From: Doge Protocol <dogeprotocol1@gmail.com> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: [pqc-forum] Key recovery attack on SIDH
Date: Saturday, July 30, 2022 06:59:48 PM ET

Came accross this today and would like to share with the community.
https://eprint.iacr.org/2022/975
Our Magma implementation breaks the instantiation SIKEp434, which aims at security level 1 of the Post-Quantum Cryptography standardization process currently ran by NIST, in about one hour on a single core.

Ran on a single core, the ap-

pended Magma code breaks the Microsoft SIKE challenges $IKEp182 and $IKEp217

in about 4 minutes and 6 minutes, respectively. A run on the SIKEp434 parame-

ters, previously believed to meet NIST's quantum security level 1, took about 62

minutes, again on a single core. We also ran the code on random instances of

SIKEp503 (level 2), SIKEp610 (level 3) and SIKEp751 (level 5), which took about

2h19m, 8h15m and 20h37m, respectively.

--

From: David Jao <djao@uwaterloo.ca> via pqc-forum@list.nist.gov
To: pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] Key recovery attack on SIDH
Date: Saturday, July 30, 2022 07:13:04 PM ET

I was waiting in order to give the authors of the paper an opportunity to announce their results to the forum, in case they should wish to do so, but since someone else has already written about it, it's fair game to chime in now.

The result is legitimate, and very impressive. Huge congratulations to Castryck and Decru.

At first sight, the attack in 2022/975 uses knowledge of the endomorphism ring of the starting curve. As mentioned on page 2 of 2022/975, a possible "tweak" to SIKE was described in Section 8 of 2021/543 which could potentially thwart this attack. The tweak consists of randomly generating a starting curve of unknown endomorphism ring as part of the public key generation process. However, attacks always get better, never worse. It is possible that after further analysis, 2022/975's apparent dependence on knowledge of the starting curve's endomorphism ring will turn out to be spurious. More analysis is needed before we would be able to make any sort of confident claim as to whether or not the tweak would thwart the new attack.

-David

On 2022-07-30 6:58 p.m., Doge Protocol wrote:

> Came accross this today and would like to share with the community.
> https://eprint.iacr.org/2022/975
> Our Magma implementation breaks the instantiation SIKEp434, which aims at security level 1 of the Post-Quantum Cryptography standardization process currently ran by NIST, in about one hour on a single core.
>
> Ran on a single core, the ap-
>
> pended Magma code breaks the Microsoft SIKE challenges $IKEp182 and $IKEp217
>
> in about 4 minutes and 6 minutes, respectively. A run on the SIKEp434 parame-
>
> ters, previously believed to meet NIST’s quantum security level 1, took about 62
>
> minutes, again on a single core. We also ran the code on random instances of

SIKEp503 (level 2), SIKEp610 (level 3) and SIKEp751 (level 5), which took about

2h19m, 8h15m and 20h37m, respectively.

--

From: Tanja Lange <tanja@hyperelliptic.org> via pqc-forum@list.nist.gov
To: pqc-forum@list.nist.gov
CC: Cottaar, Jolijn <j.cottaar1@student.tue.nl>
Subject: Re: [pqc-forum] Key recovery attack on SIDH
Date: Saturday, July 30, 2022 09:01:31 PM ET

[Beaking my silence on this list, hope I don't get a yellow card
from NIST again.]

Dear David,
Thanks for your email.

I have yet to read the paper but I should mention one idea for more
randomized starting curves that my student Jolijn Cottaar and I have
been discussing about (just to avoid the key-space reduction in SIKE).
Instead of moving away from E_0 by just a small isogeny to E_6 one
can use the big isogenies of the B-SIDH p-1 to move away far. This is
expensive but only done in generating the parameters.

This still means, though, that there is a known isogeny from E_0 and
thus the endomorphism ring of that E_A can still be computed. It
depends on the details of the attack whether having to push the small
endomorphisms though this and a twist makes the attack too expensive
(like how pairings always exist but don't always do damage) and, as
I said above, I haven't read the details, yet. I just feel that I
should put this out here and give credit to Jolijn.

All the best
        Tanja

On Sat, Jul 30, 2022 at 07:11:50PM -0400, David Jao wrote:
> I was waiting in order to give the authors of the paper an opportunity to
> announce their results to the forum, in case they should wish to do so, but
> since someone else has already written about it, it's fair game to chime in
> now.
>
> The result is legitimate, and very impressive. Huge congratulations to Castryck

> and Decru.
>
> At first sight, the attack in 2022/975 uses knowledge of the endomorphism ring
> of the starting curve. As mentioned on page 2 of 2022/975, a possible "tweak"
> to SIKE was described in Section 8 of 2021/543 which could potentially thwart
> this attack. The tweak consists of randomly generating a starting curve of
> unknown endomorphism ring as part of the public key generation process.
> However, attacks always get better, never worse. It is possible that after
> further analysis, 2022/975's apparent dependence on knowledge of the starting
> curve's endomorphism ring will turn out to be spurious. More analysis is needed
> before we would be able to make any sort of confident claim as to whether or
> not the tweak would thwart the new attack.
>
> -David
>
> On 2022-07-30 6:58 p.m., Doge Protocol wrote:
>
>   Came accross this today and would like to share with the community.
>
>   https://gcc02.safelinks.protection.outlook.com/?
url=https%3A%2F%2Feprint.iacr.org%2F2022%2F975&data=05%7C01%7Cyi-
kai.liu%40nist.gov%7C99465bd4face4bd9719108da729031b4%7C2ab5d82fd8fa4797a93e054655c61
dec%7C1%7C0%7C637948260913451336%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoi
V2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=kKx%2BB112%2BtZYVdxT
gQibOY3S638qz3P9LTpj5XzP23A%3D&reserved=0
>
>   Our Magma implementation breaks the instantiation SIKEp434, which aims at
>   security level 1 of the Post-Quantum Cryptography standardization process
>   currently ran by NIST, in about one hour on a single core.
>
>   Ran on a single core, the ap-
>   pended Magma code breaks the Microsoft SIKE challenges $IKEp182 and
> $IKEp217
>   in about 4 minutes and 6 minutes, respectively. A run on the SIKEp434
>   parame-
>   ters, previously believed to meet NIST’s quantum security level 1, took
>   about 62

