From: ToTheMars ABC <abctothemars@gmail.com> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: [pqc-forum] Why rainbow Signature is the strongest cryptocurrency algorithm?
Date: Wednesday, June 08, 2022 01:34:45 PM ET

After the introduction of NSM8, everyone should pay attention to the post-quantum signature algorithm. Compared with the major signature algorithms of NIST PQC, only the rainbow signature algorithm is most suitable for decentralized cryptocurrencies. At the same time, the rainbow signature algorithm is based on NP problem, which is mathematically unsolvable, so it is still safe

1 The 8th《National Security Memorandum》

NSM8 from the White House of U.S. , launched on January 19th，2022 which clearly require all agencies of the U.S. to finish something specially in quantum-resistance algorithms , shows it will be the beginning of a new world of quantum resistance times. All cryptos , bitcoin include, will have to upgrade its digital signature algorithm vulnerable to quantum computer to quantum-resistance digital signature algorithms:

https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/

NSM8 said：

(B) Within 60 days of the date of this memorandum, the NSA shall revise and make available to Chief Information Officers the CNSS Advisory Memorandum 01-07 (Information Assurance Cryptographic Equipment Modernization) and any associated enclosures and relevant references regarding modernization planning, use of unsupported encryption, approved mission unique protocols, quantum resistant protocols, and planning for use of quantum resistant cryptography where necessary.

and more：

2 NISTPQC

National Institute of Standards & Technology, NIST, have prepared to be able to resist quantum computing via its NISTPQC project.

So far there're 3 kinds of digital signatures, from NIST, will be probably quantum-resistant.

1st: Hash-based signatures:

XMSS, LMS:

https://csrc.nist.gov/projects/stateful-hash-based-signatures

Sphincs+ and Picnic:

https://csrc.nist.gov/Projects/post-quantum-cryptography/Round-3-Submissions

WOTS+:

https://csrc.nist.gov/glossary/term/wots_plus
RESCUE for StarkWare and Ethereum:
https://eprint.iacr.org/2020/820.pdf
2nd: Lattice:
Falcon & Dilithium：
https://csrc.nist.gov/Projects/post-quantum-cryptography/Round-3-Submissions
3rd: Multivariate:
Rainbow Signature:
https://csrc.nist.gov/Projects/post-quantum-cryptography/Round-3-Submissions

1. Weak points for above 3 kinds of digital signatures:
   1st: hash-based signature:
   《State management of Hash-based signatures》
   https://eprint.iacr.org/2016/357.pdf
   2nd: Lattice-based:
   《Non-randomness of S-unit lattices》
   https://cr.yp.to/papers/spherical-20211023.pdf
   《Report on the Security of LWE: Improved Dual Lattice Attack》
   https://zenodo.org/record/6412487
   3rd: Multivariate:
   《Breaking Rainbow Takes a Weekend on a Laptop》
   https://eprint.iacr.org/2022/214

Given strict requirements of "long-term secure, stable, smaller signature size and actually using cases" for those speicial cryptocurrencies and blockchain scenarios. the conclusion is that Multivariate is PROBABLY ONLY BEST suitable for.
Especially Rainbow Signature:
https://www.pqcrainbow.org/

--

From: Mike Ounsworth <mike.ounsworth@entrust.com> via pqc-forum <pqc-forum@list.nist.gov>
To: ToTheMars ABC <abctothemars@gmail.com>, pqc-forum <pqc-forum@list.nist.gov>
Subject: RE: [EXTERNAL] [pqc-forum] Why rainbow Signature is the strongest cryptocurrency algorithm?
Date: Wednesday, June 08, 2022 02:19:39 PM ET

I'm confused, you say that "Breaking Rainbow Takes a Weekend on a Laptop", and then conclude that Rainbow is best. That does not seem to line up.

—

Mike Ounsworth
Software Security Architect, Entrust

From: pqc-forum@list.nist.gov <pqc-forum@list.nist.gov> On Behalf Of ToTheMars ABC
Sent: June 8, 2022 12:34 PM
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: [EXTERNAL] [pqc-forum] Why rainbow Signature is the strongest cryptocurrency algorithm?

After the introduction of NSM8, everyone should pay attention to the post-quantum signature algorithm. Compared with the major signature algorithms of NIST PQC, only the rainbow signature algorithm is most suitable for decentralized cryptocurrencies. At the same time, the rainbow signature algorithm is based on NP problem, which is mathematically unsolvable, so it is still safe
1 The 8th《National Security Memorandum》
NSM8 from the White House of U.S. , launched on January 19th, 2022 which clearly require all agencies of the U.S. to finish something specially in quantum-resistance algorithms , shows it will be the beginning of a new world of quantum resistance times. All cryptos , bitcoin include, will have to upgrade its digital signature algorithm vulnerable to quantum computer to quantum-resistance digital signature algorithms:

https://gcc02.safelinks.protection.outlook.com/?
url=https%3A%2F%2Furldefense.com%2Fv3%2F__https%3A%2F%2Fwww.whitehouse.gov%2Fbriefing-room%2Fpresidential-actions%2F2022%2F01%2F19%2Fmemorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems%2F__%3B!!FJ-Y8qCqXTj2!
Yfy2pM3rSs5hyBZN9V3WpkNU95Iv-6B6OODd21D0ztNYwgpJnnb0ZzTy1NJ8kaaa5B1SVJ0q_5xatqJDRvCZyhLVZVQ%24&data=05%7C01%7Candrew.regenscheid%40nist.gov%7Cd7cb77f4e1cb4d90eac308da497b722e%7C2ab5d82fd8fa4797a93e054655c61dec%7C1%7C0%7C637903091796116958%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=b58e7s5u0CwizCzsGnEj%2FVK76L727q9K7Mo0l3riy3M%3D&reserved=0

NSM8 said：

(B) Within 60 days of the date of this memorandum, the NSA shall revise and make available to Chief Information Officers the CNSS Advisory Memorandum 01-07 (Information Assurance Cryptographic Equipment Modernization) and any associated enclosures and relevant references regarding modernization planning, use of unsupported encryption, approved mission unique protocols, quantum resistant protocols, and planning for use of quantum resistant cryptography where necessary.

and more：

2 NISTPQC

National Institute of Standards & Technology, NIST, have prepared to be able to resist quantum computing via its NISTPQC project.

So far there're 3 kinds of digital signatures, from NIST, will be probably quantum-resistant.

1st: Hash-based signatures:

XMSS, LMS:

https://gcc02.safelinks.protection.outlook.com/?
url=https%3A%2F%2Furldefense.com%2Fv3%2F__https%3A%2F%2Fcsrc.nist.gov%2Fprojects%2Fstateful-hash-based-signatures__%3B!!FJ-Y8qCqXTj2!
Yfy2pM3rSs5hyBZN9V3WpkNU95Iv-6B6OODd21D0ztNYwgpJnnb0ZzTy1NJ8kaaa5B1SVJ0q_5xatqJDRvCZVSrywV8%24&data=05%7C01%7Candrew.regenscheid%40nist.gov%7Cd7cb77f4e1cb4d90eac308da497b722e%7C2ab5d82fd8fa4797a93e054655c61dec%7C1%7C0%7C637903091796116958%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=HgGNlHFzUOdrhxHQs1TDqlwQRSn5mGghf2HhZ49FeqA%3D&reserved=0

Sphincs+ and Picnic:

https://gcc02.safelinks.protection.outlook.com/?
url=https%3A%2F%2Furldefense.com%2Fv3%2F__https%3A%2F%2Fcsrc.nist.gov%2FProjects%2Fpost-quantum-cryptography%2FRound-3-Submissions__%3B!!FJ-Y8qCqXTj2!
Yfy2pM3rSs5hyBZN9V3WpkNU95Iv-6B6OODd21D0ztNYwgpJnnb0ZzTy1NJ8kaaa5B1SVJ0q_5xatqJDRvCZK
IQ2CiQ%24&data=05%7C01%7Candrew.regenscheid%40nist.gov%7Cd7cb77f4e1cb4d90eac308da
497b722e%7C2ab5d82fd8fa4797a93e054655c61dec%7C1%7C0%7C637903091796116958%7CUnknown%7C
TWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000
%7C%7C%7C&sdata=JgE6zvk2TAOmQrWHTQtbUfwzJOQpUXrEHsAEcD3xkl0%3D&reserved=0

WOTS+:

https://gcc02.safelinks.protection.outlook.com/?
url=https%3A%2F%2Furldefense.com%2Fv3%2F__https%3A%2F%2Fcsrc.nist.gov%2Fglossary%2Fterm%2Fwots_plus__%3B!!FJ-Y8qCqXTj2!
Yfy2pM3rSs5hyBZN9V3WpkNU95Iv-6B6OODd21D0ztNYwgpJnnb0ZzTy1NJ8kaaa5B1SVJ0q_5xatqJDRvCZf
rOu8pQ%24&data=05%7C01%7Candrew.regenscheid%40nist.gov%7Cd7cb77f4e1cb4d90eac308da
497b722e%7C2ab5d82fd8fa4797a93e054655c61dec%7C1%7C0%7C637903091796116958%7CUnknown%7C
TWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000
%7C%7C%7C&sdata=soMsUlrdWN1qocYBhdZCqLUPHJrqAOsM20yZwBsIyos%3D&reserved=0

RESCUE for StarkWare and Ethereum:

https://gcc02.safelinks.protection.outlook.com/?
url=https%3A%2F%2Furldefense.com%2Fv3%2F__https%3A%2F%2Feprint.iacr.org%2F2020%2F820.pdf__%3B!!FJ-Y8qCqXTj2!
Yfy2pM3rSs5hyBZN9V3WpkNU95Iv-6B6OODd21D0ztNYwgpJnnb0ZzTy1NJ8kaaa5B1SVJ0q_5xatqJDRvCZc
xKZBSc%24&data=05%7C01%7Candrew.regenscheid%40nist.gov%7Cd7cb77f4e1cb4d90eac308da
497b722e%7C2ab5d82fd8fa4797a93e054655c61dec%7C1%7C0%7C637903091796116958%7CUnknown%7C
TWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000
%7C%7C%7C&sdata=SbOp%2BhoC00QGwbSPdflvwlnRWft36R374btVZUwjb5g%3D&reserved=0

