From: andy yi <hy8196695@gmail.com> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
CC: idqu...@gmail.com <idquantum@gmail.com>, wren....@gmail.com <wren.robson@gmail.com>, pqc-forum <pqc-forum@list.nist.gov>, s zhang <shezhangth@gmail.com>
Subject: Re: [pqc-forum] A digital currency that claims to be resistant to quantum computers
Date: Tuesday, April 26, 2022 08:52:09 AM ET

---

1. FALCON and CRYSTALS-DILITHIUM signatures are slow, not suitable for de-cryptocurrency, and because of the publication of D. J. Bernstein's s-unit attack paper, there is currently no consensus, https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/3mVeyEfYnUY/m/ZbbXR0pnDQAJ
2. XMSS is a hash function signature, which requires very strict full-scale management, and is not suitable for decentralized encryption.

https://csrc.nist.gov/CSRC/media/Projects/Stateful-Hash-Based-Signatures/documents/stateful-HBS-misuse-resistance-public-comments-April2019.pdf

https://csrc.nist.gov/CSRC/media/Publications/sp/800-208/draft/documents/sp800-208-draft-comments-received.pdf

3. WOTS+ is a hash function signature

https://eprint.iacr.org/2019/344.pdf

4.Rainbow signature, there are basically no attack cases at present, only the second round of NIST selection L1 was broken, and only need to upgrade parameters to defend

5.Here are some cryptocurrencies that use post-quantum signature algorithms

(1).QRL uses XMSS

(2).xx uses WOTS+

(3).TDC uses FALCON

(4). ARL uses CRYSTALS-DILITHIUM

(5).ABC uses rainbow

在2021年11月8日星期一 UTC+8 01:31:36<idqu...@gmail.com> 写道：

> Tidecoin is using Falcon-512 as a signature.
> http://tidecoin.org
>
> On Wednesday, October 13, 2021 at 4:51:46 PM UTC+3 wren....@gmail.com wrote:
>
> > On that I couldn't comment.
> > Best,
> >
> > Wrenna
> >
> > On Wed, 13 Oct 2021, 14:50 s zhang, <shezh...@gmail.com> wrote:
> >
> > > You are right, maybe this is one of his hype techniques.
> > >
> > > wren....@gmail.com 在 2021年10月13日 星期三下午9:46:40 [UTC+8] 的信中寫道：
> > >
> > > > It is quite difficult to evaluate technical claims made in a private space on a social media platform.
> > > > Best,
> > > >
> > > > Wrenna
> > > >
> > > > On Wed, 13 Oct 2021, 14:45 s zhang, <shezh...@gmail.com> wrote:
> > > >
> > > > > The chairman of abcmint said it publicly at clubhouse, and his supporters are convinced of it.
> > > > >
> > > > > Zang
> > > > >
> > > > > wren....@gmail.com 在 2021年10月13日 星期三下午9:40:05 [UTC+8] 的信中寫道：
> > > > >
> > > > > > I will leave it to those more qualified than I to answer your question, but it would probably help if you could provide a link to the specific claims you mention.
> > > > > > Best,
> > > > > >
> > > > > > Wrenna

On Wed, 13 Oct 2021, 14:38 s zhang, <shezh...@gmail.com> wrote:

> Thank you for your reply.
>
> According to the documents and other information you gave, there are three digital signature algorithms shortlisted for the 3rd round of the nist pqc, namely CRYSTALS-DILITHIUM, FALCON, and Rainbow, but why does the chairman of abcmint claim that other than Rainbow, the other two algorithms are not feasible for digital currency and Internet applications.
>
> Zang
>
> wren....@gmail.com 在 2021年10月13日 星期三下午9:02:52 [UTC+8] 的信中寫道：
>
> > It looks like this is a project whose vice-chairman is one of the co-creators of the Rainbow cryptosystem, and they use Rainbow, one of the Round 3 finalists in the digital signatures category. It is among three finalists to be considered for standardization in this category at the end of the third round. See NISTIR 8309, https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8309.pdf. I do not believe it has been approved for standardization at this time. For previous discussion on Rainbow in this forum, you should be able to use the Google Groups search functionality.
> >
> > Hope this helps!
> >
> > Wrenna
> >
> > On Wed, 13 Oct 2021 at 13:51, s zhang <shezh...@gmail.com> wrote:
> >
> > > Dear all,
> > >
> > > I recently heard about a post-quantum cryptocurrency (abcmint) whose founder claims that the technology used is approved by NIST and is the only solution. I would like to ask you all, can this really be approved and reliable by experts?
> > >
> > > Here is the official website of abcmint, which has various information about this cryptocurrency

official: http://www.abcmint.org/

github: https://github.com/abcmint/abcmint

Best regards.