> minutes, again on a single core. We also ran the code on random instances
> of
> SIKEp503 (level 2), SIKEp610 (level 3) and SIKEp751 (level 5), which took
> about
> 2h19m, 8h15m and 20h37m, respectively.
>
>
> --
> 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://
gcc02.safelinks.protection.outlook.com/?
url=https%3A%2F%2Fgroups.google.com%2Fa%2F&data=05%7C01%7Cyi-
kai.liu%40nist.gov%7C99465bd4face4bd9719108da729031b4%7C2ab5d82fd8fa4797a93e054655c61
dec%7C1%7C0%7C637948260913451336%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoi
V2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=cbPNSw2L7iUKuyz%2BVt
BUxULRkgNfoM72hfJR8iTuLiw%3D&reserved=0
> list.nist.gov/d/msgid/pqc-forum/
> 34f051a6-0f59-4aec-9bff-fe16511f0ae7n%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://
gcc02.safelinks.protection.outlook.com/?
url=https%3A%2F%2Fgroups.google.com%2Fa%2F&data=05%7C01%7Cyi-
kai.liu%40nist.gov%7C99465bd4face4bd9719108da729031b4%7C2ab5d82fd8fa4797a93e054655c61
dec%7C1%7C0%7C637948260913451336%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoi
V2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=cbPNSw2L7iUKuyz%2BVt
BUxULRkgNfoM72hfJR8iTuLiw%3D&reserved=0
> list.nist.gov/d/msgid/pqc-forum/
> b7b70354-7f74-c113-42d0-cbff41a6e27a%40uwaterloo.ca.

--

From: Dan Brown <danibrown%blackberry.com@gtempaccount.com> via pqc-forum <pqc-forum@list.nist.gov>
To: pqc-forum <pqc-forum@list.nist.gov>
CC: dj...@uwaterloo.ca <djao@uwaterloo.ca>
Subject: Re: [pqc-forum] Key recovery attack on SIDH
Date: Friday, August 05, 2022 11:41:25 AM ET

Should NIST now have an on-ramp for new KEMs?

On Saturday, July 30, 2022 at 7:12:56 PM UTC-4 dj...@uwaterloo.ca wrote:

> I was waiting in order to give the authors of the paper an opportunity to announce their results to the forum, in case they should wish to do so, but since someone else has already written about it, it's fair game to chime in now.
>
> The result is legitimate, and very impressive. Huge congratulations to Castryck and Decru.
>
> At first sight, the attack in 2022/975 uses knowledge of the endomorphism ring of the starting curve. As mentioned on page 2 of 2022/975, a possible "tweak" to SIKE was described in Section 8 of 2021/543 which could potentially thwart this attack. The tweak consists of randomly generating a starting curve of unknown endomorphism ring as part of the public key generation process. However, attacks always get better, never worse. It is possible that after further analysis, 2022/975's apparent dependence on knowledge of the starting curve's endomorphism ring will turn out to be spurious. More analysis is needed before we would be able to make any sort of confident claim as to whether or not the tweak would thwart the new attack.
>
> -David
>
> On 2022-07-30 6:58 p.m., Doge Protocol wrote:
>
>> Came accross this today and would like to share with the community.
>> https://eprint.iacr.org/2022/975
>> Our Magma implementation breaks the instantiation SIKEp434, which aims at security level 1 of the Post-Quantum Cryptography standardization process currently ran by NIST, in about one hour on a single core.
>>
>> Ran on a single core, the ap-

> pended Magma code breaks the Microsoft SIKE challenges $IKEp182 and $IKEp217
>
> in about 4 minutes and 6 minutes, respectively. A run on the SIKEp434 parameters, previously believed to meet NIST's quantum security level 1, took about 62 minutes, again on a single core. We also ran the code on random instances of SIKEp503 (level 2), SIKEp610 (level 3) and SIKEp751 (level 5), which took about 2h19m, 8h15m and 20h37m, respectively.
>
> --
> 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/34f051a6-0f59-4aec-9bff-fe16511f0ae7n%40list.nist.gov.

--

From: Doge Protocol <dogeprotocol1@gmail.com> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
CC: epersi...@fau.edu <epersichetti@fau.edu>, pqc-forum <pqc-forum@list.nist.gov>, dj...@uwaterloo.ca <djao@uwaterloo.ca>, danibrown%bl...@gtempaccount.com <danibrown%blackberry.com@gtempaccount.com>
Subject: Re: [pqc-forum] Key recovery attack on SIDH
Date: Saturday, August 06, 2022 06:59:45 PM ET

It might still help to have another mini program for key establishment schemes, targeting smaller public-key and cipher text sizes, just like the one planned for signature schemes. SIKE had these charecterestics and was in the 4th round, but since then has been broken. So its always good to have alternates.

Actually, post quantum cryptography program should be a continuing program and not just stop with the ones that are in scope.

If currently known pqc algorithms get broken, it may be a decade before alternatives can be found and analyzed.

Thus a continuing program will greatly benefit, in case of a security catastrophe where no pqc schemes stood the test of time.

On Friday, August 5, 2022 at 8:55:12 AM UTC-7 epersi...@fau.edu wrote:

> Hi Dan
> I believe NIST's on-ramp for new KEMs is already in place, as the 4th standardization round, featuring 3 beautiful code-based schemes ;)
>
> Best,
>
> Edoardo
>
> On Aug 5, 2022, at 11:41 AM, 'Dan Brown' via pqc-forum <pqc-...@list.nist.gov> wrote:
>
> > **EXTERNAL EMAIL :** Exercise caution when responding, opening links, or opening attachments.

Should NIST now have an on-ramp for new KEMs?

On Saturday, July 30, 2022 at 7:12:56 PM UTC-4 dj...@uwaterloo.ca wrote:

> I was waiting in order to give the authors of the paper an opportunity to announce their results to the forum, in case they should wish to do so, but since someone else has already written about it, it's fair game to chime in now.
>
> The result is legitimate, and very impressive. Huge congratulations to Castryck and Decru.
>
> At first sight, the attack in 2022/975 uses knowledge of the endomorphism ring of the starting curve. As mentioned on page 2 of 2022/975, a possible "tweak" to SIKE was described in Section 8 of 2021/543 which could potentially thwart this attack. The tweak consists of randomly generating a starting curve of unknown endomorphism ring as part of the public key generation process. However, attacks always get better, never worse. It is possible that after further analysis, 2022/975's apparent dependence on knowledge of the starting curve's endomorphism ring will turn out to be spurious. More analysis is needed before we would be able to make any sort of confident claim as to whether or not the tweak would thwart the new attack.
>
> -David
>
> On 2022-07-30 6:58 p.m., Doge Protocol wrote:
>
>> Came accross this today and would like to share with the community.
>> https://eprint.iacr.org/2022/975
>> Our Magma implementation breaks the instantiation SIKEp434, which aims at security level 1 of the Post-Quantum Cryptography standardization process currently ran by NIST, in about one hour on a single core.
>>
>> Ran on a single core, the ap-
>>
>> pended Magma code breaks the Microsoft SIKE challenges $IKEp182 and $IKEp217

> > in about 4 minutes and 6 minutes, respectively. A run on the SIKEp434 parame-
> >
> > ters, previously believed to meet NIST's quantum security level 1, took about 62
> >
> > minutes, again on a single core. We also ran the code on random instances of
> >
> > SIKEp503 (level 2), SIKEp610 (level 3) and SIKEp751 (level 5), which took about
> >
> > 2h19m, 8h15m and 20h37m, respectively.
> >
> > --
> > 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/34f051a6-0f59-4aec-9bff-fe16511f0ae7n%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+...@list.nist.gov.

