From: Carlos Aguilar <carlos2831@gmail.com> via pqc-forum@list.nist.gov
To: yang.yu0986@gmail.com
CC: pqc-forum@list.nist.gov
Subject: RE: [pqc-forum] [New Paper] Shorter Hash-and-Sign Lattice-Based Signatures
Date: Monday, July 04, 2022 05:28:59 AM ET

Thank you, these results are great! I have not found what can be expected on the number of signatures/verifications per second.
Have you a constant time implementation that can provide such results? Or an educated guess?

Thanks,

Carlos

> De : YANG YU <yang.yu0986@gmail.com>
>
> Date : 04/07/2022 03:31 (GMT+01:00)
>
> À : pqc-forum <pqc-forum@list.nist.gov>
>
> Objet : [pqc-forum] [New Paper] Shorter Hash-and-Sign Lattice-Based Signatures
>
> Dear all,
>
> We would like to share with you our recent paper ``Shorter Hash-and-Sign Lattice-Based Signatures" available at https://eprint.iacr.org/2022/785, which will be presented at CRYPTO 2022.
>
> In this work, we propose techniques to reduce the size of hash-and-sign lattice-based signatures. When applied to Falcon-512, one approach yields 410-byte signatures with the same verification key size. The other approach yields 425-byte signatures and 576-byte verification keys, further improving upon the |sig|+|vk| record of Falcon-512. The bit security in both cases is almost unchanged compared to the original scheme.
>
> More concretely, there are three strategies explored and analyzed in the paper for reducing the size of hash-and-sign lattice-based signatures:
> 1. Improved efficient coding of Gaussian vectors.
> 2. Ellipsoidal Gaussian sampling.

> 3. The use of a smaller modulus q.
>
> The first one reduces the signature size without any security loss and can directly apply to any scheme where a Gaussian vector is output on a public channel. It can be generalized to any non-uniform distribution with minimal overhead and can be implemented efficiently with off-the-shelf libraries.
>
> The other two strategies are tailored for hash-and-sign signatures over NTRU lattices, and one will typically want to apply one or the other in combination with the first one. They present trade-offs between signature size and bit security. To this end, we conduct extensive cryptanalytic work to see how far we can go.
>
> Finally, two takeaways are that:
> 1. We can achieve hash-and-sign lattice-based signatures at the NIST-I security level that are 4.9 times smaller than Dilitihum2 signatures.
> 2. This results in lattice-based signature size intermediate between those of RSA-2048 and RSA-4096, with much faster signing and comparable verification performance.
>
> Any questions, comments and suggestions welcome!
>
> Best regards,
>
> --
> Thomas Espitau, Mehdi Tibouchi, Alexandre Wallet, Yang Yu
> --
>

--

To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/CALJ7cgk-zVqVK_FYUHf8-pdqdTFmMHZMiCVKe2FF0snJGCZ8ag%40mail.gmail.com.

From: Mehdi Tibouchi <mehdi.tibouchi@normalesup.org> via pqc-forum@list.nist.gov
To: Carlos Aguilar <carlos2831@gmail.com>
CC: pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] [New Paper] Shorter Hash-and-Sign Lattice-Based Signatures
Date: Tuesday, July 05, 2022 02:43:38 AM ET

Dear Carlos,

Thanks for the kind words.

We do not have an implementation, but the proposed techniques should have little impact on performance: encoding/decoding is negligible, and the FFT multiplications are not affected by the modified sizes of certain variables, so if you apply the techniques to e.g. Falcon-512, you should get basically the same speed as the original scheme.

More precisely, referring to stategies 1–3 in the previous email, doing 1+2 should have basically no effect on either signing or verification, whereas doing 1+3 has basically no effect on signing, but would have a moderate effect on verification efficiency, since using a smaller q requires replacing the full NTT used in Falcon verification by some other multiplication algorithm (partial NTT, FFT or Karatsuba/Toom-Cook may all be suitable depending on the shape of q and the target platform). The difference should be fairly small still.

Best regards,

--
Thomas Espitau, Mehdi Tibouchi, Alexandre Wallet, Yang Yu.

