From: Moody, Dustin (Fed) <dustin.moody@nist.gov> via pqc-forum <pqc-forum@list.nist.gov>
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: [pqc-forum] Request for feedback on possible SPHINCS+ variant
Date: Wednesday, November 30, 2022 07:28:19 AM ET

All,

The design of SPHINCS+ imposes a limit on the number of allowable signatures from a given public key. For any number of signatures using the public key, g, there is some very low probability that they will reveal enough of the private key to allow an attacker to forge a signature. As g grows, so does the probability of this disaster. The total number of signatures must be kept low enough that this probability remains negligible. NIST's Call for Proposals required the ability to securely perform 2^64 signatures, which imposes requirements on the parameters of SPHINCS+. A smaller maximum number of signatures would result in somewhat smaller and faster signatures.

NIST asks for public feedback on whether such a version of SPHINCS+ would be beneficial.

NIST PQC team

From: William Whyte <wwhyte@qti.qualcomm.com> via pqc-forum@list.nist.gov
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>, pqc-forum <pqc-forum@list.nist.gov>
Subject: [pqc-forum] RE: Request for feedback on possible SPHINCS+ variant
Date: Wednesday, November 30, 2022 09:52:07 PM ET

Hi Dustin – do we have figures on how much this would save in terms of key / signature size? If it's significant, it's worth considering; if not, then not.

Cheers,

William

From: 'Moody, Dustin (Fed)' via pqc-forum <pqc-forum@list.nist.gov>
Sent: Wednesday, November 30, 2022 7:28 AM
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: [pqc-forum] Request for feedback on possible SPHINCS+ variant

WARNING: This email originated from outside of Qualcomm. Please be wary of any links or attachments, and do not enable macros.

All,

The design of SPHINCS+ imposes a limit on the number of allowable signatures from a given public key. For any number of signatures using the public key, g, there is some very low probability that they will reveal enough of the private key to allow an attacker to forge a signature. As g grows, so does the probability of this disaster. The total number of signatures must be kept low enough that this probability remains negligible. NIST's Call for Proposals required the ability to securely perform 2^64 signatures, which imposes requirements on the parameters of SPHINCS+. A smaller maximum number of signatures would result in somewhat smaller and faster signatures.

NIST asks for public feedback on whether such a version of SPHINCS+ would be beneficial.

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/SA1PR09MB8669CC55FD9EF5432F6B9C51E5159%40SA1PR09MB8669.namprd09.prod.outlook.com.

From: Andreas Hülsing <ietf@huelsing.net> via pqc-forum@list.nist.gov
To: pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] RE: Request for feedback on possible SPHINCS+ variant
Date: Thursday, December 01, 2022 03:52:05 AM ET

Dear William, dear all,

You can find the slides of my presentation of SPHINCS+ here:

https://huelsing.net/wordpress/wp-content/uploads/2022/11/20221129_sphincsp_NIST.pdf

Slide 17 shows the signature sizes when reducing the max number of signatures to different values. We also plan to publish a more detailed note on this the coming weeks.

Best wishes,

Andreas

On 01-12-2022 03:51, William Whyte wrote:

> Hi Dustin – do we have figures on how much this would save in terms of key / signature size? If it’s significant, it’s worth considering; if not, then not.
>
> Cheers,
>
> William
>
> **From:** 'Moody, Dustin (Fed)' via pqc-forum <pqc-forum@list.nist.gov>
> **Sent:** Wednesday, November 30, 2022 7:28 AM
> **To:** pqc-forum <pqc-forum@list.nist.gov>
> **Subject:** [pqc-forum] Request for feedback on possible SPHINCS+ variant
>
> **WARNING:** This email originated from outside of Qualcomm. Please be wary of any links or attachments, and do not enable macros.
>
> All,
>
> The design of SPHINCS+ imposes a limit on the number of allowable signatures from a given public key. For any number of signatures using the public key, g, there is some very low probability that they will reveal enough of the private key to allow an attacker to forge a signature. As g grows, so does the probability of this disaster.

The total number of signatures must be kept low enough that this probability remains negligible. NIST's Call for Proposals required the ability to securely perform 2^64 signatures, which imposes requirements on the parameters of SPHINCS+. A smaller maximum number of signatures would result in somewhat smaller and faster signatures.

NIST asks for public feedback on whether such a version of SPHINCS+ would be beneficial.

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/SA1PR09MB8669CC55FD9EF5432F6B9C51E5159%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/MN2PR02MB6591F991A260006BEED6B2C2F2149%40MN2PR02MB6591.namprd02.prod.outlook.com.

From: William Whyte <wwhyte@qti.qualcomm.com> via pqc-forum@list.nist.gov
To: Andreas Hülsing <ietf@huelsing.net>, pqc-forum@list.nist.gov
Subject: RE: [pqc-forum] RE: Request for feedback on possible SPHINCS+ variant
Date: Thursday, December 01, 2022 08:01:51 AM ET

Thank you!

From: pqc-forum@list.nist.gov <pqc-forum@list.nist.gov> **On Behalf Of** Andreas Hülsing
Sent: Thursday, December 1, 2022 3:51 AM
To: pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] RE: Request for feedback on possible SPHINCS+ variant

WARNING: This email originated from outside of Qualcomm. Please be wary of any links or attachments, and do not enable macros.

Dear William, dear all,

You can find the slides of my presentation of SPHINCS+ here:

https://huelsing.net/wordpress/wp-content/uploads/2022/11/20221129_sphincsp_NIST.pdf

Slide 17 shows the signature sizes when reducing the max number of signatures to different values. We also plan to publish a more detailed note on this the coming weeks.

Best wishes,

Andreas

On 01-12-2022 03:51, William Whyte wrote:

> Hi Dustin – do we have figures on how much this would save in terms of key / signature size? If it's significant, it's worth considering; if not, then not.
>
> Cheers,
>
> William
>
> ---
>
> **From:** 'Moody, Dustin (Fed)' via pqc-forum <pqc-forum@list.nist.gov>
> **Sent:** Wednesday, November 30, 2022 7:28 AM

To: pqc-forum <pqc-forum@list.nist.gov>
Subject: [pqc-forum] Request for feedback on possible SPHINCS+ variant

WARNING: This email originated from outside of Qualcomm. Please be wary of any links or attachments, and do not enable macros.

All,

The design of SPHINCS+ imposes a limit on the number of allowable signatures from a given public key. For any number of signatures using the public key, g, there is some very low probability that they will reveal enough of the private key to allow an attacker to forge a signature. As g grows, so does the probability of this disaster. The total number of signatures must be kept low enough that this probability remains negligible. NIST's Call for Proposals required the ability to securely perform 2^64 signatures, which imposes requirements on the parameters of SPHINCS+. A smaller maximum number of signatures would result in somewhat smaller and faster signatures.

NIST asks for public feedback on whether such a version of SPHINCS+ would be beneficial.

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/SA1PR09MB8669CC55FD9EF5432F6B9C51E5159%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/

MN2PR02MB6591F991A260006BEED6B2C2F2149%40MN2PR02MB6591.namprd02.prod.outlook.com.

From: Stefan Kölbl <kste@google.com> via pqc-forum <pqc-forum@list.nist.gov>
To: Joost Renes <joost.renes@nxp.com>
CC: pqc-forum@list.nist.gov
Subject: Re: [EXT] RE: [pqc-forum] RE: Request for feedback on possible SPHINCS+ variant
Date: Friday, December 02, 2022 11:02:41 AM ET

Hi Joost,
It's true that the signing side has to be careful in this case. However there are still several advantages over a stateful scheme like LMS/XMSS:

1) Security doesn't drop immediately, and depending on the actual parameter choice degrades quite slowly. For example in the plot Andreas showed at the workshop the costs for having parameters which guarantee >100 bits security if you sign 2^10 signatures too much is moderate.

2) Backing up keys is much easier, as you don't need to synchronize the state.

3) Using a single key pair with multiple signers is much easier, as you don't need to synchronize the state.

Best,

Stefan

On Fri, Dec 2, 2022 at 4:46 PM Joost Renes <joost.renes@nxp.com> wrote:

> Hi Dustin,
>
> We would like to confirm that we see value in a version of SPHINCS+ with a lower maximum number of signatures.
>
> The main applications we see are similar to LMS & XMSS, i.e., firmware update and secure boot.
>
> For these use cases
>
> 1. Key generation & signing time is not relevant (assuming a single signature for many devices);
>
> 2. During the lifetime of systems only relatively few updates are required, certainly less than 2^20.