2nd: Lattice:

Falcon & Dilithium：

https://gcc02.safelinks.protection.outlook.com/?
url=https%3A%2F%2Furldefense.com%2Fv3%2F__https%3A%2F%2Fcsrc.nist.gov%2FProjects%2Fpost-quantum-cryptography%2FRound-3-Submissions__%3B!!FJ-Y8qCqXTj2!
Yfy2pM3rSs5hyBZN9V3WpkNU95Iv-6B6OODd21D0ztNYwgpJnnb0ZzTy1NJ8kaaa5B1SVJ0q_5xatqJDRvCZK
IQ2CiQ%24&data=05%7C01%7Candrew.regenscheid%40nist.gov%7Cd7cb77f4e1cb4d90eac308da
497b722e%7C2ab5d82fd8fa4797a93e054655c61dec%7C1%7C0%7C637903091796116958%7CUnknown%7C
TWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000
%7C%7C%7C&sdata=JgE6zvk2TAOmQrWHTQtbUfwzJOQpUXrEHsAEcD3xkl0%3D&reserved=0

3rd: Multivariate:

Rainbow Signature:

https://gcc02.safelinks.protection.outlook.com/?
url=https%3A%2F%2Furldefense.com%2Fv3%2F__https%3A%2F%2Fcsrc.nist.gov%2FProjects%2Fpost-quantum-cryptography%2FRound-3-Submissions__%3B!!FJ-Y8qCqXTj2!
Yfy2pM3rSs5hyBZN9V3WpkNU95Iv-6B6OODd21D0ztNYwgpJnnb0ZzTy1NJ8kaaa5B1SVJ0q_5xatqJDRvCZKIQ2CiQ%24&data=05%7C01%7Candrew.regenscheid%40nist.gov%7Cd7cb77f4e1cb4d90eac308da497b722e%7C2ab5d82fd8fa4797a93e054655c61dec%7C1%7C0%7C637903091796116958%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=JgE6zvk2TAOmQrWHTQtbUfwzJOQpUXrEHsAEcD3xkl0%3D&reserved=0

1. Weak points for above 3 kinds of digital signatures:

1st: hash-based signature:

《State management of Hash-based signatures》

https://gcc02.safelinks.protection.outlook.com/?
url=https%3A%2F%2Furldefense.com%2Fv3%2F__https%3A%2F%2Feprint.iacr.org%2F2016%2F357.pdf__%3B!!FJ-Y8qCqXTj2!
Yfy2pM3rSs5hyBZN9V3WpkNU95Iv-6B6OODd21D0ztNYwgpJnnb0ZzTy1NJ8kaaa5B1SVJ0q_5xatqJDRvCZvpyPVZE%24&data=05%7C01%7Candrew.regenscheid%40nist.gov%7Cd7cb77f4e1cb4d90eac308da497b722e%7C2ab5d82fd8fa4797a93e054655c61dec%7C1%7C0%7C637903091796116958%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=VcES1%2F6ukp2AvvsT238Z3MeedCTLblATW31vxpJ%2FFgw%3D&reserved=0

2nd: Lattice-based:

《Non-randomness of S-unit lattices》

https://gcc02.safelinks.protection.outlook.com/?
url=https%3A%2F%2Furldefense.com%2Fv3%2F__https%3A%2F%2Fcr.yp.to%2Fpapers%2Fspherical-20211023.pdf__%3B!!FJ-Y8qCqXTj2!
Yfy2pM3rSs5hyBZN9V3WpkNU95Iv-6B6OODd21D0ztNYwgpJnnb0ZzTy1NJ8kaaa5B1SVJ0q_5xatqJDRvCZLZyV0QI%24&data=05%7C01%7Candrew.regenscheid%40nist.gov%7Cd7cb77f4e1cb4d90eac308da497b722e%7C2ab5d82fd8fa4797a93e054655c61dec%7C1%7C0%7C637903091796116958%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=qhXthvYg%2Fa5Bem%2Bi9%2F62INgyAfNwWni%2F1C5YnakA5gY%3D&reserved=0

《Report on the Security of LWE: Improved Dual Lattice Attack》

https://gcc02.safelinks.protection.outlook.com/?
url=https%3A%2F%2Furldefense.com%2Fv3%2F__https%3A%2F%2Fzenodo.org%2Frecord%2F6412487__%3B!!FJ-Y8qCqXTj2!
Yfy2pM3rSs5hyBZN9V3WpkNU95Iv-6B6OODd21D0ztNYwgpJnnb0ZzTy1NJ8kaaa5B1SVJ0q_5xatqJDRvCZGvwiKAs%24&data=05%7C01%7Candrew.regenscheid%40nist.gov%7Cd7cb77f4e1cb4d90eac308da497b722e%7C2ab5d82fd8fa4797a93e054655c61dec%7C1%7C0%7C637903091796116958%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=wWyUhcevTu8FktQakJWf7%2BvrDlEfBHsrdieDqhIfg%2F4%3D&reserved=0

3rd: Multivariate:

《Breaking Rainbow Takes a Weekend on a Laptop》

https://gcc02.safelinks.protection.outlook.com/?
url=https%3A%2F%2Furldefense.com%2Fv3%2F__https%3A%2F%2Feprint.iacr.org%2F2022%2F214_
_%3B!!FJ-Y8qCqXTj2!
Yfy2pM3rSs5hyBZN9V3WpkNU95Iv-6B6OODd21D0ztNYwgpJnnb0ZzTy1NJ8kaaa5B1SVJ0q_5xatqJDRvCZD
NTzn5Y%24&data=05%7C01%7Candrew.regenscheid%40nist.gov%7Cd7cb77f4e1cb4d90eac308da
497b722e%7C2ab5d82fd8fa4797a93e054655c61dec%7C1%7C0%7C637903091796116958%7CUnknown%7C
TWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000
%7C%7C%7C&sdata=v9DLlAoLC85P9Qq%2FWC0qJKYr5HfF4qhFnBVUPQ8n4mU%3D&reserved=0
Given strict requirements of "long-term secure, stable, smaller signature size and
actually using cases" for those speicial cryptocurrencies and blockchain scenarios.
the conclusion is that Multivariate is PROBABLY ONLY BEST suitable for.
Especially Rainbow Signature:
https://gcc02.safelinks.protection.outlook.com/?
url=https%3A%2F%2Furldefense.com%2Fv3%2F__https%3A%2F%2Fwww.pqcrainbow.org%2F__%3B!!
FJ-Y8qCqXTj2!
Yfy2pM3rSs5hyBZN9V3WpkNU95Iv-6B6OODd21D0ztNYwgpJnnb0ZzTy1NJ8kaaa5B1SVJ0q_5xatqJDRvCZ7
LfAb8E%24&data=05%7C01%7Candrew.regenscheid%40nist.gov%7Cd7cb77f4e1cb4d90eac308da
497b722e%7C2ab5d82fd8fa4797a93e054655c61dec%7C1%7C0%7C637903091796116958%7CUnknown%7C
TWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000
%7C%7C%7C&sdata=lQR9zzKLcDCEk4pGnhidpXFHSjiBGxAeQ96dLSPyifk%3D&reserved=0
--
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
mailto:pqc-forum+unsubscribe@list.nist.gov.
To view this discussion on the web visit https://
gcc02.safelinks.protection.outlook.com/?
url=https%3A%2F%2Furldefense.com%2Fv3%2F__https%3A%2F%2Fgroups.google.com%2Fa%2Flist.
nist.gov%2Fd%2Fmsgid%2Fpqc-
forum%2F92d7cf64-8efb-46d6-83c2-88b221f4c836n*40list.nist.gov%3Futm_medium%3Demail%26
utm_source%3Dfooter__%3BJQ!!FJ-Y8qCqXTj2!
Yfy2pM3rSs5hyBZN9V3WpkNU95Iv-6B6OODd21D0ztNYwgpJnnb0ZzTy1NJ8kaaa5B1SVJ0q_5xatqJDRvCZq
RxDlsg%24&data=05%7C01%7Candrew.regenscheid%40nist.gov%7Cd7cb77f4e1cb4d90eac308da
497b722e%7C2ab5d82fd8fa4797a93e054655c61dec%7C1%7C0%7C637903091796116958%7CUnknown%7C
TWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000
%7C%7C%7C&sdata=bJJVymNP%2BuEbSrxZuaxtndpr2yq7XAlJ9ONsgPHiKt4%3D&reserved=0.

--

From: truth-seeker earth <jms.monitoring@gmail.com> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
CC: abctot...@gmail.com <abctothemars@gmail.com>
Subject: [pqc-forum] Re: Why rainbow Signature is the strongest cryptocurrency algorithm?
Date: Thursday, June 09, 2022 09:29:43 PM ET

This sounds very much just like another poor attempt at doing marketing for the ABC Mint cryptocurrency https://bitcointalk.org/index.php?topic=5103397.0

Best regards

On Thursday, June 9, 2022 at 2:33:52 AM UTC+9 abctot...@gmail.com wrote:

> After the introduction of NSM8, everyone should pay attention to the post-quantum signature algorithm. Compared with the major signature algorithms of NIST PQC, only the rainbow signature algorithm is most suitable for decentralized cryptocurrencies. At the same time, the rainbow signature algorithm is based on NP problem, which is mathematically unsolvable, so it is still safe
> 1 The 8th《National Security Memorandum》
> NSM8 from the White House of U.S. , launched on January 19th，2022 which clearly require all agencies of the U.S. to finish something specially in quantum-resistance algorithms , shows it will be the beginning of a new world of quantum resistance times. All cryptos , bitcoin include, will have to upgrade its digital signature algorithm vulnerable to quantum computer to quantum-resistance digital signature algorithms:
> https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/
> NSM8 said：
> (B) Within 60 days of the date of this memorandum, the NSA shall revise and make available to Chief Information Officers the CNSS Advisory Memorandum 01-07 (Information Assurance Cryptographic Equipment Modernization) and any associated enclosures and relevant references regarding modernization planning, use of unsupported encryption, approved mission unique protocols, quantum resistant protocols, and planning for use of quantum resistant cryptography where necessary.
> and more：
> 2 NISTPQC

