement

After careful consideration during the 3rd Round of the NIST PQC Standardization Process, NIST has identified four candidate algorithms for standardization. The primary algorithms NIST recommends be implemented for most use cases areCRYSTALS-KYBER (key-establishment) and CRYSTALS-Dilithium (digital signatures).In addition, the signature schemes Falcon and SPHINCS+ will also be standardized.

Algorithms to be Standardized

Public-Key Encryption/KEMs

CRYSTALS-KYBER

Digital Signatures

CRYSTALS-Dilithium

Falcon

SPHINCS+

CRYSTALS-KYBER (key-establishment) and CRYSTALS-Dilithium (digital signatures) were both selected for their strong security and excellent performance, and NIST expects them to work well in most applications. Falcon will also be standardized by NIST since there may be use cases for which CRYSTALS-Dilithium signatures are too large. Additionally, SPHINCS+ will be standardized to avoid only relying on the security of lattices for signatures. NIST asks for public feedback on a version of SPHINCS+ with a lower number of maximum signatures.

Additionally, the following candidate KEM algorithms will advance to the fourth round:

4th Round Candidates

Public-Key Encryption/KEMs

BIKE

Classic McEliece

HQC

SIKE

Both BIKE and HQC are based on structured codes, and either would be suitable as a general-purpose KEM that is not based on lattices. NIST expects to select at most one of these two candidates for standardization at the conclusion of thefourth round. SIKE remains an attractive candidate for standardization because of its smallkey and ciphertext sizes and will continue to study it in the fourth round. ClassicMcEliece was a finalist but is not being standardized by NIST at this time. Although ClassicMcEliece is widely regarded as secure, NIST does not anticipateit being widely used due to its large public key size. NIST may choose to standardize Classic McEliece at the end of the fourth round.

For the algorithms moving on to the fourth round, NIST will allow the submission teams to provide updated specifications and implementations ("tweaks"). The deadline for these tweaks will be **October 1, 2022**. Any submission team that feels that they may not meet the deadline should contact NIST as soon as possible. NIST will review the proposed modifications and publish the accepted submissions shortly afterwards. As a general guideline, NIST expects any modifications to be relatively minor. The fourth round will proceed similarly to the previous rounds. More detailed information and guidance will be provided in another message.

A detailed description of the decision process and rationale for selection will be included in NIST Interagency or Internal Report (NISTIR) 8413, *Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process*, which will soon be available at https://csrc.nist.gov/publications and on the NIST post-quantum webpage https://nist.gov/pqcrypto. Questions may be directed to pqc-comments@nist.gov.

NIST will create new draft standards for the algorithms to be standardized and will coordinate with the submission teams to ensure that the standards comply with the specifications. As part of the drafting process, NIST will seek input on specific parameter sets to include, particularly for security category 1. When finished, the standards will be posted for public comment. After the close of the comment period, NIST will revise the draft standards as appropriate based on the feedback received. A final review, approval, and promulgation process will then follow.

NIST will hold a 4th NIST PQC Standardization Conference on November 29 – December 1, 2022. The conference details have not yet been finalized. The preliminary Call for Papers will be posted, both on the pqc-forum and the NIST PQC webpage http://nist.gov/pqcrypto.

NIST also plans to issue a new Call for Proposals for public-key (quantum-resistant) digital signature algorithms by the end of summer 2022. NIST is primarily looking to diversify its signature portfolio, so signature schemes that are not based on structured lattices are of greatest interest. NIST would like submissions for signature schemes that have short signatures and fast verification (e.g., UOV). Submissions in response to this call will be due by June 1, 2023. Submitters are encouraged to communicate with NIST ahead of time. NIST will decide which (if any) of the submitted signature algorithms to accept and will initiate a new process for evaluation. NIST expects this process to be much smaller in scope than the current PQC process. The signature schemes accepted to this process will need to be thoroughly analyzed, which will similarly take several years.

NIST would like to thank the community and all of the submission teams for their efforts in this standardization process and hopes that the teams whose schemes were not selected to advance will continue to participate by evaluating and analyzing the remaining cryptosystems alongside the cryptographic community at large. These combined efforts are crucial to the development of NIST’s future post-quantum public-key standards.

The NIST PQC team

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] RE: Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized
Date: Tuesday, July 05, 2022 01:35:34 PM ET

Call for Papers for the 4th NIST PQC Standardization Conference

Location: Virtual

November 29 – December 1, 2022

Submission deadline: September 15, 2022

(Conference without proceedings)

NIST plans to hold the 4th NIST PQC Standardization Conference from November 29 to December 1, 2022. The purpose of the conference is to discuss various aspects of the candidate algorithms and to obtain valuable feedback for informing decisions on standardization. NIST will invite the submission teams for both the selected algorithms, as well as the algorithms advancing to the fourth round, to give an update on their algorithms.

In addition, NIST is soliciting research and discussion papers, surveys, presentations, case

studies, panel proposals, and participation from all interested parties, including researchers,

system architects, implementors, vendors, and users. NIST will post the accepted papers and

presentations on the conference website after the conference; however, no formal proceedings

will be published. NIST encourages the submission of presentations and reports on preliminary

work that participants plan to publish elsewhere.

Topics for submissions should include but are not limited to:

- Classical and quantum cryptanalysis of the algorithms, including cryptanalysis of weakened or toy versions
- Analysis of relative performance or resource requirements for some or all of the algorithms
- Assessments of classical and quantum security strengths of the algorithms
- Systemization of knowledge relevant to the NIST PQC standardization process
- Substantial improvements in the implementation of algorithms
- Improved analysis or proofs of properties of finalists/candidates, even when this does not lead to any attack
- Proposed criteria to be used for selecting algorithms for standardization
- Impacts to existing applications and protocols (e.g., changes needed to accommodate specific algorithms)
- Steps or strategies for organizations to prepare for the coming transition

Submissions should be provided electronically, in PDF, for standard US letter-size paper (8.5 x

11 inches). Submitted papers must not exceed 20 pages, excluding references and appendices

(single space, with 1-inch margins using a 10 pt or larger font). Proposals for panels should be

no longer than five pages and should include possible panelists and an indication of which

panelists have confirmed their participation.

Please submit the following information to pqc2022@nist.gov:

- Name, affiliation, email, phone number (optional), postal address (optional) for the primary submitter
- First name, last name, and affiliation of each co-submitter
- Finished paper, presentation, or panel proposal in PDF format as an attachment

All submissions will be acknowledged.

General information about the conference, including registration information, will be available at the conference website: http://www.nist.gov/pqcrypto.

From: 'Moody, Dustin (Fed)' via pqc-forum <pqc-forum@list.nist.gov>
Sent: Tuesday, July 5, 2022 11:32 AM
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: [pqc-forum] Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized

Announcement

After careful consideration during the 3rd Round of the NIST PQC Standardization Process, NIST has identified four candidate algorithms for standardization. The primary algorithms NIST recommends be implemented for most use cases areCRYSTALS-KYBER (key-establishment) and CRYSTALS-Dilithium (digital signatures).In addition, the signature schemes Falcon and SPHINCS+ will also be standardized.

Algorithms to be Standardized

Public-Key Encryption/KEMs

CRYSTALS-KYBER

Digital Signatures

CRYSTALS-Dilithium

Falcon

SPHINCS+

CRYSTALS-KYBER (key-establishment) and CRYSTALS-Dilithium (digital signatures) were both selected for their strong security and excellent performance, and NIST expects them to work well in most applications. Falcon will also be standardized by NIST since there may be use cases for which CRYSTALS-Dilithium signatures are too large. Additionally, SPHINCS+ will be standardized to avoid only relying on the security of lattices for signatures. NIST asks for public feedback on a version of SPHINCS+ with a lower number of maximum signatures.

Additionally, the following candidate KEM algorithms will advance to the fourth round:

4th Round Candidates

Public-Key Encryption/KEMs

BIKE

Classic McEliece

HQC

SIKE

Both BIKE and HQC are based on structured codes, and either would be suitable as a general-purpose KEM that is not based on lattices. NIST expects to select at most one of these two candidates for standardization at the conclusion of thefourth round. SIKE remains an attractive candidate for standardization because of its smallkey and ciphertext sizes and will continue to study it in the fourth round. ClassicMcEliece was a finalist but is not being standardized by NIST at this time. Although ClassicMcEliece is widely regarded as secure, NIST does not anticipateit being widely used due to its large public key size. NIST may choose to standardize Classic McEliece at the end of the fourth round.

For the algorithms moving on to the fourth round, NIST will allow the submission teams to provide updated specifications and implementations (“tweaks”). The deadline for these tweaks will be **October 1, 2022**. Any submission team that feels that they may not meet the deadline should contact NIST as soon as possible. NIST will review the proposed modifications and publish the accepted submissions shortly afterwards. As a general guideline, NIST expects any modifications to be relatively minor. The fourth round will proceed similarly to the previous rounds. More detailed information and guidance will be provided in another message.

A detailed description of the decision process and rationale for selection will be included in NIST Interagency or Internal Report (NISTIR) 8413, *Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process,* which will soon be available at https://csrc.nist.gov/publications and on the NIST post-quantum webpage https://nist.gov/pqcrypto. Questions may be directed to pqc-comments@nist.gov.

NIST will create new draft standards for the algorithms to be standardized and will coordinate with the submission teams to ensure that the standards comply with the specifications. As part of the drafting process, NIST will seek input on specific parameter sets to include, particularly for security category 1. When finished, the standards will be posted for public comment. After the close of the comment period, NIST will revise the draft standards as appropriate based on the feedback received. A final review, approval, and promulgation process will then follow.

NIST will hold a 4th NIST PQC Standardization Conference on November 29 – December 1, 2022. The conference details have not yet been finalized. The preliminary Call for Papers will be posted, both on the pqc-forum and the NIST PQC webpage http://nist.gov/pqcrypto.

NIST also plans to issue a new Call for Proposals for public-key (quantum-resistant) digital signature algorithms by the end of summer 2022. NIST is primarily looking to diversify its signature portfolio, so signature schemes that are not based on structured lattices are of greatest interest. NIST would like submissions for signature schemes that have short signatures and fast verification (e.g., UOV). Submissions in response to this call will be due by June 1, 2023. Submitters are encouraged to communicate with NIST ahead of time. NIST will decide which (if any) of the submitted signature algorithms to accept and will initiate a new process for evaluation. NIST expects this process to be much smaller in scope than the current PQC process. The signature schemes accepted to this process will need to be thoroughly analyzed, which will similarly take several years.

NIST would like to thank the community and all of the submission teams for their efforts in this standardization process and hopes that the teams whose schemes were not selected to advance will continue to participate by evaluating and analyzing the remaining cryptosystems alongside the cryptographic community at large. These combined efforts are crucial to the development of NIST’s future post-quantum public-key standards.

The NIST PQC team

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] RE: Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized
Date: Tuesday, July 05, 2022 01:36:38 PM ET

Sorry for so many messages!

Here's the link to the official NIST announcement. Please share:

https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms

Here's the link to *NISTIR 8413: Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process*, which explains the rationale behind the decisions.

https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8413.pdf

Dustin

From: 'Moody, Dustin (Fed)' via pqc-forum <pqc-forum@list.nist.gov>
Sent: Tuesday, July 5, 2022 11:32 AM
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: [pqc-forum] Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized

Announcement

After careful consideration during the 3rd Round of the NIST PQC Standardization Process, NIST has identified four candidate algorithms for standardization. The primary algorithms NIST recommends be implemented for most use cases areCRYSTALS-KYBER (key-establishment) and CRYSTALS-Dilithium (digital signatures).In addition, the signature schemes Falcon and SPHINCS+ will also be standardized.

Algorithms to be Standardized

Public-Key Encryption/KEMs

CRYSTALS-KYBER

Digital Signatures

CRYSTALS-Dilithium

Falcon

SPHINCS+

CRYSTALS-KYBER (key-establishment) and CRYSTALS-Dilithium (digital signatures) were both selected for their strong security and excellent performance, and NIST expects them to work well in most applications. Falcon will also be standardized by NIST since there may be use cases for which CRYSTALS-Dilithium signatures are too large. Additionally, SPHINCS+ will be standardized to avoid only relying on the security of lattices for signatures. NIST asks for public feedback on a version of SPHINCS+ with a lower number of maximum signatures.

Additionally, the following candidate KEM algorithms will advance to the fourth round:

4th Round Candidates

Public-Key Encryption/KEMs

BIKE

Classic McEliece

HQC

SIKE

Both BIKE and HQC are based on structured codes, and either would be suitable as a general-purpose KEM that is not based on lattices. NIST expects to select at most one of these two candidates for standardization at the conclusion of thefourth round. SIKE remains an attractive candidate for standardization because of its smallkey and ciphertext sizes and will continue to study it in the fourth round. ClassicMcEliece was a finalist but is not being standardized by NIST at this time. Although ClassicMcEliece is widely regarded as secure, NIST does not anticipateit being widely used due to its large public key size. NIST may choose to standardize Classic McEliece at the end of the fourth round.

For the algorithms moving on to the fourth round, NIST will allow the submission teams to provide updated specifications and implementations ("tweaks"). The deadline for these tweaks will be **October 1, 2022**. Any submission team that feels that they may not meet the deadline should contact NIST as soon as possible. NIST will review the proposed modifications and publish the accepted submissions shortly afterwards. As a general guideline, NIST expects any modifications to be relatively minor. The fourth round will proceed similarly to the previous rounds. More detailed information and guidance will be provided in another message.

A detailed description of the decision process and rationale for selection will be included in NIST Interagency or Internal Report (NISTIR) 8413, *Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process*, which will soon be available at https://csrc.nist.gov/publications and on the NIST post-quantum webpage https://nist.gov/pqcrypto. Questions may be directed to pqc-comments@nist.gov.

NIST will create new draft standards for the algorithms to be standardized and will coordinate with the submission teams to ensure that the standards comply with the specifications. As part of the drafting process, NIST will seek input on specific parameter sets to include, particularly for security category 1. When finished, the standards will be posted for public comment. After the close of the comment period, NIST will revise the draft standards as appropriate based on the feedback received. A final review, approval, and promulgation process will then follow.

NIST will hold a 4th NIST PQC Standardization Conference on November 29 – December 1, 2022. The conference details have not yet been finalized. The preliminary Call for Papers will be posted, both on the pqc-forum and the NIST PQC webpage http://nist.gov/pqcrypto.

NIST also plans to issue a new Call for Proposals for public-key (quantum-resistant) digital signature algorithms by the end of summer 2022. NIST is primarily looking to diversify its signature portfolio, so signature schemes that are not based on structured lattices are of greatest interest. NIST would like submissions for signature schemes that have short signatures and fast verification (e.g., UOV). Submissions in response to this call will be due by June 1, 2023. Submitters are encouraged to communicate with NIST ahead of time. NIST will decide which (if any) of the submitted signature algorithms to accept and will initiate a new process for evaluation. NIST expects this process to be much smaller in scope than the current PQC process. The signature schemes accepted to this process will need to be thoroughly analyzed, which will similarly take several years.

NIST would like to thank the community and all of the submission teams for their efforts in this standardization process and hopes that the teams whose schemes were not selected to advance will continue to participate by evaluating and analyzing the remaining cryptosystems alongside the cryptographic community at large. These combined efforts are crucial to the development of NIST's future post-quantum public-key standards.

The NIST PQC team

--

From: ToTheMars ABC <abctothemars@gmail.com> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
CC: dustin...@nist.gov <dustin.moody@nist.gov>
Subject: [pqc-forum] Re: Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized
Date: Tuesday, July 05, 2022 01:50:37 PM ET

Can someone tell me why there is no rainbow signature in the list? Isn't it a 3rd round finalist?
瞳2022괴7墩5휑槿팍랑 UTC 17:36:32<dustin...@nist.gov> 旳矣：

> Sorry for so many messages!
>
> Here's the link to the official NIST announcement. Please share:
>
> https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms
>
> Here's the link to *NISTIR 8413: Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process*, which explains the rationale behind the decisions.
>
> https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8413.pdf
>
> Dustin
>
> **From:** 'Moody, Dustin (Fed)' via pqc-forum <pqc-...@list.nist.gov>
>
> **Sent:** Tuesday, July 5, 2022 11:32 AM
>
> **To:** pqc-forum <pqc-...@list.nist.gov>
>
> **Subject:** [pqc-forum] Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized
>
> ## Announcement
>
> After careful consideration during the 3rd Round of the NIST PQC Standardization Process, NIST has identified four candidate algorithms for standardization. The primary algorithms NIST recommends be implemented for most use cases areCRYSTALS-KYBER (key-establishment) and CRYSTALS-Dilithium (digital signatures).In addition, the signature schemes Falcon and SPHINCS+ will also be standardized.
>
> ### Algorithms to be Standardized

Public-Key Encryption/KEMs

CRYSTALS-KYBER

Digital Signatures

CRYSTALS-Dilithium

Falcon

SPHINCS+

CRYSTALS-KYBER (key-establishment) and CRYSTALS-Dilithium (digital signatures) were both selected for their strong security and excellent performance, and NIST expects them to work well in most applications. Falcon will also be standardized by NIST since there may be use cases for which CRYSTALS-Dilithium signatures are too large. Additionally, SPHINCS+ will be standardized to avoid only relying on the security of lattices for signatures. NIST asks for public feedback on a version of SPHINCS+ with a lower number of maximum signatures.

Additionally, the following candidate KEM algorithms will advance to the fourth round:

4th Round Candidates

Public-Key Encryption/KEMs

BIKE

Classic McEliece

HQC

SIKE

Both BIKE and HQC are based on structured codes, and either would be suitable as a general-purpose KEM that is not based on lattices. NIST expects to select at most one of these two candidates for standardization at the conclusion of thefourth round. SIKE remains an attractive candidate for standardization because of its smallkey and ciphertext sizes and will continue to study it in the fourth round. ClassicMcEliece was a finalist but is not being standardized by NIST at this time. Although ClassicMcEliece is widely regarded as secure, NIST does not anticipateit being widely used due to its large public key size. NIST may choose to standardize Classic McEliece at the end of the fourth round.

For the algorithms moving on to the fourth round, NIST will allow the submission teams to provide updated specifications and implementations (“tweaks”). The deadline for these tweaks will be **October 1, 2022**. Any submission team that feels that they may not meet the deadline should contact NIST as soon as possible. NIST will review the proposed modifications and publish the accepted submissions shortly afterwards. As a general guideline, NIST expects any modifications to be relatively minor. The fourth round will proceed similarly to the previous rounds. More detailed information and guidance will be provided in another message.

A detailed description of the decision process and rationale for selection will be included in NIST Interagency or Internal Report (NISTIR) 8413, *Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process,* which will soon be available at https://csrc.nist.gov/publications and on the NIST post-quantum webpage https://nist.gov/pqcrypto. Questions may be directed to pqc-co...@nist.gov.