> We acknowledge that for these use cases LMS & XMSS also fit very well, however managing the state on the signer side can be complicated and adds additional risk since this is not typically done with classical algorithms (ECC / RSA).
>
> We think it is useful to have a “small” version of SPHINCS+ to cover the use cases where maintaining such a state is difficult.
>
> Moreover, your email uses the phrase “somewhat smaller” but we think the reduction is very significant.
>
> For example, the “public key + signature” size for Dilithium2 is 3.7 kB, while an instantiation of SPHINCS+ presented by Andreas Hülsing in the NIST workshop was of size ~4 kB.
>
> This provides a PQC digital signature algorithm of similar size, but of much more conservative nature.
>
> This has the additional benefit that combining it with a classical signature might not be necessary, and will accelerate adoption.
>
> Although the above sounds quite positive, we want to note a potential caveat that while a state such as for LMS & XMSS is not necessary, with a lower number of maximum signatures the signing side must be extra careful not to sign too often.
>
> For the above use cases, assuming 1 update a day one could provide updates for ~2800 years and no issues should occur.
>
> However, these assumptions might fail in practice (eg. if keys turn out to be re-used across applications, or per-device signing is used erroneously).
>
> How does NIST or the SPHINCS+ team foresee dealing with this?
>
> If one keeps tracks of the number of signatures, one can argue this is also a state that needs to be maintained, and the advantage over LMS/XMSS disappears.
>
> Are there still any advantages of SPHINCS+ in this case, or is it only useful in scenarios where one does not track the number of signatures?
>
> Kind regards,
>
> NXP PQC team

From:pqc-forum@list.nist.gov <pqc-forum@list.nist.gov> **On Behalf Of** William Whyte
Sent: Thursday, December 1, 2022 2:01 PM
To: Andreas Hülsing <ietf@huelsing.net>; pqc-forum@list.nist.gov
Subject: [EXT] RE: [pqc-forum] RE: Request for feedback on possible SPHINCS+ variant

Caution: EXT Email

Thank you!

From:pqc-forum@list.nist.gov <pqc-forum@list.nist.gov> **On Behalf Of** Andreas Hülsing
Sent: Thursday, December 1, 2022 3:51 AM
To:pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] RE: Request for feedback on possible SPHINCS+ variant

WARNING: This email originated from outside of Qualcomm. Please be wary of any links or attachments, and do not enable macros.

Dear William, dear all,

You can find the slides of my presentation of SPHINCS+ here:

https://huelsing.net/wordpress/wp-content/uploads/2022/11/20221129_sphincsp_NIST.pdf

Slide 17 shows the signature sizes when reducing the max number of signatures to different values. We also plan to publish a more detailed note on this the coming weeks.

Best wishes,

Andreas

On 01-12-2022 03:51, William Whyte wrote:

> Hi Dustin – do we have figures on how much this would save in terms of key / signature size? If it's significant, it's worth considering; if not, then not.
>
> Cheers,
>
> William
>
> **From:** 'Moody, Dustin (Fed)' via pqc-forum <pqc-forum@list.nist.gov>
> **Sent:** Wednesday, November 30, 2022 7:28 AM

To: pqc-forum <pqc-forum@list.nist.gov>
Subject: [pqc-forum] Request for feedback on possible SPHINCS+ variant

WARNING: This email originated from outside of Qualcomm. Please be wary of any links or attachments, and do not enable macros.

All,

The design of SPHINCS+ imposes a limit on the number of allowable signatures from a given public key. For any number of signatures using the public key, g, there is some very low probability that they will reveal enough of the private key to allow an attacker to forge a signature. As g grows, so does the probability of this disaster. The total number of signatures must be kept low enough that this probability remains negligible. NIST's Call for Proposals required the ability to securely perform 2^64 signatures, which imposes requirements on the parameters of SPHINCS+. A smaller maximum number of signatures would result in somewhat smaller and faster signatures.

NIST asks for public feedback on whether such a version of SPHINCS+ would be beneficial.

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/SA1PR09MB8669CC55FD9EF5432F6B9C51E5159%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/

> > MN2PR02MB6591F991A260006BEED6B2C2F2149%40MN2PR02MB6591.namprd02.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/a0ea25da-8a7e-9d8f-e3df-9484627bf980%40huelsing.net.
>
> --
> 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/DM6PR02MB658543E1793C3AF5998C0D1EF2149%40DM6PR02MB6585.namprd02.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/AM9PR04MB816172B39772336AF31D4558FF179%40AM9PR04MB8161.eurprd04.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/CADqV7UahGEta458BvkhPKHqyMv4p99iNJ9u60yfsBn7tEFq5Og%40mail.gmail.com.

From: Paul Hoffman <paul.hoffman@icann.org> via pqc-forum@list.nist.gov
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
CC: pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [Ext] [pqc-forum] Request for feedback on possible SPHINCS+ variant
Date: Friday, December 02, 2022 12:42:23 PM ET

On Nov 30, 2022, at 4:28 AM, 'Moody, Dustin (Fed)' via pqc-forum <pqc-forum@list.nist.gov> wrote:

> The design of SPHINCS+ imposes a limit on the number of allowable signatures from a given public key. For any number of signatures using the public key, g, there is some very low probability that they will reveal enough of the private key to allow an attacker to forge a signature. As g grows, so does the probability of this disaster. The total number of signatures must be kept low enough that this probability remains negligible. NIST’s Call for Proposals required the ability to securely perform 2^64 signatures, which imposes requirements on the parameters of SPHINCS+. A smaller maximum number of signatures would result in somewhat smaller and faster signatures.
>
>
> NIST asks for public feedback on whether such a version of SPHINCS+ would be beneficial.

There are many environments where smaller public keys and/or smaller signatures are valuable. Many of those same environments would also benefit from faster validation of signatures.

An environment that relies on signing by an HSM is unlikely to sign more than 2^32 messages during a key's lifetime. In fact, many such environments would be unlikely to 2^24 messages during a key's lifetime. HSMs can easily count how many times a particular key has been used.

Even when not using an HSM, counting the number of times a key has been used is a reasonable thing to expect of when the key has any significant value. If a signature includes the signing count, it is possible for the public to see how close a signer is to the safe limit for that one key.

Thus, not only would "such a version of SPHINCS+ would be beneficial", more than one would be beneficial. I don't speak (at all!) for the DNSSEC community, but that community is known to be sensitive to message size and often has keys that are used well less than even 2^16 times. The root keys of the global DNS are used a few times a day; keys at lower levels of the DNS hierarchy can be used much more often (and often without HSMs), but "you must count your signatures and change keys well ahead of 64 thousand uses" is completely tractable from an operations standpoint.

--Paul Hoffman

From: Simon Hoerder <simon@hoerder.net> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] Request for feedback on possible SPHINCS+ variant
Date: Friday, December 02, 2022 01:15:11 PM ET

Hi all,

If you add parameters with a reduced number of signatures, I'd consider that a potential foot gun.

I can perfectly understand why those parameters are desirable but I would suggest not adding them to the main standard. Instead you could publish a SP800 that augments the generic SPHINCS+ parameter set with the optimized parameter sets that require extra rules to manage the number of signatures that can be generated. That way, everyone choosing to implement a potential foot gun would be forced to acknowledge what they're doing and adhere to the extra rules (at least if they intend to get certified).

Best,
Simon
(Speaking only for myself)

From: Peter Schwabe <peter@cryptojedi.org> via pqc-forum@list.nist.gov
To: Simon Hoerder <simon@hoerder.net>
CC: pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] Request for feedback on possible SPHINCS+ variant
Date: Saturday, December 03, 2022 07:55:41 PM ET

Simon Hoerder <simon@hoerder.net> wrote:

> Hi all,

Hi Simon, hi all,

> If you add parameters with a reduced number of signatures, I’d
> consider that a potential foot gun.
>
> I can perfectly understand why those parameters are desirable but I
> would suggest not adding them to the main standard. Instead you could
> publish a SP800 that augments the generic SPHINCS+ parameter set with
> the optimized parameter sets that require extra rules to manage the
> number of signatures that can be generated. That way, everyone
> choosing to implement a potential foot gun would be forced to
> acknowledge what they’re doing and adhere to the extra rules (at least
> if they intend to get certified).

That sounds like a very good idea to me.

> Best,
> Simon
> (Speaking only for myself)

All the best,

Peter
(also speaking only for myself)

--

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

From: Marco Amaral Henriques <maah@unicamp.br> 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: Request for feedback on possible SPHINCS+ variant
Date: Sunday, December 04, 2022 12:06:43 PM ET

Dear Dustin, dear all
In 2019 and 2020 we worked on this SPHINCS+ problem: How to change the parameters in order to reduce the maximum number of possible signatures and thus obtain smaller and faster results, without compromising security. The focus, at that time, was on reducing the impact of SPHINCS+ adoption to sign blockchain transactions.

We published a paper on Brazilian Simposium on Information Security (SBSeg 2020) showing our preliminary results on tweaking SPHINCS+ (round 2) parameters and I hope those results can be of some help in this discussion.