National Institute of Standards & Technology, NIST, have prepared to be able to resist quantum computing via its NISTPQC project.
So far there're 3 kinds of digital signatures, from NIST, will be probably quantum-resistant.
1st: Hash-based signatures:
XMSS, LMS:
https://csrc.nist.gov/projects/stateful-hash-based-signatures
Sphincs+ and Picnic:
https://csrc.nist.gov/Projects/post-quantum-cryptography/Round-3-Submissions
WOTS+:
https://csrc.nist.gov/glossary/term/wots_plus
RESCUE for StarkWare and Ethereum:
https://eprint.iacr.org/2020/820.pdf
2nd: Lattice:
Falcon & Dilithium：
https://csrc.nist.gov/Projects/post-quantum-cryptography/Round-3-Submissions
3rd: Multivariate:
Rainbow Signature:
https://csrc.nist.gov/Projects/post-quantum-cryptography/Round-3-Submissions

1. Weak points for above 3 kinds of digital signatures:
   1st: hash-based signature:
   《State management of Hash-based signatures》
   https://eprint.iacr.org/2016/357.pdf
   2nd: Lattice-based:
   《Non-randomness of S-unit lattices》
   https://cr.yp.to/papers/spherical-20211023.pdf
   《Report on the Security of LWE: Improved Dual Lattice Attack》
   https://zenodo.org/record/6412487
   3rd: Multivariate:
   《Breaking Rainbow Takes a Weekend on a Laptop》
   https://eprint.iacr.org/2022/214

Given strict requirements of "long-term secure, stable, smaller signature size and actually using cases" for those speicial cryptocurrencies and blockchain scenarios. the conclusion is that Multivariate is PROBABLY ONLY BEST suitable for.
Especially Rainbow Signature:
https://www.pqcrainbow.org/

--

From: ToTheMars ABC <abctothemars@gmail.com> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
CC: jms.mon...@gmail.com <jms.monitoring@gmail.com>, ToTheMars ABC <abctothemars@gmail.com>
Subject: [pqc-forum] Re: Why rainbow Signature is the strongest cryptocurrency algorithm?
Date: Saturday, June 11, 2022 09:30:39 AM ET

Abcmint is an experimental new digital currency who has been operating safely for more than four years.

Official website: http://www.abcmint.org/
Source code: https://github.com/abcmint/abcmint

> This sounds very much just like another poor attempt at doing marketing for the ABC Mint cryptocurrency https://bitcointalk.org/index.php?topic=5103397.0
>
> Best regards
>
> On Thursday, June 9, 2022 at 2:33:52 AM UTC+9 abctot...@gmail.com wrote:
>
> > After the introduction of NSM8, everyone should pay attention to the post-quantum signature algorithm. Compared with the major signature algorithms of NIST PQC, only the rainbow signature algorithm is most suitable for decentralized cryptocurrencies. At the same time, the rainbow signature algorithm is based on NP problem, which is mathematically unsolvable, so it is still safe
> > 1 The 8th《National Security Memorandum》
> > NSM8 from the White House of U.S. , launched on January 19th，2022 which clearly require all agencies of the U.S. to finish something specially in quantum-resistance algorithms , shows it will be the beginning of a new world of quantum resistance times. All cryptos , bitcoin include, will have to upgrade its digital signature algorithm vulnerable to quantum computer to quantum-resistance digital signature algorithms:
> > https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/
> > NSM8 said：
> > (B) Within 60 days of the date of this memorandum, the NSA shall revise and make available to Chief Information Officers the CNSS Advisory Memorandum 01-07 (Information Assurance Cryptographic Equipment Modernization) and any associated

enclosures and relevant references regarding modernization planning, use of unsupported encryption, approved mission unique protocols, quantum resistant protocols, and planning for use of quantum resistant cryptography where necessary.
and more：
2 NISTPQC
National Institute of Standards & Technology, NIST, have prepared to be able to resist quantum computing via its NISTPQC project.
So far there're 3 kinds of digital signatures, from NIST, will be probably quantum-resistant.
1st: Hash-based signatures:
XMSS, LMS:
https://csrc.nist.gov/projects/stateful-hash-based-signatures
Sphincs+ and Picnic:
https://csrc.nist.gov/Projects/post-quantum-cryptography/Round-3-Submissions
WOTS+:
https://csrc.nist.gov/glossary/term/wots_plus
RESCUE for StarkWare and Ethereum:
https://eprint.iacr.org/2020/820.pdf
2nd: Lattice:
Falcon & Dilithium：
https://csrc.nist.gov/Projects/post-quantum-cryptography/Round-3-Submissions
3rd: Multivariate:
Rainbow Signature:
https://csrc.nist.gov/Projects/post-quantum-cryptography/Round-3-Submissions

1. Weak points for above 3 kinds of digital signatures:
   1st: hash-based signature:
   《State management of Hash-based signatures》
   https://eprint.iacr.org/2016/357.pdf
   2nd: Lattice-based:
   《Non-randomness of S-unit lattices》
   https://cr.yp.to/papers/spherical-20211023.pdf
   《Report on the Security of LWE: Improved Dual Lattice Attack》
   https://zenodo.org/record/6412487
   3rd: Multivariate:
   《Breaking Rainbow Takes a Weekend on a Laptop》
   https://eprint.iacr.org/2022/214

> Given strict requirements of "long-term secure, stable, smaller signature size and actually using cases" for those speicial cryptocurrencies and blockchain scenarios. the conclusion is that Multivariate is PROBABLY ONLY BEST suitable for.
> Especially Rainbow Signature:
> https://www.pqcrainbow.org/

--

From: andy yi <hy8196695@gmail.com> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
CC: abctot...@gmail.com <abctothemars@gmail.com>, jms.mon...@gmail.com <jms.monitoring@gmail.com>
Subject: [pqc-forum] Re: Why rainbow Signature is the strongest cryptocurrency algorithm?
Date: Sunday, June 12, 2022 01:47:58 AM ET

It seems to be a marketing of the cryptocurrency Abc, if so, the tidecoin may be the bitcoin of the post-quantum era, and its current situation is very similar to the early days of bitcoin.
First of all, the code base of abc has not been maintained for 4 years, the L1 parameters of the rainbow algorithm have also been cracked, and the upgrade is still in the future. In addition, there is no engineering practice case for the rainbow algorithm, and the links to the parameter set submitted by the rainbow team to NIST have all expired. It cannot be opened and no one can contact the rainbow team, which may indicate that the entire multivariate algorithm is insecure.
Then, Tidecoin uses the falcon-512 algorithm. The falcon algorithm is very safe and runs fast. There are only 21 million in total, and it has been running well and stably for nearly 2 years. The production reduction cycle completely matches the NIST roadmap, and there are also clear route planning. Now its ownership has been transferred to the community, it is completely decentralized, there are already Korean, Chinese, English, Russian communities, and it is listed on the exchange, and it works well. In addition, Tidecoin is attracting developers and others to join the world. Anyone can apply to join, but because there is no capital investment, the development is slow. But I'm sure it will shine

Official website: www.tidecoin.co
Source code: https://github.com/tidecoin
whitepaper: https://github.com/tidecoin-old/whitepaper
falcon sign: https://www.falcon-sign.info/

在2022年6月11日星期六 UTC+8 21:29:46<abctot...@gmail.com> 写道：

> Abcmint is an experimental new digital currency who has been operating safely for more than four years.
>
> Official website: http://www.abcmint.org/
> Source code: https://github.com/abcmint/abcmint

This sounds very much just like another poor attempt at doing marketing for the ABC Mint cryptocurrency https://bitcointalk.org/index.php?topic=5103397.0

Best regards

On Thursday, June 9, 2022 at 2:33:52 AM UTC+9 abctot...@gmail.com wrote:

> After the introduction of NSM8, everyone should pay attention to the post-quantum signature algorithm. Compared with the major signature algorithms of NIST PQC, only the rainbow signature algorithm is most suitable for decentralized cryptocurrencies. At the same time, the rainbow signature algorithm is based on NP problem, which is mathematically unsolvable, so it is still safe
> 1 The 8th《National Security Memorandum》
> NSM8 from the White House of U.S. , launched on January 19th，2022 which clearly require all agencies of the U.S. to finish something specially in quantum-resistance algorithms , shows it will be the beginning of a new world of quantum resistance times. All cryptos , bitcoin include, will have to upgrade its digital signature algorithm vulnerable to quantum computer to quantum-resistance digital signature algorithms:
> https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/
> NSM8 said：
> (B) Within 60 days of the date of this memorandum, the NSA shall revise and make available to Chief Information Officers the CNSS Advisory Memorandum 01-07 (Information Assurance Cryptographic Equipment Modernization) and any associated enclosures and relevant references regarding modernization planning, use of unsupported encryption, approved mission unique protocols, quantum resistant protocols, and planning for use of quantum resistant cryptography where necessary.
> and more：
> 2 NISTPQC
> National Institute of Standards & Technology, NIST, have prepared to be able to resist quantum computing via its NISTPQC project.
> So far there're 3 kinds of digital signatures, from NIST, will be probably quantum-resistant.
> 1st: Hash-based signatures:
> XMSS, LMS:
> https://csrc.nist.gov/projects/stateful-hash-based-signatures

> > Sphincs+ and Picnic:
> > https://csrc.nist.gov/Projects/post-quantum-cryptography/Round-3-Submissions
> > WOTS+:
> > https://csrc.nist.gov/glossary/term/wots_plus
> > RESCUE for StarkWare and Ethereum:
> > https://eprint.iacr.org/2020/820.pdf
> > 2nd: Lattice:
> > Falcon & Dilithium：
> > https://csrc.nist.gov/Projects/post-quantum-cryptography/Round-3-Submissions
> > 3rd: Multivariate:
> > Rainbow Signature:
> > https://csrc.nist.gov/Projects/post-quantum-cryptography/Round-3-Submissions
> >
> > 1. Weak points for above 3 kinds of digital signatures:
> > 1st: hash-based signature:
> > 《State management of Hash-based signatures》
> > https://eprint.iacr.org/2016/357.pdf
> > 2nd: Lattice-based:
> > 《Non-randomness of S-unit lattices》
> > https://cr.yp.to/papers/spherical-20211023.pdf
> > 《Report on the Security of LWE: Improved Dual Lattice Attack》
> > https://zenodo.org/record/6412487
> > 3rd: Multivariate:
> > 《Breaking Rainbow Takes a Weekend on a Laptop》
> > https://eprint.iacr.org/2022/214
> >
> > Given strict requirements of "long-term secure, stable, smaller signature size and actually using cases" for those speicial cryptocurrencies and blockchain scenarios. the conclusion is that Multivariate is PROBABLY ONLY BEST suitable for.
> > Especially Rainbow Signature:
> > https://www.pqcrainbow.org/

--

To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/0d9fa430-3603-4546-a37e-f99bb83fbf75n%40list.nist.gov.