To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/e5691cf2-a8ce-44f7-8e82-e9915a1d06e5n%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/f641635a-a374-4508-b8fd-025d7f46b641n%40list.nist.gov.

From: John Mattsson <john.mattsson@ericsson.com> via pqc-forum <pqc-forum@list.nist.gov>
To: Doge Protocol <dogeprotocol1@gmail.com>, pqc-forum <pqc-forum@list.nist.gov>
CC: epersi...@fau.edu <epersichetti@fau.edu>, pqc-forum <pqc-forum@list.nist.gov>, dj...@uwaterloo.ca <djao@uwaterloo.ca>, danibrown%bl...@gtempaccount.com <danibrown%blackberry.com@gtempaccount.com>
Subject: Re: [pqc-forum] Key recovery attack on SIDH
Date: Sunday, August 07, 2022 05:03:21 AM ET

---

dogeprotocol1@gmail.com wrote:

>It might still help to have another mini program for key establishment schemes, targeting smaller public-key and cipher text sizes, just like the one planned for signature schemes.

>

>SIKE had these charecterestics and was in the 4th round, but since then has been broken. So its always good to have alternates.

>

>Actually, post quantum cryptography program should be a continuing program and not just stop with the ones that are in scope.

I strongly agree. I think the post quantum cryptography program needs to continue with a round 5 and beyond.

As I wrote in https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/eAaiJO1qzkA/m/N0dyUTb5AAAJ (which was sorted into the Dilithium thread because of some hidden metadata).

"But round 4 will still be limited to KEMs and Signatures, which is a great start but clearly limiting. The most obvious thing missing is maybe NIKE. Static-Static DH has been used a lot for a long time. While Static-Static and Ephemeral-Static DH have for good reasons been replaced Ephemeral-Ephemeral DH in TLS, the use of Static-Static Key Exchange and Ephemeral-Static DH for implicit authentication has increased in other areas to lower the number of flights / message size / complexity, or to move away from the insecure use of symmetrical group keys. KEMs can do implicit authentication, but not very efficiently."

If CRQCs are ever built we definitely need algorithms with as little overhead as possible as well as algorithms that can be used for Non Interactive Key Exchange. For some IoT applications you call tolerate much higher computational cost (up to some limit) to get smaller messages. Some radio technologies are brutally limited (and is expected to stay that way).

NIKE has close to zero message overhead. That is sometimes the only thing that can be done for really constrained radio protocols such as US LoRaWAN that has 11 bytes message sizes and a lot of mandatory waiting between sending messages. IETF is currently working on a Lightweight Authenticated Key Exchange (LAKE) useful for constrained radio protocols such as 6TiSCH(45 bytes messages in the targeted scenario) and European LoRaWAN (51 bytes messages). For US 11 bytes LoRaWAN (7-8 application data after headers) even LAKE is problematic and the best option is NIKE. If there is no replacement for Static-Static ECDH, these kind of systems would have to go back to using symmetric group keys or no security (which both have quite horrible security properties).

Cheers,

John Preuß Mattsson

From: pqc-forum@list.nist.gov <pqc-forum@list.nist.gov> on behalf of Doge Protocol <dogeprotocol1@gmail.com>
Date: Sunday, 7 August 2022 at 00:59
To: pqc-forum <pqc-forum@list.nist.gov>
Cc: epersi...@fau.edu <epersichetti@fau.edu>, pqc-forum <pqc-forum@list.nist.gov>, dj...@uwaterloo.ca <djao@uwaterloo.ca>, danibrown%bl...@gtempaccount.com <danibrown%blackberry.com@gtempaccount.com>
Subject: Re: [pqc-forum] Key recovery attack on SIDH

It might still help to have another mini program for key establishment schemes, targeting smaller public-key and cipher text sizes, just like the one planned for signature schemes.

SIKE had these charecterestics and was in the 4th round, but since then has been broken. So its always good to have alternates.

Actually, post quantum cryptography program should be a continuing program and not just stop with the ones that are in scope.

If currently known pqc algorithms get broken, it may be a decade before alternatives can be found and analyzed.

Thus a continuing program will greatly benefit, in case of a security catastrophe where no pqc schemes stood the test of time.

On Friday, August 5, 2022 at 8:55:12 AM UTC-7 epersi...@fau.edu wrote:

> Hi Dan

I believe NIST's on-ramp for new KEMs is already in place, as the 4th standardization round, featuring 3 beautiful code-based schemes ;)

Best,

Edoardo

On Aug 5, 2022, at 11:41 AM, 'Dan Brown' via pqc-forum <pqc-...@list.nist.gov> wrote:

> **EXTERNAL EMAIL :** Exercise caution when responding, opening links, or opening attachments.

Should NIST now have an on-ramp for new KEMs?

On Saturday, July 30, 2022 at 7:12:56 PM UTC-4 dj...@uwaterloo.ca wrote:

> I was waiting in order to give the authors of the paper an opportunity to announce their results to the forum, in case they should wish to do so, but since someone else has already written about it, it's fair game to chime in now.
>
> The result is legitimate, and very impressive. Huge congratulations to Castryck and Decru.
>
> At first sight, the attack in 2022/975 uses knowledge of the endomorphism ring of the starting curve. As mentioned on page 2 of 2022/975, a possible "tweak" to SIKE was described in Section 8 of 2021/543 which could potentially thwart this attack. The tweak consists of randomly generating a starting curve of unknown endomorphism ring as part of the public key generation process. However, attacks always get better, never worse. It is possible that after further analysis, 2022/975's apparent dependence on knowledge of the starting curve's endomorphism ring will turn out to be spurious. More analysis is needed before we would be able to make any sort of confident claim as to whether or not the tweak would thwart the new attack.
>
> -David
>
> On 2022-07-30 6:58 p.m., Doge Protocol wrote:
>
> > Came accross this today and would like to share with the community.
> >
> > https://eprint.iacr.org/2022/975

> Our Magma implementation breaks the instantiation SIKEp434, which aims at security level 1 of the Post-Quantum Cryptography standardization process currently ran by NIST, in about one hour on a single core.
>
> Ran on a single core, the ap-
>
> pended Magma code breaks the Microsoft SIKE challenges $IKEp182 and $IKEp217
>
> in about 4 minutes and 6 minutes, respectively. A run on the SIKEp434 parame-
>
> ters, previously believed to meet NIST's quantum security level 1, took about 62
>
> minutes, again on a single core. We also ran the code on random instances of
>
> SIKEp503 (level 2), SIKEp610 (level 3) and SIKEp751 (level 5), which took about
>
> 2h19m, 8h15m and 20h37m, respectively.
>
> --
> 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/34f051a6-0f59-4aec-9bff-fe16511f0ae7n%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+...@list.nist.gov.