The paper (in English) is available from the link below.

https://www.researchgate.net/publication/359975313_A_study_on_fitting_SPHINCS_to_blockchain_usage

Best regards,

Marco Amaral Henriques

School of Electrical and Computer Engineering

Campinas State University - Unicamp

São Paulo, Brazil

Em quarta-feira, 30 de novembro de 2022 às 09:28:14 UTC-3, dustin...@nist.gov escreveu:

> All,
>
> The design of SPHINCS+ imposes a limit on the number of allowable signatures from a given public key. For any number of signatures using the public key, g, there is some very low probability that they will reveal enough of the private key to allow an attacker to forge a signature. As g grows, so does the probability of this disaster. The total number of signatures must be kept low enough that this probability remains negligible. NIST's Call for

> Proposals required the ability to securely perform 2^64 signatures, which imposes requirements on the parameters of SPHINCS+. A smaller maximum number of signatures would result in somewhat smaller and faster signatures.
>
> NIST asks for public feedback on whether such a version of SPHINCS+ would be beneficial.
>
> NIST PQC team

From: Kousidis, Stavros <stavros.kousidis@bsi.bund.de> via pqc-forum <pqc-forum@list.nist.gov>
To: pqc-forum@list.nist.gov
Subject: [pqc-forum] AW: Request for feedback on possible SPHINCS+ variant
Date: Thursday, December 08, 2022 09:31:05 AM ET

Dear all,

from BSI's point of view a version of SPHINCS+ with a smaller maximum number of signatures would be beneficial to the ecosystem.

Due to the level of common trust in the security of hash-based signatures we see their deployment in (Root-)CA certificates as an important milestone to establish secure PKIs. The stateful hash-based signature schemes impose some hassle due to the state management (which we rate to be manageable for a CA). On the other hand, going for a stateless hash-based signature scheme the current versions of SPHINCS+ might generate issues in a PKI due to the large signatures and hence higher space/bandwidth requirements in comparison to the lattice-based signature schemes. A reduced-number-of-sigs version of SPHINCS+ allowing a certain number of signatures with a security margin (i.e. slow degradation in security after the maximum number of signatures have been reached) would make hash-based signatures more attractive for CA's/PKI's. In certificates, the size of PK+Sig matters, hence it could be comparable to CRYSTALS-Dilithium's space requirements.

The BSI would welcome such versions of SPHINCS+. We would also be in favor of reduced-number-of-sigs variants of SPHINCS+ for the security level 192 (in addition to 128) such that CA's would have the freedom to choose and adjust to their security demands. The benefit of such variants for a 256 security level certainly depends on the specific use case. For a CA we would assume that versions with 2^20 sigs and security margin up to 2^30 as well as 2^30 up to 2^40 would be interesting. For a CA with regular renewals the 2^20 up to 2^30 could be sufficient.

From our point of view such SPHINCS+ variants could also make hash-based signatures more attractive for their actual deployment in end-user OpenPGP / S/MIME-certificates if it is known in advance that 2^20 (or 2^30, respectively) signatures will hardly be reached by the signing entity.

Best

Stavros Kousidis, BSI

Von: 'Moody, Dustin (Fed)' via pqc-forum <pqc-forum@list.nist.gov>
Gesendet: Mittwoch, 30. November 2022 13:28
An: pqc-forum <pqc-forum@list.nist.gov>
Betreff: [pqc-forum] Request for feedback on possible SPHINCS+ variant

All,

The design of SPHINCS+ imposes a limit on the number of allowable signatures from a given public key. For any number of signatures using the public key, g, there is some very low probability that they will reveal enough of the private key to allow an attacker to forge a signature. As g grows, so does the probability of this disaster. The total number of signatures must be kept low enough that this probability remains negligible. NIST's Call for Proposals required the ability to securely perform 2^64 signatures, which imposes requirements on the parameters of SPHINCS+. A smaller maximum number of signatures would result in somewhat smaller and faster signatures.

NIST asks for public feedback on whether such a version of SPHINCS+ would be beneficial.

NIST PQC team

From: Jade Philipoom <jadep@opentitan.org> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
CC: Dominic Rizzo <domrizzo@opentitan.org>
Subject: [pqc-forum] Re: Request for feedback on possible SPHINCS+ variant
Date: Thursday, December 08, 2022 10:24:44 AM ET

Hi everyone,

The OpenTitan project would be very interested in this type of SPHINCS+ variant for firmware signing on our family of hardware roots of trust. This variant's trade-off of lower maximum signatures and slower signing speed for smaller signatures and faster verification is an ideal fit for our context. We are currently evaluating running SPHINCS+ on our unmodified hardware and have observed significant speedups from parameter sets with a lower maximum number of signatures.

Maximum signatures: We only need to sign when releasing a firmware update. The signing environment is tightly controlled, which makes it straightforward to track and limit the number of signatures. Once-a-month firmware updates over five years would require only 60 signatures; even once-a-week updates over ten years would require only 520. A signature scheme with maximum 2^10 signatures would be reasonable for this purpose.

Signature size: Our environment is by nature memory-constrained, and although current SPHINCS+ signature sizes are workable, significantly smaller ones would help.

State: A stateless scheme like SPHINCS+ is appealing for our context, compared to a stateful scheme like LMS, because it avoids the complexity, risk and cost of implementing a novel stateful signing infrastructure.

Verification speed: Signature verifications happen on every boot, so verification speed is an important constraint. Signing, on the other hand, happens so rarely that we can tolerate a speed as slow as several minutes. We've measured a > 4x speedup from a parameter set with maximum 2^20 signatures, as compared to shake-128s-simple with maximum 2^64 signatures. That change makes our implementation of SPHINCS+ similar in speed to equivalently-secure classical signature verification.

Best,
Jade Philipoom, OpenTitan

On Thursday, December 8, 2022 at 3:31:02 PM UTC+1 Kousidis, Stavros wrote:

> Dear all,
>
> from BSI's point of view a version of SPHINCS+ with a smaller maximum number of signatures would be beneficial to the ecosystem.
>
> Due to the level of common trust in the security of hash-based signatures we see their deployment in (Root-)CA certificates as an important milestone to establish secure PKIs. The stateful hash-based signature schemes impose some hassle due to the state management (which we rate to be manageable for a CA). On the other hand, going for a stateless hash-based signature scheme the current versions of SPHINCS+ might generate issues in a PKI due to the large signatures and hence higher space/bandwidth requirements in comparison to the lattice-based signature schemes. A reduced-number-of-sigs version of SPHINCS+ allowing a certain number of signatures with a security margin (i.e. slow degradation in security after the maximum number of signatures have been reached) would make hash-based signatures more attractive for CA's/PKI's. In certificates, the size of PK+Sig matters, hence it could be comparable to CRYSTALS-Dilithium's space requirements.
>
> The BSI would welcome such versions of SPHINCS+. We would also be in favor of reduced-number-of-sigs variants of SPHINCS+ for the security level 192 (in addition to 128) such that CA's would have the freedom to choose and adjust to their security demands. The benefit of such variants for a 256 security level certainly depends on the specific use case. For a CA we would assume that versions with 2^20 sigs and security margin up to 2^30 as well as 2^30 up to 2^40 would be interesting. For a CA with regular renewals the 2^20 up to 2^30 could be sufficient.
>
> From our point of view such SPHINCS+ variants could also make hash-based signatures more attractive for their actual deployment in end-user OpenPGP / S/MIME-certificates if it is known in advance that 2^20 (or 2^30, respectively) signatures will hardly be reached by the signing entity.
>
> Best
>
> Stavros Kousidis, BSI
>
> ---
>
> **Von:** 'Moody, Dustin (Fed)' via pqc-forum <pqc-...@list.nist.gov>
>
> **Gesendet:** Mittwoch, 30. November 2022 13:28

> **An:** pqc-forum <pqc-...@list.nist.gov>
> **Betreff:** [pqc-forum] Request for feedback on possible SPHINCS+ variant
>
> All,
>
> The design of SPHINCS+ imposes a limit on the number of allowable signatures from a given public key. For any number of signatures using the public key, g, there is some very low probability that they will reveal enough of the private key to allow an attacker to forge a signature. As g grows, so does the probability of this disaster. The total number of signatures must be kept low enough that this probability remains negligible. NIST's Call for Proposals required the ability to securely perform 2^64 signatures, which imposes requirements on the parameters of SPHINCS+. A smaller maximum number of signatures would result in somewhat smaller and faster signatures.
>
> NIST asks for public feedback on whether such a version of SPHINCS+ would be beneficial.
>
> 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/SA1PR09MB8669CC55FD9EF5432F6B9C51E5159%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/d0b0b53e-9eac-4572-be63-7e283218007cn%40list.nist.gov.