On Mon, Jul 04, 2022 at 11:28:32AM +0200, Carlos Aguilar wrote:
> Thank you, these results are great! I have not found what can be expected
> on the number of signatures/verifications per second.
>
> Have you a constant time implementation that can provide such results? Or

> an educated guess?
>
> Thanks,
>
> Carlos
>
>
>
> >
> > De : YANG YU <yang.yu0986@gmail.com>
> > Date : 04/07/2022 03:31 (GMT+01:00)
> > À : pqc-forum <pqc-forum@list.nist.gov>
> > Objet : [pqc-forum] [New Paper] Shorter Hash-and-Sign Lattice-Based
> > Signatures
> >
> > Dear all,
> >
> > We would like to share with you our recent paper ``Shorter Hash-and-Sign
> > Lattice-Based Signatures'' available at https://
gcc02.safelinks.protection.outlook.com/?
url=https%3A%2F%2Feprint.iacr.org%2F2022%2F785&data=05%7C01%7Cyi-
kai.liu%40nist.gov%7C2483ca16a19b43d9d06808da5e51ae5d%7C2ab5d82fd8fa4797a93e054655c61
dec%7C1%7C0%7C637926002178691820%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoi
V2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=dL3nTv%2BlsSvDpjVzXi
abWMEvlZEC%2FT6psqIg8tOFiX8%3D&reserved=0,
> > which will be presented at CRYPTO 2022.
> >
> > In this work, we propose techniques to reduce the size of hash-and-sign
> > lattice-based signatures. When applied to Falcon-512, one approach yields
> > 410-byte signatures with the same verification key size. The other approach
> > yields 425-byte signatures and 576-byte verification keys, further
> > improving upon the |sig|+|vk| record of Falcon-512. The bit security in
> > both cases is almost unchanged compared to the original scheme.
> >
> > More concretely, there are three strategies explored and analyzed in the
> > paper for reducing the size of hash-and-sign lattice-based signatures:
> > 1. Improved efficient coding of Gaussian vectors.

> > 2. Ellipsoidal Gaussian sampling.
> > 3. The use of a smaller modulus q.
> >
> > The first one reduces the signature size without any security loss and can
> > directly apply to any scheme where a Gaussian vector is output on a public
> > channel. It can be generalized to any non-uniform distribution with minimal
> > overhead and can be implemented efficiently with off-the-shelf libraries.
> >
> > The other two strategies are tailored for hash-and-sign signatures over
> > NTRU lattices, and one will typically want to apply one or the other in
> > combination with the first one. They present trade-offs between signature
> > size and bit security. To this end, we conduct extensive cryptanalytic work
> > to see how far we can go.
> >
> > Finally, two takeaways are that:
> > 1. We can achieve hash-and-sign lattice-based signatures at the NIST-I
> > security level that are 4.9 times smaller than Dilitihum2 signatures.
> > 2. This results in lattice-based signature size intermediate between those
> > of RSA-2048 and RSA-4096, with much faster signing and comparable
> > verification performance.
> >
> > Any questions, comments and suggestions welcome!
> >
> > Best regards,
> >
> > --
> > Thomas Espitau, Mehdi Tibouchi, Alexandre Wallet, Yang Yu
> >
> > --
> > 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/25c8ce20-bae1-4838-aa52-00abbabbcc10n%40list.nist.gov

> > <https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/25c8ce20-bae1-4838-aa52-00abbabbcc10n%40list.nist.gov?utm_medium=email&utm_source=footer>
> > .
> >
> >
>
> --
> 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/CALJ7cgk-zVqVK_FYUHf8-pdqdTFmMHZMiCVKe2FF0snJGCZ8ag%40mail.gmail.com.

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

From: Carlos Aguilar <carlos2831@gmail.com> via pqc-forum@list.nist.gov
To: Mehdi Tibouchi <mehdi.tibouchi@normalesup.org>
CC: pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] [New Paper] Shorter Hash-and-Sign Lattice-Based Signatures
Date: Tuesday, July 05, 2022 05:44:33 AM ET

That's quite nice!

Thank you for your reply

Best,

Carlos

Le mar. 5 juil. 2022 à 08:43, Mehdi Tibouchi <mehdi.tibouchi@normalesup.org> a écrit :

> Dear Carlos,
>
> Thanks for the kind words.
>
> We do not have an implementation, but the proposed techniques should have
> little impact on performance: encoding/decoding is negligible, and the
> FFT multiplications are not affected by the modified sizes of certain
> variables, so if you apply the techniques to e.g. Falcon-512, you should
> get basically the same speed as the original scheme.
>
> More precisely, referring to stategies 1–3 in the previous email, doing
> 1+2 should have basically no effect on either signing or verification,
> whereas doing 1+3 has basically no effect on signing, but would have a
> moderate effect on verification efficiency, since using a smaller q
> requires replacing the full NTT used in Falcon verification by some other
> multiplication algorithm (partial NTT, FFT or Karatsuba/Toom-Cook may all
> be suitable depending on the shape of q and the target platform). The
> difference should be fairly small still.
>
> Best regards,
>
> --
> Thomas Espitau, Mehdi Tibouchi, Alexandre Wallet, Yang Yu.