To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/e5691cf2-a8ce-44f7-8e82-e9915a1d06e5n%40list.nist.gov.

--

From: Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu> via pqc-forum@list.nist.gov
To: John Mattsson <john.mattsson@ericsson.com>, pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] Key recovery attack on SIDH
Date: Sunday, August 07, 2022 09:45:43 AM ET
Attachments: smime.p7m

I agree with John. We sorely lack QR DH-like key agreements, as opposed to key encapsulation mechanisms.

TNX

--

V/R,

Uri

There are two ways to design a system. One is to make it so simple there are obviously no deficiencies.

The other is to make it so complex there are no obvious deficiencies.

- C. A. R. Hoare

> **From:** 'John Mattsson' via pqc-forum
> **Reply-To:** John Mattsson
> **Date:** Sunday, August 7, 2022 at 05:03
> **To:** Doge Protocol , pqc-forum
> **Cc:** "epersi...@fau.edu" , pqc-forum , "dj...@uwaterloo.ca" , "danibrown%bl...@gtempaccount.com"
> **Subject:** Re: [pqc-forum] Key recovery attack on SIDH
>
> dogeprotocol1@gmail.com wrote:
>
> >It might still help to have another mini program for key establishment schemes, targeting smaller public-key and cipher text sizes, just like the one planned for signature schemes.
>
> >
>
> >SIKE had these charecterestics and was in the 4th round, but since then has been broken. So its always good to have alternates.

>

>Actually, post quantum cryptography program should be a continuing program and not just stop with the ones that are in scope.

I strongly agree. I think the post quantum cryptography program needs to continue with a round 5 and beyond.

As I wrote in https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/eAaiJO1qzkA/m/N0dyUTb5AAAJ (which was sorted into the Dilithium thread because of some hidden metadata).

"But round 4 will still be limited to KEMs and Signatures, which is a great start but clearly limiting. The most obvious thing missing is maybe NIKE. Static-Static DH has been used a lot for a long time. While Static-Static and Ephemeral-Static DH have for good reasons been replaced Ephemeral-Ephemeral DH in TLS, the use of Static-Static Key Exchange and Ephemeral-Static DH for implicit authentication has increased in other areas to lower the number of flights / message size / complexity, or to move away from the insecure use of symmetrical group keys. KEMs can do implicit authentication, but not very efficiently."

If CRQCs are ever built we definitely need algorithms with as little overhead as possible as well as algorithms that can be used for Non Interactive Key Exchange. For some IoT applications you call tolerate much higher computational cost (up to some limit) to get smaller messages. Some radio technologies are brutally limited (and is expected to stay that way).

NIKE has close to zero message overhead. That is sometimes the only thing that can be done for really constrained radio protocols such as US LoRaWAN that has 11 bytes message sizes and a lot of mandatory waiting between sending messages. IETF is currently working on a Lightweight Authenticated Key Exchange (LAKE) useful for constrained radio protocols such as 6TiSCH (45 bytes messages in the targeted scenario) and European LoRaWAN (51 bytes messages). For US 11 bytes LoRaWAN (7-8 application data after headers) even LAKE is problematic and the best option is NIKE. If there is no replacement for Static-Static ECDH, these kind of systems would have to go back to using symmetric group keys or no security (which both have quite horrible security properties).

Cheers,

John Preuß Mattsson

From: pqc-forum@list.nist.gov on behalf of Doge Protocol
Date: Sunday, 7 August 2022 at 00:59
To: pqc-forum
Cc: epersi...@fau.edu , pqc-forum , dj...@uwaterloo.ca , danibrown%bl...@gtempaccount.com
Subject: Re: [pqc-forum] Key recovery attack on SIDH

It might still help to have another mini program for key establishment schemes, targeting smaller public-key and cipher text sizes, just like the one planned for signature schemes.

SIKE had these charecterestics and was in the 4th round, but since then has been broken. So its always good to have alternates.

Actually, post quantum cryptography program should be a continuing program and not just stop with the ones that are in scope.

If currently known pqc algorithms get broken, it may be a decade before alternatives can be found and analyzed.

Thus a continuing program will greatly benefit, in case of a security catastrophe where no pqc schemes stood the test of time.

On Friday, August 5, 2022 at 8:55:12 AM UTC-7 epersi...@fau.edu wrote:

> Hi Dan
>
> I believe NIST's on-ramp for new KEMs is already in place, as the 4th standardization round, featuring 3 beautiful code-based schemes ;)
>
> Best,
>
> Edoardo
>
> > On Aug 5, 2022, at 11:41 AM, 'Dan Brown' via pqc-forum <pqc-...@list.nist.gov> wrote:
> >
> > > **EXTERNAL EMAIL :** Exercise caution when responding, opening links, or opening attachments.
> >
> > Should NIST now have an on-ramp for new KEMs?
> >
> > On Saturday, July 30, 2022 at 7:12:56 PM UTC-4 dj...@uwaterloo.ca wrote:

I was waiting in order to give the authors of the paper an opportunity to announce their results to the forum, in case they should wish to do so, but since someone else has already written about it, it's fair game to chime in now.

The result is legitimate, and very impressive. Huge congratulations to Castryck and Decru.

At first sight, the attack in 2022/975 uses knowledge of the endomorphism ring of the starting curve. As mentioned on page 2 of 2022/975, a possible "tweak" to SIKE was described in Section 8 of 2021/543 which could potentially thwart this attack. The tweak consists of randomly generating a starting curve of unknown endomorphism ring as part of the public key generation process. However, attacks always get better, never worse. It is possible that after further analysis, 2022/975's apparent dependence on knowledge of the starting curve's endomorphism ring will turn out to be spurious. More analysis is needed before we would be able to make any sort of confident claim as to whether or not the tweak would thwart the new attack.