From: Aymeric Genêt <aymeric.gen@gmail.com> via pqc-forum@list.nist.gov
To: Jade Philipoom <jadep@opentitan.org>
CC: pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] Re: Request for feedback on possible SPHINCS+ variant
Date: Thursday, December 08, 2022 01:19:10 PM ET

Hello everyone,

For a very short number of signatures (< 2^10), I suggest using a large few-time signature scheme (such as FORS, the first layer in SPHINCS), as I don't think that the entire structure of SPHINCS+ is therefore necessary.

This would keep your signatures hash-based and stateless, make the scheme simpler (fewer things can go wrong), reduce the complexity of the signing and verification times, and clearly distinguish itself from SPHINCS+ (as only a few number of signatures is allowed by design). The design could also allow a trade-off between the signature and the public key sizes to fit your needs.

In this spirit, I would recommend to have a look at PRUNE-HORST (https://github.com/gravity-postquantum/prune-horst) which was submitted to the NIST post-quantum project but was quickly eliminated because of the too-short number of signatures allowed. The scheme is certainly outdated due to the recent advances with SPHINCS+, but with a proper update, I believe that the idea is worth the consideration.

Best regards,
Aymeric

On Thu, Dec 8, 2022 at 4:24 PM Jade Philipoom <jadep@opentitan.org> wrote:

> Hi everyone,
>
> The OpenTitan project would be very interested in this type of SPHINCS+ variant for firmware signing on our family of hardware roots of trust. This variant’s trade-off of lower maximum signatures and slower signing speed for smaller signatures and faster verification is an ideal fit for our context. We are currently evaluating running SPHINCS+ on our unmodified hardware and have observed significant speedups from parameter sets with a lower maximum number of signatures.

> Maximum signatures: We only need to sign when releasing a firmware update. The signing environment is tightly controlled, which makes it straightforward to track and limit the number of signatures. Once-a-month firmware updates over five years would require only 60 signatures; even once-a-week updates over ten years would require only 520. A signature scheme with maximum 2^10 signatures would be reasonable for this purpose.
>
> Signature size: Our environment is by nature memory-constrained, and although current SPHINCS+ signature sizes are workable, significantly smaller ones would help.
>
> State: A stateless scheme like SPHINCS+ is appealing for our context, compared to a stateful scheme like LMS, because it avoids the complexity, risk and cost of implementing a novel stateful signing infrastructure.
>
> Verification speed: Signature verifications happen on every boot, so verification speed is an important constraint. Signing, on the other hand, happens so rarely that we can tolerate a speed as slow as several minutes. We've measured a > 4x speedup from a parameter set with maximum 2^20 signatures, as compared to shake-128s-simple with maximum 2^64 signatures. That change makes our implementation of SPHINCS+ similar in speed to equivalently-secure classical signature verification.
>
> Best,
> Jade Philipoom, OpenTitan
> On Thursday, December 8, 2022 at 3:31:02 PM UTC+1 Kousidis, Stavros wrote:
>
> > Dear all,
> >
> > from BSI's point of view a version of SPHINCS+ with a smaller maximum number of signatures would be beneficial to the ecosystem.
> >
> > Due to the level of common trust in the security of hash-based signatures we see their deployment in (Root-)CA certificates as an important milestone to establish secure PKIs. The stateful hash-based signature schemes impose some hassle due to the state management (which we rate to be manageable for a CA). On the other hand, going for a stateless hash-based signature scheme the current versions of SPHINCS+ might generate issues in a PKI due to the large signatures and hence higher space/bandwidth requirements in comparison to the lattice-based signature schemes. A reduced-number-

> > of-sigs version of SPHINCS+ allowing a certain number of signatures with a security margin (i.e. slow degradation in security after the maximum number of signatures have been reached) would make hash-based signatures more attractive for CA's/PKI's. In certificates, the size of PK+Sig matters, hence it could be comparable to CRYSTALS-Dilithium's space requirements.
> >
> > The BSI would welcome such versions of SPHINCS+. We would also be in favor of reduced-number-of-sigs variants of SPHINCS+ for the security level 192 (in addition to 128) such that CA's would have the freedom to choose and adjust to their security demands. The benefit of such variants for a 256 security level certainly depends on the specific use case. For a CA we would assume that versions with 2^20 sigs and security margin up to 2^30 as well as 2^30 up to 2^40 would be interesting. For a CA with regular renewals the 2^20 up to 2^30 could be sufficient.
> >
> > From our point of view such SPHINCS+ variants could also make hash-based signatures more attractive for their actual deployment in end-user OpenPGP / S/MIME-certificates if it is known in advance that 2^20 (or 2^30, respectively) signatures will hardly be reached by the signing entity.
> >
> > Best
> >
> > Stavros Kousidis, BSI
> >
> > ---
> >
> > **Von:** 'Moody, Dustin (Fed)' via pqc-forum <pqc-...@list.nist.gov>
> > **Gesendet:** Mittwoch, 30. November 2022 13:28
> > **An:** pqc-forum <pqc-...@list.nist.gov>
> > **Betreff:** [pqc-forum] Request for feedback on possible SPHINCS+ variant
> >
> > All,
> >
> > The design of SPHINCS+ imposes a limit on the number of allowable signatures from a given public key. For any number of signatures using the public key, g, there is some very low probability that they will reveal enough of the private key to allow an attacker to forge a signature. As g grows, so does the probability of this disaster. The total number of signatures must be kept low enough that this probability remains negligible. NIST’s Call for Proposals required the ability to securely perform 2^64 signatures, which imposes requirements on the parameters of SPHINCS+. A smaller maximum number of signatures would result in somewhat smaller and faster signatures.

>> NIST asks for public feedback on whether such a version of SPHINCS+ would be beneficial.
>>
>> 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/SA1PR09MB8669CC55FD9EF5432F6B9C51E5159%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/d0b0b53e-9eac-4572-be63-7e283218007cn%40list.nist.gov.

--
You received this message because you are subscribed to the Google Groups "pqc-forum" group.
To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.
To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/CALX2hLxOigpmX-8XzuSF3dOaxMnR0UMKzqgtFHkREWCXu24iwg%40mail.gmail.com.

From: Mike Ounsworth <mike.ounsworth@entrust.com> via pqc-forum <pqc-forum@list.nist.gov>
To: Aymeric Genêt <aymeric.gen@gmail.com>, Jade Philipoom <jadep@opentitan.org>
CC: pqc-forum <pqc-forum@list.nist.gov>
Subject: RE: [EXTERNAL] Re: [pqc-forum] Re: Request for feedback on possible SPHINCS+ variant
Date: Thursday, December 08, 2022 01:58:09 PM ET

Hi Aymeric,

That sounds interesting! Of course the industry would need it to be a FIPS-approved algorithm. Would you consider submitting a pure FORS variant to the NIST on-ramp?

Mike Ounsworth
Software Security Architect, Entrust

From: pqc-forum@list.nist.gov <pqc-forum@list.nist.gov> **On Behalf Of** Aymeric Genêt
Sent: December 8, 2022 12:18 PM
To: Jade Philipoom <jadep@opentitan.org>
Cc: pqc-forum <pqc-forum@list.nist.gov>
Subject: [EXTERNAL] Re: [pqc-forum] Re: Request for feedback on possible SPHINCS+ variant

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

Hello everyone,

For a very short number of signatures (< 2^10), I suggest using a large few-time signature scheme (such as FORS, the first layer in SPHINCS), as I don't think that the entire structure of SPHINCS+ is therefore necessary.

This would keep your signatures hash-based and stateless, make the scheme simpler (fewer things can go wrong), reduce the complexity of the signing and verification times, and clearly distinguish itself from SPHINCS+ (as only a few number of signatures is allowed by design). The design could also allow a trade-off between the signature and the public key sizes to fit your needs.

In this spirit, I would recommend to have a look at PRUNE-HORST (https://github.com/gravity-postquantum/prune-horst) which was submitted to the NIST post-quantum project but was quickly eliminated because of the too-short number of signatures allowed. The scheme is certainly outdated due to the recent advances with SPHINCS+, but with a proper update, I believe that the idea is worth the consideration.