Zang

--
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/f3023c10-89c8-4ca0-ad22-a574ee5a2ed3n%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/e81b3764-f719-418b-a7f5-4dddb31954aan%40list.nist.gov.

From: Doge Protocol <dogeprotocol1@gmail.com> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
CC: hy81...@gmail.com <hy8196695@gmail.com>, idqu...@gmail.com <idquantum@gmail.com>, wren....@gmail.com <wren.robson@gmail.com>, pqc-forum <pqc-forum@list.nist.gov>, s zhang <shezhangth@gmail.com>
Subject: Re: [pqc-forum] A digital currency that claims to be resistant to quantum computers
Date: Thursday, April 28, 2022 02:49:31 PM ET

Point (4) on Rainbow is not necessarily true. Please see paper by Ward Beullens: https://eprint.iacr.org/2022/214.pdf
Snippet from the paper (snipping off some of the text, since there are formatting issues of power values in the forum editor):

"We estimate that a key recovery for the SL 1 parameter set of the third-round submission requires only a factor ... <snip>. For the parameter sets targeting NIST security levels 3 and 5, we find that the attack can be improved by combining the new technique with the rectangular MinRank attack of Beullens [4]. "

On Tuesday, April 26, 2022 at 5:48:55 AM UTC-7 hy81...@gmail.com wrote:

> 1. FALCON and CRYSTALS-DILITHIUM signatures are slow, not suitable for de-cryptocurrency, and because of the publication of D. J. Bernstein's s-unit attack paper, there is currently no consensus, https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/3mVeyEfYnUY/m/ZbbXR0pnDQAJ
> 2. XMSS is a hash function signature, which requires very strict full-scale management, and is not suitable for decentralized encryption.
>
> https://csrc.nist.gov/CSRC/media/Projects/Stateful-Hash-Based-Signatures/documents/stateful-HBS-misuse-resistance-public-comments-April2019.pdf
>
> https://csrc.nist.gov/CSRC/media/Publications/sp/800-208/draft/documents/sp800-208-draft-comments-received.pdf
>
> 3. WOTS+ is a hash function signature
>
> https://eprint.iacr.org/2019/344.pdf
>
> 4.Rainbow signature, there are basically no attack cases at present, only the second round of NIST selection L1 was broken, and only need to upgrade parameters to defend
>
> 5.Here are some cryptocurrencies that use post-quantum signature algorithms

(1).QRL uses XMSS

(2).xx uses WOTS+

(3).TDC uses FALCON

(4). ARL uses CRYSTALS-DILITHIUM

(5).ABC uses rainbow

在2021年11月8日星期一 UTC+8 01:31:36<idqu...@gmail.com> 写道：

> Tidecoin is using Falcon-512 as a signature.
> http://tidecoin.org
>
> On Wednesday, October 13, 2021 at 4:51:46 PM UTC+3 wren....@gmail.com wrote:
>
> > On that I couldn't comment.
> > Best,
> >
> > Wrenna
> >
> > On Wed, 13 Oct 2021, 14:50 s zhang, <shezh...@gmail.com> wrote:
> >
> > > You are right, maybe this is one of his hype techniques.
> > >
> > > wren....@gmail.com 在 2021年10月13日 星期三下午9:46:40 [UTC+8] 的信中寫道：
> > >
> > > > It is quite difficult to evaluate technical claims made in a private space on a social media platform.
> > > > Best,
> > > >
> > > > Wrenna
> > > >
> > > > On Wed, 13 Oct 2021, 14:45 s zhang, <shezh...@gmail.com> wrote:
> > > >
> > > > > The chairman of abcmint said it publicly at clubhouse, and his supporters are convinced of it.

