From: Vadim Lyubashevsky <vadim1980@gmail.com> via pqc-forum@list.nist.gov
To: Taylor R Campbell <campbell+pqc-forum@mumble.net>
CC: pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] OFFICIAL COMMENT: CRYSTALS-Dilithium
Date: Friday, July 08, 2022 09:12:08 AM ET

Hi Taylor, all,

On Fri, 2022-07-08 at 13:03 +0000, Taylor R Campbell wrote:

> > Date: Fri, 08 Jul 2022 11:47:30 +0200
> >
> > From: Vadim Lyubashevsky <vadim1980@gmail.com>
> >
> > On Thu, 2022-07-07 at 11:50 +0000, 'John Mattsson' via pqc-forum wrote:
> >
> > > The current specification of CRYSTALS-Dilithium provides two versions. One deterministic and one randomized. I strongly think NIST should also standardize a hedged version where the seed is derived from a random string, a key, and the message.
> >
> > The "hedged" version can simply replace the current randomized version which does not take the key and the message as inputs. Since the key is short and the message is already hashed anyway, including these two things in the seed creation will probably have a negligible performance effect.
> >
> > If people think it's a good idea, it should be easy to incorporate and I suspect that it's better having just 2 versions of the algorithm instead of 3.
>
> Don't have two or three versions -- have just one!
>
> Signature creation should be defined to be a deterministic function of

> 1. secret key,
>
> 2. message, and
>
> 3. a randomization string.
>
> - Users can make deterministic signatures by setting the randomization
>
> string to something fixed in an application like the empty string.

This is exactly what the two versions of the algorithm would look like using the "deterministic" and "hedged" modes. If you think that this counts as just one version, then great!

Best,

Vadim

From: Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu> via pqc-forum@list.nist.gov
To: Vadim Lyubashevsky <vadim1980@gmail.com>
CC: Taylor R Campbell <campbell+pqc-forum@mumble.net>, pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] OFFICIAL COMMENT: CRYSTALS-Dilithium
Date: Friday, July 08, 2022 11:35:25 AM ET
Attachments: smime.p7m

I like this proposal.
Thanks!

Regards,
Uri

> On Jul 8, 2022, at 09:13, Vadim Lyubashevsky wrote:
>
> Hi Taylor, all,
>
> On Fri, 2022-07-08 at 13:03 +0000, Taylor R Campbell wrote:
>
> > > Date: Fri, 08 Jul 2022 11:47:30 +0200
> > >
> > > From: Vadim Lyubashevsky <vadim1980@gmail.com>
> > >
> > > On Thu, 2022-07-07 at 11:50 +0000, 'John Mattsson' via pqc-forum wrote:
> > >
> > > > The current specification of CRYSTALS-Dilithium provides two versions. One deterministic and one randomized. I strongly think NIST should also standardize a hedged version where the seed is derived from a random string, a key, and the message.
> > >
> > > The "hedged" version can simply replace the current randomized version which does not take the key and the message as inputs. Since the key is short and the message is already hashed anyway, including these two

> > things in the seed creation will probably have a negligible performance
> >
> > effect.
> >
> > If people think it's a good idea, it should be easy to incorporate and
> >
> > I suspect that it's better having just 2 versions of the algorithm
> >
> > instead of 3.
>
> Don't have two or three versions -- have just one!
>
> Signature creation should be defined to be a deterministic function of
>
> 1. secret key,
>
> 2. message, and
>
> 3. a randomization string.
>
> - Users can make deterministic signatures by setting the randomization
>
> string to something fixed in an application like the empty string.

This is exactly what the two versions of the algorithm would look like using the "deterministic" and "hedged" modes. If you think that this counts as just one version, then great!

Best,

Vadim

--
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/f637a042d20b89ee65c687364989fdb085581dfd.camel%40gmail.com.

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