Best regards,
Aymeric

On Thu, Dec 8, 2022 at 4:24 PM Jade Philipoom <jadep@opentitan.org> wrote:

> Hi everyone,
>
> The OpenTitan project would be very interested in this type of SPHINCS+ variant for firmware signing on our family of hardware roots of trust. This variant’s trade-off of lower maximum signatures and slower signing speed for smaller signatures and faster verification is an ideal fit for our context. We are currently evaluating running SPHINCS+ on our unmodified hardware and have observed significant speedups from parameter sets with a lower maximum number of signatures.
>
> Maximum signatures: We only need to sign when releasing a firmware update. The signing environment is tightly controlled, which makes it straightforward to track and limit the number of signatures. Once-a-month firmware updates over five years would require only 60 signatures; even once-a-week updates over ten years would require only 520. A signature scheme with maximum 2^10 signatures would be reasonable for this purpose.
>
> Signature size: Our environment is by nature memory-constrained, and although current SPHINCS+ signature sizes are workable, significantly smaller ones would help.
>
> State: A stateless scheme like SPHINCS+ is appealing for our context, compared to a stateful scheme like LMS, because it avoids the complexity, risk and cost of implementing a novel stateful signing infrastructure.
>
> Verification speed: Signature verifications happen on every boot, so verification speed is an important constraint. Signing, on the other hand, happens so rarely that we can tolerate a speed as slow as several minutes. We’ve measured a > 4x speedup from a parameter set with maximum 2^20 signatures, as compared to shake-128s-simple with maximum 2^64 signatures. That change makes our implementation of SPHINCS+ similar in speed to equivalently-secure classical signature verification.

> Best,
> Jade Philipoom, OpenTitan
>
> On Thursday, December 8, 2022 at 3:31:02 PM UTC+1 Kousidis, Stavros wrote:
>
> > Dear all,
> >
> > from BSI's point of view a version of SPHINCS+ with a smaller maximum number of signatures would be beneficial to the ecosystem.
> >
> > Due to the level of common trust in the security of hash-based signatures we see their deployment in (Root-)CA certificates as an important milestone to establish secure PKIs. The stateful hash-based signature schemes impose some hassle due to the state management (which we rate to be manageable for a CA). On the other hand, going for a stateless hash-based signature scheme the current versions of SPHINCS+ might generate issues in a PKI due to the large signatures and hence higher space/bandwidth requirements in comparison to the lattice-based signature schemes. A reduced-number-of-sigs version of SPHINCS+ allowing a certain number of signatures with a security margin (i.e. slow degradation in security after the maximum number of signatures have been reached) would make hash-based signatures more attractive for CA's/PKI's. In certificates, the size of PK+Sig matters, hence it could be comparable to CRYSTALS-Dilithium's space requirements.
> >
> > The BSI would welcome such versions of SPHINCS+. We would also be in favor of reduced-number-of-sigs variants of SPHINCS+ for the security level 192 (in addition to 128) such that CA's would have the freedom to choose and adjust to their security demands. The benefit of such variants for a 256 security level certainly depends on the specific use case. For a CA we would assume that versions with 2^20 sigs and security margin up to 2^30 as well as 2^30 up to 2^40 would be interesting. For a CA with regular renewals the 2^20 up to 2^30 could be sufficient.
> >
> > From our point of view such SPHINCS+ variants could also make hash-based signatures more attractive for their actual deployment in end-user OpenPGP / S/MIME-certificates if it is known in advance that 2^20 (or 2^30, respectively) signatures will hardly be reached by the signing entity.
> >
> > Best
> >
> > Stavros Kousidis, BSI

> > **Von:** 'Moody, Dustin (Fed)' via pqc-forum <pqc-...@list.nist.gov>
> > **Gesendet:** Mittwoch, 30. November 2022 13:28
> > **An:** pqc-forum <pqc-...@list.nist.gov>
> > **Betreff:** [pqc-forum] Request for feedback on possible SPHINCS+ variant
> >
> > All,
> >
> > The design of SPHINCS+ imposes a limit on the number of allowable signatures from a given public key. For any number of signatures using the public key, g, there is some very low probability that they will reveal enough of the private key to allow an attacker to forge a signature. As g grows, so does the probability of this disaster. The total number of signatures must be kept low enough that this probability remains negligible. NIST's Call for Proposals required the ability to securely perform 2^64 signatures, which imposes requirements on the parameters of SPHINCS+. A smaller maximum number of signatures would result in somewhat smaller and faster signatures.
> >
> > NIST asks for public feedback on whether such a version of SPHINCS+ would be beneficial.
> >
> > 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/SA1PR09MB8669CC55FD9EF5432F6B9C51E5159%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/d0b0b53e-9eac-4572-be63-7e283218007cn%40list.nist.gov.

--
You received this message because you are subscribed to the Google Groups "pqc-forum" group.
To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.
To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/CALX2hLxOigpmX-8XzuSF3dOaxMnR0UMKzqgtFHkREWCXu24iwg%40mail.gmail.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: Aymeric Genêt <aymeric.gen@gmail.com> via pqc-forum@list.nist.gov
To: Mike Ounsworth <mike.ounsworth@entrust.com>
CC: pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [EXTERNAL] Re: [pqc-forum] Re: Request for feedback on possible SPHINCS+ variant
Date: Thursday, December 08, 2022 03:17:25 PM ET

Hi Mike,
> Would you consider submitting a pure FORS variant to the NIST on-ramp?

I don't think I will, but if you (or someone else) are up to the challenge, feel free to take the idea.

Best regards,

Aymeric

On Thu, Dec 8, 2022 at 7:57 PM Mike Ounsworth <Mike.Ounsworth@entrust.com> wrote:

> Hi Aymeric,
>
> That sounds interesting! Of course the industry would need it to be a FIPS-approved algorithm. Would you consider submitting a pure FORS variant to the NIST on-ramp?
>
> ---
> Mike Ounsworth
> Software Security Architect, Entrust
>
> ---
>
> **From:**pqc-forum@list.nist.gov <pqc-forum@list.nist.gov> **On Behalf Of** Aymeric Genêt
> **Sent:** December 8, 2022 12:18 PM
> **To:** Jade Philipoom <jadep@opentitan.org>
> **Cc:** pqc-forum <pqc-forum@list.nist.gov>
> **Subject:** [EXTERNAL] Re: [pqc-forum] Re: Request for feedback on possible SPHINCS+ variant
>
> WARNING: This email originated outside of Entrust.
> DO NOT CLICK links or attachments unless you trust the sender and know the content is safe.
>
> Hello everyone,

> For a very short number of signatures (< 2^10), I suggest using a large few-time signature scheme (such as FORS, the first layer in SPHINCS), as I don't think that the entire structure of SPHINCS+ is therefore necessary.
>
> This would keep your signatures hash-based and stateless, make the scheme simpler (fewer things can go wrong), reduce the complexity of the signing and verification times, and clearly distinguish itself from SPHINCS+ (as only a few number of signatures is allowed by design). The design could also allow a trade-off between the signature and the public key sizes to fit your needs.
>
> In this spirit, I would recommend to have a look at PRUNE-HORST (https://github.com/gravity-postquantum/prune-horst) which was submitted to the NIST post-quantum project but was quickly eliminated because of the too-short number of signatures allowed. The scheme is certainly outdated due to the recent advances with SPHINCS+, but with a proper update, I believe that the idea is worth the consideration.
>
> Best regards,
> Aymeric
>
> On Thu, Dec 8, 2022 at 4:24 PM Jade Philipoom <jadep@opentitan.org> wrote:
>
> > Hi everyone,
> >
> > The OpenTitan project would be very interested in this type of SPHINCS+ variant for firmware signing on our family of hardware roots of trust. This variant's trade-off of lower maximum signatures and slower signing speed for smaller signatures and faster verification is an ideal fit for our context. We are currently evaluating running SPHINCS+ on our unmodified hardware and have observed significant speedups from parameter sets with a lower maximum number of signatures.
> >
> > Maximum signatures: We only need to sign when releasing a firmware update. The signing environment is tightly controlled, which makes it straightforward to track and limit the number of signatures. Once-a-month firmware updates over five years would require only 60 signatures; even once-a-week updates over ten years would require only 520. A signature scheme with maximum 2^10 signatures would be reasonable for this purpose.
> >
> > Signature size: Our environment is by nature memory-constrained, and although current SPHINCS+ signature sizes are workable, significantly smaller ones would help.