Zang

wren....@gmail.com 在 2021年10月13日 星期三下午9:40:05 [UTC+8] 的信中寫道：

> I will leave it to those more qualified than I to answer your question, but it would probably help if you could provide a link to the specific claims you mention.
> Best,
>
> Wrenna
>
> On Wed, 13 Oct 2021, 14:38 s zhang, <shezh...@gmail.com> wrote:
>
> > Thank you for your reply.
> >
> > According to the documents and other information you gave, there are three digital signature algorithms shortlisted for the 3rd round of the nist pqc, namely CRYSTALS-DILITHIUM, FALCON, and Rainbow, but why does the chairman of abcmint claim that other than Rainbow, the other two algorithms are not feasible for digital currency and Internet applications.
> >
> > Zang
> >
> > wren....@gmail.com 在 2021年10月13日 星期三下午9:02:52 [UTC+8] 的信中寫道：
> >
> > > It looks like this is a project whose vice-chairman is one of the co-creators of the Rainbow cryptosystem, and they use Rainbow, one of the Round 3 finalists in the digital signatures category. It is among three finalists to be considered for standardization in this category at the end of the third round. See NISTIR 8309, https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8309.pdf. I do not believe it has been approved for standardization at this time. For previous discussion on Rainbow in this forum, you should be able to use the Google Groups search functionality.
> > >
> > > Hope this helps!
> > >
> > > Wrenna

On Wed, 13 Oct 2021 at 13:51, s zhang <shezh...@gmail.com> wrote:

> Dear all,
>
> I recently heard about a post-quantum cryptocurrency (abcmint) whose founder claims that the technology used is approved by NIST and is the only solution. I would like to ask you all, can this really be approved and reliable by experts?
>
> Here is the official website of abcmint, which has various information about this cryptocurrency
>
> official: http://www.abcmint.org/
>
> github: https://github.com/abcmint/abcmint
>
> Best regards.
>
> Zang

> --
> 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/f3023c10-89c8-4ca0-ad22-a574ee5a2ed3n%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/58932728-523a-4f9b-85eb-ae1151ccff64n%40list.nist.gov.

From: Ruben Niederhagen <ruben@polycephaly.org> via pqc-forum@list.nist.gov
To: Doge Protocol <dogeprotocol1@gmail.com>
CC: pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] A digital currency that claims to be resistant to quantum computers
Date: Thursday, April 28, 2022 08:22:16 PM ET

---

a

> On Apr 29, 2022, at 02:48, Doge Protocol <dogeprotocol1@gmail.com> wrote:
>
> Point (4) on Rainbow is not necessarily true. Please see paper by Ward Beullens: https://eprint.iacr.org/2022/214.pdf
> Snippet from the paper (snipping off some of the text, since there are formatting issues of power values in the forum editor):
>
> *"We estimate that a key recovery for the SL 1 parameter set of the third-round submission requires only a factor ... <snip>. For the parameter sets targeting NIST security levels 3 and 5, we find that the attack can be improved by combining the new technique with the rectangular MinRank attack of Beullens [4]. "*

The paper goes on in the same paragraph with: „*Estimates of the complexities of the simple and combined attacks against the Rainbow parameter sets submitted to NIST are given in Table 1.*“

From said Table 1 you can see that the impact also of the combined attacks on the higher Rainbow parameter sets 3 and 5 is more moderate than on level 1 by cutting off “only” 20 bits of security from the higher parameter sets, leaving them significantly over the boundary of 128 bits with 157 and 206 bits of security respectively (for the “finals” parameter sets).

Best regards

Ruben

From: Christopher J Peikert <cpeikert@alum.mit.edu> via pqc-forum@list.nist.gov
To: Ruben Niederhagen <ruben@polycephaly.org>
CC: Doge Protocol <dogeprotocol1@gmail.com>, pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] A digital currency that claims to be resistant to quantum computers
Date: Thursday, April 28, 2022 08:34:58 PM ET

On Thu, Apr 28, 2022 at 8:21 PM Ruben Niederhagen <ruben@polycephaly.org> wrote:

> From said Table 1 you can see that the impact also of the combined attacks on the higher Rainbow parameter sets 3 and 5 is more moderate than on level 1 by cutting off “only” 20 bits of security from the higher parameter sets, leaving them significantly over the boundary of 128 bits with 157 and 206 bits of security respectively (for the “finals” parameter sets).

The NIST category 1 boundary is about 2^143 (classical) gates, not 2^128. For category 3 it is about 2^207 gates.

Table 1 gives estimated gate counts for the attacks, so its numbers can be compared against the NIST criteria, though it’s not clear to me whether/how memory figures into these numbers.

Sincerely yours in cryptography,

Chris

--
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/CACOo0Qgs%3DdrSpeGSJNLHia5Pn9B%3D-%2B7qjVmGUEC-F3qW%3DgWPkg%40mail.gmail.com.