From: andy yi <hy8196695@gmail.com> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
CC: abctot...@gmail.com <abctothemars@gmail.com>, jms.mon...@gmail.com <jms.monitoring@gmail.com>
Subject: [pqc-forum] Re: Why rainbow Signature is the strongest cryptocurrency algorithm?
Date: Sunday, June 12, 2022 08:23:39 PM ET

It seems to be a marketing of the cryptocurrency Abc, if so, the tidecoin may be the bitcoin of the post-quantum era, and its current situation is very similar to the early days of bitcoin. Tidecoin uses the falcon-512 algorithm. The falcon algorithm is very safe and runs fast. There are only 21 million in total, and it has been running well and stably for nearly 2 years. The production reduction cycle completely matches the NIST roadmap, and there are also clear route planning. Now its ownership has been transferred to the community, it is completely decentralized, and it works well. In addition, Tidecoin is attracting developers and others to join the world. Anyone can apply to join, but because there is no capital investment, the development is slow. But I'm sure it will shine

Official website: www.tidecoin.co
Source code: https://github.com/tidecoin
whitepaper: https://github.com/tidecoin-old/whitepaper
falcon sign: https://www.falcon-sign.info/

在2022年6月11日星期六 UTC+8 21:29:46<abctot...@gmail.com> 写道：

> Abcmint is an experimental new digital currency who has been operating safely for more than four years.
>
> Official website: http://www.abcmint.org/
> Source code: https://github.com/abcmint/abcmint
>
> > This sounds very much just like another poor attempt at doing marketing for the ABC Mint cryptocurrency https://bitcointalk.org/index.php?topic=5103397.0
> >
> > Best regards
> >
> > On Thursday, June 9, 2022 at 2:33:52 AM UTC+9 abctot...@gmail.com wrote:

After the introduction of NSM8, everyone should pay attention to the post-quantum signature algorithm. Compared with the major signature algorithms of NIST PQC, only the rainbow signature algorithm is most suitable for decentralized cryptocurrencies. At the same time, the rainbow signature algorithm is based on NP problem, which is mathematically unsolvable, so it is still safe

1 The 8th《National Security Memorandum》

NSM8 from the White House of U.S. , launched on January 19th，2022 which clearly require all agencies of the U.S. to finish something specially in quantum-resistance algorithms , shows it will be the beginning of a new world of quantum resistance times. All cryptos , bitcoin include, will have to upgrade its digital signature algorithm vulnerable to quantum computer to quantum-resistance digital signature algorithms:

https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/

NSM8 said：

(B) Within 60 days of the date of this memorandum, the NSA shall revise and make available to Chief Information Officers the CNSS Advisory Memorandum 01-07 (Information Assurance Cryptographic Equipment Modernization) and any associated enclosures and relevant references regarding modernization planning, use of unsupported encryption, approved mission unique protocols, quantum resistant protocols, and planning for use of quantum resistant cryptography where necessary.

and more：

2 NISTPQC

National Institute of Standards & Technology, NIST, have prepared to be able to resist quantum computing via its NISTPQC project.

So far there're 3 kinds of digital signatures, from NIST, will be probably quantum-resistant.

1st: Hash-based signatures:

XMSS, LMS:

https://csrc.nist.gov/projects/stateful-hash-based-signatures

Sphincs+ and Picnic:

https://csrc.nist.gov/Projects/post-quantum-cryptography/Round-3-Submissions

WOTS+:

https://csrc.nist.gov/glossary/term/wots_plus

RESCUE for StarkWare and Ethereum:

https://eprint.iacr.org/2020/820.pdf

2nd: Lattice:

> > Falcon & Dilithium：
> > https://csrc.nist.gov/Projects/post-quantum-cryptography/Round-3-Submissions
> > 3rd: Multivariate:
> > Rainbow Signature:
> > https://csrc.nist.gov/Projects/post-quantum-cryptography/Round-3-Submissions
> >
> > 1. Weak points for above 3 kinds of digital signatures:
> >   1st: hash-based signature:
> >   《State management of Hash-based signatures》
> >   https://eprint.iacr.org/2016/357.pdf
> >   2nd: Lattice-based:
> >   《Non-randomness of S-unit lattices》
> >   https://cr.yp.to/papers/spherical-20211023.pdf
> >   《Report on the Security of LWE: Improved Dual Lattice Attack》
> >   https://zenodo.org/record/6412487
> >   3rd: Multivariate:
> >   《Breaking Rainbow Takes a Weekend on a Laptop》
> >   https://eprint.iacr.org/2022/214
> >
> > Given strict requirements of "long-term secure, stable, smaller signature size and actually using cases" for those speicial cryptocurrencies and blockchain scenarios. the conclusion is that Multivariate is PROBABLY ONLY BEST suitable for.
> > Especially Rainbow Signature:
> > https://www.pqcrainbow.org/

--

From: ToTheMars ABC <abctothemars@gmail.com> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
CC: hy81...@gmail.com <hy8196695@gmail.com>, ToTheMars ABC <abctothemars@gmail.com>, jms.mon...@gmail.com <jms.monitoring@gmail.com>
Subject: [pqc-forum] Re: Why rainbow Signature is the strongest cryptocurrency algorithm?
Date: Monday, July 04, 2022 06:05:39 AM ET

In response to your comment that "rainbow algorithm have also been cracked"
Abc Chairman Liu Jin has said "Anyone who cracks Abc's rainbow signature will be awarded a $400,000 bonus", have you heard of anyone getting it so far?

Also you mentioned "the code base of Abc has not been maintained for 4 years".
Mr. Liu Jin has said many times that their project is recognized by many cryptographers as stable and secure, so why does a secure and stable project need to be maintained? Could it be that you found the vulnerability of abc?

Also you mentioned "In addition, there is no engineering practice case for the rainbow algorithm, and the links to the parameter set submitted by the rainbow team to NIST have all expired."

I don't understand why you say you can't contact the team, whether it's the rainbow signature practice team, or the abc team, many people are contacted, for example, Mr. Liu Jin and Ruben Niederhagen of the abc team, or Professor Bo-Yin Yang of the rainbow signature team can be contacted.

Mr. Liu Jin, Chairman of Abc
twitter: https://twitter.com/amisrepresented
linkedin: https://tw.linkedin.com/in/liujinabcardo?trk=org-employees
Abc official: http://abcmint.org

ABC Foundation member Ruben Niederhagen: http://polycephaly.org

Rainbow Signature and uov team Prof. Bo-Yin Yang: moscito@gmail.com

As for your statement that "Tidecoin uses the falcon-512 algorithm"
Mr. Liu said, "The falcon algorithm is a very controversial algorithm, which is suspected to be related to a plagiarist, and the algorithm is not secure." Is it reliable that Tidecoin uses an

insecure and controversial algorithm?

Finally, if you want to learn more about pqc, you can follow Mr. Liu Jin on twitter: https://twitter.com/amisrepresented

andy yi <hy8196695@gmail.com> 于2022年6月12日周日 05:47写道：

> It seems to be a marketing of the cryptocurrency Abc, if so, the tidecoin may be the bitcoin of the post-quantum era, and its current situation is very similar to the early days of bitcoin. First of all, the code base of abc has not been maintained for 4 years, the L1 parameters of the rainbow algorithm have also been cracked, and the upgrade is still in the future. In addition, there is no engineering practice case for the rainbow algorithm, and the links to the parameter set submitted by the rainbow team to NIST have all expired. It cannot be opened and no one can contact the rainbow team, which may indicate that the entire multivariate algorithm is insecure.
> Then, Tidecoin uses the falcon-512 algorithm. The falcon algorithm is very safe and runs fast. There are only 21 million in total, and it has been running well and stably for nearly 2 years. The production reduction cycle completely matches the NIST roadmap, and there are also clear route planning. Now its ownership has been transferred to the community, it is completely decentralized, there are already Korean, Chinese, English, Russian communities, and it is listed on the exchange, and it works well. In addition, Tidecoin is attracting developers and others to join the world. Anyone can apply to join, but because there is no capital investment, the development is slow. But I'm sure it will shine
>
> Official website: www.tidecoin.co
> Source code: https://github.com/tidecoin
> whitepaper: https://github.com/tidecoin-old/whitepaper
> falcon sign: https://www.falcon-sign.info/

From: ToTheMars ABC <abctothemars@gmail.com> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
CC: ToTheMars ABC <abctothemars@gmail.com>, hy81...@gmail.com <hy8196695@gmail.com>, jms.mon...@gmail.com <jms.monitoring@gmail.com>
Subject: [pqc-forum] Re: Why rainbow Signature is the strongest cryptocurrency algorithm?
Date: Monday, July 04, 2022 06:13:46 AM ET

Mr. Liu Jin predicts that in the next few decades, the only truly usable digital signature solution that can resist quantum computer cracking is the rainbow signature.