>> State: A stateless scheme like SPHINCS+ is appealing for our context, compared to a stateful scheme like LMS, because it avoids the complexity, risk and cost of implementing a novel stateful signing infrastructure.
>>
>> Verification speed: Signature verifications happen on every boot, so verification speed is an important constraint. Signing, on the other hand, happens so rarely that we can tolerate a speed as slow as several minutes. We’ve measured a > 4x speedup from a parameter set with maximum 2^20 signatures, as compared to shake-128s-simple with maximum 2^64 signatures. That change makes our implementation of SPHINCS+ similar in speed to equivalently-secure classical signature verification.
>>
>> Best,
>> Jade Philipoom, OpenTitan
>>
>> On Thursday, December 8, 2022 at 3:31:02 PM UTC+1 Kousidis, Stavros wrote:
>>
>>> Dear all,
>>>
>>> from BSI's point of view a version of SPHINCS+ with a smaller maximum number of signatures would be beneficial to the ecosystem.
>>>
>>> Due to the level of common trust in the security of hash-based signatures we see their deployment in (Root-)CA certificates as an important milestone to establish secure PKIs. The stateful hash-based signature schemes impose some hassle due to the state management (which we rate to be manageable for a CA). On the other hand, going for a stateless hash-based signature scheme the current versions of SPHINCS+ might generate issues in a PKI due to the large signatures and hence higher space/bandwidth requirements in comparison to the lattice-based signature schemes. A reduced-number-of-sigs version of SPHINCS+ allowing a certain number of signatures with a security margin (i.e. slow degradation in security after the maximum number of signatures have been reached) would make hash-based signatures more attractive for CA's/PKI's. In certificates, the size of PK+Sig matters, hence it could be comparable to CRYSTALS-Dilithium's space requirements.
>>>
>>> The BSI would welcome such versions of SPHINCS+. We would also be in favor of reduced-number-of-sigs variants of SPHINCS+ for the security level 192 (in addition to 128) such that CA's would have the freedom to choose and adjust to their security demands. The benefit of such variants for a 256 security level certainly depends on the

> > > specific use case. For a CA we would assume that versions with 2^20 sigs and security margin up to 2^30 as well as 2^30 up to 2^40 would be interesting. For a CA with regular renewals the 2^20 up to 2^30 could be sufficient.
> > >
> > > From our point of view such SPHINCS+ variants could also make hash-based signatures more attractive for their actual deployment in end-user OpenPGP / S/MIME-certificates if it is known in advance that 2^20 (or 2^30, respectively) signatures will hardly be reached by the signing entity.
> > >
> > > Best
> > >
> > > Stavros Kousidis, BSI
> > >
> > > ---
> > >
> > > **Von:** 'Moody, Dustin (Fed)' via pqc-forum <pqc-...@list.nist.gov>
> > > **Gesendet:** Mittwoch, 30. November 2022 13:28
> > > **An:** pqc-forum <pqc-...@list.nist.gov>
> > > **Betreff:** [pqc-forum] Request for feedback on possible SPHINCS+ variant
> > >
> > > All,
> > >
> > > The design of SPHINCS+ imposes a limit on the number of allowable signatures from a given public key. For any number of signatures using the public key, g, there is some very low probability that they will reveal enough of the private key to allow an attacker to forge a signature. As g grows, so does the probability of this disaster. The total number of signatures must be kept low enough that this probability remains negligible. NIST's Call for Proposals required the ability to securely perform 2^64 signatures, which imposes requirements on the parameters of SPHINCS+. A smaller maximum number of signatures would result in somewhat smaller and faster signatures.
> > >
> > > NIST asks for public feedback on whether such a version of SPHINCS+ would be beneficial.
> > >
> > > 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/SA1PR09MB8669CC55FD9EF5432F6B9C51E5159%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/d0b0b53e-9eac-4572-be63-7e283218007cn%40list.nist.gov.
>
> --
> You received this message because you are subscribed to the Google Groups "pqc-forum" group.
> To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.
> To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/CALX2hLxOigpmX-8XzuSF3dOaxMnR0UMKzqgtFHkREWCXu24iwg%40mail.gmail.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.*

--
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/CALX2hLx%2ByrJmu-oe2-%3DUwVJPnajtcNBGmRFZTgmx%2BGJQLhu2FA%40mail.gmail.com.

From: Marina Moore <mnm678@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: Request for feedback on possible SPHINCS+ variant
Date: Thursday, December 15, 2022 08:35:35 AM ET

Hi Dustin,

We are members of the Uptane Standards group writing in favor of a smaller signatures SPHINC+ variant. The Uptane Standard provides a framework for secure over-the-air automotive updates used throughout the automotive industry. This standard has a need for smaller signatures due to limitations of networking and storage of the electronic control units (ECUs) in automobiles. The standard includes many uses of cryptographic keys, many of which are not used frequently and so can handle a small maximum number of signatures.

Uptane implementations sign metadata about software updates for a few different purposes, and some of these are used infrequently. Some of this software update package metadata is used to direct updates and guarantee timeliness, and keys that sign this metadata are used frequently (many times a day), while other keys, such as those used for the root of trust (a kind of root CA for the system), are only used 3-4 times a year. The keys in this latter category are the most security critical in our Uptane system and would benefit from a smaller SPHINCS variant to help us speed up adoption. As few as 2^10 uses would last more than 200 years for keys only used 4 times a year.

In the automotive space, key size is one of the primary concerns. Key generation and signing is done by the OEMs and Tier1 suppliers, so these operations are done on machines that have access to significant computational resources and hardware security components. On the other hand, any data that is sent to a vehicle has both size and computational overhead issues. So the key size, signature size, and verification requirements are of particular concern.

Thanks,

Marina Moore

Justin Cappos

Ira McDonald

Uptane Standards Group

On Wednesday, November 30, 2022 at 7:28:14 AM UTC-5 dustin...@nist.gov wrote:

> All,
>
> The design of SPHINCS+ imposes a limit on the number of allowable signatures from a given public key. For any number of signatures using the public key, g, there is some very low probability that they will reveal enough of the private key to allow an attacker to forge a signature. As g grows, so does the probability of this disaster. The total number of signatures must be kept low enough that this probability remains negligible. NIST’s Call for Proposals required the ability to securely perform 2^64 signatures, which imposes requirements on the parameters of SPHINCS+. A smaller maximum number of signatures would result in somewhat smaller and faster signatures.
>
> NIST asks for public feedback on whether such a version of SPHINCS+ would be beneficial.
>
> NIST PQC team

From: Stefan Kölbl <kste@google.com> via pqc-forum <pqc-forum@list.nist.gov>
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] Re: Request for feedback on possible SPHINCS+ variant
Date: Thursday, December 15, 2022 01:55:34 PM ET

Hi everyone,
The note which includes our parameter search and security degradation evaluation is now available: https://eprint.iacr.org/2022/1725

This includes the evaluation for the L1 parameters presented at the NIST workshop, and the results of the search for the higher security levels as well. I hope this helps everyone to get a better understanding of what kind of trade-offs are possible and the risk involved when exceeding the signature limits.

Best,

Stefan

On Thu, Dec 15, 2022 at 2:35 PM Marina Moore <mnm678@gmail.com> wrote:

> Hi Dustin,
>
> We are members of the Uptane Standards group writing in favor of a smaller signatures SPHINC+ variant. The Uptane Standard provides a framework for secure over-the-air automotive updates used throughout the automotive industry. This standard has a need for smaller signatures due to limitations of networking and storage of the electronic control units (ECUs) in automobiles. The standard includes many uses of cryptographic keys, many of which are not used frequently and so can handle a small maximum number of signatures.
>
> Uptane implementations sign metadata about software updates for a few different purposes, and some of these are used infrequently. Some of this software update package metadata is used to direct updates and guarantee timeliness, and keys that sign this metadata are used frequently (many times a day), while other keys, such as those used for the root of trust (a kind of root CA for the system), are only used 3-4 times a year. The keys in this latter category are the most security critical in our Uptane system and would benefit from a smaller SPHINCS variant to help us speed up adoption. As few as 2^10 uses would last more than 200 years for keys only used 4 times a year.

> In the automotive space, key size is one of the primary concerns. Key generation and signing is done by the OEMs and Tier1 suppliers, so these operations are done on machines that have access to significant computational resources and hardware security components. On the other hand, any data that is sent to a vehicle has both size and computational overhead issues. So the key size, signature size, and verification requirements are of particular concern.
>
> Thanks,
>
> Marina Moore
>
> Justin Cappos
>
> Ira McDonald
>
> Uptane Standards Group
>
> On Wednesday, November 30, 2022 at 7:28:14 AM UTC-5 dustin...@nist.gov wrote:
>
>> All,
>>
>> The design of SPHINCS+ imposes a limit on the number of allowable signatures from a given public key. For any number of signatures using the public key, g, there is some very low probability that they will reveal enough of the private key to allow an attacker to forge a signature. As g grows, so does the probability of this disaster. The total number of signatures must be kept low enough that this probability remains negligible. NIST’s Call for Proposals required the ability to securely perform 2^64 signatures, which imposes requirements on the parameters of SPHINCS+. A smaller maximum number of signatures would result in somewhat smaller and faster signatures.
>>
>> NIST asks for public feedback on whether such a version of SPHINCS+ would be beneficial.
>>
>> 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/a03ba349-82cf-4ac3-b17b-554a0ef89e2fn%40list.nist.gov.