-David

On 2022-07-30 6:58 p.m., Doge Protocol wrote:

> Came accross this today and would like to share with the community.
>
> https://eprint.iacr.org/2022/975
>
> Our Magma implementation breaks the instantiation SIKEp434, which aims at security level 1 of the Post-Quantum Cryptography standardization process currently ran by NIST, in about one hour on a single core.
>
> Ran on a single core, the ap-
>
> pended Magma code breaks the Microsoft SIKE challenges $IKEp182 and $IKEp217
>
> in about 4 minutes and 6 minutes, respectively. A run on the SIKEp434 parame-

> > ters, previously believed to meet NIST’s quantum security level 1, took about 62
> >
> > minutes, again on a single core. We also ran the code on random instances of
> >
> > SIKEp503 (level 2), SIKEp610 (level 3) and SIKEp751 (level 5), which took about
> >
> > 2h19m, 8h15m and 20h37m, respectively.
> >
> > --
> > 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/34f051a6-0f59-4aec-9bff-fe16511f0ae7n%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+...@list.nist.gov.
>
> To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/e5691cf2-a8ce-44f7-8e82-e9915a1d06e5n%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/f641635a-a374-4508-b8fd-025d7f46b641n%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/HE1PR0701MB30509FC9401142C7D722017A89609%40HE1PR0701MB3050.eurprd07.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/32B9ACF9-18EF-4ABA-B0A0-E5798EFEE4E1%40ll.mit.edu.

From: Tony Arcieri <bascule@gmail.com> via pqc-forum@list.nist.gov
To: John Mattsson <john.mattsson@ericsson.com>
CC: Doge Protocol <dogeprotocol1@gmail.com>, pqc-forum <pqc-forum@list.nist.gov>, epersi...@fau.edu <epersichetti@fau.edu>, dj...@uwaterloo.ca <djao@uwaterloo.ca>, danibrown%bl...@gtempaccount.com <danibrown%blackberry.com@gtempaccount.com>
Subject: Re: [pqc-forum] Key recovery attack on SIDH
Date: Sunday, August 07, 2022 09:55:38 AM ET

On Sun, Aug 7, 2022 at 3:03 AM 'John Mattsson' via pqc-forum <pqc-forum@list.nist.gov> wrote:

> *While Static-Static and Ephemeral-Static DH have for good reasons been replaced Ephemeral-Ephemeral DH in TLS, the use of Static-Static Key Exchange and Ephemeral-Static DH for implicit authentication has increased in other areas to lower the number of flights / message size / complexity*

Static and ephemeral D-H can also be combined in several different key agreement patterns. See 3DH as used in the Signal Protocol, Noise, and OPTLS: such systems combine static D-H identity keys with ephemeral D-H keys for confidentiality, allowing 1-RTT semi-static and 0-RTT key agreement modes.

--
Tony Arcieri

From: Lanlan Pan <abbypan@gmail.com> via pqc-forum@list.nist.gov
To: Tony Arcieri <bascule@gmail.com>
CC: John Mattsson <john.mattsson@ericsson.com>, Doge Protocol <dogeprotocol1@gmail.com>, pqc-forum <pqc-forum@list.nist.gov>, epersi...@fau.edu <epersichetti@fau.edu>, dj...@uwaterloo.ca <djao@uwaterloo.ca>, danibrown%bl...@gtempaccount.com <danibrown%blackberry.com@gtempaccount.com>
Subject: Re: [pqc-forum] Key recovery attack on SIDH
Date: Wednesday, August 10, 2022 11:20:47 AM ET

Tony Arcieri <bascule@gmail.com> 于2022年8月7日周日 21:55写道：

> On Sun, Aug 7, 2022 at 3:03 AM 'John Mattsson' via pqc-forum <pqc-forum@list.nist.gov> wrote:
>
> > *While Static-Static and Ephemeral-Static DH have for good reasons been replaced Ephemeral-Ephemeral DH in TLS, the use of Static-Static Key Exchange and Ephemeral-Static DH for implicit authentication has increased in other areas to lower the number of flights / message size / complexity*
>
> Static and ephemeral D-H can also be combined in several different key agreement patterns. See 3DH as used in the Signal Protocol, Noise, and OPTLS: such systems combine static D-H identity keys with ephemeral D-H keys for confidentiality, allowing 1-RTT semi-static and 0-RTT key agreement modes.

3DH's implicit authentication is helpful to cult down iot message size.

And, when and how to provision/bootstrap the long-term identity keys.

> --
> Tony Arcieri
>
> --
> 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/CAHOTMV%2BXU_dsQOa_42JHvBsBzN8F46knvj%3DdJY0p0uQ1fUuhyw%40mail.gmail.com.

--

From: Dan Brown <danibrown%blackberry.com@gtempaccount.com> via pqc-forum <pqc-forum@list.nist.gov>
To: pqc-forum <pqc-forum@list.nist.gov>
CC: epersi...@fau.edu <epersichetti@fau.edu>, pqc-forum <pqc-forum@list.nist.gov>, dj...@uwaterloo.ca <djao@uwaterloo.ca>, Dan Brown <danibrown%blackberry.com@gtempaccount.com>
Subject: Re: [pqc-forum] Key recovery attack on SIDH
Date: Wednesday, August 10, 2022 01:34:27 PM ET

Hi Edoardo,

To clarify my question, I wanted to know if something similar to

"New Call for Proposals: Digital Signature Algorithms with Short Signatures and Fast Verification
NIST also plans to issue a new Call for Proposals for public-key (quantum-resistant) digital signature algorithms by the end of summer 2022. NIST is primarily looking to diversify its signature portfolio, so signature schemes that are not based on structured lattices are of greatest interest. NIST would like submissions for signature schemes that have short signatures and fast verification."

from

https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4

would be worthwhile for KEMs?

To elaborate, suppose that NIST picks BIKE from Round 4. The NIST PQC KEM portfolio would then have diversity 2 (lattice + code). For comparison, the currently proposed NIST PQC signature portfolio has diversity 2 (lattice+hash, or 2.5 if you want to credit Falcon and Dilithium with some diversity). The new call could increase this to 3 (or 4). So, why not increase the KEM portfolio diversity too?

Maybe, a new KEM call would distract from Round 4, so a new call for KEMs ought to be delayed? Maybe, diversity on the efficiency side of KEM, would be covered by Round 4, whereas for signatures it is still lacking (e.g. Sphincs+ too big, or even Falcon too big)? Maybe, there's some other pragmatic reason against new KEM call?

Best regards,

Dan

PS1. My question was motivated by the Castryck-Decru SIKE attack, which hits the diversity of Round 4 candidates, unless there is a fix.