在2022年7月4日星期一 UTC 10:05:28<ToTheMars ABC> 写道：

> In response to your comment that "rainbow algorithm have also been cracked"
> Abc Chairman Liu Jin has said "Anyone who cracks Abc's rainbow signature will be awarded a $400,000 bonus", have you heard of anyone getting it so far?
>
> Also you mentioned "the code base of Abc has not been maintained for 4 years".
> Mr. Liu Jin has said many times that their project is recognized by many cryptographers as stable and secure, so why does a secure and stable project need to be maintained? Could it be that you found the vulnerability of abc?
>
> Also you mentioned "In addition, there is no engineering practice case for the rainbow algorithm, and the links to the parameter set submitted by the rainbow team to NIST have all expired."
>
> I don't understand why you say you can't contact the team, whether it's the rainbow signature practice team, or the abc team, many people are contacted, for example, Mr. Liu Jin and Ruben Niederhagen of the abc team, or Professor Bo-Yin Yang of the rainbow signature team can be contacted.
>
> Mr. Liu Jin, Chairman of Abc
> twitter: https://twitter.com/amisrepresented
> linkedin: https://tw.linkedin.com/in/liujinabcardo?trk=org-employees
> Abc official: http://abcmint.org
>
> ABC Foundation member Ruben Niederhagen: http://polycephaly.org
>
> Rainbow Signature and uov team Prof. Bo-Yin Yang: mos...@gmail.com

As for your statement that "Tidecoin uses the falcon-512 algorithm"
Mr. Liu said, "The falcon algorithm is a very controversial algorithm, which is suspected to be related to a plagiarist, and the algorithm is not secure." Is it reliable that Tidecoin uses an insecure and controversial algorithm?

Finally, if you want to learn more about pqc, you can follow Mr. Liu Jin on twitter: https://twitter.com/amisrepresented

andy yi <hy81...@gmail.com> 于2022年6月12日周日 05:47写道：

> It seems to be a marketing of the cryptocurrency Abc, if so, the tidecoin may be the bitcoin of the post-quantum era, and its current situation is very similar to the early days of bitcoin.
> First of all, the code base of abc has not been maintained for 4 years, the L1 parameters of the rainbow algorithm have also been cracked, and the upgrade is still in the future. In addition, there is no engineering practice case for the rainbow algorithm, and the links to the parameter set submitted by the rainbow team to NIST have all expired. It cannot be opened and no one can contact the rainbow team, which may indicate that the entire multivariate algorithm is insecure.
> Then, Tidecoin uses the falcon-512 algorithm. The falcon algorithm is very safe and runs fast. There are only 21 million in total, and it has been running well and stably for nearly 2 years. The production reduction cycle completely matches the NIST roadmap, and there are also clear route planning. Now its ownership has been transferred to the community, it is completely decentralized, there are already Korean, Chinese, English, Russian communities, and it is listed on the exchange, and it works well. In addition, Tidecoin is attracting developers and others to join the world. Anyone can apply to join, but because there is no capital investment, the development is slow. But I'm sure it will shine
>
> Official website: www.tidecoin.co
> Source code: https://github.com/tidecoin
> whitepaper: https://github.com/tidecoin-old/whitepaper
> falcon sign: https://www.falcon-sign.info/

--

From: Ruben Niederhagen <ruben@polycephaly.org> via pqc-forum@list.nist.gov
To: ToTheMars ABC <abctothemars@gmail.com>, pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] Re: Why rainbow Signature is the strongest cryptocurrency algorithm?
Date: Monday, July 04, 2022 08:15:43 AM ET

On 04/07/2022 18:05, ToTheMars ABC wrote:
> ABC Foundation member Ruben Niederhagen: https://
gcc02.safelinks.protection.outlook.com/?
url=http%3A%2F%2Fpolycephaly.org%2F&data=05%7C01%7Cyi-
kai.liu%40nist.gov%7C59879da0e360436dc7f808da5db6e87c%7C2ab5d82fd8fa4797a93e054655c61
dec%7C1%7C0%7C637925337435315370%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoi
V2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=YaUjSR%2FzPCeyC%2F0P
%2FQvHLDuSFEfH%2FYKIf9lHhMIcciI%3D&reserved=0

Just for the record: I am not member of the ABC Foundation and I am also
not affiliated with any other cryptocurrency.

Best regards
   Ruben

--
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/4413fdbd-7296-81df-74f6-cf419a74a45b%40polycephaly.org.

From: ToTheMars ABC <abctothemars@gmail.com> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
CC: Ruben Niederhagen <ruben@polycephaly.org>, ToTheMars ABC <abctothemars@gmail.com>
Subject: Re: [pqc-forum] Re: Why rainbow Signature is the strongest cryptocurrency algorithm?
Date: Monday, July 04, 2022 10:56:15 AM ET

I'm sorry, but the chairman of the ABC Foundation has mentioned your relationship with him many times, and some people in the ABC community have contacted you, so everyone in the ABC community has mistaken you for a member of the ABC Foundation.

在2022年7月4日星期一 UTC 12:15:12<Ruben Niederhagen> 写道：

> On 04/07/2022 18:05, ToTheMars ABC wrote:
> > ABC Foundation member Ruben Niederhagen: http://polycephaly.org
>
> Just for the record: I am not member of the ABC Foundation and I am also
> not affiliated with any other cryptocurrency.
>
> Best regards
> Ruben

From: Matthias Kannwischer <m.kannwischer@gmail.com> via pqc-forum@list.nist.gov
To: ToTheMars ABC <abctothemars@gmail.com>, pqc-forum <pqc-forum@list.nist.gov>
CC: Lorenz Panny <lorenz@yx7.cc>
Subject: Re: [pqc-forum] Re: Why rainbow Signature is the strongest cryptocurrency algorithm?
Date: Thursday, July 07, 2022 03:08:13 AM ET

Dear ToTheMars ABC, dear all,

On Mon, 4 Jul 2022 at 18:05, ToTheMars ABC <abctothemars@gmail.com> wrote:

> In response to your comment that "rainbow algorithm have also been cracked"
> Abc Chairman Liu Jin has said "Anyone who cracks Abc's rainbow signature will be awarded a $400,000 bonus", have you heard of anyone getting it so far?

as has been pointed out before, the level-1 parameter sets of Rainbow are practically broken by https://ia.cr/2022/214.
This obviously also applies to the Rainbow(16,32,32,32) instance used in Abcmint.

We have successfully recovered the secret key corresponding to the public key with address 84cJso7keg6SHW4vbNVbXccimCZrz7WoESXTtw12b5UsWqmm5.
This address is one of the wealthiest on the chain with a balance of 9M ABC. There is only one address with a higher balance, but as it has no outgoing transactions, we don't know the public key.

The private key was recovered within a few hours of wall-clock time using a slightly tweaked version of Ward Beullens' attack software (which in turn makes use of Ruben Niederhagen's XL implementation).

The forged signature for the message
"There is no pot of gold at the end of the Rainbow." (ASCII)
is
"TqERiKoFpkDEOEUGrq2WfH/
XvTxP8dzbUxUpD1UyTUyLnVUaZcqW9IV+bTLIuamWS+XVKFcslYHLnxNcjcjnCA==" (Base64)

The Abcmint client does offer functionality to verify signatures like these, but the feature was apparently implemented incorrectly and only allows verifying messages signed with a private key in the user's own wallet. Thus, we instead publish code to verify this signature using the Abcmint codebase as well as our own Sage script:

https://github.com/mkannwischer/breaking-abc

We hope this clears up any remaining doubts about the applicability of the attack to the Abcmint blockchain. Please inform us how to collect the promised $400,000.

Cheers,
Lorenz and Matthias

--

From: andy yi <hy8196695@gmail.com> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
CC: Matthias Kannwischer <m.kannwischer@gmail.com>, Lorenz Panny <lorenz@yx7.cc>, abctot...@gmail.com <abctothemars@gmail.com>
Subject: Re: [pqc-forum] Re: Why rainbow Signature is the strongest cryptocurrency algorithm?
Date: Thursday, July 07, 2022 05:39:51 AM ET

Today may be a historic day. This is the first time in the history of cryptocurrency that a cryptocurrency has been cracked because of its encryption algorithm. I think this is also a preview of Q-Day, so I hope that abc can be upgraded as soon as possible.

在2022年7月7日星期四 UTC+8 15:08:03<Matthias Kannwischer> 写道：

> Dear ToTheMars ABC, dear all,
>
> On Mon, 4 Jul 2022 at 18:05, ToTheMars ABC <abctot...@gmail.com> wrote:
>
> > In response to your comment that "rainbow algorithm have also been cracked"
> > Abc Chairman Liu Jin has said "Anyone who cracks Abc's rainbow signature will be awarded a $400,000 bonus", have you heard of anyone getting it so far?
> as has been pointed out before, the level-1 parameter sets of Rainbow are practically broken by https://ia.cr/2022/214.
> This obviously also applies to the Rainbow(16,32,32,32) instance used in Abcmint.
>
> We have successfully recovered the secret key corresponding to the public key with address 84cJso7keg6SHW4vbNVbXccimCZrz7WoESXTtw12b5UsWqmm5.
> This address is one of the wealthiest on the chain with a balance of 9M ABC. There is only one address with a higher balance, but as it has no outgoing transactions, we don't know the public key.
>
> The private key was recovered within a few hours of wall-clock time using a slightly tweaked version of Ward Beullens' attack software (which in turn makes use of Ruben Niederhagen's XL implementation).
>
> The forged signature for the message
> "There is no pot of gold at the end of the Rainbow." (ASCII)
> is
> "TqERiKoFpkDEOEUGrq2WfH/

> XvTxP8dzbUxUpD1UyTUyLnVUaZcqW9IV+bTLIuamWS+XVKFcslYHLnxNcjcjnCA==" (Base64)
>
> The Abcmint client does offer functionality to verify signatures like these, but the feature was apparently implemented incorrectly and only allows verifying messages signed with a private key in the user's own wallet. Thus, we instead publish code to verify this signature using the Abcmint codebase as well as our own Sage script:
>
> https://github.com/mkannwischer/breaking-abc
>
> We hope this clears up any remaining doubts about the applicability of the attack to the Abcmint blockchain. Please inform us how to collect the promised $400,000.
>
> Cheers,
> Lorenz and Matthias

From: John Mattsson <john.mattsson@ericsson.com> via pqc-forum <pqc-forum@list.nist.gov>
To: andy yi <hy8196695@gmail.com>, pqc-forum <pqc-forum@list.nist.gov>
CC: Matthias Kannwischer <m.kannwischer@gmail.com>, Lorenz Panny <lorenz@yx7.cc>, abctot...@gmail.com <abctothemars@gmail.com>
Subject: Re: [pqc-forum] Re: Why rainbow Signature is the strongest cryptocurrency algorithm?
Date: Thursday, July 07, 2022 05:56:14 AM ET

I think everything that need to be said about cryptocurrencies and blockchains are summarized in this recent letter to congress.

https://concerned.tech

NIST should publish that letter as a report and shut down this thread advertising specific cryptocurrencies.