--

From: Andreas Hülsing <ietf@huelsing.net> via pqc-forum@list.nist.gov
To: pqc-forum@list.nist.gov, contact@sphincs.org
Subject: Re: [pqc-forum] Request for feedback on possible SPHINCS+ variant
Date: Monday, December 19, 2022 02:48:41 AM ET

Dear pqc-list,

As mentioned in my talk at the 4th NIST conference, the SPHINCS+ team is interested in feedback regarding a smaller number of max signatures (as already mentioned in Dustin's mail) and regarding the SPHINCS+C proposal.
We already saw the feedback so far on the list regarding max signatures and appreciate it!

The SPHINCS+C proposal can be found at https://eprint.iacr.org/2022/778

For the reduced max signatures parameters, a short note is available at https://eprint.iacr.org/2022/1725.

What is especially important for us to learn is if there are applications that cannot use SPHINCS+ in its current form but would get enabled by one or the other proposal.
However, we are of course also interested in hearing more about applications where the reduced costs are not critical but still helpful.

Moreover, regarding the max signatures proposal, we have the following questions:
* Is there an interest in this for parameters at a security level > I? (Right now we mainly looked at level I security)
* What applications would benefit?
* What would be the number of expected signatures?
* Does the reduced size / better speed make a fundamental difference?
* How important is signature vs verification speed?

Regarding SPHINCS+C we have the following questions:
* What applications would benefit?
* How important is signature vs verification speed?
* How relevant is constant signing time (not be confused with constant time implementation)
* Does the reduced size / better speed make a fundamental difference?

Best wishes,

Andreas & the SPHINCS+ team

On 30-11-2022 13:28, 'Moody, Dustin (Fed)' via pqc-forum wrote:

> All,
>
> The design of SPHINCS+ imposes a limit on the number of allowable signatures from a given public key. For any number of signatures using the public key, g, there is some very low probability that they will reveal enough of the private key to allow an attacker to forge a signature. As g grows, so does the probability of this disaster. The total number of signatures must be kept low enough that this probability remains negligible. NIST’s Call for Proposals required the ability to securely perform 2^64 signatures, which imposes requirements on the parameters of SPHINCS+. A smaller maximum number of signatures would result in somewhat smaller and faster signatures.
>
> NIST asks for public feedback on whether such a version of SPHINCS+ would be beneficial.
>
> 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/SA1PR09MB8669CC55FD9EF5432F6B9C51E5159%40SA1PR09MB8669.namprd09.prod.outlook.com.

From: Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu> via pqc-forum@list.nist.gov
To: Andreas Hülsing <ietf@huelsing.net>
CC: pqc-forum@list.nist.gov, contact@sphincs.org
Subject: Re: [pqc-forum] Request for feedback on possible SPHINCS+ variant
Date: Monday, December 19, 2022 08:53:14 AM ET
Attachments: smime.p7m

Re. Max signatures.

Yes there is interest in Security Level greater than 1.

Considering mostly for firmware signing and Root CA.

Hard to say how many signatures - offhand, 2^20 should be plenty, 2^10 might be too small. Perhaps others who educated more time and thought to this question could tell more.

Probably, smaller size is preferred to faster speed. Probably, faster verification is more important than faster signing.

Probably, constant-time signing is preferred.

Regards,
Uri

> On Dec 19, 2022, at 02:48, Andreas Hülsing wrote:
>
> Dear pqc-list,
>
> As mentioned in my talk at the 4th NIST conference, the SPHINCS+ team is interested in feedback regarding a smaller number of max signatures (as already mentioned in Dustin's mail) and regarding the SPHINCS+C proposal.
> We already saw the feedback so far on the list regarding max signatures and appreciate it!
>
> The SPHINCS+C proposal can be found at https://eprint.iacr.org/2022/778

For the reduced max signatures parameters, a short note is available at https://eprint.iacr.org/2022/1725.

What is especially important for us to learn is if there are applications that cannot use SPHINCS+ in its current form but would get enabled by one or the other proposal.
However, we are of course also interested in hearing more about applications where the reduced costs are not critical but still helpful.

Moreover, regarding the max signatures proposal, we have the following questions:
* Is there an interest in this for parameters at a security level > I? (Right now we mainly looked at level I security)
* What applications would benefit?
* What would be the number of expected signatures?
* Does the reduced size / better speed make a fundamental difference?
* How important is signature vs verification speed?

Regarding SPHINCS+C we have the following questions:
* What applications would benefit?
* How important is signature vs verification speed?
* How relevant is constant signing time (not be confused with constant time implementation)
* Does the reduced size / better speed make a fundamental difference?

Best wishes,

Andreas & the SPHINCS+ team

On 30-11-2022 13:28, 'Moody, Dustin (Fed)' via pqc-forum wrote:

> All,
>
> The design of SPHINCS+ imposes a limit on the number of allowable signatures from a given public key. For any number of signatures using the public key, g, there is some very low probability that they will reveal enough of the private key to allow an attacker to forge a signature. As g

>> grows, so does the probability of this disaster. The total number of signatures must be kept low enough that this probability remains negligible. NIST’s Call for Proposals required the ability to securely perform 2^64 signatures, which imposes requirements on the parameters of SPHINCS+. A smaller maximum number of signatures would result in somewhat smaller and faster signatures.
>>
>> NIST asks for public feedback on whether such a version of SPHINCS+ would be beneficial.
>>
>> NIST PQC team
>>
>>

>

From: Andrew Fregly <amfregly@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: Request for feedback on possible SPHINCS+ variant
Date: Thursday, January 05, 2023 01:52:12 PM ET

Dustin,

A NIST initiative to establish parameter sets for SPHINCS+ that will make signature sizes smaller could also be helpful for DNSSEC.

In many scenarios, DNSSEC has practical limits on the number of signatures that are generated under any particular public key with this varying based on DNS zone size, percentage of the zone that is signed (in cases where less than the entire zone is signed), signature lifetimes, and the frequency of ceremonial processes that drive key rollovers.

Based on current top-level zone metrics, a parameter set for a maximum number of signatures of 2^40 would be more than sufficient for projected DNSSEC deployments with 2^30 likely sufficient for all but the largest top-level DNS zones. A smaller signature size would lessen the impact of SPHINCS+ signatures on resolver caches and authoritative servers using in-memory databases for large zones. It would also help when the Merkle Tree Ladder mode of operation [1] is applied to DNSSEC by lessening the size overhead when a ladder signed with SPHINCS+ is transmitted or stored.

Merkle Tree Ladder mode of operation for DNSSEC in “batch” mode could also reduce the number of signing operations for SPHINCS+ to the point where a parameter set for 2^20 signatures would likely be viable as this would support ladder updates on one-second intervals for DNS zones that do a zone signing key rollover every 10 days.

[1] Fregly, A,., Harvey, J., Kaliski, B., and Sheth, S.: Merkle Tree Ladder Mode: Reducing the Size Impact of NIST PQC Signature Algorithms in Practice. In: Cryptology ePrint Archive, Paper 2022/1730, https://eprint.iacr.org/2022/1730

Regards,

Andrew Fregly

On Wednesday, November 30, 2022 at 7:28:14 AM UTC-5 dustin...@nist.gov wrote:

> All,
>
> The design of SPHINCS+ imposes a limit on the number of allowable signatures from a given public key. For any number of signatures using the public key, g, there is some very low probability that they will reveal enough of the private key to allow an attacker to forge a signature. As g grows, so does the probability of this disaster. The total number of signatures must be kept low enough that this probability remains negligible. NIST's Call for Proposals required the ability to securely perform 2^64 signatures, which imposes requirements on the parameters of SPHINCS+. A smaller maximum number of signatures would result in somewhat smaller and faster signatures.
>
> NIST asks for public feedback on whether such a version of SPHINCS+ would be beneficial.
>
> NIST PQC team

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: Request for feedback on possible SPHINCS+ variant
Date: Saturday, January 07, 2023 11:11:17 AM ET
Attachments: smime.p7m

Andrew Fregly writes:

> Merkle Tree Ladder mode of operation for DNSSEC in “batch” mode could also reduce the number of signing operations for SPHINCS+ to the point where a parameter set for 2^20 signatures would likely be viable as this would support ladder updates on one-second intervals for DNS zones that do a zone signing key rollover every 10 days.

To help people evaluate the potential real-world impact of this MTL example, can you please comment on whether MTL is patent-free?

——D. J. Bernstein (speaking for myself)

P.S. I asked "Is MTL patent-free?" at the Fourth PQC Standardization Conference. The answer at that time was "We’re just presenting the research today and will answer other questions if and as we promote MTL mode as a candidate for standardization."

From: dustin...@nist.gov <dustin.moody@nist.gov> via pqc-forum <pqc-forum@list.nist.gov>
To: pqc-forum <pqc-forum@list.nist.gov>
CC: Andreas Hülsing <ietf@huelsing.net>, contact@sphincs.org
Subject: Re: [pqc-forum] Request for feedback on possible SPHINCS+ variant
Date: Tuesday, January 10, 2023 03:29:54 PM ET

Hello and happy new year everybody!
The SPHINCS+ team requested feedback on SPHINCS+C (as described in Andreas' post):

"Regarding SPHINCS+C we have the following questions:
* What applications would benefit?
* How important is signature vs verification speed?
* How relevant is constant signing time (not be confused with constant time implementation)
* Does the reduced size / better speed make a fundamental difference?"