NIST will create new draft standards for the algorithms to be standardized and will coordinate with the submission teams to ensure that the standards comply with the specifications. As part of the drafting process, NIST will seek input on specific parameter sets to include, particularly for security category 1. When finished, the standards will be posted for public comment. After the close of the comment period, NIST will revise the draft standards as appropriate based on the feedback received. A final review, approval, and promulgation process will then follow.

NIST will hold a 4th NIST PQC Standardization Conference on November 29 쬚 December 1, 2022. The conference details have not yet been finalized. The preliminary Call for Papers will be posted, both on the pqc-forum and the NIST PQC webpage http://nist.gov/pqcrypto.

NIST also plans to issue a new Call for Proposals for public-key (quantum-resistant) digital signature algorithms by the end of summer 2022. NIST is primarily looking to diversify its signature portfolio, so signature schemes that are not based on structured lattices are of greatest interest. NIST would like submissions for signature schemes that have short signatures and fast verification (e.g., UOV). Submissions in response to this call will be due by June 1, 2023. Submitters are encouraged to communicate with NIST ahead of time. NIST will decide which (if any) of the submitted signature algorithms to accept and will initiate a new process for evaluation. NIST expects this process to be much

> smaller in scope than the current PQC process. The signature schemes accepted to this process will need to be thoroughly analyzed, which will similarly take several years.
>
> NIST would like to thank the community and all of the submission teams for their efforts in this standardization process and hopes that the teams whose schemes were not selected to advance will continue to participate by evaluating and analyzing the remaining cryptosystems alongside the cryptographic community at large. These combined efforts are crucial to the development of NIST's future post-quantum public-key standards.
>
> The 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/SA1PR09MB866933A15C3568FC510B4B68E5819%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/6dcf19bd-afa4-4ee6-98f6-e3b8012d0013n%40list.nist.gov.

From: Gustavo Banegas <gustavo@cryptme.in> via pqc-forum <pqc-forum@list.nist.gov>
To: ToTheMars ABC <abctothemars@gmail.com>, pqc-forum <pqc-forum@list.nist.gov>
CC: dustin...@nist.gov <dustin.moody@nist.gov>
Subject: Re: [pqc-forum] Re: Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized
Date: Tuesday, July 05, 2022 01:54:23 PM ET

Well,
As Dustin pointed in the first email, there is a report that details all the choices. It includes why some of the schemes were not selected. For Rainbow, please read page 51.

All the best,
Gustavo

On July 5, 2022 7:50:26 PM GMT+02:00, ToTheMars ABC <abctothemars@gmail.com> wrote:

> Can someone tell me why there is no rainbow signature in the list? Isn't it a 3rd round finalist?
> ÔÚ2022Äę7ÔÂ5ČŐĐÇĆÚ¶ţ UTC 17:36:32<dustin...@nist.gov> Đ´µŔŁş
>
> > Sorry for so many messages!
> >
> > Hereˇ¯s the link to the official NIST announcement. Please share:
> >
> > https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms
> >
> > Hereˇ¯s the link to *NISTIR 8413: Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process*, which explains the rationale behind the decisions.
> >
> > https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8413.pdf
> >
> > Dustin
> >
> > ---
> >
> > **From:** 'Moody, Dustin (Fed)' via pqc-forum <pqc-...@list.nist.gov>
> > **Sent:** Tuesday, July 5, 2022 11:32 AM
> > **To:** pqc-forum <pqc-...@list.nist.gov>
> > **Subject:** [pqc-forum] Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized

> > **Announcement**
> >
> > After careful consideration during the 3rd Round of the NIST PQC Standardization Process, NIST has identified four candidate algorithms for standardization. The primary algorithms NIST recommends be implemented for most use cases areCRYSTALS-KYBER (key-establishment) and CRYSTALS-Dilithium (digital signatures).In addition, the signature schemes Falcon and SPHINCS+ will also be standardized.
> >
> > **Algorithms to be Standardized**
> >
> > Public-Key Encryption/KEMs
> >
> > CRYSTALS-KYBER
> >
> > Digital Signatures
> >
> > CRYSTALS-Dilithium
> >
> > Falcon
> >
> > SPHINCS+
> >
> > CRYSTALS-KYBER (key-establishment) and CRYSTALS-Dilithium (digital signatures) were both selected for their strong security and excellent performance, and NIST expects them to work well in most applications. Falcon will also be standardized by NIST since there may be use cases for which CRYSTALS-Dilithium signatures are too large. Additionally, SPHINCS+ will be standardized to avoid only relying on the security of lattices for signatures. NIST asks for public feedback on a version of SPHINCS+ with a lower number of maximum signatures.
> >
> > Additionally, the following candidate KEM algorithms will advance to the fourth round:
> >
> > **4th Round Candidates**
> >
> > Public-Key Encryption/KEMs
> >
> > BIKE
> >
> > Classic McEliece
> >
> > HQC
> >
> > SIKE

> > Both BIKE and HQC are based on structured codes, and either would be suitable as a general-purpose KEM that is not based on lattices. NIST expects to select at most one of these two candidates for standardization at the conclusion of thefourth round. SIKE remains an attractive candidate for standardization because of its smallkey and ciphertext sizes and will continue to study it in the fourth round. ClassicMcEliece was a finalist but is not being standardized by NIST at this time. Although ClassicMcEliece is widely regarded as secure, NIST does not anticipateit being widely used due to its large public key size. NIST may choose to standardize Classic McEliece at the end of the fourth round.
> >
> > For the algorithms moving on to the fourth round, NIST will allow the submission teams to provide updated specifications and implementations (ˇ°tweaksˇ±). The deadline for these tweaks will be **October 1, 2022**. Any submission team that feels that they may not meet the deadline should contact NIST as soon as possible. NIST will review the proposed modifications and publish the accepted submissions shortly afterwards. As a general guideline, NIST expects any modifications to be relatively minor. The fourth round will proceed similarly to the previous rounds. More detailed information and guidance will be provided in another message.
> >
> > A detailed description of the decision process and rationale for selection will be included in NIST Interagency or Internal Report (NISTIR) 8413, *Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process,* which will soon be available at https://csrc.nist.gov/publications and on the NIST post-quantum webpage https://nist.gov/pqcrypto. Questions may be directed to pqc-co...@nist.gov.
> >
> > NIST will create new draft standards for the algorithms to be standardized and will coordinate with the submission teams to ensure that the standards comply with the specifications. As part of the drafting process, NIST will seek input on specific parameter sets to include, particularly for security category 1. When finished, the standards will be posted for public comment. After the close of the comment period, NIST will revise the draft standards as appropriate based on the feedback received. A final review, approval, and promulgation process will then follow.
> >
> > NIST will hold a 4th NIST PQC Standardization Conference on November 29 ¨C December 1, 2022. The conference details have not yet been finalized. The preliminary Call for Papers will be posted, both on the pqc-forum and the NIST PQC webpage http://nist.gov/pqcrypto.

> > NIST also plans to issue a new Call for Proposals for public-key (quantum-resistant) digital signature algorithms by the end of summer 2022. NIST is primarily looking to diversify its signature portfolio, so signature schemes that are not based on structured lattices are of greatest interest. NIST would like submissions for signature schemes that have short signatures and fast verification (e.g., UOV). Submissions in response to this call will be due by June 1, 2023. Submitters are encouraged to communicate with NIST ahead of time. NIST will decide which (if any) of the submitted signature algorithms to accept and will initiate a new process for evaluation. NIST expects this process to be much smaller in scope than the current PQC process. The signature schemes accepted to this process will need to be thoroughly analyzed, which will similarly take several years.
> >
> > NIST would like to thank the community and all of the submission teams for their efforts in this standardization process and hopes that the teams whose schemes were not selected to advance will continue to participate by evaluating and analyzing the remaining cryptosystems alongside the cryptographic community at large. These combined efforts are crucial to the development of NISTˇŻs future post-quantum public-key standards.
> >
> > The 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/SA1PR09MB866933A15C3568FC510B4B68E5819%40SA1PR09MB8669.namprd09.prod.outlook.com.

--
Sent from my Android device with K-9 Mail. Please excuse my brevity.

From: D. J. Bernstein <djb@cr.yp.to> via pqc-forum@list.nist.gov
To: pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] RE: Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized
Date: Tuesday, July 05, 2022 04:04:19 PM ET
Attachments: smime.p7m

'Moody, Dustin (Fed)' via pqc-forum writes:

> NIST and Dr. Jintai Ding announce intentions to enter into a patent
> license agreement

Great. Is there a specific schedule for the completion of this agreement?

  [implementors and end users]

> will not need a separate license

That's good to hear. But will the agreement have limitations and poison pills similar to the "grant" that NIST previously obtained from ISARA (https://web.archive.org/web/20201101181903/https://www.isara.com/nist-grant.html)?

In any case, congratulations to Dr. Ding and the rest of the Kyber team regarding Kyber's selection for standardization!

---D. J. Bernstein

P.S. Also, regarding signatures, congratulations to the Dilithium and Falcon teams! And, since I'm just one of a huge number of members of the SPHINCS+ team, maybe I'm allowed to congratulate SPHINCS+ too.

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] Re: Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized
Date: Wednesday, July 06, 2022 12:24:48 PM ET

FYI

CNRS has posted a statement on their website.

https://www.cnrs.fr/fr/accord-de-licence-entre-le-nist-le-cnrs-et-luniversite-de-limoges-le-rayonnement-international-de

Dustin Moody

NIST PQC

From: 'Moody, Dustin (Fed)' via pqc-forum <pqc-forum@list.nist.gov>
Sent: Tuesday, July 5, 2022 1:36 PM
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: [pqc-forum] RE: Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized

Sorry for so many messages!

Here's the link to the official NIST announcement. Please share:

https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms

Here's the link to *NISTIR 8413: Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process*, which explains the rationale behind the decisions.

https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8413.pdf

Dustin

From: 'Moody, Dustin (Fed)' via pqc-forum <pqc-forum@list.nist.gov>
Sent: Tuesday, July 5, 2022 11:32 AM

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

Subject: [pqc-forum] Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized

Announcement

After careful consideration during the 3rd Round of the NIST PQC Standardization Process, NIST has identified four candidate algorithms for standardization. The primary algorithms NIST recommends be implemented for most use cases areCRYSTALS-KYBER (key-establishment) and CRYSTALS-Dilithium (digital signatures).In addition, the signature schemes Falcon and SPHINCS+ will also be standardized.

Algorithms to be Standardized

Public-Key Encryption/KEMs

CRYSTALS-KYBER

Digital Signatures

CRYSTALS-Dilithium

Falcon

SPHINCS+

CRYSTALS-KYBER (key-establishment) and CRYSTALS-Dilithium (digital signatures) were both selected for their strong security and excellent performance, and NIST expects them to work well in most applications. Falcon will also be standardized by NIST since there may be use cases for which CRYSTALS-Dilithium signatures are too large. Additionally, SPHINCS+ will be standardized to avoid only relying on the security of lattices for signatures. NIST asks for public feedback on a version of SPHINCS+ with a lower number of maximum signatures.

Additionally, the following candidate KEM algorithms will advance to the fourth round:

4th Round Candidates

Public-Key Encryption/KEMs

BIKE

Classic McEliece

HQC

SIKE

Both BIKE and HQC are based on structured codes, and either would be suitable as a general-purpose KEM that is not based on lattices. NIST expects to select at most one of these two candidates for standardization at the conclusion of thefourth round. SIKE remains an attractive candidate for standardization because of its smallkey and ciphertext sizes and will continue to study it in the fourth round. ClassicMcEliece was a finalist but is not being standardized by NIST at this time. Although ClassicMcEliece is widely regarded as secure, NIST does not anticipateit being widely used due to its large public key size. NIST may choose to standardize Classic McEliece at the end of the fourth round.

For the algorithms moving on to the fourth round, NIST will allow the submission teams to provide updated specifications and implementations (“tweaks”). The deadline for these tweaks will be **October 1, 2022**. Any submission team that feels that they may not meet the deadline should contact NIST as soon as possible. NIST will review the proposed modifications and publish the accepted submissions shortly afterwards. As a general guideline, NIST expects any modifications to be relatively minor. The fourth round will proceed similarly to the previous rounds. More detailed information and guidance will be provided in another message.

A detailed description of the decision process and rationale for selection will be included in NIST Interagency or Internal Report (NISTIR) 8413, *Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process,* which will soon be available at https://csrc.nist.gov/publications and on the NIST post-quantum webpage https://nist.gov/pqcrypto. Questions may be directed to pqc-comments@nist.gov.

NIST will create new draft standards for the algorithms to be standardized and will coordinate with the submission teams to ensure that the standards comply with the specifications. As part of the drafting process, NIST will seek input on specific parameter sets to include, particularly for security category 1. When finished, the standards will be posted for public comment. After the close of the comment period, NIST will revise the draft standards as appropriate based on the feedback received. A final review, approval, and promulgation process will then follow.

NIST will hold a 4th NIST PQC Standardization Conference on November 29 – December 1, 2022. The conference details have not yet been finalized. The preliminary Call for Papers will be posted, both on the pqc-forum and the NIST PQC webpage http://nist.gov/pqcrypto.

NIST also plans to issue a new Call for Proposals for public-key (quantum-resistant) digital signature algorithms by the end of summer 2022. NIST is primarily looking to diversify its signature portfolio, so signature schemes that are not based on structured lattices are of greatest interest. NIST would like submissions for signature schemes that have short signatures and fast verification (e.g., UOV). Submissions in response to this call will be due by June 1, 2023. Submitters are encouraged to communicate with NIST ahead of time. NIST will decide which (if any) of the submitted signature algorithms to accept and will initiate a new process for evaluation. NIST expects this process to be much smaller in scope than the current PQC process. The signature schemes accepted to this process will need to be thoroughly analyzed, which will similarly take several years.

NIST would like to thank the community and all of the submission teams for their efforts in this standardization process and hopes that the teams whose schemes were not selected to advance will continue to participate by evaluating and analyzing the remaining cryptosystems alongside the cryptographic community at large. These combined efforts are crucial to the development of NIST's future post-quantum public-key standards.

The 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/SA1PR09MB866933A15C3568FC510B4B68E5819%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/SA1PR09MB866994EA8023F512F6E1C5FEE5819%40SA1PR09MB8669.namprd09.prod.outlook.com.

From: Scott Fluhrer (sfluhrer) <sfluhrer@cisco.com> via pqc-forum <pqc-forum@list.nist.gov>
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>, pqc-forum <pqc-forum@list.nist.gov>
Subject: [pqc-forum] RE: Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized
Date: Wednesday, July 06, 2022 01:14:35 PM ET

Can we get the text of the actual license agreement between NIST and CNRS/University of Limoges?

From: 'Moody, Dustin (Fed)' via pqc-forum <pqc-forum@list.nist.gov>
Sent: Wednesday, July 6, 2022 12:24 PM
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: [pqc-forum] Re: Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized

FYI

CNRS has posted a statement on their website.

https://www.cnrs.fr/fr/accord-de-licence-entre-le-nist-le-cnrs-et-luniversite-de-limoges-le-rayonnement-international-de

Dustin Moody

NIST PQC

From: 'Moody, Dustin (Fed)' via pqc-forum <pqc-forum@list.nist.gov>
Sent: Tuesday, July 5, 2022 1:36 PM
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: [pqc-forum] RE: Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized

Sorry for so many messages!

Here’s the link to the official NIST announcement. Please share:

https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms

Here's the link to *NISTIR 8413: Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process*, which explains the rationale behind the decisions.

https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8413.pdf

Dustin

From: 'Moody, Dustin (Fed)' via pqc-forum <pqc-forum@list.nist.gov>
Sent: Tuesday, July 5, 2022 11:32 AM
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: [pqc-forum] Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized

Announcement

After careful consideration during the 3rd Round of the NIST PQC Standardization Process, NIST has identified four candidate algorithms for standardization. The primary algorithms NIST recommends be implemented for most use cases areCRYSTALS-KYBER (key-establishment) and CRYSTALS-Dilithium (digital signatures).In addition, the signature schemes Falcon and SPHINCS+ will also be standardized.

Algorithms to be Standardized

Public-Key Encryption/KEMs

CRYSTALS-KYBER

Digital Signatures

CRYSTALS-Dilithium

Falcon

SPHINCS+

CRYSTALS-KYBER (key-establishment) and CRYSTALS-Dilithium (digital signatures) were both selected for their strong security and excellent performance, and NIST expects them to work well in most applications. Falcon will also be standardized by NIST since there may be use cases for which CRYSTALS-Dilithium signatures are too large. Additionally, SPHINCS+ will be standardized to avoid only relying on the security of lattices for signatures. NIST asks for public feedback on a version of SPHINCS+ with a lower number of maximum signatures.

Additionally, the following candidate KEM algorithms will advance to the fourth round:

4th Round Candidates

Public-Key Encryption/KEMs

BIKE

Classic McEliece

HQC

SIKE

Both BIKE and HQC are based on structured codes, and either would be suitable as a general-purpose KEM that is not based on lattices. NIST expects to select at most one of these two candidates for standardization at the conclusion of thefourth round. SIKE remains an attractive candidate for standardization because of its smallkey and ciphertext sizes and will continue to study it in the fourth round. ClassicMcEliece was a finalist but is not being standardized by NIST at this time. Although ClassicMcEliece is widely regarded as secure, NIST does not anticipateit being widely used due to its large public key size. NIST may choose to standardize Classic McEliece at the end of the fourth round.

For the algorithms moving on to the fourth round, NIST will allow the submission teams to provide updated specifications and implementations (“tweaks”). The deadline for these tweaks will be **October 1, 2022**. Any submission team that feels that they may not meet the deadline should contact NIST as soon as possible. NIST will review the proposed modifications and publish the accepted submissions shortly afterwards. As a general guideline, NIST expects any modifications to be relatively minor. The fourth round will proceed similarly to the previous rounds. More detailed information and guidance will be provided in another message.

A detailed description of the decision process and rationale for selection will be included in NIST Interagency or Internal Report (NISTIR) 8413, *Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process,* which will soon be available at https://csrc.nist.gov/publications and on the NIST post-quantum webpage https://nist.gov/pqcrypto. Questions may be directed to pqc-comments@nist.gov.

NIST will create new draft standards for the algorithms to be standardized and will coordinate with the submission teams to ensure that the standards comply with the specifications. As part of the drafting process, NIST will seek input on specific parameter sets to include, particularly for security category 1. When finished, the standards will be posted for public comment. After the close of the comment period, NIST will revise the draft standards as appropriate based on the feedback received. A final review, approval, and promulgation process will then follow.

NIST will hold a 4th NIST PQC Standardization Conference on November 29 – December 1, 2022. The conference details have not yet been finalized. The preliminary Call for Papers will be posted, both on the pqc-forum and the NIST PQC webpage http://nist.gov/pqcrypto.