Cheers,

John

Get Outlook for iOS

From: pqc-forum@list.nist.gov <pqc-forum@list.nist.gov> on behalf of andy yi <hy8196695@gmail.com>
Sent: Thursday, July 7, 2022 11:39:39 AM
To: pqc-forum <pqc-forum@list.nist.gov>
Cc: Matthias Kannwischer <m.kannwischer@gmail.com>; Lorenz Panny <lorenz@yx7.cc>; abctot...@gmail.com <abctothemars@gmail.com>
Subject: Re: [pqc-forum] Re: Why rainbow Signature is the strongest cryptocurrency algorithm?

Today may be a historic day. This is the first time in the history of cryptocurrency that a cryptocurrency has been cracked because of its encryption algorithm. I think this is also a preview of Q-Day, so I hope that abc can be upgraded as soon as possible.

在2022年7月7日星期四 UTC+8 15:08:03<Matthias Kannwischer> 写道：

> Dear ToTheMars ABC, dear all,
>
> On Mon, 4 Jul 2022 at 18:05, ToTheMars ABC <abctot...@gmail.com> wrote:

> In response to your comment that "rainbow algorithm have also been cracked"
> Abc Chairman Liu Jin has said "Anyone who cracks Abc's rainbow signature will be awarded a $400,000 bonus", have you heard of anyone getting it so far?

as has been pointed out before, the level-1 parameter sets of Rainbow are practically broken by https://ia.cr/2022/214.
This obviously also applies to the Rainbow(16,32,32,32) instance used in Abcmint.

We have successfully recovered the secret key corresponding to the public key with address 84cJso7keg6SHW4vbNVbXccimCZrz7WoESXTtw12b5UsWqmm5.
This address is one of the wealthiest on the chain with a balance of 9M ABC. There is only one address with a higher balance, but as it has no outgoing transactions, we don't know the public key.

The private key was recovered within a few hours of wall-clock time using a slightly tweaked version of Ward Beullens' attack software (which in turn makes use of Ruben Niederhagen's XL implementation).

The forged signature for the message
"There is no pot of gold at the end of the Rainbow." (ASCII)
is
"TqERiKoFpkDEOEUGrq2WfH/
XvTxP8dzbUxUpD1UyTUyLnVUaZcqW9IV+bTLIuamWS+XVKFcslYHLnxNcjcjnCA==" (Base64)

The Abcmint client does offer functionality to verify signatures like these, but the feature was apparently implemented incorrectly and only allows verifying messages signed with a private key in the user's own wallet. Thus, we instead publish code to verify this signature using the Abcmint codebase as well as our own Sage script:

https://github.com/mkannwischer/breaking-abc

We hope this clears up any remaining doubts about the applicability of the attack to the Abcmint blockchain. Please inform us how to collect the promised $400,000.

Cheers,
Lorenz and Matthias

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/aff39ddb-04bb-4644-a0f1-6a9813aa0757n%40list.nist.gov.

From: Ruben Niederhagen <ruben@polycephaly.org> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] Re: Why rainbow Signature is the strongest cryptocurrency algorithm?
Date: Thursday, July 07, 2022 05:58:38 AM ET

On 07/07/2022 15:07, Matthias Kannwischer wrote:
> The private key was recovered within a few hours of wall-clock time using a
> slightly tweaked version of Ward Beullens' attack software (which in turn
> makes use of Ruben Niederhagen's XL implementation).

The XL implementation [1] is joint work of Chen-Mou Cheng, Tung Chou,
Ruben Niederhagen, and Bo-Yin Yang.

Best regards
   Ruben

[1] Chen-Mou Cheng, Tung Chou, Ruben Niederhagen and Bo-Yin Yang:
"Solving Quadratic Equations with XL on Parallel Architectures"
Cryptographic Hardware and Embedded Systems – CHES 2012, Lecture Notes
in Computer Science, Vol. 7428, pp. 356–373. Springer, 2012.
https://link.springer.com/chapter/10.1007/978-3-642-33027-8_21

From: Greg Maxwell <gmaxwell@gmail.com> via pqc-forum@list.nist.gov
To: andy yi <hy8196695@gmail.com>
CC: pqc-forum <pqc-forum@list.nist.gov>, Matthias Kannwischer <m.kannwischer@gmail.com>, Lorenz Panny <lorenz@yx7.cc>, abctot...@gmail.com <abctothemars@gmail.com>
Subject: Re: [pqc-forum] Re: Why rainbow Signature is the strongest cryptocurrency algorithm?
Date: Thursday, July 07, 2022 07:29:41 AM ET

On Thu, Jul 7, 2022 at 9:39 AM andy yi <hy8196695@gmail.com> wrote:

> Today may be a historic day. This is the first time in the history of cryptocurrency that a cryptocurrency has been cracked because of its encryption algorithm.

Not at all. Just to give an example, IOTA's signature scheme suffered signature forgeries. (https://github.com/mit-dci/tangled-curl/blob/master/vuln-iota.md). Interestingly, that is also an example of a "post quantum" scheme that wasn't classically secure (in that case a lamport like signature constructed out of a usenet-kook-grade adhoc hash function). I can think of other signature scheme vulnerabilities in 'cryptocurrencies' too, though less applicable to this list.

It's true that most of the time cryptocurrency cryptographic flaws come from things other than the digital signature algorithm -- but that's merely a result of the fact that there are so many other things their authors can break in their quest to brew novel snake oil flavors. With so many other knobs to twiddle that they usually leave the digital signature part alone.

From: andy yi <hy8196695@gmail.com> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
CC: gmax...@gmail.com <gmaxwell@gmail.com>, pqc-forum <pqc-forum@list.nist.gov>, Matthias Kannwischer <m.kannwischer@gmail.com>, Lorenz Panny <lorenz@yx7.cc>, abctot...@gmail.com <abctothemars@gmail.com>, andy yi <hy8196695@gmail.com>
Subject: Re: [pqc-forum] Re: Why rainbow Signature is the strongest cryptocurrency algorithm?
Date: Thursday, July 07, 2022 08:42:39 PM ET

Even so, I still think it is unique, because the algorithm parameters used in abc are directly provided by Professor Ding, which is different from other cryptocurrencies. It can upgrade the parameters, etc. Rainbow team After submitting the new parameters, abc can complete the upgrade. https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/6bJFzU_h44I

在2022年7月7日星期四 UTC+8 19:29:34<gmax...@gmail.com> 写道：

> On Thu, Jul 7, 2022 at 9:39 AM andy yi <hy81...@gmail.com> wrote:
> > Today may be a historic day. This is the first time in the history of cryptocurrency that a cryptocurrency has been cracked because of its encryption algorithm.
>
> Not at all. Just to give an example, IOTA's signature scheme suffered
> signature forgeries. (
> https://github.com/mit-dci/tangled-curl/blob/master/vuln-iota.md).
> Interestingly, that is also an example of a "post quantum" scheme that
> wasn't classically secure (in that case a lamport like signature
> constructed out of a usenet-kook-grade adhoc hash function). I can
> think of other signature scheme vulnerabilities in 'cryptocurrencies'
> too, though less applicable to this list.
>
> It's true that most of the time cryptocurrency cryptographic flaws
> come from things other than the digital signature algorithm -- but
> that's merely a result of the fact that there are so many other things
> their authors can break in their quest to brew novel snake oil
> flavors. With so many other knobs to twiddle that they usually leave
> the digital signature part alone.

From: mahamadou.x.diarra@gmail.com via pqc-forum@list.nist.gov
To: andy yi <hy8196695@gmail.com>
CC: pqc-forum <pqc-forum@list.nist.gov>, gmax...@gmail.com <gmaxwell@gmail.com>, Matthias Kannwischer <m.kannwischer@gmail.com>, Lorenz Panny <lorenz@yx7.cc>, abctot...@gmail.com <abctothemars@gmail.com>
Subject: Re: [pqc-forum] Re: Why rainbow Signature is the strongest cryptocurrency algorithm?
Date: Thursday, July 07, 2022 11:18:04 PM ET

When & how is rainbow team planning to keep their word and pays up the 400,000$ reward???
Abcmint has been trashed! Keep your word

On Fri, Jul 8, 2022, 09:42 andy yi <hy8196695@gmail.com> wrote:

> Even so, I still think it is unique, because the algorithm parameters used in abc are directly provided by Professor Ding, which is different from other cryptocurrencies. It can upgrade the parameters, etc. Rainbow team After submitting the new parameters, abc can complete the upgrade. https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/6bJFzU_h44I
>
> 在2022年7月7日星期四 UTC+8 19:29:34<gmax...@gmail.com> 写道：
>
> > On Thu, Jul 7, 2022 at 9:39 AM andy yi <hy81...@gmail.com> wrote:
> > > Today may be a historic day. This is the first time in the history of cryptocurrency that a cryptocurrency has been cracked because of its encryption algorithm.
> >
> > Not at all. Just to give an example, IOTA's signature scheme suffered signature forgeries. (https://github.com/mit-dci/tangled-curl/blob/master/vuln-iota.md). Interestingly, that is also an example of a "post quantum" scheme that wasn't classically secure (in that case a lamport like signature constructed out of a usenet-kook-grade adhoc hash function). I can think of other signature scheme vulnerabilities in 'cryptocurrencies' too, though less applicable to this list.
> >
> > It's true that most of the time cryptocurrency cryptographic flaws come from things other than the digital signature algorithm -- but that's merely a result of the fact that there are so many other things their authors can break in their quest to brew novel snake oil

> flavors. With so many other knobs to twiddle that they usually leave
> the digital signature part alone.

--

--

From: ToTheMars ABC <abctothemars@gmail.com> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
CC: hy81...@gmail.com <hy8196695@gmail.com>, gmax...@gmail.com <gmaxwell@gmail.com>, pqc-forum <pqc-forum@list.nist.gov>, Matthias Kannwischer <m.kannwischer@gmail.com>, Lorenz Panny <lorenz@yx7.cc>, ToTheMars ABC <abctothemars@gmail.com>
Subject: Re: [pqc-forum] Re: Why rainbow Signature is the strongest cryptocurrency algorithm?
Date: Monday, July 11, 2022 05:29:15 AM ET

You are right, ABC is the first cryptocurrency signed with rainbow, only code. So it's very valuable.