It doesn't seem to have gotten a lot of responses yet. NIST would like to encourage responses so we know if there is/isn't community support for considering SPHINCS+C. Thank you,

Dustin Moody

NIST

On Monday, December 19, 2022 at 2:48:33 AM UTC-5 Andreas Hülsing wrote:

> Dear pqc-list,
>
> As mentioned in my talk at the 4th NIST conference, the SPHINCS+ team is interested in feedback regarding a smaller number of max signatures (as already mentioned in Dustin's mail) and regarding the SPHINCS+C proposal.
> We already saw the feedback so far on the list regarding max signatures and appreciate it!
>
> The SPHINCS+C proposal can be found at https://eprint.iacr.org/2022/778
>
> For the reduced max signatures parameters, a short note is available at https://eprint.iacr.org/2022/1725.
>
> What is especially important for us to learn is if there are applications that cannot use SPHINCS+ in its current form but would get enabled by one or the other proposal.
> However, we are of course also interested in hearing more about applications where the

> reduced costs are not critical but still helpful.
>
> Moreover, regarding the max signatures proposal, we have the following questions:
> * Is there an interest in this for parameters at a security level > I? (Right now we mainly looked at level I security)
> * What applications would benefit?
> * What would be the number of expected signatures?
> * Does the reduced size / better speed make a fundamental difference?
> * How important is signature vs verification speed?
>
> Regarding SPHINCS+C we have the following questions:
> * What applications would benefit?
> * How important is signature vs verification speed?
> * How relevant is constant signing time (not be confused with constant time implementation)
> * Does the reduced size / better speed make a fundamental difference?
>
> Best wishes,
>
> Andreas & the SPHINCS+ team
>
> On 30-11-2022 13:28, 'Moody, Dustin (Fed)' via pqc-forum wrote:
>
>> All,
>>
>> The design of SPHINCS+ imposes a limit on the number of allowable signatures from a given public key. For any number of signatures using the public key, g, there is some very low probability that they will reveal enough of the private key to allow an attacker to forge a signature. As g grows, so does the probability of this disaster. The total number of signatures must be kept low enough that this probability remains negligible. NIST’s Call for Proposals required the ability to securely perform 2^64 signatures, which imposes requirements on the parameters of SPHINCS+. A smaller maximum number of signatures would result in somewhat smaller and faster signatures.
>>
>> NIST asks for public feedback on whether such a version of SPHINCS+ would be beneficial.

> 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/SA1PR09MB8669CC55FD9EF5432F6B9C51E5159%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/55f1ac0a-305e-446e-bf5e-15cd562fddb3n%40list.nist.gov.

From: Scott Fluhrer (sfluhrer) <sfluhrer@cisco.com> via pqc-forum <pqc-forum@list.nist.gov>
To: dustin...@nist.gov <dustin.moody@nist.gov>, pqc-forum <pqc-forum@list.nist.gov>
CC: Andreas Hülsing <ietf@huelsing.net>, contact@sphincs.org
Subject: RE: [pqc-forum] Request for feedback on possible SPHINCS+ variant
Date: Tuesday, January 10, 2023 04:44:18 PM ET

If we were to be so bold as to add something to the questionnaire, I'd ask a fifth question:

- How critical is signing time?

One way to decrease the size of a signature is to select a parameter set that takes longer to sign. Now, in the range that the 'S' Sphincs+ parameters live, you need to increase signing time a lot to shrink the signatures a little; for example, if you were willing to spend 10x as much time to generate a signature, you might be able to shrink the signature 10%. Is this a viable trade-off?

> **From:** dustin...@nist.gov <dustin.moody@nist.gov>
> **Sent:** Tuesday, January 10, 2023 3:30 PM
> **To:** pqc-forum <pqc-forum@list.nist.gov>
> **Cc:** Andreas Hülsing <ietf@huelsing.net>; contact@sphincs.org
> **Subject:** Re: [pqc-forum] Request for feedback on possible SPHINCS+ variant
>
> Hello and happy new year everybody!
>
> The SPHINCS+ team requested feedback on SPHINCS+C (as described in Andreas' post):
>
> "Regarding SPHINCS+C we have the following questions:
> * What applications would benefit?
> * How important is signature vs verification speed?
> * How relevant is constant signing time (not be confused with constant time implementation)
> * Does the reduced size / better speed make a fundamental difference?"
>
> It doesn't seem to have gotten a lot of responses yet. NIST would like to encourage responses so we know if there is/isn't community support for considering SPHINCS+C. Thank you,
>
> Dustin Moody
>
> NIST

> On Monday, December 19, 2022 at 2:48:33 AM UTC-5 Andreas Hülsing wrote:
>
> > Dear pqc-list,
> >
> > As mentioned in my talk at the 4th NIST conference, the SPHINCS+ team is interested in feedback regarding a smaller number of max signatures (as already mentioned in Dustin's mail) and regarding the SPHINCS+C proposal.
> > We already saw the feedback so far on the list regarding max signatures and appreciate it!
> >
> > The SPHINCS+C proposal can be found at https://eprint.iacr.org/2022/778
> >
> > For the reduced max signatures parameters, a short note is available at https://eprint.iacr.org/2022/1725.
> >
> > What is especially important for us to learn is if there are applications that cannot use SPHINCS+ in its current form but would get enabled by one or the other proposal. However, we are of course also interested in hearing more about applications where the reduced costs are not critical but still helpful.
> >
> > Moreover, regarding the max signatures proposal, we have the following questions:
> > * Is there an interest in this for parameters at a security level > I? (Right now we mainly looked at level I security)
> > * What applications would benefit?
> > * What would be the number of expected signatures?
> > * Does the reduced size / better speed make a fundamental difference?
> > * How important is signature vs verification speed?
> >
> > Regarding SPHINCS+C we have the following questions:
> > * What applications would benefit?
> > * How important is signature vs verification speed?
> > * How relevant is constant signing time (not be confused with constant time implementation)
> > * Does the reduced size / better speed make a fundamental difference?
> >
> > Best wishes,

> Andreas & the SPHINCS+ team
>
> On 30-11-2022 13:28, 'Moody, Dustin (Fed)' via pqc-forum wrote:
>
> > All,
> >
> > The design of SPHINCS+ imposes a limit on the number of allowable signatures from a given public key. For any number of signatures using the public key, g, there is some very low probability that they will reveal enough of the private key to allow an attacker to forge a signature. As g grows, so does the probability of this disaster. The total number of signatures must be kept low enough that this probability remains negligible. NIST’s Call for Proposals required the ability to securely perform 2^64 signatures, which imposes requirements on the parameters of SPHINCS+. A smaller maximum number of signatures would result in somewhat smaller and faster signatures.
> >
> > NIST asks for public feedback on whether such a version of SPHINCS+ would be beneficial.
> >
> > 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/SA1PR09MB8669CC55FD9EF5432F6B9C51E5159%40SA1PR09MB8669.namprd09.prod.outlook.com.

From: Burt Kaliski <bkaliski%verisign.com@gtempaccount.com> via pqc-forum <pqc-forum@list.nist.gov>
To: pqc-forum <pqc-forum@list.nist.gov>
CC: pqc-...@list.nist.gov <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] Re: Request for feedback on possible SPHINCS+ variant
Date: Friday, January 13, 2023 02:02:05 PM ET

Thanks for adding my answer from the conference for reference.

Indeed, we intend to answer such questions if and as we promote MTL mode as a candidate for standardization, for instance in conjunction with submitting an Internet-Draft to IETF.

-- Burt

On Saturday, January 7, 2023 at 11:11:14 AM UTC-5 D. J. Bernstein wrote:

Andrew Fregly writes:
> Merkle Tree Ladder mode of operation for DNSSEC in “batch” mode could also
> reduce the number of signing operations for SPHINCS+ to the point where a
> parameter set for 2^20 signatures would likely be viable as this would
> support ladder updates on one-second intervals for DNS zones that do a zone
> signing key rollover every 10 days.

To help people evaluate the potential real-world impact of this MTL
example, can you please comment on whether MTL is patent-free?

---D. J. Bernstein (speaking for myself)

P.S. I asked "Is MTL patent-free?" at the Fourth PQC Standardization
Conference. The answer at that time was "We’re just presenting the
research today and will answer other questions if and as we promote MTL
mode as a candidate for standardization."

--
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/33ed4d55-ebf1-4f00-aa6c-ed21750004bfn%40list.nist.gov.