NIST also plans to issue a new Call for Proposals for public-key (quantum-resistant) digital signature algorithms by the end of summer 2022. NIST is primarily looking to diversify its signature portfolio, so signature schemes that are not based on structured lattices are of greatest interest. NIST would like submissions for signature schemes that have short signatures and fast verification (e.g., UOV). Submissions in response to this call will be due by June 1, 2023. Submitters are encouraged to communicate with NIST ahead of time. NIST will decide which (if any) of the submitted signature algorithms to accept and will initiate a new process for evaluation. NIST expects this process to be much smaller in scope than the current PQC process. The signature schemes accepted to this process will need to be thoroughly analyzed, which will similarly take several years.

NIST would like to thank the community and all of the submission teams for their efforts in this standardization process and hopes that the teams whose schemes were not selected to advance will continue to participate by evaluating and analyzing the remaining cryptosystems alongside the cryptographic community at large. These combined efforts are crucial to the development of NIST’s future post-quantum public-key standards.

The NIST PQC team

--

To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/SA1PR09MB866933A15C3568FC510B4B68E5819%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/SA1PR09MB866994EA8023F512F6E1C5FEE5819%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/SA1PR09MB86697183D3615A85EB2FAC3BE5809%40SA1PR09MB8669.namprd09.prod.outlook.com.

From: John Mattsson <john.mattsson@ericsson.com> via pqc-forum <pqc-forum@list.nist.gov>
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: [pqc-forum] Re: Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized
Date: Wednesday, July 06, 2022 02:01:32 PM ET

Hi,

Do anybody know if we can expect an update of the CNSA suite in a few days or will it take months? That is another very important announcement. The NSA PQC FAQ states:

"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"

https://www.nsa.gov/Cybersecurity/Post-Quantum-Cybersecurity-Resources/

Suite B was very influencial. The algorithms, modes, and parameters chosen for CNSA will likely have a big influence onenterprises and various industries.

Cheers,

John Preuß Mattsson

From: EL HASSANE LAAJI <e.laaji@ump.ac.ma> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] Re: Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized
Date: Wednesday, July 06, 2022 02:18:08 PM ET

Hi.

Congratulations to the teams whose schemes were selected.
I ask if the NTRU scheme (Public-Key Encryption/KEMs), will die???
Best regards.

Le mer. 6 juil. 2022 à 19:01, 'John Mattsson' via pqc-forum <pqc-forum@list.nist.gov> a écrit :

> Hi,
>
> Do anybody know if we can expect an update of the CNSA suite in a few days or will it take months? That is another very important announcement. The NSA PQC FAQ states:
>
> "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"
>
> https://www.nsa.gov/Cybersecurity/Post-Quantum-Cybersecurity-Resources/
>
> Suite B was very influencial. The algorithms, modes, and parameters chosen for CNSA will likely have a big influence onenterprises and various industries.
>
> Cheers,
>
> John Preuß Mattsson
>
> --

> HE1PR0701MB3050DE85057A661E22566FB989809%40HE1PR0701MB3050.eurprd07.prod.outlook.com.

--

From: Mike Ounsworth <mike.ounsworth@entrust.com> via pqc-forum <pqc-forum@list.nist.gov>
To: John Mattsson <john.mattsson@ericsson.com>, pqc-forum <pqc-forum@list.nist.gov>
Subject: [pqc-forum] RE: Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized
Date: Wednesday, July 06, 2022 02:24:58 PM ET

I assume that the standards need to be written before they can be adopted into the CNSA Suite?

Mike Ounsworth

From: 'John Mattsson' via pqc-forum <pqc-forum@list.nist.gov>
Sent: July 6, 2022 1:01 PM
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: [EXTERNAL] [pqc-forum] Re: Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized

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

Hi,

Do anybody know if we can expect an update of the CNSA suite in a few days or will it take months? That is another very important announcement. The NSA PQC FAQ states:

"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"

https://www.nsa.gov/Cybersecurity/Post-Quantum-Cybersecurity-Resources/

Suite B was very influencial. The algorithms, modes, and parameters chosen for CNSA will likely have a big influence on enterprises and various industries.

Cheers,

John Preuß Mattsson

--
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/HE1PR0701MB3050DE85057A661E22566FB989809%40HE1PR0701MB3050.eurprd07.prod.outlook.com.

Any email and files/attachments transmitted with it are confidential and are intended solely for the use of the individual or entity to whom they are addressed. If this message has been sent to you in error, you must not copy, distribute or disclose of the information it contains. Please notify Entrust immediately and delete the message from your system.

From: Q R <amzoti@gmail.com> via pqc-forum@list.nist.gov
To: John Mattsson <john.mattsson@ericsson.com>
CC: pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] Re: Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized
Date: Wednesday, July 06, 2022 02:37:08 PM ET

That is an excellent question.

I cannot imagine how anyone can implement these without having the final standards from NIST.

It does not seem like a good approach to just say - go use the algorithms as-is because it seems like there is a lot of work yet to be done with finalizing parameters, making algorithms more human readable, providing guidance on how to use alg and security levels, etc.

The current NSA guidance ups key sizes to help protect against Q-Day and Y2Q and NIST also added support for hybrid shared keys, pre-shared keys and ITU added hybrid certificates.

As I currently understand it, teams should be
- creating a data inventory with sensitivity
- creating a crypto inventory with details
- determining is a hybrid method is needed to protect against the store-now / decrypt later attack
- figuring out ways to add crypto agility from internal, open-source and commercial products
- doing the NIST guidance on preparing for PQC transition
- experimenting with things like Open Quantum Safe and its spinoffs (TLS, SSH, S/MIME ...)
- learning how to do optimizations for lattice based methods
- exploring all their use cases for the different devices and how these algorithms may impact choosing parameters sets and which algs to use

Bottom line, I know NSA wants to move fast once the standards are
complete, but it does seem immature that that is now.

However, I cannot speak for anyone so take all my comments with a grain of salt.

-Amzoti

On 7/6/22, 'John Mattsson' via pqc-forum <pqc-forum@list.nist.gov> wrote:
> Hi,
>
> Do anybody know if we can expect an update of the CNSA suite in a few days
> or will it take months? That is another very important announcement. The NSA
> PQC FAQ states:
>
> "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"
>
> https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.nsa.gov%2FCybersecurity%2FPost-Quantum-Cybersecurity-Resources%2F&amp;data=05%7C01%7Cyi-kai.liu%40nist.gov%7C0fd4a80c9cf749c0f59e08da5f7e86c8%7C2ab5d82fd8fa4797a93e054655c61dec%7C1%7C0%7C637927294284440846%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&amp;sdata=6YHflB2ikaCWMoqwSE%2FpWiGr%2FRSuVe2QvtKhQhaXGMc%3D&amp;reserved=0
>
> Suite B was very influencial. The algorithms, modes, and parameters chosen
> for CNSA will likely have a big influence on enterprises and various
> industries.
>
> Cheers,
> John Preuß Mattsson
>
> --
> 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/
HE1PR0701MB3050DE85057A661E22566FB989809%40HE1PR0701MB3050.eurprd07.prod.outlook.com.
>

--

From: Moody, Dustin (Fed) <dustin.moody@nist.gov> via pqc-forum <pqc-forum@list.nist.gov>
To: Doge Protocol <dogeprotocol1@gmail.com>, pqc-forum <pqc-forum@list.nist.gov>
Subject: [pqc-forum] RE: Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized
Date: Thursday, July 07, 2022 01:56:03 PM ET

As stated in our announcement yesterday: "NIST also plans to issue a new Call for Proposals for public-key (quantum-resistant) digital signature algorithms by the end of summer 2022. NIST is primarily looking to diversify its signature portfolio, so signature schemes that are not based on structured lattices are of greatest interest. NIST would like submissions for signature schemes that have short signatures and fast verification. Submissions in response to this call will be due by June 1, 2023. Submitters are encouraged to communicate with NIST ahead of time. NIST will decide which (if any) of the submitted signature algorithms to accept and will initiate a new process for evaluation. NIST expects this process to be much smaller in scope than the current PQC process. The signature schemes accepted to this process will need to be thoroughly analyzed, which will similarly take several years."

We're willing to look at any (including lattice-based) signature scheme, but we will only move them forward in the "on-ramp" standardization process if they align with the stated priorities above. For lattice-based signatures, they would also need to substantially improve over what we already selected. NIST will consider the submissions on a case by case basis. You can look for more detailed information when the new call for signatures is released.

Dustin Moody

NIST

From: Doge Protocol <dogeprotocol1@gmail.com>
Sent: Tuesday, July 5, 2022 12:27 PM
To: pqc-forum <pqc-forum@list.nist.gov>
Cc: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized

Thanks NIST team!

>>>NIST would like submissions for signature schemes that have short signatures and fast verification (e.g., UOV).

On this, will having shorter public keys also be a pre-requisite for submissions or only shorter signatures is a pre-req?

Yesterday there was a paper posted that improves on Falcon signature size. Would this and similar improvements in the future also be considered eligible for submission?

On Tuesday, July 5, 2022 at 8:32:17 AM UTC-7 dustin...@nist.gov wrote:

> **Announcement**
>
> After careful consideration during the 3rd Round of the NIST PQC Standardization Process, NIST has identified four candidate algorithms for standardization. The primary algorithms NIST recommends be implemented for most use cases areCRYSTALS-KYBER (key-establishment) and CRYSTALS-Dilithium (digital signatures).In addition, the signature schemes Falcon and SPHINCS+ will also be standardized.
>
> **Algorithms to be Standardized**
>
> Public-Key Encryption/KEMs
>
> CRYSTALS-KYBER
>
> Digital Signatures
>
> CRYSTALS-Dilithium
>
> Falcon
>
> SPHINCS+
>
> CRYSTALS-KYBER (key-establishment) and CRYSTALS-Dilithium (digital signatures) were both selected for their strong security and excellent performance, and NIST expects them to work well in most applications. Falcon will also be standardized by NIST since there may be use cases for which CRYSTALS-Dilithium signatures are too large. Additionally, SPHINCS+ will be standardized to avoid only relying on the security of lattices for signatures. NIST asks for public feedback on a version of SPHINCS+ with a lower number of maximum signatures.
>
> Additionally, the following candidate KEM algorithms will advance to the fourth round:
>
> **4th Round Candidates**

> Public-Key Encryption/KEMs
>
> BIKE
>
> Classic McEliece
>
> HQC
>
> SIKE
>
> Both BIKE and HQC are based on structured codes, and either would be suitable as a general-purpose KEM that is not based on lattices. NIST expects to select at most one of these two candidates for standardization at the conclusion of thefourth round. SIKE remains an attractive candidate for standardization because of its smallkey and ciphertext sizes and will continue to study it in the fourth round. ClassicMcEliece was a finalist but is not being standardized by NIST at this time. Although ClassicMcEliece is widely regarded as secure, NIST does not anticipateit being widely used due to its large public key size. NIST may choose to standardize Classic McEliece at the end of the fourth round.
>
> For the algorithms moving on to the fourth round, NIST will allow the submission teams to provide updated specifications and implementations ("tweaks"). The deadline for these tweaks will be **October 1, 2022**. Any submission team that feels that they may not meet the deadline should contact NIST as soon as possible. NIST will review the proposed modifications and publish the accepted submissions shortly afterwards. As a general guideline, NIST expects any modifications to be relatively minor. The fourth round will proceed similarly to the previous rounds. More detailed information and guidance will be provided in another message.
>
> A detailed description of the decision process and rationale for selection will be included in NIST Interagency or Internal Report (NISTIR) 8413, *Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process*, which will soon be available at https://csrc.nist.gov/publications and on the NIST post-quantum webpage https://nist.gov/pqcrypto. Questions may be directed to pqc-co...@nist.gov.
>
> NIST will create new draft standards for the algorithms to be standardized and will coordinate with the submission teams to ensure that the standards comply with the specifications. As part of the drafting process, NIST will seek input on specific parameter sets to include, particularly for security category 1. When finished, the standards will be posted for public comment. After the close of the comment period, NIST will revise the

> draft standards as appropriate based on the feedback received. A final review, approval, and promulgation process will then follow.
>
> NIST will hold a 4th NIST PQC Standardization Conference on November 29 – December 1, 2022. The conference details have not yet been finalized. The preliminary Call for Papers will be posted, both on the pqc-forum and the NIST PQC webpage http://nist.gov/pqcrypto.
>
> NIST also plans to issue a new Call for Proposals for public-key (quantum-resistant) digital signature algorithms by the end of summer 2022. NIST is primarily looking to diversify its signature portfolio, so signature schemes that are not based on structured lattices are of greatest interest. NIST would like submissions for signature schemes that have short signatures and fast verification (e.g., UOV). Submissions in response to this call will be due by June 1, 2023. Submitters are encouraged to communicate with NIST ahead of time. NIST will decide which (if any) of the submitted signature algorithms to accept and will initiate a new process for evaluation. NIST expects this process to be much smaller in scope than the current PQC process. The signature schemes accepted to this process will need to be thoroughly analyzed, which will similarly take several years.
>
> NIST would like to thank the community and all of the submission teams for their efforts in this standardization process and hopes that the teams whose schemes were not selected to advance will continue to participate by evaluating and analyzing the remaining cryptosystems alongside the cryptographic community at large. These combined efforts are crucial to the development of NIST’s future post-quantum public-key standards.
>
> The NIST PQC team

From: Scott Fluhrer (sfluhrer) <sfluhrer@cisco.com> via pqc-forum <pqc-forum@list.nist.gov>
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>, pqc-forum <pqc-forum@list.nist.gov>
CC: Jonathan Felten (jfelten) <jfelten@cisco.com>
Subject: [pqc-forum] RE: Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized
Date: Friday, July 15, 2022 02:55:20 PM ET

Let me be more explicit.

I have not talked to the Cisco execs; I cannot imagine that they would approve the use of Kyber without an assessment of the Cisco liability (and associated licensing fees, if any).

I have not talked to the Cisco lawyers; I cannot imagine that they would be willing to give any such assurance without an examination of the licenses (and an examination of the press releases would not be sufficient).

Hence, until we get the text of the licenses (both the one signed with CNRS and the one to be signed with Algo Consulting), Cisco cannot use Kyber. If continues to be true, we will need to seek an alternative solution.

> **From:** Scott Fluhrer (sfluhrer)
> **Sent:** Wednesday, July 6, 2022 1:14 PM
> **To:** Moody, Dustin (Fed) <dustin.moody@nist.gov>; pqc-forum <pqc-forum@list.nist.gov>
> **Subject:** RE: Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized
>
> Can we get the text of the actual license agreement between NIST and CNRS/University of Limoges?
>
>> **From:** 'Moody, Dustin (Fed)' via pqc-forum <pqc-forum@list.nist.gov>
>> **Sent:** Wednesday, July 6, 2022 12:24 PM
>> **To:** pqc-forum <pqc-forum@list.nist.gov>
>> **Subject:** [pqc-forum] Re: Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized
>>
>> FYI
>>
>> CNRS has posted a statement on their website.

https://www.cnrs.fr/fr/accord-de-licence-entre-le-nist-le-cnrs-et-luniversite-de-limoges-le-rayonnement-international-de

Dustin Moody

NIST PQC

From: 'Moody, Dustin (Fed)' via pqc-forum <pqc-forum@list.nist.gov>
Sent: Tuesday, July 5, 2022 1:36 PM
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: [pqc-forum] RE: Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized

Sorry for so many messages!

Here's the link to the official NIST announcement. Please share:

https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms

Here's the link to *NISTIR 8413: Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process*, which explains the rationale behind the decisions.

https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8413.pdf

Dustin

From: 'Moody, Dustin (Fed)' via pqc-forum <pqc-forum@list.nist.gov>
Sent: Tuesday, July 5, 2022 11:32 AM
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: [pqc-forum] Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized

Announcement

After careful consideration during the 3rd Round of the NIST PQC Standardization Process, NIST has identified four candidate algorithms for standardization. The primary algorithms NIST recommends be implemented for most use cases areCRYSTALS-KYBER (key-establishment) and CRYSTALS-

Dilithium (digital signatures).In addition, the signature schemes Falcon and SPHINCS+ will also be standardized.

Algorithms to be Standardized

Public-Key Encryption/KEMs

CRYSTALS-KYBER

Digital Signatures

CRYSTALS-Dilithium

Falcon

SPHINCS+

CRYSTALS-KYBER (key-establishment) and CRYSTALS-Dilithium (digital signatures) were both selected for their strong security and excellent performance, and NIST expects them to work well in most applications. Falcon will also be standardized by NIST since there may be use cases for which CRYSTALS-Dilithium signatures are too large. Additionally, SPHINCS+ will be standardized to avoid only relying on the security of lattices for signatures. NIST asks for public feedback on a version of SPHINCS+ with a lower number of maximum signatures.

Additionally, the following candidate KEM algorithms will advance to the fourth round:

4th Round Candidates

Public-Key Encryption/KEMs

BIKE

Classic McEliece

HQC

SIKE

Both BIKE and HQC are based on structured codes, and either would be suitable as a general-purpose KEM that is not based on lattices. NIST expects to select at most one of these two candidates for standardization at the conclusion of thefourth round. SIKE remains an attractive candidate for standardization because of its smallkey and ciphertext sizes and will continue to study it in the fourth round. ClassicMcEliece was a finalist but is not being standardized by NIST at this time. Although ClassicMcEliece is widely regarded as secure, NIST does not anticipateit being widely used due to its large public key size. NIST may choose to standardize Classic McEliece at the end of the fourth round.

For the algorithms moving on to the fourth round, NIST will allow the submission teams to provide updated specifications and implementations (“tweaks”). The deadline for these tweaks will be **October 1, 2022**. Any submission team that feels that they may not meet the deadline should contact NIST as soon as possible. NIST will review the proposed modifications and publish the accepted submissions shortly afterwards. As a general guideline, NIST expects any modifications to be relatively minor. The fourth round will proceed similarly to the previous rounds. More detailed information and guidance will be provided in another message.

A detailed description of the decision process and rationale for selection will be included in NIST Interagency or Internal Report (NISTIR) 8413, *Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process,* which will soon be available at https://csrc.nist.gov/publications and on the NIST post-quantum webpage https://nist.gov/pqcrypto. Questions may be directed to pqc-comments@nist.gov.

NIST will create new draft standards for the algorithms to be standardized and will coordinate with the submission teams to ensure that the standards comply with the specifications. As part of the drafting process, NIST will seek input on specific parameter sets to include, particularly for security category 1. When finished, the standards will be posted for public comment. After the close of the comment period, NIST will revise the draft standards as appropriate based on the feedback received. A final review, approval, and promulgation process will then follow.

NIST will hold a 4th NIST PQC Standardization Conference on November 29 – December 1, 2022. The conference details have not yet been finalized. The preliminary Call for Papers will be posted, both on the pqc-forum and the NIST PQC webpage http://nist.gov/pqcrypto.