Legendary cryptographer @claucece sums up all the digital signature algorithms!

Remember! The shorter the signature length i.e. the signature size (bytes) in the last column, the friendlier it is to cryptocurrency mining miners!

From Mr. Liu Jin's twitter

在2022年7月8日星期五 UTC 00:42:28<hy81...@gmail.com> 写道：

> Even so, I still think it is unique, because the algorithm parameters used in abc are directly provided by Professor Ding, which is different from other cryptocurrencies. It can upgrade the parameters, etc. Rainbow team After submitting the new parameters, abc can complete the upgrade. https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/6bJFzU_h44I
>
> 在2022年7月7日星期四 UTC+8 19:29:34<gmax...@gmail.com> 写道：
>
> > On Thu, Jul 7, 2022 at 9:39 AM andy yi <hy81...@gmail.com> wrote:
> > > Today may be a historic day. This is the first time in the history of cryptocurrency that a cryptocurrency has been cracked because of its encryption algorithm.
> >
> > Not at all. Just to give an example, IOTA's signature scheme suffered
> > signature forgeries. (
> > https://github.com/mit-dci/tangled-curl/blob/master/vuln-iota.md).
> > Interestingly, that is also an example of a "post quantum" scheme that
> > wasn't classically secure (in that case a lamport like signature
> > constructed out of a usenet-kook-grade adhoc hash function). I can
> > think of other signature scheme vulnerabilities in 'cryptocurrencies'

> too, though less applicable to this list.
>
> It's true that most of the time cryptocurrency cryptographic flaws come from things other than the digital signature algorithm -- but that's merely a result of the fact that there are so many other things their authors can break in their quest to brew novel snake oil flavors. With so many other knobs to twiddle that they usually leave the digital signature part alone.

--

From: ToTheMars ABC <abctothemars@gmail.com> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
CC: ToTheMars ABC <abctothemars@gmail.com>, hy81...@gmail.com <hy8196695@gmail.com>, gmax...@gmail.com <gmaxwell@gmail.com>, pqc-forum <pqc-forum@list.nist.gov>, Matthias Kannwischer <m.kannwischer@gmail.com>, Lorenz Panny <lorenz@yx7.cc>
Subject: Re: [pqc-forum] Re: Why rainbow Signature is the strongest cryptocurrency algorithm?
Date: Thursday, July 21, 2022 07:53:03 AM ET

Although the rainbow signature is no longer on the NIST PQC list, Mr. Liu Jin said, the next 20 years, 100 years or more, the shortest signature length and can resist quantum computer cracking digital signature algorithm, or only based on multivariate cryptography (Multivariate cryptography) rainbow signature algorithm, this is a fucking mathematical decision! No one can change it!

Mr. Liu Jin's twitter

在2022年7月11日星期一 UTC 09:29:03<ToTheMars ABC> 写道：

> You are right, ABC is the first cryptocurrency signed with rainbow, only code. So it's very valuable.
>
> Legendary cryptographer @claucece sums up all the digital signature algorithms!
>
> Remember! The shorter the signature length i.e. the signature size (bytes) in the last column, the friendlier it is to cryptocurrency mining miners!
> From Mr. Liu Jin's twitter
>
> 在2022年7月8日星期五 UTC 00:42:28<hy81...@gmail.com> 写道：
>
> > Even so, I still think it is unique, because the algorithm parameters used in abc are directly provided by Professor Ding, which is different from other cryptocurrencies. It can upgrade the parameters, etc. Rainbow team After submitting the new parameters, abc can complete the upgrade. https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/6bJFzU_h44I
> >
> > 在2022年7月7日星期四 UTC+8 19:29:34<gmax...@gmail.com> 写道：

> > On Thu, Jul 7, 2022 at 9:39 AM andy yi <hy81...@gmail.com> wrote:
> > > Today may be a historic day. This is the first time in the history of cryptocurrency that a cryptocurrency has been cracked because of its encryption algorithm.
> >
> > Not at all. Just to give an example, IOTA's signature scheme suffered signature forgeries. (https://github.com/mit-dci/tangled-curl/blob/master/vuln-iota.md). Interestingly, that is also an example of a "post quantum" scheme that wasn't classically secure (in that case a lamport like signature constructed out of a usenet-kook-grade adhoc hash function). I can think of other signature scheme vulnerabilities in 'cryptocurrencies' too, though less applicable to this list.
>
> It's true that most of the time cryptocurrency cryptographic flaws come from things other than the digital signature algorithm -- but that's merely a result of the fact that there are so many other things their authors can break in their quest to brew novel snake oil flavors. With so many other knobs to twiddle that they usually leave the digital signature part alone.

From: Bank BSC <bankofbsc@gmail.com> via pqc-forum@list.nist.gov
To: ToTheMars ABC <abctothemars@gmail.com>
CC: pqc-forum <pqc-forum@list.nist.gov>, hy81...@gmail.com <hy8196695@gmail.com>, gmax...@gmail.com <gmaxwell@gmail.com>, Matthias Kannwischer <m.kannwischer@gmail.com>, Lorenz Panny <lorenz@yx7.cc>
Subject: Re: [pqc-forum] Re: Why rainbow Signature is the strongest cryptocurrency algorithm?
Date: Thursday, July 21, 2022 08:29:23 AM ET

---

why this NIST mailing list becomes a bullshit cryptocurrency scammer system?

On Thu, Jul 21, 2022 at 7:52 AM ToTheMars ABC <abctothemars@gmail.com> wrote:

> Although the rainbow signature is no longer on the NIST PQC list, Mr. Liu Jin said, the next 20 years, 100 years or more, the shortest signature length and can resist quantum computer cracking digital signature algorithm, or only based on multivariate cryptography (Multivariate cryptography) rainbow signature algorithm, this is a fucking mathematical decision! No one can change it!
>
> Mr. Liu Jin's twitter
>
> 在2022年7月11日星期一 UTC 09:29:03<ToTheMars ABC> 写道：
>
> > You are right, ABC is the first cryptocurrency signed with rainbow, only code. So it's very valuable.
> >
> > Legendary cryptographer @claucece sums up all the digital signature algorithms!
> >
> > Remember! The shorter the signature length i.e. the signature size (bytes) in the last column, the friendlier it is to cryptocurrency mining miners!
> > From Mr. Liu Jin's twitter
> >
> > 在2022年7月8日星期五 UTC 00:42:28<hy81...@gmail.com> 写道：
> >
> > > Even so, I still think it is unique, because the algorithm parameters used in abc are directly provided by Professor Ding, which is different from other cryptocurrencies. It can upgrade the parameters, etc. Rainbow team After submitting the new parameters,

> > abc can complete the upgrade. https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/6bJFzU_h44I
> >
> > 在2022年7月7日星期四 UTC+8 19:29:34<gmax...@gmail.com> 写道：
> >
> > > On Thu, Jul 7, 2022 at 9:39 AM andy yi <hy81...@gmail.com> wrote:
> > > > Today may be a historic day. This is the first time in the history of cryptocurrency that a cryptocurrency has been cracked because of its encryption algorithm.
> > >
> > > Not at all. Just to give an example, IOTA's signature scheme suffered signature forgeries. (https://github.com/mit-dci/tangled-curl/blob/master/vuln-iota.md). Interestingly, that is also an example of a "post quantum" scheme that wasn't classically secure (in that case a lamport like signature constructed out of a usenet-kook-grade adhoc hash function). I can think of other signature scheme vulnerabilities in 'cryptocurrencies' too, though less applicable to this list.
> > >
> > > It's true that most of the time cryptocurrency cryptographic flaws come from things other than the digital signature algorithm -- but that's merely a result of the fact that there are so many other things their authors can break in their quest to brew novel snake oil flavors. With so many other knobs to twiddle that they usually leave the digital signature part alone.
>
> --
> 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/254ae41a-f91c-4472-b3b2-cce76b91006cn%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/CAMa6AcKH-%2B%3DQ73kXXnTnpxNmBa-J3OLiW8LfLY1Cq2e0B0_XCQ%40mail.gmail.com.

From: ToTheMars ABC <abctothemars@gmail.com> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
CC: bank...@gmail.com <bankofbsc@gmail.com>, pqc-forum <pqc-forum@list.nist.gov>, hy81...@gmail.com <hy8196695@gmail.com>, gmax...@gmail.com <gmaxwell@gmail.com>, Matthias Kannwischer <m.kannwischer@gmail.com>, Lorenz Panny <lorenz@yx7.cc>, ToTheMars ABC <abctothemars@gmail.com>
Subject: Re: [pqc-forum] Re: Why rainbow Signature is the strongest cryptocurrency algorithm?
Date: Thursday, July 21, 2022 09:16:38 AM ET

---

abcmint is a post-quantum secure blockchain project led by Mr. Liu Jin and approved by famous cryptographers around the world, not a scam project.

The official website of abcmint coin is http://abcmint.org

Mr. Liu Jin's twitter

在2022年7月21日星期四 UTC 12:29:18<bank...@gmail.com> 写道：

> why this NIST mailing list becomes a bullshit cryptocurrency scammer system?
>
> On Thu, Jul 21, 2022 at 7:52 AM ToTheMars ABC <abctot...@gmail.com> wrote:
>
> > Although the rainbow signature is no longer on the NIST PQC list, Mr. Liu Jin said, the next 20 years, 100 years or more, the shortest signature length and can resist quantum computer cracking digital signature algorithm, or only based on multivariate cryptography (Multivariate cryptography) rainbow signature algorithm, this is a fucking mathematical decision! No one can change it!
> >
> > Mr. Liu Jin's twitter
> >
> > 在2022年7月11日星期一 UTC 09:29:03<ToTheMars ABC> 写道：
> >
> > > You are right, ABC is the first cryptocurrency signed with rainbow, only code. So it's very valuable.
> > >
> > > Legendary cryptographer @claucece sums up all the digital signature algorithms!