On Mon, Jul 04, 2022 at 11:28:32AM +0200, Carlos Aguilar wrote:
> Thank you, these results are great! I have not found what can be expected
> on the number of signatures/verifications per second.
>
> Have you a constant time implementation that can provide such results? Or
> an educated guess?
>
> Thanks,
>
> Carlos
>
>
>
> > De : YANG YU <yang.yu0986@gmail.com>
> > Date : 04/07/2022 03:31 (GMT+01:00)
> > À : pqc-forum <pqc-forum@list.nist.gov>
> > Objet : [pqc-forum] [New Paper] Shorter Hash-and-Sign Lattice-Based
> > Signatures
> >
> > Dear all,
> >
> > We would like to share with you our recent paper ``Shorter Hash-and-Sign
> > Lattice-Based Signatures" available at https://eprint.iacr.org/2022/785,
> > which will be presented at CRYPTO 2022.
> >
> > In this work, we propose techniques to reduce the size of hash-and-sign
> > lattice-based signatures. When applied to Falcon-512, one approach yields
> > 410-byte signatures with the same verification key size. The other approach
> > yields 425-byte signatures and 576-byte verification keys, further
> > improving upon the |sig|+|vk| record of Falcon-512. The bit security in
> > both cases is almost unchanged compared to the original scheme.
> >
> > More concretely, there are three strategies explored and analyzed in the

> > paper for reducing the size of hash-and-sign lattice-based signatures:
> > 1. Improved efficient coding of Gaussian vectors.
> > 2. Ellipsoidal Gaussian sampling.
> > 3. The use of a smaller modulus q.
> >
> > The first one reduces the signature size without any security loss and can
> > directly apply to any scheme where a Gaussian vector is output on a public
> > channel. It can be generalized to any non-uniform distribution with minimal
> > overhead and can be implemented efficiently with off-the-shelf libraries.
> >
> > The other two strategies are tailored for hash-and-sign signatures over
> > NTRU lattices, and one will typically want to apply one or the other in
> > combination with the first one. They present trade-offs between signature
> > size and bit security. To this end, we conduct extensive cryptanalytic work
> > to see how far we can go.
> >
> > Finally, two takeaways are that:
> > 1. We can achieve hash-and-sign lattice-based signatures at the NIST-I
> > security level that are 4.9 times smaller than Dilitihum2 signatures.
> > 2. This results in lattice-based signature size intermediate between those
> > of RSA-2048 and RSA-4096, with much faster signing and comparable
> > verification performance.
> >
> > Any questions, comments and suggestions welcome!
> >
> > Best regards,
> >
> > --
> > Thomas Espitau, Mehdi Tibouchi, Alexandre Wallet, Yang Yu
> >
> > --
> > 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/25c8ce20-bae1-4838-

> aa52-00abbabbcc10n%40list.nist.gov
> > > <https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/25c8ce20-bae1-4838-aa52-00abbabbcc10n%40list.nist.gov?utm_medium=email&utm_source=footer>
> > .
> >
> >
>
> --
> 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/CALJ7cgk-zVqVK_FYUHf8-pdqdTFmMHZMiCVKe2FF0snJGCZ8ag%40mail.gmail.com.

--
You received this message because you are subscribed to the Google Groups "pqc-forum" group.
To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.
To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/CALJ7cgm_e54m2SpKTAP7syHa1He_cG%3D2EOH%3DWtFbdZJy6emLmg%40mail.gmail.com.

From: Doge Protocol <dogeprotocol1@gmail.com> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
CC: mehdi.t...@normalesup.org <mehdi.tibouchi@normalesup.org>, pqc-...@list.nist.gov <pqc-forum@list.nist.gov>, carlo...@gmail.com <carlos2831@gmail.com>
Subject: Re: [pqc-forum] [New Paper] Shorter Hash-and-Sign Lattice-Based Signatures
Date: Tuesday, July 05, 2022 12:30:36 PM ET

Is an implementation in the works? If so, any timeline for an implementation, so that performance can be quantitatively measured?