NIST also plans to issue a new Call for Proposals for public-key (quantum-resistant) digital signature algorithms by the end of summer 2022. NIST is primarily looking to diversify its signature portfolio, so signature schemes that are not based on structured lattices are of greatest interest. NIST would like submissions for signature schemes that have short signatures and fast verification (e.g., UOV). Submissions in response to this call will be due by June 1, 2023. Submitters are encouraged to communicate with NIST ahead of time. NIST will decide which (if any) of the submitted signature algorithms to accept and will initiate a new process for evaluation. NIST expects this process to be much smaller in scope than the current PQC process. The signature schemes accepted to this process will need to be thoroughly analyzed, which will similarly take several years.

NIST would like to thank the community and all of the submission teams for their efforts in this standardization process and hopes that the teams whose schemes were not selected to advance will continue to participate by evaluating and analyzing the remaining cryptosystems alongside the cryptographic community at large. These combined efforts are crucial to the development of NIST's future post-quantum public-key standards.

The 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/SA1PR09MB866933A15C3568FC510B4B68E5819%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/SA1PR09MB866994EA8023F512F6E1C5FEE5819%40SA1PR09MB8669.namprd09.prod.outlook.com.

From: Daniel Apon <dapon.crypto@gmail.com> via pqc-forum@list.nist.gov
To: Scott Fluhrer (sfluhrer) <sfluhrer@cisco.com>
CC: Moody, Dustin (Fed) <dustin.moody@nist.gov>, pqc-forum <pqc-forum@list.nist.gov>, Jonathan Felten (jfelten) <jfelten@cisco.com>
Subject: Re: [pqc-forum] RE: Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized
Date: Friday, July 15, 2022 03:12:58 PM ET

This connects to another pressing issue, for which there is not yet a concrete recommendation from NIST, at least as far as I'm aware:

When does NIST recommend that an interested organization should begin their actual migration to post-quantum cryptography *deployment* based on the July 5th, 2022 announcement?
(Of course, prior to such a "go" date, many practical, preliminary steps can be completed in preparation for the migration date. But that aside..)

As this issue arises in context: Scott says that Cisco cannot use Kyber until Cisco receives the text of the licenses (CNRS/Algo) -- and presumably has sufficient, interluding time for Cisco lawyers to examine the text of the licenses.

1) At which point in time does NIST intend for (for example) Cisco -- or any other organization -- to begin migration to Kyber (or Dilithium/Falcon/SPHINCS+)?
2) At which point in time will the text of the licenses (CNRS/Algo) be posted publicly?

Speaking in my personal capacity in my role at MITRE (having not spoken with MITRE execs or MITRE lawyers either),
--Daniel

On Fri, Jul 15, 2022 at 2:55 PM 'Scott Fluhrer (sfluhrer)' via pqc-forum <pqc-forum@list.nist.gov> wrote:

> Let me be more explicit.
>
> I have not talked to the Cisco execs; I cannot imagine that they would approve the use of Kyber without an assessment of the Cisco liability (and associated licensing fees, if any).

> I have not talked to the Cisco lawyers; I cannot imagine that they would be willing to give any such assurance without an examination of the licenses (and an examination of the press releases would not be sufficient).
>
> Hence, until we get the text of the licenses (both the one signed with CNRS and the one to be signed with Algo Consulting), Cisco cannot use Kyber. If continues to be true, we will need to seek an alternative solution.
>
> ---
>
>> **From:** Scott Fluhrer (sfluhrer)
>> **Sent:** Wednesday, July 6, 2022 1:14 PM
>> **To:** Moody, Dustin (Fed) <dustin.moody@nist.gov>; pqc-forum <pqc-forum@list.nist.gov>
>> **Subject:** RE: Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized
>>
>> Can we get the text of the actual license agreement between NIST and CNRS/ University of Limoges?
>
> ---
>
>>> **From:** 'Moody, Dustin (Fed)' via pqc-forum <pqc-forum@list.nist.gov>
>>> **Sent:** Wednesday, July 6, 2022 12:24 PM
>>> **To:** pqc-forum <pqc-forum@list.nist.gov>
>>> **Subject:** [pqc-forum] Re: Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized
>>>
>>> FYI
>>>
>>> CNRS has posted a statement on their website.
>>>
>>> https://www.cnrs.fr/fr/accord-de-licence-entre-le-nist-le-cnrs-et-luniversite-de-limoges-le-rayonnement-international-de
>>>
>>> Dustin Moody
>>>
>>> NIST PQC
>>>
>>> **From:** 'Moody, Dustin (Fed)' via pqc-forum <pqc-forum@list.nist.gov>
>>> **Sent:** Tuesday, July 5, 2022 1:36 PM
>>> **To:** pqc-forum <pqc-forum@list.nist.gov>
>>> **Subject:** [pqc-forum] RE: Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized

Sorry for so many messages!

Here’s the link to the official NIST announcement. Please share:

https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms

Here’s the link to *NISTIR 8413: Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process*, which explains the rationale behind the decisions.

https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8413.pdf

Dustin

From: 'Moody, Dustin (Fed)' via pqc-forum <pqc-forum@list.nist.gov>
Sent: Tuesday, July 5, 2022 11:32 AM
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: [pqc-forum] Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized

Announcement

After careful consideration during the 3rd Round of the NIST PQC Standardization Process, NIST has identified four candidate algorithms for standardization. The primary algorithms NIST recommends be implemented for most use cases areCRYSTALS-KYBER (key-establishment) and CRYSTALS-Dilithium (digital signatures).In addition, the signature schemes Falcon and SPHINCS+ will also be standardized.

Algorithms to be Standardized

Public-Key Encryption/KEMs

CRYSTALS-KYBER

Digital Signatures

CRYSTALS-Dilithium

Falcon

SPHINCS+

CRYSTALS-KYBER (key-establishment) and CRYSTALS-Dilithium (digital signatures) were both selected for their strong security and excellent performance, and NIST expects them to work well in most applications. Falcon will also be standardized by NIST since there may be use cases for which CRYSTALS-Dilithium signatures are too large. Additionally, SPHINCS+ will be standardized to avoid only relying on the security of lattices for signatures. NIST asks for public feedback on a version of SPHINCS+ with a lower number of maximum signatures.

Additionally, the following candidate KEM algorithms will advance to the fourth round:

4th Round Candidates

Public-Key Encryption/KEMs

BIKE

Classic McEliece

HQC

SIKE

Both BIKE and HQC are based on structured codes, and either would be suitable as a general-purpose KEM that is not based on lattices. NIST expects to select at most one of these two candidates for standardization at the conclusion of thefourth round. SIKE remains an attractive candidate for standardization because of its smallkey and ciphertext sizes and will continue to study it in the fourth round. ClassicMcEliece was a finalist but is not being standardized by NIST at this time. Although ClassicMcEliece is widely regarded as secure, NIST does not anticipateit being widely used due to its large public key size. NIST may choose to standardize Classic McEliece at the end of the fourth round.

For the algorithms moving on to the fourth round, NIST will allow the submission teams to provide updated specifications and implementations (“tweaks”). The deadline for these tweaks will be **October 1, 2022**. Any submission team that feels that they may not meet the deadline should contact NIST as soon as possible. NIST will review the proposed modifications and publish the accepted submissions shortly afterwards. As a general guideline, NIST expects any modifications to be relatively minor. The fourth round will proceed similarly to the previous rounds. More detailed information and guidance will be provided in another message.

A detailed description of the decision process and rationale for selection will be included in NIST Interagency or Internal Report (NISTIR) 8413, *Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process*, which will soon be available at https://csrc.nist.gov/publications and on the NIST post-quantum webpage https://nist.gov/pqcrypto. Questions may be directed to pqc-comments@nist.gov.

NIST will create new draft standards for the algorithms to be standardized and will coordinate with the submission teams to ensure that the standards comply with the specifications. As part of the drafting process, NIST will seek input on specific parameter sets to include, particularly for security category 1. When finished, the standards will be posted for public comment. After the close of the comment period, NIST will revise the draft standards as appropriate based on the feedback received. A final review, approval, and promulgation process will then follow.

NIST will hold a 4th NIST PQC Standardization Conference on November 29 – December 1, 2022. The conference details have not yet been finalized. The preliminary Call for Papers will be posted, both on the pqc-forum and the NIST PQC webpage http://nist.gov/pqcrypto.

NIST also plans to issue a new Call for Proposals for public-key (quantum-resistant) digital signature algorithms by the end of summer 2022. NIST is primarily looking to diversify its signature portfolio, so signature schemes that are not based on structured lattices are of greatest interest. NIST would like submissions for signature schemes that have short signatures and fast verification (e.g., UOV). Submissions in response to this call will be due by June 1, 2023. Submitters are encouraged to communicate with NIST ahead of time. NIST will decide which (if any) of the submitted signature algorithms to accept and will initiate a new process for evaluation. NIST expects this process to be much smaller in scope than the current PQC process. The signature schemes accepted to this process will need to be thoroughly analyzed, which will similarly take several years.

NIST would like to thank the community and all of the submission teams for their efforts in this standardization process and hopes that the teams whose schemes were not selected to advance will continue to participate by evaluating and analyzing the remaining cryptosystems alongside the cryptographic community at large. These combined efforts are crucial to the development of NIST's future post-quantum public-key standards.

The NIST PQC team

--

--

--

> SA1PR09MB86697183D3615A85EB2FAC3BE5809%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/DM4PR11MB5455A7327EC94163B5E67668C18B9%40DM4PR11MB5455.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/CAPxHsS%2BLTcz%2BwzfrkbyfRn1rvbSHgNBgqnLo_iBYZZPgpHk34A%40mail.gmail.com.

From: Daniel Apon <dapon.crypto@gmail.com> via pqc-forum@list.nist.gov
To: Scott Fluhrer (sfluhrer) <sfluhrer@cisco.com>
CC: Moody, Dustin (Fed) <dustin.moody@nist.gov>, pqc-forum <pqc-forum@list.nist.gov>, Jonathan Felten (jfelten) <jfelten@cisco.com>
Subject: Re: [pqc-forum] RE: Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized
Date: Friday, July 15, 2022 03:17:18 PM ET

The particularly relevant question I'm also asking about is when NIST will go from algorithm specification selection to parameterization / tweak finalization for the selected algorithms.

The obvious date is the release of the full standards documents in ~2024 (ETA).
Will there be a safe fixed point in parameterization/tweaks for early-adopters/deployers prior to the standards documentation release in ~2024?

Cheers

On Fri, Jul 15, 2022 at 3:12 PM Daniel Apon <dapon.crypto@gmail.com> wrote:

> This connects to another pressing issue, for which there is not yet a concrete recommendation from NIST, at least as far as I'm aware:
>
> When does NIST recommend that an interested organization should begin their actual migration to post-quantum cryptography *deployment* based on the July 5th, 2022 announcement?
> (Of course, prior to such a "go" date, many practical, preliminary steps can be completed in preparation for the migration date. But that aside..)
>
> As this issue arises in context: Scott says that Cisco cannot use Kyber until Cisco receives the text of the licenses (CNRS/Algo) -- and presumably has sufficient, interluding time for Cisco lawyers to examine the text of the licenses.
>
> 1) At which point in time does NIST intend for (for example) Cisco -- or any other organization -- to begin migration to Kyber (or Dilithium/Falcon/SPHINCS+)?
> 2) At which point in time will the text of the licenses (CNRS/Algo) be posted publicly?
>
> Speaking in my personal capacity in my role at MITRE (having not spoken with MITRE execs

> or MITRE lawyers either),
> --Daniel
>
> On Fri, Jul 15, 2022 at 2:55 PM 'Scott Fluhrer (sfluhrer)' via pqc-forum <pqc-forum@list.nist.gov> wrote:
>
>> Let me be more explicit.
>>
>> I have not talked to the Cisco execs; I cannot imagine that they would approve the use of Kyber without an assessment of the Cisco liability (and associated licensing fees, if any).
>>
>> I have not talked to the Cisco lawyers; I cannot imagine that they would be willing to give any such assurance without an examination of the licenses (and an examination of the press releases would not be sufficient).
>>
>> Hence, until we get the text of the licenses (both the one signed with CNRS and the one to be signed with Algo Consulting), Cisco cannot use Kyber. If continues to be true, we will need to seek an alternative solution.
>>
>> ---
>>
>> **From:** Scott Fluhrer (sfluhrer)
>> **Sent:** Wednesday, July 6, 2022 1:14 PM
>> **To:** Moody, Dustin (Fed) <dustin.moody@nist.gov>; pqc-forum <pqc-forum@list.nist.gov>
>> **Subject:** RE: Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized
>>
>> Can we get the text of the actual license agreement between NIST and CNRS/University of Limoges?
>>
>> ---
>>
>> **From:** 'Moody, Dustin (Fed)' via pqc-forum <pqc-forum@list.nist.gov>
>> **Sent:** Wednesday, July 6, 2022 12:24 PM
>> **To:** pqc-forum <pqc-forum@list.nist.gov>
>> **Subject:** [pqc-forum] Re: Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized
>>
>> FYI
>>
>> CNRS has posted a statement on their website.

https://www.cnrs.fr/fr/accord-de-licence-entre-le-nist-le-cnrs-et-luniversite-de-limoges-le-rayonnement-international-de

Dustin Moody

NIST PQC

From: 'Moody, Dustin (Fed)' via pqc-forum <pqc-forum@list.nist.gov>
Sent: Tuesday, July 5, 2022 1:36 PM
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: [pqc-forum] RE: Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized

Sorry for so many messages!

Here’s the link to the official NIST announcement. Please share:

https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms

Here’s the link to *NISTIR 8413: Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process*, which explains the rationale behind the decisions.

https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8413.pdf

Dustin

From: 'Moody, Dustin (Fed)' via pqc-forum <pqc-forum@list.nist.gov>
Sent: Tuesday, July 5, 2022 11:32 AM
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: [pqc-forum] Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized

Announcement

After careful consideration during the 3rd Round of the NIST PQC Standardization Process, NIST has identified four candidate algorithms for standardization. The primary algorithms NIST recommends be implemented for most use cases areCRYSTALS-KYBER (key-establishment)

> > and CRYSTALS-Dilithium (digital signatures).In addition, the signature schemes Falcon and SPHINCS+ will also be standardized.
> >
> > ### Algorithms to be Standardized
> >
> > Public-Key Encryption/KEMs
> >
> > CRYSTALS-KYBER
> >
> > Digital Signatures
> >
> > CRYSTALS-Dilithium
> >
> > Falcon
> >
> > SPHINCS+
> >
> > CRYSTALS-KYBER (key-establishment) and CRYSTALS-Dilithium (digital signatures) were both selected for their strong security and excellent performance, and NIST expects them to work well in most applications. Falcon will also be standardized by NIST since there may be use cases for which CRYSTALS-Dilithium signatures are too large. Additionally, SPHINCS+ will be standardized to avoid only relying on the security of lattices for signatures. NIST asks for public feedback on a version of SPHINCS+ with a lower number of maximum signatures.
> >
> > Additionally, the following candidate KEM algorithms will advance to the fourth round:
> >
> > ### 4th Round Candidates
> >
> > Public-Key Encryption/KEMs
> >
> > BIKE
> >
> > Classic McEliece
> >
> > HQC
> >
> > SIKE
> >
> > Both BIKE and HQC are based on structured codes, and either would be suitable as a general-purpose KEM that is not based on lattices. NIST

expects to select at most one of these two candidates for standardization at the conclusion of thefourth round. SIKE remains an attractive candidate for standardization because of its smallkey and ciphertext sizes and will continue to study it in the fourth round. ClassicMcEliece was a finalist but is not being standardized by NIST at this time. Although ClassicMcEliece is widely regarded as secure, NIST does not anticipateit being widely used due to its large public key size. NIST may choose to standardize Classic McEliece at the end of the fourth round.

For the algorithms moving on to the fourth round, NIST will allow the submission teams to provide updated specifications and implementations (“tweaks”). The deadline for these tweaks will be **October 1, 2022**. Any submission team that feels that they may not meet the deadline should contact NIST as soon as possible. NIST will review the proposed modifications and publish the accepted submissions shortly afterwards. As a general guideline, NIST expects any modifications to be relatively minor. The fourth round will proceed similarly to the previous rounds. More detailed information and guidance will be provided in another message.

A detailed description of the decision process and rationale for selection will be included in NIST Interagency or Internal Report (NISTIR) 8413*, Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process,* which will soon be available at https://csrc.nist.gov/publications and on the NIST post-quantum webpage https://nist.gov/pqcrypto. Questions may be directed to pqc-comments@nist.gov.

NIST will create new draft standards for the algorithms to be standardized and will coordinate with the submission teams to ensure that the standards comply with the specifications. As part of the drafting process, NIST will seek input on specific parameter sets to include, particularly for security category 1. When finished, the standards will be posted for public comment. After the close of the comment period, NIST will revise the draft standards as appropriate based on the feedback received. A final review, approval, and promulgation process will then follow.

NIST will hold a 4th NIST PQC Standardization Conference on November 29 – December 1, 2022. The conference details have not yet been finalized.

The preliminary Call for Papers will be posted, both on the pqc-forum and the NIST PQC webpage http://nist.gov/pqcrypto.

NIST also plans to issue a new Call for Proposals for public-key (quantum-resistant) digital signature algorithms by the end of summer 2022. NIST is primarily looking to diversify its signature portfolio, so signature schemes that are not based on structured lattices are of greatest interest. NIST would like submissions for signature schemes that have short signatures and fast verification (e.g., UOV). Submissions in response to this call will be due by June 1, 2023. Submitters are encouraged to communicate with NIST ahead of time. NIST will decide which (if any) of the submitted signature algorithms to accept and will initiate a new process for evaluation. NIST expects this process to be much smaller in scope than the current PQC process. The signature schemes accepted to this process will need to be thoroughly analyzed, which will similarly take several years.

NIST would like to thank the community and all of the submission teams for their efforts in this standardization process and hopes that the teams whose schemes were not selected to advance will continue to participate by evaluating and analyzing the remaining cryptosystems alongside the cryptographic community at large. These combined efforts are crucial to the development of NIST’s future post-quantum public-key standards.

The 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/SA1PR09MB866933A15C3568FC510B4B68E5819%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/SA1PR09MB866994EA8023F512F6E1C5FEE5819%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/SA1PR09MB86697183D3615A85EB2FAC3BE5809%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/DM4PR11MB5455A7327EC94163B5E67668C18B9%40DM4PR11MB5455.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/CAPxHsSLs%2B%2BbbLHdzF_LVStZWGLvvGcJKYEn3CW6Oa5ZhCushMA%40mail.gmail.com.

From: D. J. Bernstein <djb@cr.yp.to> via pqc-forum@list.nist.gov
To: pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] RE: Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized
Date: Friday, July 15, 2022 11:33:49 PM ET
Attachments: smime.p7m

'Scott Fluhrer (sfluhrer)' via pqc-forum writes:

> If continues to be true, we will need to seek an alternative solution.

