From: Andreas Hülsing <ietf@huelsing.net> via pqc-forum@list.nist.gov
To: pqc-comments@nist.gov
CC: pqc-forum@list.nist.gov
Subject: [pqc-forum] ROUND 3 OFFICIAL COMMENT: SPHINCS+
Date: Friday, June 10, 2022 03:55:11 AM ET
Attachments: sphincs_-r3.1-specification.pdf
r3.1_modifications.pdf

Dear all,

In response to the recently posted issue with the SHA2 instantiation of SPHINCS+, we decided to change the function we use in the concerned implementations from SHA2-256 to SHA2-512. The problem was caused by the small internal state of SHA2. With this change, this problem is solved.

We updated our specification, also including other changes that we announced on this list since the 3rd round submission. In the attachment you also find a list of all the modifications we made. The code in our public github repository (https://github.com/sphincs/sphincsplus) is also updated.

Best wishes,

Andreas

From: Doge Protocol <dogeprotocol1@gmail.com> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
CC: Andreas Hülsing <ietf@huelsing.net>, pqc-...@list.nist.gov <pqc-forum@list.nist.gov>, pqc-co...@nist.gov <pqc-comments@nist.gov>
Subject: [pqc-forum] Re: ROUND 3 OFFICIAL COMMENT: SPHINCS+
Date: Friday, June 10, 2022 01:08:41 PM ET

From table in the paper, SHA2-256 corresponds to security level 1 (n = 16) and SHA2-512 corresponds to security levels 3,5 (n=24 , n= 32). Does this mean only security levels 3,5 should be considered for SPHINCS+ and level 1 is not applicable since it has below problem? Is understanding correct?

https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/FVItvyRea28/m/-oKR3ZKpDAAJ

On Friday, June 10, 2022 at 12:54:41 AM UTC-7 Andreas Hülsing wrote:

> Dear all,
>
> In response to the recently posted issue with the SHA2 instantiation of SPHINCS+, we decided to change the function we use in the concerned implementations from SHA2-256 to SHA2-512. The problem was caused by the small internal state of SHA2. With this change, this problem is solved.
>
> We updated our specification, also including other changes that we announced on this list since the 3rd round submission. In the attachment you also find a list of all the modifications we made. The code in our public github repository (https://github.com/sphincs/sphincsplus) is also updated.
>
> Best wishes,
>
> Andreas

--

From: Bas Westerbaan <bas@cloudflare.com> via pqc-forum <pqc-forum@list.nist.gov>
To: Doge Protocol <dogeprotocol1@gmail.com>
CC: Andreas Hülsing <ietf@huelsing.net>, pqc-...@list.nist.gov <pqc-forum@list.nist.gov>, pqc-co...@nist.gov <pqc-comments@nist.gov>
Subject: Re: [pqc-forum] Re: ROUND 3 OFFICIAL COMMENT: SPHINCS+
Date: Friday, June 10, 2022 01:15:03 PM ET

On Fri, Jun 10, 2022 at 7:08 PM Doge Protocol <dogeprotocol1@gmail.com> wrote:

> Does this mean only security levels 3,5 should be considered for SPHINCS+ and level 1 is not applicable since it has below problem? Is understanding correct?

No. Antonov's attack only applied to levels 3 and 5. Read the end of step 1.1.1.

Best,

Bas

--

From: Andreas Hülsing <ietf@huelsing.net> via pqc-forum@list.nist.gov
To: Doge Protocol <dogeprotocol1@gmail.com>, pqc-forum <pqc-forum@list.nist.gov>
CC: pqc-co...@nist.gov <pqc-comments@nist.gov>
Subject: [pqc-forum] Re: ROUND 3 OFFICIAL COMMENT: SPHINCS+
Date: Friday, June 10, 2022 05:11:02 PM ET

The document only contains parameters that we consider to achieve the claimed security level. So, all the proposed parameter sets can be used. The security of SHA2-256 is sufficient for the instantiations of all functions at security level 1 (and therefore the level 1 parameters using SHA2 can be used safely). Only at security levels 3 and 5, SHA2-256 is not sufficient for the instantiation of tweakable hash functions that take input messages of a length that is more than one message block length. Therefore, we switched the instantiation of the H and T functions to SHA2-512 at security levels 3 and 5.