PS2. What's the impact of the new Maino-Martindale SIKE attack? https://eprint.iacr.org/2022/1026.pdf

On Friday, August 5, 2022 at 11:55:12 AM UTC-4 epersi...@fau.edu wrote:

> Hi Dan
> I believe NIST's on-ramp for new KEMs is already in place, as the 4th standardization round, featuring 3 beautiful code-based schemes ;)
>
> Best,
>
> Edoardo
>
> On Aug 5, 2022, at 11:41 AM, 'Dan Brown' via pqc-forum <pqc-...@list.nist.gov> wrote:
>
> > **EXTERNAL EMAIL :** Exercise caution when responding, opening links, or opening attachments.
>
> Should NIST now have an on-ramp for new KEMs?
>
> On Saturday, July 30, 2022 at 7:12:56 PM UTC-4 dj...@uwaterloo.ca wrote:
>
> > I was waiting in order to give the authors of the paper an opportunity to announce their results to the forum, in case they should wish to do so, but since someone else has already written about it, it's fair game to chime in now.
> >
> > The result is legitimate, and very impressive. Huge congratulations to Castryck and Decru.
> >
> > At first sight, the attack in 2022/975 uses knowledge of the endomorphism ring of the starting curve. As mentioned on page 2 of 2022/975, a possible "tweak" to SIKE was described in Section 8 of 2021/543 which could potentially thwart

this attack. The tweak consists of randomly generating a starting curve of unknown endomorphism ring as part of the public key generation process. However, attacks always get better, never worse. It is possible that after further analysis, 2022/975's apparent dependence on knowledge of the starting curve's endomorphism ring will turn out to be spurious. More analysis is needed before we would be able to make any sort of confident claim as to whether or not the tweak would thwart the new attack.

-David

On 2022-07-30 6:58 p.m., Doge Protocol wrote:

> Came accross this today and would like to share with the community.
> https://eprint.iacr.org/2022/975
> Our Magma implementation breaks the instantiation SIKEp434, which aims at security level 1 of the Post-Quantum Cryptography standardization process currently ran by NIST, in about one hour on a single core.
>
> Ran on a single core, the ap-
>
> pended Magma code breaks the Microsoft SIKE challenges $IKEp182 and $IKEp217
>
> in about 4 minutes and 6 minutes, respectively. A run on the SIKEp434 parame-
>
> ters, previously believed to meet NIST’s quantum security level 1, took about 62
>
> minutes, again on a single core. We also ran the code on random instances of
>
> SIKEp503 (level 2), SIKEp610 (level 3) and SIKEp751 (level 5), which took about
>
> 2h19m, 8h15m and 20h37m, respectively.
>
> --
> 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/34f051a6-0f59-4aec-9bff-fe16511f0ae7n%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+...@list.nist.gov.
>
> To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/e5691cf2-a8ce-44f7-8e82-e9915a1d06e5n%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/6c35dc25-c0ea-431b-ad9f-072227cb5b47n%40list.nist.gov.

From: Edoardo Persichetti <epersichetti@fau.edu> via pqc-forum <pqc-forum@list.nist.gov>
To: Dan Brown <danibrown%blackberry.com@gtempaccount.com>
CC: pqc-forum <pqc-forum@list.nist.gov>, dj...@uwaterloo.ca <djao@uwaterloo.ca>
Subject: Re: [pqc-forum] Key recovery attack on SIDH
Date: Wednesday, August 10, 2022 03:20:39 PM ET

Hi Dan
I apologize for the facetious tone of my previous email, and thank you for your kind reply. Indeed, we all know (and are excited about!) NIST's on-ramp for signatures. This is what my opinion is, and what I understood from the process.

The on-ramp for signatures derived from a lack of diversity in the final choices, as we know. However, there was also a "numerical" gap in the number of options. By this I mean that the list of finalists was already very short before what happened to Rainbow.

Consider this: at the end of Round 3, NIST standardized 100% of lattice-based finalists, plus SPHINCS+, leaving behind only Picnic and GeMMS. On the other hand, for KEMs, NIST had already 3 equally good finalists to choose from, choosing only Kyber but reserving the right to "fall back" on NTRU, not to mention NTRUPrime, Frodo etc. I believe NIST was looking to provide diversity for KEMs out of Round 4; with your metric, Round 4 could provide the same "2.5" diversity if, for example, both Classic McEliece and BIKE are selected. However, if more alternatives are needed, I suppose NIST prefers to select from the existing round of candidates rather than opening a new round; the most pragmatic reason is the large amount of overhead necessary to run such a round, as well as the effort required to maintain such a large pool of standards.

Best,

Edoardo

p.s. I am not an expert on isogenies so I can't accurately comment on the topic, but my impression is that there is no way back for SIKE.

> On Aug 10, 2022, at 1:33 PM, 'Dan Brown' via pqc-forum <pqc-forum@list.nist.gov> wrote:
>
>

Hi Edoardo,

To clarify my question, I wanted to know if something similar to

"New Call for Proposals: Digital Signature Algorithms with Short Signatures and Fast Verification
NIST also plans to issue a new Call for Proposals for public-key (quantum-resistant) digital signature algorithms by the end of summer 2022. NIST is primarily looking to diversify its signature portfolio, so signature schemes that are not based on structured lattices are of greatest interest. NIST would like submissions for signature schemes that have short signatures and fast verification."

from

https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4

would be worthwhile for KEMs?

To elaborate, suppose that NIST picks BIKE from Round 4. The NIST PQC KEM portfolio would then have diversity 2 (lattice + code). For comparison, the currently proposed NIST PQC signature portfolio has diversity 2 (lattice+hash, or 2.5 if you want to credit Falcon and Dilithium with some diversity). The new call could increase this to 3 (or 4). So, why not increase the KEM portfolio diversity too?

Maybe, a new KEM call would distract from Round 4, so a new call for KEMs ought to be delayed? Maybe, diversity on the efficiency side of KEM, would be covered by Round 4, whereas for signatures it is still lacking (e.g. Sphincs+ too big, or even Falcon too big)? Maybe, there's some other pragmatic reason against new KEM call?

Best regards,

Dan

PS1. My question was motivated by the Castryck-Decru SIKE attack, which hits the diversity of Round 4 candidates, unless there is a fix.

PS2. What's the impact of the new Maino-Martindale SIKE attack? https://eprint.iacr.org/2022/1026.pdf

On Friday, August 5, 2022 at 11:55:12 AM UTC-4 epersi...@fau.edu wrote:

> Hi Dan
> I believe NIST's on-ramp for new KEMs is already in place, as the 4th standardization round, featuring 3 beautiful code-based schemes ;)
>
> Best,
>
> Edoardo
>
> On Aug 5, 2022, at 11:41 AM, 'Dan Brown' via pqc-forum <pqc-...@list.nist.gov> wrote:
>
> > **EXTERNAL EMAIL :** Exercise caution when responding, opening links, or opening attachments.
>
> Should NIST now have an on-ramp for new KEMs?
>
> On Saturday, July 30, 2022 at 7:12:56 PM UTC-4 dj...@uwaterloo.ca wrote:
>
> > I was waiting in order to give the authors of the paper an opportunity to announce their results to the forum, in case they should wish to do so, but since someone else has already written about it, it's fair game to chime in now.
> >
> > The result is legitimate, and very impressive. Huge congratulations to Castryck and Decru.
> >
> > At first sight, the attack in 2022/975 uses knowledge of the endomorphism ring of the starting curve. As mentioned on page 2 of 2022/975, a possible "tweak" to SIKE was described in Section 8 of 2021/543 which could potentially thwart this attack. The tweak consists of randomly generating a starting curve of unknown endomorphism ring as part of the public key generation process. However, attacks always get better, never worse. It is possible that

after further analysis, 2022/975's apparent dependence on knowledge of the starting curve's endomorphism ring will turn out to be spurious. More analysis is needed before we would be able to make any sort of confident claim as to whether or not the tweak would thwart the new attack.