NIST's new report already points to a solution (see page 18):

> If the agreements are not executed by the end of 2022, NIST may consider selecting NTRU instead of KYBER. NTRU was proposed in 1996, and U.S. patents were dedicated to the public in 2007.

(I have no idea how whoever reviewed this could have imagined that "2007" was correct. If NTRU had been patent-free in 2007 then why didn't people try rolling it out in response to the Snowden revelations? In fact, the main NTRU patent expired in 2017, and the company didn't give up on the patent until earlier in 2017.)

The same report says NIST is confident in NTRU's security:

> One of the difficult choices NIST faced was deciding between KYBER, NTRU, and Saber. All three were selected as finalists and were very comparable to each other. NIST is confident in the security that each provides.

Regarding performance, the report says

> A significant factor in the decision to choose KYBER over NTRU was NTRU's performance (particularly key generation), which was not quite as efficient as that of KYBER

but also admits how insignificant this "significant factor" is in the real world:

> Most applications would be able to use any of them without significant performance penalties.

So NIST could have simply selected the patent-free option back in 2021. What happened instead was NIST delaying for half a year working on patent buyouts for Kyber. Many wheels in the deployment ecosystem were waiting for NIST, and were slowed down by half a year as a result. This translates directly into half a year of user data given to attackers.

There's nothing in the report considering the security damage caused by this delay, let alone explaining how this damage is outweighed by the small advantages that the report attributes to Kyber.

Maybe the patent-buyout details will be published next week. Maybe we'll see that the details are adequate, unlike the poison-pill "grant" that NIST negotiated with ISARA:

> https://web.archive.org/web/20201101181903/https://www.isara.com/nist-grant.html

And maybe NIST will release an analysis convincingly explaining why we shouldn't be worried about the patents that NIST hasn't said anything about so far, such as CN107566121A.

Or maybe NIST simply doesn't grasp the magnitude of the problem here. NIST's report briefly says that "an evaluation factor is whether a patent might hinder adoption", but this is a remarkable retreat from the call for submissions, which used the word "critical":

> NIST believes it is critical that this process leads to cryptographic standards that can be freely implemented in security technologies and products.

Figuring out what patents are out there, and what's safe from those patents given the complications of patent law, takes tons of work and should have been emphasized from the beginning of NISTPQC. Instead NIST discouraged public patent analysis, instead deciding to handle patents behind the scenes as an afterthought. This mistake has already created half a year of delay.

This looks like a great opportunity for agile tech companies to get ahead of the game by rolling out NTRU. The business case is clear, with ample cover provided by NIST's report:

* We can act now to help protect users against quantum computers. There's broad awareness of the quantum threat, and users will appreciate hearing that we're taking action.

* NIST selected Kyber and seems to have some patent agreements for Kyber, but many companies are stalled waiting to see whether those agreements really deal with the full scale of the patent problem. Main scenarios to consider are "yes", "no", and "still won't be sure by 2023".

* Meanwhile NIST's report says NTRU is patent-free, says NIST is "confident in the security" of NTRU, and says most applications can use NTRU "without significant performance penalties".

* NIST's report even says "If the agreements are not executed by the end of 2022, NIST may consider selecting NTRU instead of KYBER." The report is _not_ saying that there's something wrong with NTRU.

* NIST's report says that some small performance advantages of Kyber over NTRU were a "significant factor" in NIST's decision to choose Kyber. Those performance advantages are irrelevant to us, and NIST calls other Kyber advantages "marginal". We care much more about issues that are barely covered in NIST's report, such as deployment timelines and patents.

* We can go ahead with rolling out NTRU right now, while running experiments with Kyber in parallel to make sure we can easily swap in Kyber later if that turns out to be the right thing to do.

I'm concerned about various risks here that were downplayed or ignored in NIST's report. In particular, the NTRU submission is _not_ exactly the 1996 version of NTRU, so it _could_ be covered by patents that haven't come to public attention (even if the risks are lower than for Kyber); also, one should _not_ be confident in the security of any of these systems. The analysis in https://ntruprime.cr.yp.to/warnings.html indicates that Streamlined NTRU Prime (as in sntrup761, now used by default in OpenSSH) has somewhat lower patent risks and somewhat lower security risks than the NTRU submission. However, from the perspective of users whose data is being intercepted and recorded by large-scale attackers right now, it's hard to imagine how any of these risks are comparable to the damage caused by further delay.

---D. J. Bernstein

From: Daniel Apon <dapon.crypto@gmail.com> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] RE: Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized
Date: Saturday, July 16, 2022 12:30:01 AM ET

"in response to the Snowden revelations"

Thanks, Dad.

Perhaps you could explain to the Public why you're so aggressively targeting, in public, your PhD student's submission with political nonsense?

On Fri, Jul 15, 2022 at 11:32 PM D. J. Bernstein <djb@cr.yp.to> wrote:

> 'Scott Fluhrer (sfluhrer)' via pqc-forum writes:
> > If continues to be true, we will need to seek an alternative solution.
>
> NIST's new report already points to a solution (see page 18):
>
> If the agreements are not executed by the end of 2022, NIST may
> consider selecting NTRU instead of KYBER. NTRU was proposed in 1996,
> and U.S. patents were dedicated to the public in 2007.
>
> (I have no idea how whoever reviewed this could have imagined that
> "2007" was correct. If NTRU had been patent-free in 2007 then why didn't
> people try rolling it out in response to the Snowden revelations? In
> fact, the main NTRU patent expired in 2017, and the company didn't give
> up on the patent until earlier in 2017.)
>
> The same report says NIST is confident in NTRU's security:
>
> One of the difficult choices NIST faced was deciding between KYBER,
> NTRU, and Saber. All three were selected as finalists and were very
> comparable to each other. NIST is confident in the security that each
> provides.

> Regarding performance, the report says
>
> A significant factor in the decision to choose KYBER over NTRU was NTRU's performance (particularly key generation), which was not quite as efficient as that of KYBER
>
> but also admits how insignificant this "significant factor" is in the real world:
>
> Most applications would be able to use any of them without significant performance penalties.
>
> So NIST could have simply selected the patent-free option back in 2021. What happened instead was NIST delaying for half a year working on patent buyouts for Kyber. Many wheels in the deployment ecosystem were waiting for NIST, and were slowed down by half a year as a result. This translates directly into half a year of user data given to attackers.
>
> There's nothing in the report considering the security damage caused by this delay, let alone explaining how this damage is outweighed by the small advantages that the report attributes to Kyber.
>
> Maybe the patent-buyout details will be published next week. Maybe we'll see that the details are adequate, unlike the poison-pill "grant" that NIST negotiated with ISARA:
>
> https://web.archive.org/web/20201101181903/https://www.isara.com/nist-grant.html
>
> And maybe NIST will release an analysis convincingly explaining why we shouldn't be worried about the patents that NIST hasn't said anything about so far, such as CN107566121A.
>
> Or maybe NIST simply doesn't grasp the magnitude of the problem here. NIST's report briefly says that "an evaluation factor is whether a patent might hinder adoption", but this is a remarkable retreat from the call for submissions, which used the word "critical":

> NIST believes it is critical that this process leads to cryptographic
> standards that can be freely implemented in security technologies and
> products.
>
> Figuring out what patents are out there, and what's safe from those
> patents given the complications of patent law, takes tons of work and
> should have been emphasized from the beginning of NISTPQC. Instead NIST
> discouraged public patent analysis, instead deciding to handle patents
> behind the scenes as an afterthought. This mistake has already created
> half a year of delay.
>
> This looks like a great opportunity for agile tech companies to get
> ahead of the game by rolling out NTRU. The business case is clear, with
> ample cover provided by NIST's report:
>
> * We can act now to help protect users against quantum computers.
> There's broad awareness of the quantum threat, and users will
> appreciate hearing that we're taking action.
>
> * NIST selected Kyber and seems to have some patent agreements for
> Kyber, but many companies are stalled waiting to see whether those
> agreements really deal with the full scale of the patent problem.
> Main scenarios to consider are "yes", "no", and "still won't be
> sure by 2023".
>
> * Meanwhile NIST's report says NTRU is patent-free, says NIST is
> "confident in the security" of NTRU, and says most applications can
> use NTRU "without significant performance penalties".
>
> * NIST's report even says "If the agreements are not executed by the
> end of 2022, NIST may consider selecting NTRU instead of KYBER."
> The report is _not_ saying that there's something wrong with NTRU.
>
> * NIST's report says that some small performance advantages of Kyber
> over NTRU were a "significant factor" in NIST's decision to choose
> Kyber. Those performance advantages are irrelevant to us, and NIST
> calls other Kyber advantages "marginal". We care much more about

> issues that are barely covered in NIST's report, such as deployment
> timelines and patents.
>
> * We can go ahead with rolling out NTRU right now, while running
> experiments with Kyber in parallel to make sure we can easily swap
> in Kyber later if that turns out to be the right thing to do.
>
> I'm concerned about various risks here that were downplayed or ignored
> in NIST's report. In particular, the NTRU submission is _not_ exactly
> the 1996 version of NTRU, so it _could_ be covered by patents that
> haven't come to public attention (even if the risks are lower than for
> Kyber); also, one should _not_ be confident in the security of any of
> these systems. The analysis in https://ntruprime.cr.yp.to/warnings.html
> indicates that Streamlined NTRU Prime (as in sntrup761, now used by
> default in OpenSSH) has somewhat lower patent risks and somewhat lower
> security risks than the NTRU submission. However, from the perspective
> of users whose data is being intercepted and recorded by large-scale
> attackers right now, it's hard to imagine how any of these risks are
> comparable to the damage caused by further delay.
>
> ---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/20220716033215.988731.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/CAPxHsS%2BSedtHc0wjpwugz7uoPq-kH_sa2CgkEqpYFQYQjs0rwQ%40mail.gmail.com.

From: EL HASSANE LAAJI <e.laaji@ump.ac.ma> via pqc-forum@list.nist.gov
To: pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] RE: Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized
Date: Saturday, July 16, 2022 06:56:59 PM ET

Hi

> One of the difficult choices NIST faced was deciding between KYBER,
>NTRU, and Saber. All three were selected as finalists and were very
>comparable to each other. NIST is confident in the security that each
> provides.

> Regarding performance, the report says

> A significant factor in the decision to choose KYBER over NTRU was
> NTRU's performance (particularly key generation), which was not quite
> as efficient as that of KYBER

I think it is possible to increase NTRU's performance.

I create a release of NTRU-HPS, but defined in the ring of the form "Rq=Zq[X]/(X^n+1)", that uses NTT algorithm combined with our Fast Modular Multiplication Algorithm (FMMA) (inspired by NewHope method). We obtained drastic results as shown in the table:

6.2 Performance benchmarking of *NTRUrobust, Saber, and Kyber*

In this subsection, we present the performance results of our NTRUrobust release compared to the FairSaber and Kyber1024 releases of SABER and KYBER post-quantum KEM schemes, which their parameter sets meet the category 5 security Levels.

with parameters *{n=1024, q=65537, p=2}*

Table 2: Performance benchmarking between NTRUrobust, FireSaber, and Kyber1024 releases. The result values are given in milliseconds (ms):

	Keys Gen (ms)	Encap (ms)	Decap (ms)
Kyber1024	0.46	0.63	0.63
FireSaber	2,51	3.12	3.43
NTRUrobust	1,25	0.47	0,62

NB: We note that all implementations are performed on a PC-TOSHIBA with an Intel(R) Core(TM) i7-2630QM CPU, 2 GHz processor, RAM 8 GO, under environment Windows 7-32 bits andDev-C++ 4.9.9.2.

The reader can see our paper at the link:
https://www.researchgate.net/project/NEW-EFFICIENT-AND-ROBUST-NTRU-POST-QUANTUM-KEY-EXCHANGE-RELEASE-NTRU-ROBUST

Best regards.

Le sam. 16 juil. 2022 à 04:32, D. J. Bernstein <djb@cr.yp.to> a écrit :

> 'Scott Fluhrer (sfluhrer)' via pqc-forum writes:
> \> If continues to be true, we will need to seek an alternative solution.
>
> NIST's new report already points to a solution (see page 18):
>
> If the agreements are not executed by the end of 2022, NIST may consider selecting NTRU instead of KYBER. NTRU was proposed in 1996, and U.S. patents were dedicated to the public in 2007.
>
> (I have no idea how whoever reviewed this could have imagined that "2007" was correct. If NTRU had been patent-free in 2007 then why didn't people try rolling it out in response to the Snowden revelations? In fact, the main NTRU patent expired in 2017, and the company didn't give up on the patent until earlier in 2017.)
>
> The same report says NIST is confident in NTRU's security:
>
> One of the difficult choices NIST faced was deciding between KYBER, NTRU, and Saber. All three were selected as finalists and were very comparable to each other. NIST is confident in the security that each provides.
>
> Regarding performance, the report says
>
> A significant factor in the decision to choose KYBER over NTRU was NTRU's performance (particularly key generation), which was not quite as efficient as that of KYBER

> but also admits how insignificant this "significant factor" is in the
> real world:
>
> Most applications would be able to use any of them without
> significant performance penalties.
>
> So NIST could have simply selected the patent-free option back in 2021.
> What happened instead was NIST delaying for half a year working on
> patent buyouts for Kyber. Many wheels in the deployment ecosystem were
> waiting for NIST, and were slowed down by half a year as a result. This
> translates directly into half a year of user data given to attackers.
>
> There's nothing in the report considering the security damage caused by
> this delay, let alone explaining how this damage is outweighed by the
> small advantages that the report attributes to Kyber.
>
> Maybe the patent-buyout details will be published next week. Maybe we'll
> see that the details are adequate, unlike the poison-pill "grant" that
> NIST negotiated with ISARA:
>
> https://web.archive.org/web/20201101181903/https://www.isara.com/nist-grant.html
>
> And maybe NIST will release an analysis convincingly explaining why we
> shouldn't be worried about the patents that NIST hasn't said anything
> about so far, such as CN107566121A.
>
> Or maybe NIST simply doesn't grasp the magnitude of the problem here.
> NIST's report briefly says that "an evaluation factor is whether a
> patent might hinder adoption", but this is a remarkable retreat from the
> call for submissions, which used the word "critical":
>
> NIST believes it is critical that this process leads to cryptographic
> standards that can be freely implemented in security technologies and
> products.
>
> Figuring out what patents are out there, and what's safe from those

> patents given the complications of patent law, takes tons of work and should have been emphasized from the beginning of NISTPQC. Instead NIST discouraged public patent analysis, instead deciding to handle patents behind the scenes as an afterthought. This mistake has already created half a year of delay.
>
> This looks like a great opportunity for agile tech companies to get ahead of the game by rolling out NTRU. The business case is clear, with ample cover provided by NIST's report:
>
> * We can act now to help protect users against quantum computers. There's broad awareness of the quantum threat, and users will appreciate hearing that we're taking action.
>
> * NIST selected Kyber and seems to have some patent agreements for Kyber, but many companies are stalled waiting to see whether those agreements really deal with the full scale of the patent problem. Main scenarios to consider are "yes", "no", and "still won't be sure by 2023".
>
> * Meanwhile NIST's report says NTRU is patent-free, says NIST is "confident in the security" of NTRU, and says most applications can use NTRU "without significant performance penalties".
>
> * NIST's report even says "If the agreements are not executed by the end of 2022, NIST may consider selecting NTRU instead of KYBER." The report is _not_ saying that there's something wrong with NTRU.
>
> * NIST's report says that some small performance advantages of Kyber over NTRU were a "significant factor" in NIST's decision to choose Kyber. Those performance advantages are irrelevant to us, and NIST calls other Kyber advantages "marginal". We care much more about issues that are barely covered in NIST's report, such as deployment timelines and patents.
>
> * We can go ahead with rolling out NTRU right now, while running experiments with Kyber in parallel to make sure we can easily swap

> in Kyber later if that turns out to be the right thing to do.
>
> I'm concerned about various risks here that were downplayed or ignored
> in NIST's report. In particular, the NTRU submission is _not_ exactly
> the 1996 version of NTRU, so it _could_ be covered by patents that
> haven't come to public attention (even if the risks are lower than for
> Kyber); also, one should _not_ be confident in the security of any of
> these systems. The analysis in https://ntruprime.cr.yp.to/warnings.html
> indicates that Streamlined NTRU Prime (as in sntrup761, now used by
> default in OpenSSH) has somewhat lower patent risks and somewhat lower
> security risks than the NTRU submission. However, from the perspective
> of users whose data is being intercepted and recorded by large-scale
> attackers right now, it's hard to imagine how any of these risks are
> comparable to the damage caused by further delay.
>
> ---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/20220716033215.988731.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/CAAVXnrvEjgaFg3effR3s3z%3DLnW5%2B6QmT0po8r2cDDR8WdZ9gGQ%40mail.gmail.com.

From: Brian Hagen <brian.hagen@null.net> via pqc-forum@list.nist.gov
To: pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] RE: Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized
Date: Saturday, July 16, 2022 07:30:45 PM ET

"D. J. Bernstein" <djb@cr.yp.to> writes:

> NIST's new report already points to a solution (see page 18):
>
> If the agreements are not executed by the end of 2022, NIST may
> consider selecting NTRU instead of KYBER. NTRU was proposed in 1996,
> and U.S. patents were dedicated to the public in 2007.
>
> (I have no idea how whoever reviewed this could have imagined that
> "2007" was correct. If NTRU had been patent-free in 2007 then why didn't
> people try rolling it out in response to the Snowden revelations? In
> fact, the main NTRU patent expired in 2017, and the company didn't give
> up on the patent until earlier in 2017.

What about US7929688B2 and US7773746B2? You've previously said that US7929688B2 is "a potential problem for the 2005 NTRU parameter sets, Streamlined NTRU Prime, the HRSS NTRU KEM, etc."

-b

From: D. J. Bernstein <djb@cr.yp.to> via pqc-forum@list.nist.gov
To: pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] RE: Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized
Date: Saturday, July 16, 2022 09:32:12 PM ET
Attachments: smime.p7m

Brian Hagen writes:

> What about US7929688B2 and US7773746B2? You've previously said that US7929688B2
> is "a potential problem for the 2005 NTRU parameter sets, Streamlined NTRU
> Prime, the HRSS NTRU KEM, etc."

Yes, https://cr.yp.to/patents/us/7929688.html says that the patent "might be stretched to cover similar formulas to eliminate decryption failures in other variants of NTRU, so it's a potential problem" etc. (Similar comments apply to 7773746.)

"Stretched" is alluding to how patent coverage is expanded via court procedures, such as _Markman_ hearings and the doctrine of equivalents. Patent novices think it's enough to say that a patent doesn't literally apply to any of the proposals at hand; in reality, land mines _can_ blow up even when you don't step directly on them.