Best wishes,

Andreas

On 10-06-2022 19:08, Doge Protocol wrote:

> From table in the paper, SHA2-256 corresponds to security level 1 (n = 16) and SHA2-512 corresponds to security levels 3,5 (n=24 , n= 32). Does this mean only security levels 3,5 should be considered for SPHINCS+ and level 1 is not applicable since it has below problem? Is understanding correct?
>
> https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/FVItvyRea28/m/-oKR3ZKpDAAJ
>
> On Friday, June 10, 2022 at 12:54:41 AM UTC-7 Andreas Hülsing wrote:
>
> > Dear all,
> >
> > In response to the recently posted issue with the SHA2 instantiation of SPHINCS+, we decided to change the function we use in the concerned implementations from SHA2-256 to SHA2-512. The problem was caused by the small internal state of SHA2. With this change, this problem is solved.

> We updated our specification, also including other changes that we announced on this list since the 3rd round submission. In the attachment you also find a list of all the modifications we made. The code in our public github repository (https://github.com/sphincs/sphincsplus) is also updated.
>
> Best wishes,
>
> Andreas

From: Sydney Antonov <ska84@protonmail.com>
To: Andreas Hülsing <ietf@huelsing.net>
CC: pqc-comments@nist.gov, pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] ROUND 3 OFFICIAL COMMENT: SPHINCS+
Date: Monday, June 13, 2022 09:35:10 AM ET

> In response to the recently posted issue with the SHA2 instantiation of
> SPHINCS+, we decided to change the function we use in the concerned
> implementations from SHA2-256 to SHA2-512. The problem was caused by the
> small internal state of SHA2. With this change, this problem is solved.

While this prevents my attack when collisions must be found using
generic attacks, it would still be able to gain some advantage
if better chosen-prefix collisions attacks on SHA-2 were found
like with MD5 and SHA-1. I find this concerning because SPHINCS+
is designed to be collision-resilient and this means it isn't
tightly chosen-prefix-collision-resilient.

Sydney

From: Bas Westerbaan <bas@cloudflare.com> via pqc-forum <pqc-forum@list.nist.gov>
To: Doge Protocol <dogeprotocol1@gmail.com>
CC: pqc-forum <pqc-forum@list.nist.gov>, Andreas Hülsing <ietf@huelsing.net>, pqc-co...@nist.gov <pqc-comments@nist.gov>
Subject: Re: [pqc-forum] Re: ROUND 3 OFFICIAL COMMENT: SPHINCS+
Date: Monday, June 13, 2022 12:46:56 PM ET

It depends on the platform and parameter set; on some it's faster and on some it's slower. Here you can see the differences for a Ryzen 5 1600: https://github.com/sphincs/sphincsplus/pull/31#issuecomment-1146220423:~:text=commented-,10%20days%20ago,-sphincs%2Dsha256%2D256s

On Mon, Jun 13, 2022 at 6:41 PM Doge Protocol <dogeprotocol1@gmail.com> wrote:

> Is there any impact/trade-off, such as in performance, on account of this change to SHA2-512?
>
> On Friday, June 10, 2022 at 2:11:06 PM UTC-7 Andreas Hülsing wrote:
>
> > The document only contains parameters that we consider to achieve the claimed security level. So, all the proposed parameter sets can be used. The security of SHA2-256 is sufficient for the instantiations of all functions at security level 1 (and therefore the level 1 parameters using SHA2 can be used safely). Only at security levels 3 and 5, SHA2-256 is not sufficient for the instantiation of tweakable hash functions that take input messages of a length that is more than one message block length. Therefore, we switched the instantiation of the H and T functions to SHA2-512 at security levels 3 and 5.
> >
> > Best wishes,
> >
> > Andreas
> >
> > On 10-06-2022 19:08, Doge Protocol wrote:
> >
> > > From table in the paper, SHA2-256 corresponds to security level 1 (n = 16) and SHA2-512 corresponds to security levels 3,5 (n=24 , n= 32). Does this mean only security levels 3,5 should be considered for SPHINCS+ and level 1 is not applicable since it has below problem? Is understanding correct? https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/FVItvyRea28/m/-oKR3ZKpDAAJ

On Friday, June 10, 2022 at 12:54:41 AM UTC-7 Andreas Hülsing wrote:

> Dear all,
>
> In response to the recently posted issue with the SHA2 instantiation of SPHINCS+, we decided to change the function we use in the concerned implementations from SHA2-256 to SHA2-512. The problem was caused by the
> small internal state of SHA2. With this change, this problem is solved.
>
> We updated our specification, also including other changes that we announced on this list since the 3rd round submission. In the attachment you also find a list of all the modifications we made. The code in our public github repository (https://github.com/sphincs/sphincsplus) is also updated.
>
> Best wishes,
>
> Andreas

--
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/CAMjbhoWxDBPEUks53UyCqiXopWL7crFRji%2Bdsx2-JRzwwh-y9Q%40mail.gmail.com.