-David

On 2022-07-30 6:58 p.m., Doge Protocol wrote:

> Came accross this today and would like to share with the community.
> https://eprint.iacr.org/2022/975
> Our Magma implementation breaks the instantiation SIKEp434, which aims at security level 1 of the Post-Quantum Cryptography standardization process currently ran by NIST, in about one hour on a single core.
>
> Ran on a single core, the ap-
>
> pended Magma code breaks the Microsoft SIKE challenges $IKEp182 and $IKEp217
>
> in about 4 minutes and 6 minutes, respectively. A run on the SIKEp434 parame-
>
> ters, previously believed to meet NIST's quantum security level 1, took about 62
>
> minutes, again on a single core. We also ran the code on random instances of
>
> SIKEp503 (level 2), SIKEp610 (level 3) and SIKEp751 (level 5), which took about
>
> 2h19m, 8h15m and 20h37m, respectively.
>
> --
> 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/34f051a6-0f59-4aec-9bff-fe16511f0ae7n%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+...@list.nist.gov.
>
> To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/e5691cf2-a8ce-44f7-8e82-e9915a1d06e5n%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/6c35dc25-c0ea-431b-ad9f-072227cb5b47n%40list.nist.gov.

From: Christopher J Peikert <cpeikert@alum.mit.edu> via pqc-forum@list.nist.gov
To: David Jao <djao@uwaterloo.ca>
CC: pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] Key recovery attack on SIDH
Date: Wednesday, August 10, 2022 11:05:33 PM ET

On Sat, Jul 30, 2022 at 7:13 PM David Jao <djao@uwaterloo.ca> wrote:

> At first sight, the attack in 2022/975 uses knowledge of the endomorphism ring of the starting curve. As mentioned on page 2 of 2022/975, a possible "tweak" to SIKE was described in Section 8 of 2021/543 which could potentially thwart this attack. The tweak consists of randomly generating a starting curve of unknown endomorphism ring as part of the public key generation process. However, attacks always get better, never worse. It is possible that after further analysis, 2022/975's apparent dependence on knowledge of the starting curve's endomorphism ring will turn out to be spurious. More analysis is needed before we would be able to make any sort of confident claim as to whether or not the tweak would thwart the new attack.

A (two-page) paper just appeared on eprint that claims to break this tweaked version in polynomial time. (I can't verify the details, but it looks plausible.)

https://eprint.iacr.org/2022/1038

Sincerely yours in cryptography,

Chris

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: danibrown%bl...@gtempaccount.com <danibrown%blackberry.com@gtempaccount.com>
Subject: Re: [pqc-forum] Key recovery attack on SIDH
Date: Thursday, August 11, 2022 05:26:33 PM ET

In response to the question "Should NIST now have an on-ramp for new KEMs?" we wanted to share our current view. We are initiating the call for additional signatures primarily because we want a digital signature scheme that is not based on lattices and can be easily used by most applications. For the KEMs, we feel that with the candidates in the 4th round we will be able to achieve that same objective. Thus for now, we do not have any plans to initiate a new call for KEMs.

Standardization efforts in PQC will undoubtedly continue for many years, and new and ongoing research results will impact this. So we also are not ruling out that we could call for additional KEMs at some point in the future.

Dustin Moody

NIST

On Friday, August 5, 2022 at 11:41:13 AM UTC-4 danibrown%bl...@gtempaccount.com wrote:

> Should NIST now have an on-ramp for new KEMs?
>
> On Saturday, July 30, 2022 at 7:12:56 PM UTC-4 dj...@uwaterloo.ca wrote:
>
> > I was waiting in order to give the authors of the paper an opportunity to announce their results to the forum, in case they should wish to do so, but since someone else has already written about it, it's fair game to chime in now.
> >
> > The result is legitimate, and very impressive. Huge congratulations to Castryck and Decru.
> >
> > At first sight, the attack in 2022/975 uses knowledge of the endomorphism ring of the starting curve. As mentioned on page 2 of 2022/975, a possible "tweak" to SIKE was described in Section 8 of 2021/543 which could potentially thwart this attack. The tweak consists of randomly generating a starting curve of unknown endomorphism ring as part of the public key generation process. However, attacks always get better, never worse. It

is possible that after further analysis, 2022/975's apparent dependence on knowledge of the starting curve's endomorphism ring will turn out to be spurious. More analysis is needed before we would be able to make any sort of confident claim as to whether or not the tweak would thwart the new attack.

-David

On 2022-07-30 6:58 p.m., Doge Protocol wrote:

> Came accross this today and would like to share with the community.
> https://eprint.iacr.org/2022/975
> Our Magma implementation breaks the instantiation SIKEp434, which aims at security level 1 of the Post-Quantum Cryptography standardization process currently ran by NIST, in about one hour on a single core.
>
> Ran on a single core, the ap-
>
> pended Magma code breaks the Microsoft SIKE challenges $IKEp182 and $IKEp217
>
> in about 4 minutes and 6 minutes, respectively. A run on the SIKEp434 parame-
>
> ters, previously believed to meet NIST's quantum security level 1, took about 62
>
> minutes, again on a single core. We also ran the code on random instances of
>
> SIKEp503 (level 2), SIKEp610 (level 3) and SIKEp751 (level 5), which took about
>
> 2h19m, 8h15m and 20h37m, respectively.

> > list.nist.gov/d/msgid/pqc-forum/34f051a6-0f59-4aec-9bff-fe16511f0ae7n%40list.nist.gov.

--

From: Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] Key recovery attack on SIDH
Date: Thursday, August 11, 2022 05:35:30 PM ET
Attachments: smime.p7m

NIST.IR report pointed out that Falcon implementations could be difficult to validate, because of its use of floating point.
There was Zalcon proposal that came late, but seemed to address the main shortcomings of Falcon. Since NIST already announced its plans to standardize Falcon - IMHO, it would be nice if Zalcon was considered for the 4th round, it's "late coming" perhaps compensated by its similarities with the winner Falcon.

Thanks.