Fortunately, there's prior art directly on point. The same page goes on to review two papers from the prior art that already eliminated decryption failures in the original NTRU system:

* One paper is the Crypto 2000 Jaulmes--Joux paper. The only weakness here is that this paper doesn't explicitly justify the statement "For appropriate parameter choices, we can ensure that all coefficients of the polynomial ... lie between -q/2 and q/2". One would thus have to explain to a judge that anyone of ordinary skill in the art would have understood how to do this; realistically, this means convincing the judge that _the judge_ would have understood how to do this from the information available.

* The other paper is the original 1996 NTRU conference handout, which

> has a section "NTRU with 0% decoding failure", and doesn't have the above weakness. At least in the U.S., conference handouts count as prior art.

Would Panasonic be able to come up with an interpretation of words of the patent claims to avoid covering the prior art? Conceivably. Would it then be able to argue that (e.g.) Google's deployment of ntruhrss701 is performing substantially the same function in substantially the same way with substantially the same result?

I don't see how. But this example illustrates that a proper analysis of patent risks is _much_ more complicated than "NTRU was proposed in 1996, and U.S. patents were dedicated to the public". As I wrote in my previous message:

> Figuring out what patents are out there, and what's safe from those patents given the complications of patent law, takes tons of work and should have been emphasized from the beginning of NISTPQC. ...
>
> I'm concerned about various risks here that were downplayed or ignored in NIST's report. In particular, the NTRU submission is _not_ exactly the 1996 version of NTRU, so it _could_ be covered by patents that haven't come to public attention (even if the risks are lower than for Kyber); also, one should _not_ be confident in the security of any of these systems.

---D. J. Bernstein

From: Christopher J Peikert <cpeikert@alum.mit.edu> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] RE: Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized
Date: Friday, July 22, 2022 02:30:02 PM ET

On Fri, Jul 15, 2022 at 11:32 PM D. J. Bernstein <djb@cr.yp.to> wrote:

> The analysis in https://ntruprime.cr.yp.to/warnings.html
> indicates that Streamlined NTRU Prime (as in sntrup761, now used by
> default in OpenSSH) has somewhat lower patent risks and somewhat lower
> security risks than the NTRU submission.

This analysis is sorely lacking in both respects (security and patents).

On security risks:

A proper risk evaluation should account for the amount of scrutiny that has been devoted to a system's mathematical structures and associated problems. Those that have received little scrutiny should be considered risky. See, e.g., what happened to Rainbow -- which was proposed in 2005 -- once it finally underwent sustained analysis in recent years.

NTRU Prime's security relies *entirely* on a rather new structure -- namely, deterministic "small rounding" errors -- that has seen very little public cryptanalytic effort. (See this thread for details.) By contrast, the NTRU submission relies on long-scrutinized "random noise" for its errors. In this respect, NTRU "classic" is less risky.

The above-linked page omits (small) rounding from the risk analysis, shown under "Known attack avenues not ruled out by theorems." The authors might say that this is because rounding is not a *known* attack avenue. But that's only because nobody seems to have seriously tried much. That's no reason to omit it from the risk evaluation -- indeed, it's a source of risk.

On patent risks:

I can't see what justifies the claim that Streamlined NTRU Prime (SNTRUP) "has somewhat lower patent risks" than the NTRU submission. The above-linked table claims no risk to either of them from two known patents, so any difference would have to lie elsewhere. Where?

If anything, the argument that NTRU LPRime, Kyber, and SABER are at risk from patent 9246675 could *also* be applied to SNTRUP -- but not to the NTRU submission.

In essence, the argument is this: the patent covers ciphertext-compression-by-rounding (which SNTRUP uses), and the "doctrine of equivalents" broadens the patent's claims to any underlying "noisy agreement" mechanism known at the time of the patent (LWE, its Ring/Module variants, etc.).

Well, the prior art teaches how to interchange LWE-style and NTRU-style noisy agreement, which SNTRUP uses. See, e.g., this Eurocrypt'11 paper and the January 2012 talk about this STOC 2012 paper ("On-the-Fly Multiparty Computation...")

So, *if* the above argument really puts those other proposals at risk from the patent, then Streamlined NTRU Prime is at risk too. By contrast, the NTRU submission doesn't use rounding-based compression, so the argument doesn't apply to it.

Now, to be absolutely clear: the above argument is deeply flawed, and should not lead us to believe that *any* of the above-named NISTPQC submissions are at real risk from the patent. (The fact that NIST is licensing the patent reduces the risk even further -- at least for the NIST-selected algorithms.)

This is because the patent describes a different method of compression -- not the "drop some bits" rounding used by NISTPQC schemes, which comes from abundant prior art. Courts have repeatedly ruled that the doctrine of equivalents cannot be used to "ensnare" prior art; see, e.g., this review.

Here is some of the prior art that describes "drop some bits" compression for a variety of (Ring/Module-)LWE encryption schemes and other applications; there is likely even more out there:

- Section 4.2 of this: "it is possible to improve their efficiency (without sacrificing correctness) by discretizing the LWE distribution more ‘coarsely’ using a relatively small modulus q'...";
- this: "'derandomization' of LWE: deterministic [rounding] errors. Also gives more practical ... encryption";
- this: "the underlying intuition is that Z_p can 'approximate' Z_q by simple scaling, up to a small error..." and "As a nice byproduct of this technique, the ciphertexts ... become very short";

- this, explicitly for Ring/Module-LWE (called GLWE therein): "The transformation from c to c' involves simply scaling by (p/q) and rounding..."

Sincerely yours in cryptography,

Chris

From: D. J. Bernstein <djb@cr.yp.to> via pqc-forum@list.nist.gov
To: pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] RE: Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized
Date: Friday, July 22, 2022 07:12:15 PM ET
Attachments: smime.p7m

Christopher J Peikert writes:

> This analysis is sorely lacking in both respects (security and patents).

The specific pieces alleged to be missing are, in fact, in Sections 3.5, 3.6, 3.18, and 5.3 of a paper giving details of the analysis. That paper is linked from the top of https://ntruprime.cr.yp.to/warnings.html.

For example, regarding "I can't see what justifies the claim that Streamlined NTRU Prime (SNTRUP) 'has somewhat lower patent risks' than the NTRU submission":

* Section 3.18 of the paper says "Instability also contributes to general patent risks" and explains why.

* The corresponding instability lines of the comparison table show that ntruhrss, ntruhps, and sntrup all changed in 2019.04, but that sntrup's PKE goes all the way back to 2016.05---the only changes to sntrup after that were at the CCA layer---while ntruhrss and ntruhps changed their PKE much more recently.

To be clear, the risks of unknown patents covering, e.g., Google's ntruhrss deployment aren't anywhere near the risks incurred by Kyber, which is even less stable (one has to review patents all the way through October 2020) and starting from major components patented in 2010 and 2012. Maybe NIST has succeeded in buying out those two patents, but what's being done about the systemic problem? Two landmines disarmed (hopefully), but Kyber is still stuck in the middle of a minefield!

It's important to avoid underestimating the number of post-quantum patents out there, the costs of analyzing patent applicability, and the real-world damage that comes from botching the handling of patents. It seems that NIST delayed everything by (at least) half a year working on those two patent buyouts. https://blog.cr.yp.to/20220129-plagiarism.html reviews the evidence that patents were a major contributor to years of delay in post-quantum rollout before that.

———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/20220722231144.70235.qmail%40cr.yp.to.

From: John Mattsson <john.mattsson@ericsson.com> via pqc-forum <pqc-forum@list.nist.gov>
To: pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] RE: Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized
Date: Sunday, July 24, 2022 08:13:59 AM ET

I have talked to our lawyers many times. What they say is that public discussion on specific alleged patentstypically benefits the patent holder.

Cheers,

John

From: Billy Brumley <bbrumley@gmail.com> via pqc-forum@list.nist.gov
To: pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] RE: Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized
Date: Sunday, July 24, 2022 12:38:39 PM ET

> I have talked to our lawyers many times. What they say is that public discussion on specific alleged patents typically benefits the patent holder.

There is a lot of truth to this, and Dan even writes it down in his blog post he linked https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fblog.cr.yp.to%2F20220129-plagiarism.html&amp;data=05%7C01%7Cyi-kai.liu%40nist.gov%7Cae74d46744414e8fd7a908da6d92f3d1%7C2ab5d82fd8fa4797a93e054655c61dec%7C1%7C0%7C637942775190321148%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&amp;sdata=Z%2ByS4EkX0hqVxbljqLyHEON%2FYtTHZmEg8ofxl6%2BkB28%3D&amp;reserved=0
(which I don't encourage anyone to read who thinks they might be at risk for infringing on PQC-related IP)

> Actually, because intentional patent infringement is subjected to triple damages under patent law, the lawyers at big companies try to avoid sending email that could end up making any subsequent infringement sound intentional.

Despite what Dan wrote, it's not just the lawyers. When part of your (engineering or academic) job is protecting IP by internally filing Invention Disclosures (IDFs), companies / employers actively discourage you from searching for prior art for exactly those reasons. In fact they encourage you to file IDFs for any of your ideas: Why would the company seek a patent, if they knew it was covered already? This provides a paper trail to later argue against the amplified damages of intentional patent infringement, if needed. (Especially because, in the industry case, the IDF and any subsequent patent is commonly just a cover-your-ass strategy, since you've already implemented / deployed the idea in question.)

For those reasons, I agree with John's company's lawyers.

Cheers,

BBB

--

From: Christopher J Peikert <cpeikert@alum.mit.edu> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: [pqc-forum] NTRU vs Streamlined NTRU Prime: comparing risks
Date: Sunday, July 24, 2022 10:53:52 PM ET

(Breaking this out into its own thread, the topic being the following statement from this message:

"The analysis in https://ntruprime.cr.yp.to/warnings.html indicates that Streamlined NTRU Prime (as in sntrup761, now used by default in OpenSSH) has somewhat lower patent risks and somewhat lower security risks than the NTRU submission."

I replied with a critique of that analysis, on both security and patents. I'm now responding to a reply to that message.)

On Fri, Jul 22, 2022 at 7:12 PM D. J. Bernstein <djb@cr.yp.to> wrote:

> Christopher J Peikert writes:
> > This analysis is sorely lacking in both respects (security and patents).
>
> The specific pieces alleged to be missing are, in fact, in Sections 3.5,
> 3.6, 3.18, and 5.3 of a paper giving details of the analysis. That paper
> is linked from the top of https://ntruprime.cr.yp.to/warnings.html.

As I said: this analysis is sorely lacking. It does not substantiate the claim that Streamlined NTRU Prime (SNTRUP) is superior to the NTRU submission on security and patent risks. Mainly, this is because it omits or unjustifiably dismisses the significant ways in which SNTRUP has *higher* risks. But it also invites specious conclusions of SNTRUP's superiority on certain risks, where a closer look shows that NTRU is clearly better off.

(In my view, the omitted and dismissed risks outweigh the ones for which SNTRUP *might* really be superior, but that's a matter of judgement.)

The rest of this message gives an expanded critique of the analysis, focusing mostly on the cited sections, along with a much more thorough investigation of the NTRU-vs-SNTRUP comparison.

Summary on security risks:

- Section 3.5 does not account for the larger risk (very little scrutiny) of SNTRUP’s small-rounding errors, versus NTRU’s (long-scrutinized) random errors. Instead, it implicitly but unjustifiably treats them as having indistinguishable risk.
- On other security risks, none of the other three cited sections shows that SNTRUP is superior. Two sections fail to show any advantage in either direction. And for the third section (on stability), a proper evaluation favors NTRU, owing to its overall much-older design and substantial advantage in scrutiny.

Summary on patent risks:

- The claimed larger risk of NTRU vs SNTRUP is based entirely on a crude comparison of their underlying PKEs' publication dates, and the hypothetical of a relevant patent being filed in the interim. (NB: the table assigns a date to NTRU that looks wrong by ~21 months, about 60% of the claimed gap.)
- Merely comparing most-recent-publication dates is of very little value in assessing actual risks. Looking at the substance of the PKEs:
    - NTRU's is identical to the original 1998 NTRU proposal, except for two small tweaks whose ideas date back to 2006 or earlier (in related contexts).
    - SNTRUP's uses a technique that was first proposed in 2011.
    - So, NTRU's window of vulnerability to patents is *extremely* narrow, if not fully closed, while SNTRUP's window is larger.
- Moreover, the analysis omits that for a *known* patent, *its own* (dubious) argument about the risks to other proposals would also apply to SNTRUP, but not to NTRU.

Details on security risks:

Section 3.5 describes the criteria for “known attack avenue,” and says why (small) rounding doesn’t currently qualify as one. This is not responsive to what I wrote about rounding, which did not even dispute this categorization.

What I wrote is that the lack of a known attack avenue does *not* justify omitting small-rounding from the risk evaluation, because so little effort has been put into finding such an avenue.

Indeed, SNTRUP's security relies *entirely* on small rounding. This is a rather new structure that has received very little public scrutiny, and therefore represents a significant amount of uncertainty/risk. I don't know of any dispute about these points from anyone. (If there is, I would like to know.)

Section 3.6 is about implementation risks, and explains why they are *not* included in the risk table. In short: assessment alone is a major unresolved research question, and the targets are moving. It doesn’t mention NTRU at all. I don’t see how this sheds any light on the comparison with SNTRUP.

Section 5.3 concerns proofs and their (in)applicability; there’s no contribution to the NTRU-vs-SNTRUP comparison here either.

Section 3.18 addresses both security and patent risks of "(PKE) instability." For security, the motivation for stability is the need for scrutiny. In this respect, NTRU clearly has the advantage: it is much older and has seen vastly more scrutiny than SNTRUP. (See below for details of their PKEs and the timing.)

Details on patent risks (Sections 3.17 and 3.18):

> For example, regarding "I can't see what justifies the claim that
> Streamlined NTRU Prime (SNTRUP) 'has somewhat lower patent risks' than
> the NTRU submission":
>
> * Section 3.18 of the paper says "Instability also contributes to
> general patent risks" and explains why.
>
> * The corresponding instability lines of the comparison table show
> that ntruhrss, ntruhps, and sntrup all changed in 2019.04, but that
> sntrup's PKE goes all the way back to 2016.05---the only changes
> to sntrup after that were at the CCA layer---while ntruhrss and
> ntruhps changed their PKE much more recently.

Ok, so the extent of the claimed NTRU-vs-SNTRUP risk difference is: the publication dates of their underlying PKEs (2019.04 vs 2016.05, supposedly), and the hypothetical of a patent filed during that gap which would cover some part of the later PKE, while still avoiding the prior art.

Again: this analysis is sorely lacking, to say the least.

Firstly, it does not consider the actual designs of the PKEs, nor the prior art and its dates, nor the nature of the changes (if any) relative to the prior art. Let's look at those now.

The very first paragraph of the 2019 NTRU submission says "Modulo a few small changes introduced by [HRSS'17], the correct DPKE that we describe here is obtained by applying the [NTRU] preprint's transformations for determinism and correctness to the PPKE from ANTS'98."

If that’s true, then NTRU’s PKE design should be dated no later than HRSS's publication date of 2017.07, not 2019.04. That's a ~21 month difference, or about 60% of the gap stated in the risks table.

More importantly, HRSS’s small changes consist entirely of:

1. The obvious, old, and widely used idea of sampling small coefficients independently (instead of with fixed weight), and
2. A key-generation tweak that makes f*h a multiple of (x-1), for security and simplicity reasons. This also is an old idea: e.g., Peikert-Rosen’06 uses the same kind of trick for similar reasons (in a different context), and it likely appears in other old works too.

In sum, this leaves an *extremely* narrow window, if any, for a hypothetical patent that somehow covers HRSS’s small tweaks, while also avoiding all the old prior art starting from 1998.

This narrow window should be compared to the one for SNTRUP’s PKE, which includes larger and newer changes relative to original NTRU: e.g., generating errors by deterministic small rounding, which (to my knowledge) was first proposed in 2011.

Secondly, the analysis misses the point that a *known* patent threatens SNTRUP, but not NTRU—at least according to its *own* (dubious) doctrine-of-equivalents argument, which it says puts other submissions at risk (see Section 3.17).

Again, the DOE argument and assertions made in Section 3.17 are seriously flawed and overbroad, not least because they fail to account for “ensnarement” of the abundant prior art.

But regardless of the DOE argument’s (de)merits, it should be applied consistently for a fair comparison of proposals. In this case, the argument would put SNTRUP at higher risk than NTRU from this patent.

Sincerely yours in cryptography,

Chris

forum/CACOo0QhbavG58F8%2B%2B3HSTekrJJzdarGQsVq1D_Ddg%3DGrO4gr-w%40mail.gmail.com.

From: Christopher J Peikert <cpeikert@alum.mit.edu> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: [pqc-forum] Re: NTRU vs Streamlined NTRU Prime: comparing risks
Date: Monday, July 25, 2022 11:49:36 AM ET

> On Fri, Jul 22, 2022 at 7:12 PM D. J. Bernstein <djb@cr.yp.to> wrote:
>
> > * The corresponding instability lines of the comparison table show that ntruhrss, ntruhps, and sntrup all changed in 2019.04, but that sntrup's PKE goes all the way back to 2016.05---the only changes to sntrup after that were at the CCA layer---while ntruhrss and ntruhps changed their PKE much more recently.

This "appendix" to my previous message gives a detailed analysis of the stability of the NTRU submission's PKE (HRSS variant), relying and expanding on Section 2.2 of the specification.

This analysis is much more useful than merely looking at its "date of last published change" -- supposedly 2019.04, but that's misleading for the purposes of evaluating the PKE's stability (see below).

Summary:

- For the central security property of one-wayness (OW-CPA), stability almost entirely dates to 1998, except for small and likely beneficial tweaks that are unchanged since 2017.07.
- The subsequent 2019.04 change does not affect one-wayness, because it doesn't touch anything that appears in the OW-CPA experiment. It is relevant only to the CCA layer.

The submission seeks two main properties from its PKE:

- One-wayness (OW-CPA):
    - This is the central security property. It can only be conjectured, not proved, except possibly based on other unproven conjectures.
    - So, our confidence must come from cryptanalytic scrutiny and any relevant reductions. This is why stability is desirable: any changes might call for re-doing/re-checking a lot of prior work.

  - Importantly, one-wayness depends only on how *public keys and ciphertexts* are generated, and not on secret keys or decryption. So, only changes to the former can matter for stability here.
- "Rigidity":
  - This is a structural property, desired for (and only for) the CCA transformation.
  - It depends on the definition of decryption and secret keys, but it can be proved unconditionally, and often easily. So, PKE stability is not so important here; upon any changes, it suffices to (re-)check a short proof.
  - The rigidity of NTRU's PKE is (easily) proved at the end of Section 2.3. So, we won't consider rigidity any further here.