On Monday, July 4, 2022 at 11:43:27 PM UTC-7 mehdi.t...@normalesup.org wrote:

> Dear Carlos,
>
> Thanks for the kind words.
>
> We do not have an implementation, but the proposed techniques should have little impact on performance: encoding/decoding is negligible, and the FFT multiplications are not affected by the modified sizes of certain variables, so if you apply the techniques to e.g. Falcon-512, you should get basically the same speed as the original scheme.
>
> More precisely, referring to stategies 1–3 in the previous email, doing 1+2 should have basically no effect on either signing or verification, whereas doing 1+3 has basically no effect on signing, but would have a moderate effect on verification efficiency, since using a smaller q requires replacing the full NTT used in Falcon verification by some other multiplication algorithm (partial NTT, FFT or Karatsuba/Toom-Cook may all be suitable depending on the shape of q and the target platform). The difference should be fairly small still.
>
> Best regards,
>
> --
> Thomas Espitau, Mehdi Tibouchi, Alexandre Wallet, Yang Yu.

On Mon, Jul 04, 2022 at 11:28:32AM +0200, Carlos Aguilar wrote:
> Thank you, these results are great! I have not found what can be expected
> on the number of signatures/verifications per second.
>
> Have you a constant time implementation that can provide such results? Or
> an educated guess?
>
> Thanks,
>
> Carlos
>
>
>
> > De : YANG YU <yang....@gmail.com>
> > Date : 04/07/2022 03:31 (GMT+01:00)
> > À : pqc-forum <pqc-...@list.nist.gov>
> > Objet : [pqc-forum] [New Paper] Shorter Hash-and-Sign Lattice-Based
> > Signatures
> >
> > Dear all,
> >
> > We would like to share with you our recent paper ``Shorter Hash-and-Sign
> > Lattice-Based Signatures" available at https://eprint.iacr.org/2022/785,
> > which will be presented at CRYPTO 2022.
> >
> > In this work, we propose techniques to reduce the size of hash-and-sign
> > lattice-based signatures. When applied to Falcon-512, one approach yields
> > 410-byte signatures with the same verification key size. The other approach
> > yields 425-byte signatures and 576-byte verification keys, further
> > improving upon the |sig|+|vk| record of Falcon-512. The bit security in
> > both cases is almost unchanged compared to the original scheme.
> >
> > More concretely, there are three strategies explored and analyzed in the
> > paper for reducing the size of hash-and-sign lattice-based signatures:
> > 1. Improved efficient coding of Gaussian vectors.
> > 2. Ellipsoidal Gaussian sampling.

> > 3. The use of a smaller modulus q.
> >
> > The first one reduces the signature size without any security loss and can
> > directly apply to any scheme where a Gaussian vector is output on a public
> > channel. It can be generalized to any non-uniform distribution with minimal
> > overhead and can be implemented efficiently with off-the-shelf libraries.
> >
> > The other two strategies are tailored for hash-and-sign signatures over
> > NTRU lattices, and one will typically want to apply one or the other in
> > combination with the first one. They present trade-offs between signature
> > size and bit security. To this end, we conduct extensive cryptanalytic work
> > to see how far we can go.
> >
> > Finally, two takeaways are that:
> > 1. We can achieve hash-and-sign lattice-based signatures at the NIST-I
> > security level that are 4.9 times smaller than Dilitihum2 signatures.
> > 2. This results in lattice-based signature size intermediate between those
> > of RSA-2048 and RSA-4096, with much faster signing and comparable
> > verification performance.
> >
> > Any questions, comments and suggestions welcome!
> >
> > Best regards,
> >
> > --
> > Thomas Espitau, Mehdi Tibouchi, Alexandre Wallet, Yang Yu
> >
> > --
> > 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/25c8ce20-bae1-4838-aa52-00abbabbcc10n%40list.nist.gov
> > <https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/25c8ce20-bae1-4838-aa52-00abbabbcc10n%40list.nist.gov?utm_medium=email&utm_source=footer>

> > .
> >
> >
>
> --
> 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/CALJ7cgk-zVqVK_FYUHf8-pdqdTFmMHZMiCVKe2FF0snJGCZ8ag%40mail.gmail.com.

--
You received this message because you are subscribed to the Google Groups "pqc-forum" group.
To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.
To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/0b9f349c-59fa-4639-b900-d73e0a286b6cn%40list.nist.gov.