Regards,
Uri

> On Aug 11, 2022, at 17:27, 'dustin...@nist.gov' via pqc-forum wrote:
>
> In response to the question "Should NIST now have an on-ramp for new KEMs?" we wanted to share our current view. We are initiating the call for additional signatures primarily because we want a digital signature scheme that is not based on lattices and can be easily used by most applications. For the KEMs, we feel that with the candidates in the 4th round we will be able to achieve that same objective. Thus for now, we do not have any plans to initiate a new call for KEMs.
>
> Standardization efforts in PQC will undoubtedly continue for many years, and new and ongoing research results will impact this. So we also are not ruling out that we could call for additional KEMs at some point in the future.
>
> Dustin Moody
>
> NIST

On Friday, August 5, 2022 at 11:41:13 AM UTC-4
danibrown%bl...@gtempaccount.com wrote:

> Should NIST now have an on-ramp for new KEMs?
>
> On Saturday, July 30, 2022 at 7:12:56 PM UTC-4 dj...@uwaterloo.ca wrote:
>
> > I was waiting in order to give the authors of the paper an opportunity to announce their results to the forum, in case they should wish to do so, but since someone else has already written about it, it's fair game to chime in now.
> >
> > The result is legitimate, and very impressive. Huge congratulations to Castryck and Decru.
> >
> > At first sight, the attack in 2022/975 uses knowledge of the endomorphism ring of the starting curve. As mentioned on page 2 of 2022/975, a possible "tweak" to SIKE was described in Section 8 of 2021/543 which could potentially thwart this attack. The tweak consists of randomly generating a starting curve of unknown endomorphism ring as part of the public key generation process. However, attacks always get better, never worse. It is possible that after further analysis, 2022/975's apparent dependence on knowledge of the starting curve's endomorphism ring will turn out to be spurious. More analysis is needed before we would be able to make any sort of confident claim as to whether or not the tweak would thwart the new attack.
> >
> > -David
> >
> > On 2022-07-30 6:58 p.m., Doge Protocol wrote:
> >
> > > Came accross this today and would like to share with the community.
> > > https://eprint.iacr.org/2022/975
> > > Our Magma implementation breaks the instantiation SIKEp434, which aims at security level 1 of the Post-Quantum Cryptography standardization process currently ran by NIST, in about one hour on a single core.
> > >
> > > Ran on a single core, the ap-

> > pended Magma code breaks the Microsoft SIKE challenges $IKEp182 and $IKEp217
> >
> > in about 4 minutes and 6 minutes, respectively. A run on the SIKEp434 parame-
> >
> > ters, previously believed to meet NIST's quantum security level 1, took about 62
> >
> > minutes, again on a single core. We also ran the code on random instances of
> >
> > SIKEp503 (level 2), SIKEp610 (level 3) and SIKEp751 (level 5), which took about
> >
> > 2h19m, 8h15m and 20h37m, respectively.
>
> --
> 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/34f051a6-0f59-4aec-9bff-fe16511f0ae7n%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/668dbc04-b681-4ee2-b2e2-d5665df71ed4n%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/ECB1F432-7917-400C-A926-9D85698AA94B%40ll.mit.edu.

From: Jacob Alperin-Sheriff <jacobmas@gmail.com> via pqc-forum@list.nist.gov
To: dustin...@nist.gov <dustin.moody@nist.gov>
CC: danibrown%bl...@gtempaccount.com <danibrown%blackberry.com@gtempaccount.com>, pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] Key recovery attack on SIDH
Date: Friday, August 12, 2022 06:57:43 AM ET

Is this true even now that the one markedly different scheme is totally broken? HQC and RQC still have similarities to lattice schemes in conceptual design after all

On Thu, Aug 11, 2022 at 5:26 PM 'dustin...@nist.gov' via pqc-forum <pqc-forum@list.nist.gov> wrote:

> In response to the question "Should NIST now have an on-ramp for new KEMs?" we wanted to share our current view. We are initiating the call for additional signatures primarily because we want a digital signature scheme that is not based on lattices and can be easily used by most applications. For the KEMs, we feel that with the candidates in the 4th round we will be able to achieve that same objective. Thus for now, we do not have any plans to initiate a new call for KEMs.
>
> Standardization efforts in PQC will undoubtedly continue for many years, and new and ongoing research results will impact this. So we also are not ruling out that we could call for additional KEMs at some point in the future.
>
> Dustin Moody
>
> NIST
>
> On Friday, August 5, 2022 at 11:41:13 AM UTC-4 danibrown%bl...@gtempaccount.com wrote:
>
> > Should NIST now have an on-ramp for new KEMs?
> >
> > On Saturday, July 30, 2022 at 7:12:56 PM UTC-4 dj...@uwaterloo.ca wrote:

I was waiting in order to give the authors of the paper an opportunity to announce their results to the forum, in case they should wish to do so, but since someone else has already written about it, it's fair game to chime in now.

The result is legitimate, and very impressive. Huge congratulations to Castryck and Decru.

At first sight, the attack in 2022/975 uses knowledge of the endomorphism ring of the starting curve. As mentioned on page 2 of 2022/975, a possible "tweak" to SIKE was described in Section 8 of 2021/543 which could potentially thwart this attack. The tweak consists of randomly generating a starting curve of unknown endomorphism ring as part of the public key generation process. However, attacks always get better, never worse. It is possible that after further analysis, 2022/975's apparent dependence on knowledge of the starting curve's endomorphism ring will turn out to be spurious. More analysis is needed before we would be able to make any sort of confident claim as to whether or not the tweak would thwart the new attack.

-David

On 2022-07-30 6:58 p.m., Doge Protocol wrote:

> Came accross this today and would like to share with the community.
> https://eprint.iacr.org/2022/975
> Our Magma implementation breaks the instantiation SIKEp434, which aims at security level 1 of the Post-Quantum Cryptography standardization process currently ran by NIST, in about one hour on a single core.
>
> Ran on a single core, the ap-
>
> pended Magma code breaks the Microsoft SIKE challenges $IKEp182 and $IKEp217
>
> in about 4 minutes and 6 minutes, respectively. A run on the SIKEp434 parame-
>
> ters, previously believed to meet NIST’s quantum security level 1, took about 62
>
> minutes, again on a single core. We also ran the code on random instances of

> > SIKEp503 (level 2), SIKEp610 (level 3) and SIKEp751 (level 5), which took about
> >
> > 2h19m, 8h15m and 20h37m, respectively.
> >
> > --
> > 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/34f051a6-0f59-4aec-9bff-fe16511f0ae7n%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/668dbc04-b681-4ee2-b2e2-d5665df71ed4n%40list.nist.gov.

--
-Jacob Alperin-Sheriff

--
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/CAM7-xUv%2B%2BcCQdK%3DOzyBvS3icQpjVKVY6yKUTkSA_09cn-o_7_g%40mail.gmail.com.