The rest of this message reviews the PKE's stability with respect to one-wayness, i.e., generation of its public keys and ciphertexts.

Public keys:

These are generated exactly as in the first-round NTRU-HRSS submission, which is equivalent (modulo choice of PRG) to what's defined in every version of the HRSS paper, starting 2017.07.

(Note that the factor of 3 can be introduced either during key-gen or encryption, with no effect on one-wayness, since 3 is invertible in the relevant ring.)

The only changes between the HRSS paper and ANTS'98 NTRU are in using independent coefficients for small polynomials, and making the public key a multiple of (X-1). Both changes are old ideas, improve simplicity and aid security review, and have been carefully analyzed. So, stability almost entirely dates to 1998, with a small (and likely beneficial) piece dating to 2017.07.

Ciphertexts:

These also are generated exactly as in the first-round NTRU-HRSS submission, which again is equivalent to what's defined in the HRSS paper.

(Note that the PKE's interface was tweaked to take r as an explicit input for CCA purposes, but r is still generated in exactly the same way.)

The only changes between the HRSS paper and ANTS'98 NTRU is in making the "message" m a multiple of (X-1), paralleling the change for public keys (and with the same likely benefits). So again, stability almost entirely dates to 1998.

Sincerely yours in cryptography,

Chris

From: John Schanck <jmschanck@gmail.com> via pqc-forum@list.nist.gov
To: Christopher J Peikert <cpeikert@alum.mit.edu>
CC: pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] Re: NTRU vs Streamlined NTRU Prime: comparing risks
Date: Monday, July 25, 2022 01:07:17 PM ET

Hi Chris, thanks for this review of the stability of the NTRU PKE.

On Mon, Jul 25, 2022 at 8:48 AM Christopher J Peikert <cpeikert@alum.mit.edu> wrote:

> The only changes between the HRSS paper and ANTS'98 NTRU are in using
> independent coefficients for small polynomials, and making the public key a
> multiple of (X-1).

Another change in HRSS is the sign twiddling trick for f and g, which reduces the minimal q needed for perfect correctness. Summarizing this as "making the public key a multiple of (X-1)" could lead to some confusion about priority.

As you said, the public key is made to be a multiple of (X-1) for security and simplicity reasons. But this is orthogonal to the sign twiddling trick, which is done for compactness and correctness. Section 2.2.4 of the round 3 submission says:

"Use of T+ [the sign twiddling trick] implies that the scheme is correct when q > 8 sqrt(2) (n - 1), which is a factor of sqrt(2) better than the naive bound."

The "naive bound" is the one found in the "NTRU with 0% decoding failure" section of the 1996 NTRU preprint. The improved bound is original to HRSS17. No method of parameter generation published prior to HRSS17 would produce ntruhrss701.

Cheers,
John

--

From: Christopher J Peikert <cpeikert@alum.mit.edu> via pqc-forum@list.nist.gov
To: John Schanck <jmschanck@gmail.com>
CC: pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] Re: NTRU vs Streamlined NTRU Prime: comparing risks
Date: Monday, July 25, 2022 01:58:10 PM ET

On Mon, Jul 25, 2022 at 1:07 PM John Schanck <jmschanck@gmail.com> wrote:

> On Mon, Jul 25, 2022 at 8:48 AM Christopher J Peikert
> <cpeikert@alum.mit.edu> wrote:
> > The only changes between the HRSS paper and ANTS'98 NTRU are in using
> > independent coefficients for small polynomials, and making the public key a
> > multiple of (X-1).
>
> Another change in HRSS is the sign twiddling trick for f and g

John, thanks for pointing this out. I had thought the choices of f and g were covered by the other change -- "sampling small coefficients independently (instead of with fixed weight)" -- but this missed the post-sampling sign flips, which very slightly violate independence (by at most one bit of min-entropy).

If I'm reading everything correctly, this was present in the HRSS'17 paper and remained unchanged through the NTRU submissions. So for the purposes of one-wayness, the PKE has been stable since (no later than) 2017.07.

Sincerely yours in cryptography,

Chris

From: D. J. Bernstein <djb@cr.yp.to> via pqc-forum@list.nist.gov
To: pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] Re: NTRU vs Streamlined NTRU Prime: comparing risks
Date: Monday, July 25, 2022 11:32:55 PM ET
Attachments: smime.p7m

Round-2 NTRU submission document: "The (merged) NTRU submission is based on the [Eurocrypt 2018] Saito-Xagawa-Yamakawa variant of NTRU-HRSS-KEM, but it eliminates an expensive part of the decapsulation routine. This efficiency enhancement maintains interoperability with the Saito-Xagawa-Yamakawa variant, has no impact on security, and cancels some of the added cost of the DPKE." (page 20)

https://web.archive.org/web/20210925230439/https://ntru.org/f/ntru-20190330.pdf
(dated 2019.03 but not obviously posted then; posted by NIST in 2019.04)

Also: "our DPKE is slightly different from the NTRU DPKE proposed by Saito, Xagawa, and Yamakawa ([36, Figure 10])." (page 4)

Anyone rewinding to the 2017 paper https://eprint.iacr.org/2017/667.pdf sees that the 2017 PKE was generating r randomly: see Algorithm 2. A DPKE is different: it's a _deterministic_ PKE, no randomness allowed. (For the importance of this PKE feature for security analyses, see, e.g., https://cr.yp.to/papers.html#footloose.)

Unless there are other references directly on point, one has to conclude that the PKE for ntruhrss and ntruhps, not just the CCA conversion, has a publication date of 2019.04, _not_ 2017.07.

(To understand how this instability matters for patent risks, imagine a patent troll filing a patent in 2017.08 on a deterministic version of the PKE. How exactly would we know? Has anyone done a search? What exactly was searched? The risk here is much lower than the risks for Kyber, but it's not zero.)

And yet we see some commentator on pqc-forum claiming that "NTRU's PKE design should be dated no later than HRSS's publication date of 2017.07, not 2019.04"———and that this closes "60% of the gap" to how early the sntrup PKE was published (namely, 2016.05). Fascinating.

Some components of the 2019.04 round-2 NTRU submission were already in https://eprint.iacr.org/2018/1174 some months earlier (2018.12), and it's worth checking exactly what matches so as to be able to limit patent searches accordingly. But 2018.12 is still nowhere near 2016.05, or even 2017.07. Claiming that something was published earlier than it actually was is a recipe for botching patent searches.

———D. J. Bernstein

From: John Schanck <jmschanck@gmail.com> via pqc-forum@list.nist.gov
To: pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] Re: NTRU vs Streamlined NTRU Prime: comparing risks
Date: Tuesday, July 26, 2022 01:10:51 AM ET

On Mon, Jul 25, 2022 at 8:31 PM D. J. Bernstein <djb@cr.yp.to> wrote:

> Also: "our DPKE is slightly different from the NTRU DPKE proposed by Saito, Xagawa, and Yamakawa ([36, Figure 10])." (page 4)

Saito, Xagawa, and Yamakawa have a reduction mod p in the recovery of r that was not present in Section 4.2 of the 1996 preprint.

ePrint 2018/1174 drops the reduction mod p in favor of a fast method for recognizing malformed ciphertexts. The DPKE is what you would get by applying Section 4.2 of the 1996 preprint to HRSS'17.

The NTRU submission's DPKE is exactly the one described in ePrint 2018/1174.

The contribution of ePrint 2018/1174 is best described as an optional efficiency enhancement——the DPKE remains wire-compatible with the one described by Saito, Xagawa, and Yamakawa.

> Unless there are other references directly on point, one has to conclude that the PKE for ntruhrss and ntruhps, not just the CCA conversion, has a publication date of 2019.04, _not_ 2017.07.

Summary of the dates:

 - 2017.07: probabilistic NTRU HRSS. https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Feprint.iacr.org%2F2017%2F667&amp;data=05%7C01%7Cyi-kai.liu%40nist.gov%7C481cf818bdf24f068a3408da6ec534d6%7C2ab5d82fd8fa4797a93e054655c61dec%7C1%7C0%7C637944090518749337%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&amp;sdata=ufwNuXFL9gofyQrxVLXayLkG67Nam2HlofHX4gr8N3Q%3D&amp;reserved=0.

 - 2017.10: deterministic NTRU HRSS. https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Feprint.iacr.org%2F2017%2F1005&amp;data=05%7C01%7Cyi-kai.liu%40nist.gov%7C481cf818bdf24f068a3408da6ec534d6%7C2ab5d82fd8fa4797a93e054655c61dec%7C1%7C0%7C637944090518749337%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&amp;sdata=dCeOTCqRZ6S%2FFg84SWXExIbXkdpc7Yu2baXPOuzIgtc%3D&amp;reserved=0.
 - 2018.12: an optional efficiency enhancement. https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Feprint.iacr.org%2F2018%2F1174&amp;data=05%7C01%7Cyi-kai.liu%40nist.gov%7C481cf818bdf24f068a3408da6ec534d6%7C2ab5d82fd8fa4797a93e054655c61dec%7C1%7C0%7C637944090518749337%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&amp;sdata=H64rO6bWUIooaXaltXHb86seT%2Bduiv5vOyQTzHnIhUI%3D&amp;reserved=0.

John

--

From: D. J. Bernstein <djb@cr.yp.to> via pqc-forum@list.nist.gov
To: pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] Re: NTRU vs Streamlined NTRU Prime: comparing risks
Date: Tuesday, July 26, 2022 03:56:37 AM ET
Attachments: smime.p7m

John Schanck writes:

[regarding something slower than the round-2 NTRU submission]

> The DPKE is what you would get by applying Section 4.2 of the 1996
> preprint to HRSS'17.

Under patent law, to argue that something isn't new and thus isn't patentable under 35 U.S.C. § 102, you have to point to _one_ prior art reference that has _all_ of the elements of the patent claim. See, e.g., _Verdegaal Bros. v. Union Oil Co. of California_, 814 F.2d 628 (Fed. Cir. 1987), at 631.

Did the round-2 NTRU PKE appear _in the 2017 HRSS paper_, as another commentator has claimed? No. This sort of misinformation has zero chance of holding up in court.

To argue that something is _obvious_ and thus not patentable under 35 U.S.C. § 103, you can combine multiple references, but you have to convince a non-expert tribunal (typically a pro-patent court in Texas) that this combination was obvious at the time to someone of ordinary skill in the art. Meanwhile the patent holder pulls out experts saying that, no, it wasn't obvious.

Should you make an obviousness argument if you're dragged into court? Yes, of course. Does that argument justify a commentator claiming that X+Y appeared in a paper, when in fact the paper presented only X? No. Is an obviousness argument a substitute for patent searches? No.

> The contribution of ePrint 2018/1174 is best described as an optional
> efficiency enhancement

Sure, just like a large part of the cryptographic literature, just like many patents. Certicom sued Sony for infringement of patent 6704870, which can be described as an optional efficiency enhancement.

There's a real-world problem of figuring out what's patented, and the pursuit of optional efficiency enhancements is one of the contributing factors to this problem. A full risk analysis takes this into account, and doesn't tolerate misinformation such as "NTRU was proposed in 1996" or "NTRU's PKE design should be dated no later than HRSS's publication date of 2017.07".

Let me again emphasize that, compared to the Kyber patent risks, I see much smaller patent risks in Google's ntruhrss deployment, the OpenSSH sntrup deployment, etc. The 1996 version of NTRU left much less room for improvement than the 2010 system from Gaborit--Aguilar-Melchor and Lyubashevsky--Peikert--Regev; there are various ways to measure this, and it's reflected in the timeframe of the patents that we know about.

> The NTRU submission's DPKE is exactly the one described in ePrint
> 2018/1174.

Sounds like 2018.12 is the publication date. Here are "about 35,321" patent applications using the word "cryptography" with priority dates between 2016.05.13 and 2018.12.03:

   https://patents.google.com/?q=%22cryptography%22&before=priority:20181203&after=priority:20160513

If NIST had taken patents seriously from the outset then it could have checked all these (and many older patents) by now (since only a small fraction require detailed analyses), and could even have been reasonably thorough in finding applications not using the word "cryptography". But the unfortunate reality is that this work hasn't been done.

---D. J. Bernstein

--

From: Christopher J Peikert <cpeikert@alum.mit.edu> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] Re: NTRU vs Streamlined NTRU Prime: comparing risks
Date: Tuesday, July 26, 2022 11:42:19 AM ET

Dan, it seems your only stated dispute with my detailed NTRU-vs-SNTRUP risk analysis concerns a side point, about the specific priority date of the NTRU PKE, which would only be relevant to patent risks. (I do insist that for evaluating *security* risks, the proper date is 2017.07, not 2019.04; see below.)

Happily, this issue doesn't affect anything else in my analysis, which doesn't rely on any specific priority date. Indeed, it rejects mere date comparisons and instead considers the PKEs' contents, changes relative to prior art, known patents, etc.

To recall: "[For patents,] the extent of the claimed NTRU-vs-SNTRUP risk difference is: the publication dates of their underlying PKEs (2019.04 vs 2016.05, supposedly), and the hypothetical of a patent filed during that gap which would cover some part of the later PKE, while still avoiding the prior art."

On this basis alone, you suggested that SNTRUP has (slightly) lower patent risks than the NTRU submission. Do you still maintain that reasoning and conclusion?

...Even following my analysis of the PKEs' contents and changes relative to prior art?

...Including the point that SNTRUP would be at *higher* risk from a *known* patent, at least according to your own (dubious) doctrine-of-equivalents argument, which you say puts other submissions at risk?

Beyond patent risks, you also made a claim about the relative *security* risks of NTRU vs SNTRUP.

The "risks" paper argues that "PKE instability" is important for evaluating security risks. But its table measures stability only by most-recent-change dates. This conflates changes that might affect security with those that do not.

It also does not consider the contents of the PKEs, the nature of the changes relative to older work, the amount of scrutiny of those changes, etc. These factors should inform the stability evaluation, and the security assessment more broadly.

My "appendix" message showed that NTRU's PKE has had no changes affecting its conjectured security since 2017.07 (not 2019.04, the date in the "risks" table). And it has only small, likely beneficial changes relative to the NTRU PKE from 1998, which has received extensive scrutiny.

By contrast, SNTRUP's PKE has significantly larger changes relative to 1998 NTRU, some of which -- like relying entirely on rounding for security -- have seen very little public scrutiny.

Following this analysis, which PKE would you say has more stability, and why? And considering all the factors that have been raised, which proposal would you say is superior on security risks overall, and why?

Sincerely yours in cryptography,

Chris

--

From: D. J. Bernstein <djb@cr.yp.to> via pqc-forum@list.nist.gov
To: pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] Re: NTRU vs Streamlined NTRU Prime: comparing risks
Date: Tuesday, July 26, 2022 07:28:32 PM ET
Attachments: smime.p7m

Christopher J Peikert writes:

> Dan, it seems your only stated dispute with my detailed NTRU-vs-SNTRUP
> risk analysis

No. Most of what Dr. Peikert has been saying consists of repeating arguments that he made before, while ignoring readily available evidence contradicting those arguments. His wording now focuses on the question of whether _I_ pointed out a contradiction——and in some cases I did, so he's not correctly reporting the status of the discussion.

For example:

* Dr. Peikert's email dated 2 Dec 2020 14:34:00 -0500 claimed that 2009 Peikert protects Kyber against Ding's 2012 patent, because all of these share "rounding away some low bits".

* My email dated 11 Dec 2020 16:08:14 +0100 explained in considerable detail how a court would evaluate and reject that argument.

* Dr. Peikert's email dated 22 Jul 2022 14:28:54 -0400 once again claims that 2009 Peikert protects Kyber against Ding's 2012 patent, because all of these share "ciphertext-compression-by-rounding".

Aside from minor changes in wording, Dr. Peikert's July 2022 argument is simply a repetition of his December 2020 argument. I pointed out back in December 2020 how flawed the argument was. So why is the reader being told in July 2022 that the argument hasn't been disputed?

A scientist would acknowledge disputes, try to resolve the disputes, admit errors to set the record straight, and investigate the facts in the first place to reduce the frequency of errors. A politician would simply keep repeating himself, carrying out a denial-of-service attack against the fact-checkers. Which path is Dr. Peikert choosing?

To be clear, there _are_ some new mistakes here. In particular:

* "the table assigns a date to NTRU that looks wrong by ~21 months, about 60% of the claimed gap";

* "If that’s true, then NTRU’s PKE design should be dated no later than HRSS's publication date of 2017.07, not 2019.04. That's a ~21 month difference, or about 60% of the gap stated in the risks table".

The misinformation here is dangerous: it can easily mislead people into failing to check PKE-related patents after 2017.07. So I took the time to point out that, no, this PKE does _not_ appear in the 2017.07 paper. Is Dr. Peikert ever going to issue a clear erratum?

---D. J. Bernstein

From: Daniel Apon <dapon.crypto@gmail.com> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] Re: NTRU vs Streamlined NTRU Prime: comparing risks
Date: Tuesday, July 26, 2022 10:03:19 PM ET

Dear Dan,

You wrote:

" And yet we see some commentator on pqc-forum claiming that "NTRU's PKE
design should be dated no later than HRSS's publication date of 2017.07,
not 2019.04"---and that this closes "60% of the gap" to how early the
sntrup PKE was published (namely, 2016.05). Fascinating."

Would you please specify which specific commentator on the pqc-forum, by name, to which you are referring here?

Given how specific some points in your messages are, I appreciate your attention to not unfortunately (intentionally or not) obfuscating this identification in your messaging.

Best regards,
--Daniel

On Tue, Jul 26, 2022 at 7:28 PM D. J. Bernstein <djb@cr.yp.to> wrote:

> Christopher J Peikert writes:
> \> Dan, it seems your only stated dispute with my detailed NTRU-vs-SNTRUP
> \> risk analysis
>
> No. Most of what Dr. Peikert has been saying consists of repeating
> arguments that he made before, while ignoring readily available evidence
> contradicting those arguments. His wording now focuses on the question
> of whether _I_ pointed out a contradiction---and in some cases I did, so
> he's not correctly reporting the status of the discussion.
>
> For example:

> * Dr. Peikert's email dated 2 Dec 2020 14:34:00 -0500 claimed that 2009 Peikert protects Kyber against Ding's 2012 patent, because all of these share "rounding away some low bits".
>
> * My email dated 11 Dec 2020 16:08:14 +0100 explained in considerable detail how a court would evaluate and reject that argument.
>
> * Dr. Peikert's email dated 22 Jul 2022 14:28:54 -0400 once again claims that 2009 Peikert protects Kyber against Ding's 2012 patent, because all of these share "ciphertext-compression-by-rounding".
>
> Aside from minor changes in wording, Dr. Peikert's July 2022 argument is simply a repetition of his December 2020 argument. I pointed out back in December 2020 how flawed the argument was. So why is the reader being told in July 2022 that the argument hasn't been disputed?
>
> A scientist would acknowledge disputes, try to resolve the disputes, admit errors to set the record straight, and investigate the facts in the first place to reduce the frequency of errors. A politician would simply keep repeating himself, carrying out a denial-of-service attack against the fact-checkers. Which path is Dr. Peikert choosing?
>
> To be clear, there _are_ some new mistakes here. In particular:
>
> * "the table assigns a date to NTRU that looks wrong by ~21 months, about 60% of the claimed gap";
>
> * "If that’s true, then NTRU’s PKE design should be dated no later than HRSS's publication date of 2017.07, not 2019.04. That's a ~21 month difference, or about 60% of the gap stated in the risks table".
>
> The misinformation here is dangerous: it can easily mislead people into failing to check PKE-related patents after 2017.07. So I took the time to point out that, no, this PKE does _not_ appear in the 2017.07 paper. Is Dr. Peikert ever going to issue a clear erratum?

> ---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/20220726232753.321892.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/CAPxHsSLx25e1Be%2BR6S8pumhgTpSHrBf8Ovg-3yLv-F4cp5MiSQ%40mail.gmail.com.

From: Christopher J Peikert <cpeikert@alum.mit.edu> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] Re: NTRU vs Streamlined NTRU Prime: comparing risks
Date: Wednesday, July 27, 2022 12:18:30 AM ET

Dan, I'm reminded of the old lawyer's maxim: When the facts are on your side, pound the facts. When the law is on your side, pound the law. When neither is on your side... pound the table!

On Tue, Jul 26, 2022 at 7:28 PM D. J. Bernstein <djb@cr.yp.to> wrote:

> Christopher J Peikert writes:
> > Dan, it seems your only stated dispute with my detailed NTRU-vs-SNTRUP
> > risk analysis
>
> No. Most of what Dr. Peikert has been saying consists of repeating
> arguments that he made before

That's plainly false, as anyone can see from just the opening and summary points of my detailed risk comparison -- little of which I argued before last week (the exception being the risks of small rounding, of course). I encourage everyone to read it and see for themselves -- and I encourage you not to misrepresent it.

I'll address the two specific points you've raised here about the contents of my analysis. For perspective, both are patent-related details that are incidental to my full evaluation, and don't relate to the security comparison at all. A pity -- but one pounds the table with whatever one has, I suppose.

Regarding the prior dispute about Kyber's risk from a known patent:

> Aside from minor changes in wording, Dr. Peikert's July 2022 argument is
> simply a repetition of his December 2020 argument.

This is another major misrepresentation. I made the new (to my knowledge) point that if Kyber really is/was at risk according to *your* type of argument, then so is SNTRUP -- but not NTRU.

This point is incidental to my overall evaluation, because I find your argument dubious, due to multiple prior-art papers that your summary misleadingly omits. But the argument should be applied consistently for a fair comparison. If I'm as wrong about this as you claim, then SNTRUP faces a concrete risk that NTRU doesn't.

Regarding the precise NTRU PKE publication date, for patent (but not security) risks:

John Schanck pointed out, and you agreed, that the date is no later than 2018.12 (not 2019.04, as the "risks" table says). I certainly agree with that, so I hereby adjust my stated date accordingly.

This change is also incidental, because the precise publication date only matters to a very narrow hypothetical, and looking at contents is much more informative to the risk evaluation.

For example, John also said that the PKE "is what you would get by applying Section 4.2 of the 1996 preprint to HRSS'17." You argued that this wouldn't be enough to kill a hypothetical patent's "novelty," but that one can and should argue "obviousness." This is the kind of analysis that is lacking from the "risks" paper's mere publication-date-based comparison.

Sincerely yours in cryptography,

Chris

--
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/CACOo0QhaH0cqd%3D6djXSMGrirH-v4YcsMKwcGiaycSQ3gKWfgnA%40mail.gmail.com.

From: D. J. Bernstein <djb@cr.yp.to> via pqc-forum@list.nist.gov
To: pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] RE: Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized
Date: Thursday, July 28, 2022 10:06:46 AM ET
Attachments: smime.p7m

Billy Brumley writes:

> Despite what Dan wrote, it's not just the lawyers.

Not sure what you're disputing. The text didn't say it's _just_ the lawyers; on the contrary, the very next sentence has the "TLS managers" and "higher-ups" falling into line!

Basically, whenever the company is doing X, the company has an incentive to avoid having ever generated any paper trail showing knowledge of a patent on X, because of the triple-damages rule.

> When part of your (engineering or academic) job is protecting IP by internally filing Invention Disclosures (IDFs), companies / employers actively discourage you from searching for prior art for exactly those reasons.

That's typical for large companies, yes. Large companies aren't going to go out of business from stepping on the occasional land mine, and they figure that the cost of triple damages in those cases outweighs the benefit of avoiding some patents. (Sometimes small companies imitate this even when they _could_ go out of business.)

On the other hand, when one wants to figure out what can be universally deployed (because the actual objective is, e.g., to protect billions of users against the damage caused by future quantum computers), then it's clearly essential to understand what patents are out there and what they cover. That's why one finds, for example, the following:

   * https://www.ietf.org/rfc/rfc8179.txt requires IETF participants to
     immediately disclose all of their relevant patents, so as to allow

an "informed decision about the use of a particular technology"---exactly the opposite of the ostrich approach.

* Lemley's 2002 paper "Intellectual Property Rights and Standard-Setting Organizations" studied policies for dozens of big standards organizations, finding that most required immediate patent disclosure and that the rest "generally imposed other conditions that obviated the need for disclosure", such as requiring royalty-free licensing whether or not patents were disclosed. Here's a newer survey of related results: https://dc.law.utah.edu/cgi/viewcontent.cgi?article=1010&context=scholarship

* The NISTPQC call for submissions requires NIST to collect and publish patent statements _and_ to evaluate the extent to which any patents could hinder adoption of each submission. ("NIST does not object in principle to algorithms or implementations which may require the use of a patent claim, where technical reasons justify this approach, but will consider any factors which could hinder adoption in the evaluation process.")

The alternative, the ostrich approach, isn't _guaranteed_ to produce disastrously unusable standards, but there's a high enough chance and a high enough impact that _of course_ standards-development organizations adopt policies accordingly. See Lemley's 2002 paper for a detailed analysis of the incentives here.

In short, the company lawyer's claim that "public discussion on specific alleged patents typically benefits the patent holder" is very far out of whack with the amply documented behavior of standards-development organizations. These organizations _do not_---and, given their objectives, _should not_---handle patents the same way that large companies typically do.

---D. J. Bernstein

--

From: Billy Brumley <bbrumley@gmail.com> via pqc-forum@list.nist.gov
To: pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] RE: Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized
Date: Friday, July 29, 2022 02:02:52 AM ET

Howdy Dan,

I agree with what you wrote.

On Thu, Jul 28, 2022 at 5:06 PM D. J. Bernstein <djb@cr.yp.to> wrote:

>
> Billy Brumley writes:
> > Despite what Dan wrote, it's not just the lawyers.
>
> Not sure what you're disputing. The text didn't say it's _just_ the lawyers; on the contrary, the very next sentence has the "TLS managers" and "higher-ups" falling into line!

Right, the text didn't say that. What prompted my response is the possibility of your text being misinterpreted that way. But it's crystal clear now.

For a standardization effort, ofc "the ostrich approach" isn't sustainable. So when you wrote

> it's clearly essential to understand what patents are out there and what they cover

I 110% agree with you. But IMO, IPR experts should be leading that discussion.

The main message I wanted to deliver is this: Most academics have zero experience with IPR, so they should understand the risks before they go commenting about specific IPR in public. As an academic, it might seem harmless to follow some hyperlink to a patent in one of the discussions here, read it, and comment about it in this public forum. But doing so carries risk——the Internet never forgets :)

(Nothing I wrote should be construed to suggest any _particular individual_ commenting on IPR in this thread is or is not qualified to do so. If you have experience with IPR and know what you're doing, feel free to ignore this message and my previous one.)

Happy Friday!

BBB

--

From: John Mattsson <john.mattsson@ericsson.com> via pqc-forum <pqc-forum@list.nist.gov>
To: Billy Brumley <bbrumley@gmail.com>, pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] RE: Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized
Date: Thursday, August 11, 2022 05:28:41 AM ET

I agree very much with Billy Brumley that IPR experts should be leading the discussion. Technical people often have a very naive view when it comes to these topics. Public discussion of specific alleged IPR might e.g., benefit the IPR owner in several different ways:

- It is easier to claim that the infringement is willful in an infringement case.

- Technical discussion about an alleged IPR is often useful in an infringement case.

- The discussion might be used in an anti-trust case.

I think all systems used by SDOs have some negative side-effects. You might e.g., be able to convince a jury that the third-party declarations used in IETF is a statement that the RFC is infringing on the IPR. 3GPP is quite accepting to IPR and they are not as visible as in the IETF, but 3GPP have very hard commitments to FRAND licensing where anything not following FRAND licensing must be removed from the standards. NIST requires declaration of IPRs but have to my knowledge not been enforcing FRAND licensing in practice.

I don't think you can discuss IRP without discussing licensing terms. IPR licensed under predictable FRAND licenses with low fees are not bankrupting anybody. IRP with unpredictable licensing, very high license fees, or no licensing is a different story.

Cheers,

John

From: pqc-forum@list.nist.gov <pqc-forum@list.nist.gov> on behalf of Billy Brumley <bbrumley@gmail.com>
Date: Friday, 29 July 2022 at 08:04
To: pqc-forum@list.nist.gov <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] RE: Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized

John Mattsson <john.mattsson@ericsson.com>

Howdy Dan,

I agree with what you wrote.

On Thu, Jul 28, 2022 at 5:06 PM D. J. Bernstein <djb@cr.yp.to> wrote:
>
> Billy Brumley writes:
> > Despite what Dan wrote, it's not just the lawyers.
>
> Not sure what you're disputing. The text didn't say it's _just_ the
> lawyers; on the contrary, the very next sentence has the "TLS managers"
> and "higher-ups" falling into line!

Right, the text didn't say that. What prompted my response is the
possibility of your text being misinterpreted that way. But it's
crystal clear now.

For a standardization effort, ofc "the ostrich approach" isn't
sustainable. So when you wrote

> it's clearly essential to understand what patents are out there and what they cover

I 110% agree with you. But IMO, IPR experts should be leading that discussion.

The main message I wanted to deliver is this: Most academics have zero
experience with IPR, so they should understand the risks before they
go commenting about specific IPR in public. As an academic, it might
seem harmless to follow some hyperlink to a patent in one of the
discussions here, read it, and comment about it in this public forum.
But doing so carries risk---the Internet never forgets :)

(Nothing I wrote should be construed to suggest any _particular
individual_ commenting on IPR in this thread is or is not qualified to
do so. If you have experience with IPR and know what you're doing,
feel free to ignore this message and my previous one.)

Happy Friday!

BBB

--

You received this message because you are subscribed to the Google Groups "pqc-forum" group.
To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.
To view this discussion on the web visit https://protect2.fireeye.com/v1/url?k=31323334-501cfaf3-313273af-454445554331-8ab12e1659c8d732&q=1&e=dc288a6c-0946-442d-bee3-345f147bb2b0&u=https%3A%2F%2Fgroups.google.com%2Fa%2Flist.nist.gov%2Fd%2Fmsgid%2Fpqc-forum%2FCAFeDd5a7c05VQt9J2ApNT8skw238wq1tgpu7BWQYcuRVtFYmeQ%2540mail.gmail.com.

From: Greg Maxwell <gmaxwell@gmail.com> via pqc-forum@list.nist.gov
To: John Mattsson <john.mattsson@ericsson.com>
CC: Billy Brumley <bbrumley@gmail.com>, pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] RE: Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized
Date: Thursday, August 11, 2022 05:55:46 AM ET

On Thu, Aug 11, 2022 at 9:28 AM 'John Mattsson' via pqc-forum <pqc-forum@list.nist.gov> wrote:

> I don't think you can discuss IRP without discussing licensing terms. IPR licensed under predictable FRAND licenses with low fees are not bankrupting anybody. IRP with unpredictable licensing, very high license fees, or no licensing is a different story.

"Low fees" bankrupt free software developers, who distribute millions to hundreds of millions of copies, where not only a penny per copy would be a ruinous cost but the cost of even _counting_ the copies would be ruinous. Adopting 'low fee' patent encumbered technology can also put a downstream adopter of free software in violation of their upstream software licenses.

Cryptographic algorithms with meaningful encumbrance do not achieve widespread deployment in public protocols. Users eschew cryptography or use alternatives, and I can't see why this wouldn't be doubly true for PQC since the risks it addresses are more speculative than typical. This is a plain "usability" limitation: Cryptosystems that require patent licensing are inferior for use by the general public, no less than one that requires the user to authenticate by putting a shoe on their head. In specialized applications-- proprietary protocols in embedded devices, drm, etc-- the situation may be different (though when specialized applications use bespoke crypto they often get it wrong...)

Moreover, any incorporation of patents with non-trivial requirements into a public standard almost always unethically extends the patent holders monopoly beyond the value it provides: If someone has a technique that makes an approach 5% faster or more bandwidth efficient (for example) you rationally might be willing to pay up to the value of that improvement to you. But when the patented techniques is mandatory to implement in an otherwise open standard you'll need to pay for the technique even if its "benefit" is of no value to you, allowing the patent holder to extract rents purely because their technique was bundled and you need to be compatible with the standard.

This argument is elaborated further in a comment to the FTC I contributed to back in 2011:
https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.ftc.gov%2Fsites%2Fdefault%2Ffiles%2Fdocuments%2Fpublic_comments%2Frequest-comments-and-announcement-workshop-standard-setting-issues-project-no.p111204-00020%25C2%25A0%2F00020-60532.pdf&amp;data=05%7C01%7Cyi-kai.liu%40nist.gov%7Caf30929249414163ccfb08da7b7fa758%7C2ab5d82fd8fa4797a93e054655c61dec%7C1%7C0%7C637958085464417884%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&amp;sdata=COTZ6%2FkEq1E%2FNhJONTOx0ddsszRROXvvu8DwpnEndf8%3D&amp;reserved=0

I think this is particularly clear in the context of PQC since we can look at the various proposals which have and lack various known specific potential patent encumbrances and even if we attribute all the advantages of one proposal vs another to the potentially encumbered techniques (which is clearly too conservative an analysis) it's clear that their value to an implementer is fairly small because the fitness from an implementer's perspective of the various finalists doesn't differ that much. I've certainly not seen commentary that the least efficient lattice finalists wouldn't be acceptable in applications where the most efficient would.

From: Scott Fluhrer (sfluhrer) <sfluhrer@cisco.com> via pqc-forum <pqc-forum@list.nist.gov>
To: John Mattsson <john.mattsson@ericsson.com>, Billy Brumley <bbrumley@gmail.com>, pqc-forum@list.nist.gov
Subject: RE: [pqc-forum] RE: Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized
Date: Thursday, August 11, 2022 08:48:07 AM ET

I don’t know what public discussion with IPR experts would do; NIST and the patent holders have signed licenses or are in the process of doing so and public discussion would not change those terms. Each individual organization needs to examine those licensing terms, and decide whether or not those terms are acceptable (and if not, then search for an alternative).

That said, when does NIST intend to publish the license agreements? It would be very hard to expect organizations to abide by licensing terms they have not seen.

From: 'John Mattsson' via pqc-forum <pqc-forum@list.nist.gov>
Sent: Thursday, August 11, 2022 5:28 AM
To: Billy Brumley <bbrumley@gmail.com>; pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] RE: Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized

I agree very much with Billy Brumley that IPR experts should be leading the discussion. Technical people often have a very naive view when it comes to these topics. Public discussion of specific alleged IPR might e.g., benefit the IPR owner in several different ways:

- It is easier to claim that the infringement is willful in an infringement case.

- Technical discussion about an alleged IPR is often useful in an infringement case.

- The discussion might be used in an anti-trust case.

I think all systems used by SDOs have some negative side-effects. You might e.g., be able to convince a jury that the third-party declarations used in IETF is a statement that the RFC is infringing on the IPR. 3GPP is quite accepting to IPR and they are not as visible as in the IETF, but 3GPP have very hard commitments to FRAND licensing where anything not following FRAND licensing must be removed from the standards. NIST requires declaration of IPRs but have to my knowledge not been enforcing FRAND licensing in practice.

I don't think you can discuss IRP without discussing licensing terms. IPR licensed under predictable FRAND licenses with low fees are not bankrupting anybody. IRP with unpredictable licensing, very high license fees, or no licensing is a different story.

Cheers,

John

From: pqc-forum@list.nist.gov <pqc-forum@list.nist.gov> on behalf of Billy Brumley <bbrumley@gmail.com>
Date: Friday, 29 July 2022 at 08:04
To: pqc-forum@list.nist.gov <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] RE: Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized

Howdy Dan,

I agree with what you wrote.

On Thu, Jul 28, 2022 at 5:06 PM D. J. Bernstein <djb@cr.yp.to> wrote:
>
> Billy Brumley writes:
> > Despite what Dan wrote, it's not just the lawyers.
>
> Not sure what you're disputing. The text didn't say it's _just_ the
> lawyers; on the contrary, the very next sentence has the "TLS managers"
> and "higher-ups" falling into line!

Right, the text didn't say that. What prompted my response is the
possibility of your text being misinterpreted that way. But it's
crystal clear now.

For a standardization effort, ofc "the ostrich approach" isn't
sustainable. So when you wrote

> it's clearly essential to understand what patents are out there and what they cover

I 110% agree with you. But IMO, IPR experts should be leading that discussion.

The main message I wanted to deliver is this: Most academics have zero
experience with IPR, so they should understand the risks before they
go commenting about specific IPR in public. As an academic, it might
seem harmless to follow some hyperlink to a patent in one of the
discussions here, read it, and comment about it in this public forum.
But doing so carries risk---the Internet never forgets :)

(Nothing I wrote should be construed to suggest any _particular
individual_ commenting on IPR in this thread is or is not qualified to
do so. If you have experience with IPR and know what you're doing,
feel free to ignore this message and my previous one.)

Happy Friday!

BBB

--
You received this message because you are subscribed to the Google Groups "pqc-forum" group.
To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.
To view this discussion on the web visit https://protect2.fireeye.com/v1/url?k=31323334-501cfaf3-313273af-454445554331-8ab12e1659c8d732&q=1&e=dc288a6c-0946-442d-bee3-345f147bb2b0&u=https%3A%2F%2Fgroups.google.com%2Fa%2Flist.nist.gov%2Fd%2Fmsgid%2Fpqc-forum%2FCAFeDd5a7c05VQt9J2ApNT8skw238wq1tgpu7BWQYcuRVtFYmeQ%2540mail.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/HE1PR0701MB30500F3BF23B8BA8B0FDFB9489649%40HE1PR0701MB3050.eurprd07.prod.outlook.com.