> Remember! The shorter the signature length i.e. the signature size (bytes) in the last column, the friendlier it is to cryptocurrency mining miners!
> From Mr. Liu Jin's twitter
>
> 在2022年7月8日星期五 UTC 00:42:28<hy81...@gmail.com> 写道：
>
> > Even so, I still think it is unique, because the algorithm parameters used in abc are directly provided by Professor Ding, which is different from other cryptocurrencies. It can upgrade the parameters, etc. Rainbow team After submitting the new parameters, abc can complete the upgrade. https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/6bJFzU_h44I
> >
> > 在2022年7月7日星期四 UTC+8 19:29:34<gmax...@gmail.com> 写道：
> >
> > > On Thu, Jul 7, 2022 at 9:39 AM andy yi <hy81...@gmail.com> wrote:
> > > > Today may be a historic day. This is the first time in the history of cryptocurrency that a cryptocurrency has been cracked because of its encryption algorithm.
> > >
> > > Not at all. Just to give an example, IOTA's signature scheme suffered signature forgeries. (https://github.com/mit-dci/tangled-curl/blob/master/vuln-iota.md). Interestingly, that is also an example of a "post quantum" scheme that wasn't classically secure (in that case a lamport like signature constructed out of a usenet-kook-grade adhoc hash function). I can think of other signature scheme vulnerabilities in 'cryptocurrencies' too, though less applicable to this list.
> > >
> > > It's true that most of the time cryptocurrency cryptographic flaws come from things other than the digital signature algorithm -- but that's merely a result of the fact that there are so many other things their authors can break in their quest to brew novel snake oil flavors. With so many other knobs to twiddle that they usually leave the digital signature part alone.

> 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/254ae41a-f91c-4472-b3b2-cce76b91006cn%40list.nist.gov.

--

From: Bank BSC <bankofbsc@gmail.com> via pqc-forum@list.nist.gov
To: ToTheMars ABC <abctothemars@gmail.com>
CC: pqc-forum <pqc-forum@list.nist.gov>, hy81...@gmail.com <hy8196695@gmail.com>, gmax...@gmail.com <gmaxwell@gmail.com>, Matthias Kannwischer <m.kannwischer@gmail.com>, Lorenz Panny <lorenz@yx7.cc>
Subject: Re: [pqc-forum] Re: Why rainbow Signature is the strongest cryptocurrency algorithm?
Date: Sunday, July 24, 2022 07:45:53 AM ET

---

if not scammer, why not keep your promise and pay the $400,000?

>>>>>> "Abc Chairman Liu Jin has said "Anyone who cracks Abc's rainbow signature will be awarded a $400,000 bonus", have you heard of anyone getting it so far?"

Dear ToTheMars ABC, dear all,

On Mon, 4 Jul 2022 at 18:05, ToTheMars ABC <abctothemars@gmail.com> wrote:

> In response to your comment that "rainbow algorithm have also been cracked"
> Abc Chairman Liu Jin has said "Anyone who cracks Abc's rainbow signature will be awarded a $400,000 bonus", have you heard of anyone getting it so far?

as has been pointed out before, the level-1 parameter sets of Rainbow are practically broken by https://ia.cr/2022/214.
This obviously also applies to the Rainbow(16,32,32,32) instance used in Abcmint.

We have successfully recovered the secret key corresponding to the public key with address 84cJso7keg6SHW4vbNVbXccimCZrz7WoESXTtw12b5UsWqmm5.
This address is one of the wealthiest on the chain with a balance of 9M ABC. There is only one address with a higher balance, but as it has no outgoing transactions, we don't know the public key.

The private key was recovered within a few hours of wall-clock time using a slightly tweaked version of Ward Beullens' attack software (which in turn makes use of Ruben Niederhagen's XL implementation).

The forged signature for the message
"There is no pot of gold at the end of the Rainbow." (ASCII)
is
"TqERiKoFpkDEOEUGrq2WfH/

XvTxP8dzbUxUpD1UyTUyLnVUaZcqW9IV+bTLIuamWS+XVKFcslYHLnxNcjcjnCA==" (Base64)

The Abcmint client does offer functionality to verify signatures like these, but the feature was apparently implemented incorrectly and only allows verifying messages signed with a private key in the user's own wallet. Thus, we instead publish code to verify this signature using the Abcmint codebase as well as our own Sage script:

https://github.com/mkannwischer/breaking-abc

We hope this clears up any remaining doubts about the applicability of the attack to the Abcmint blockchain. Please inform us how to collect the promised $400,000.

Cheers,
Lorenz and Matthias

On Thu, Jul 21, 2022 at 9:16 AM ToTheMars ABC <abctothemars@gmail.com> wrote:

> abcmint is a post-quantum secure blockchain project led by Mr. Liu Jin and approved by famous cryptographers around the world, not a scam project.
>
> The official website of abcmint coin is http://abcmint.org
>
> Mr. Liu Jin's twitter
>
> 在2022年7月21日星期四 UTC 12:29:18<bank...@gmail.com> 写道：
>
> > why this NIST mailing list becomes a bullshit cryptocurrency scammer system?
> >
> > On Thu, Jul 21, 2022 at 7:52 AM ToTheMars ABC <abctot...@gmail.com> wrote:
> >
> > > Although the rainbow signature is no longer on the NIST PQC list, Mr. Liu Jin said, the next 20 years, 100 years or more, the shortest signature length and can resist quantum computer cracking digital signature algorithm, or only based on multivariate cryptography (Multivariate cryptography) rainbow signature algorithm, this is a fucking mathematical decision! No one can change it!
> > >
> > > Mr. Liu Jin's twitter

在2022年7月11日星期一 UTC 09:29:03<ToTheMars ABC> 写道：

> You are right, ABC is the first cryptocurrency signed with rainbow, only code. So it's very valuable.
>
> Legendary cryptographer @claucece sums up all the digital signature algorithms!
>
> Remember! The shorter the signature length i.e. the signature size (bytes) in the last column, the friendlier it is to cryptocurrency mining miners!
> From Mr. Liu Jin's twitter
>
> 在2022年7月8日星期五 UTC 00:42:28<hy81...@gmail.com> 写道：
>
> > Even so, I still think it is unique, because the algorithm parameters used in abc are directly provided by Professor Ding, which is different from other cryptocurrencies. It can upgrade the parameters, etc. Rainbow team After submitting the new parameters, abc can complete the upgrade. https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/6bJFzU_h44I
> >
> > 在2022年7月7日星期四 UTC+8 19:29:34<gmax...@gmail.com> 写道：
> >
> > > On Thu, Jul 7, 2022 at 9:39 AM andy yi <hy81...@gmail.com> wrote:
> > > > Today may be a historic day. This is the first time in the history of cryptocurrency that a cryptocurrency has been cracked because of its encryption algorithm.
> > >
> > > Not at all. Just to give an example, IOTA's signature scheme suffered signature forgeries. (https://github.com/mit-dci/tangled-curl/blob/master/vuln-iota.md). Interestingly, that is also an example of a "post quantum" scheme that wasn't classically secure (in that case a lamport like signature constructed out of a usenet-kook-grade adhoc hash function). I can think of other signature scheme vulnerabilities in 'cryptocurrencies' too, though less applicable to this list.
> > >
> > > It's true that most of the time cryptocurrency cryptographic flaws

> > > > come from things other than the digital signature algorithm -- but that's merely a result of the fact that there are so many other things their authors can break in their quest to brew novel snake oil flavors. With so many other knobs to twiddle that they usually leave the digital signature part alone.
> > > --
> > > 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/254ae41a-f91c-4472-b3b2-cce76b91006cn%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/CAMa6AcKx7CA%3DDv5Yj-wStc0W-wWiN%3DE%2BDjzoi1Ukn-j64e1bQg%40mail.gmail.com.

From: ToTheMars ABC <abctothemars@gmail.com> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
CC: bank...@gmail.com <bankofbsc@gmail.com>, pqc-forum <pqc-forum@list.nist.gov>, hy81...@gmail.com <hy8196695@gmail.com>, gmax...@gmail.com <gmaxwell@gmail.com>, Matthias Kannwischer <m.kannwischer@gmail.com>, Lorenz Panny <lorenz@yx7.cc>, ToTheMars ABC <abctothemars@gmail.com>
Subject: Re: [pqc-forum] Re: Why rainbow Signature is the strongest cryptocurrency algorithm?
Date: Monday, July 25, 2022 04:43:58 AM ET

If you have any questions about abcmint being cracked, you can ask Jin Liu, the chairman of abcmint, and he will approve the authenticity of the crack instead of talking nonsense here. Here is Jin Liu's contact information:

https://twitter.com/abcardo

https://twitter.com/amisrepresented

https://www.linkedin.com/in/liujinabcardo?trk=org-employees

abcmint Project Official Website:

http://www.abcmint.org

在2022年7月24日星期日 UTC 11:45:44<bank...@gmail.com> 写道：

> if not scammer, why not keep your promise and pay the $400,000?
>
> >>>>>> "Abc Chairman Liu Jin has said "Anyone who cracks Abc's rainbow signature will be awarded a $400,000 bonus", have you heard of anyone getting it so far?"
>
> Dear ToTheMars ABC, dear all,
>
> On Mon, 4 Jul 2022 at 18:05, ToTheMars ABC <abctot...@gmail.com> wrote:
>
> > In response to your comment that "rainbow algorithm have also been cracked"
> > Abc Chairman Liu Jin has said "Anyone who cracks Abc's rainbow signature will be awarded a $400,000 bonus", have you heard of anyone getting it so far?
>
> as has been pointed out before, the level-1 parameter sets of Rainbow are practically broken by https://ia.cr/2022/214.
> This obviously also applies to the Rainbow(16,32,32,32) instance used in Abcmint.

We have successfully recovered the secret key corresponding to the public key with address 84cJso7keg6SHW4vbNVbXccimCZrz7WoESXTtw12b5UsWqmm5.
This address is one of the wealthiest on the chain with a balance of 9M ABC. There is only one address with a higher balance, but as it has no outgoing transactions, we don't know the public key.

The private key was recovered within a few hours of wall-clock time using a slightly tweaked version of Ward Beullens' attack software (which in turn makes use of Ruben Niederhagen's XL implementation).

The forged signature for the message
"There is no pot of gold at the end of the Rainbow." (ASCII)
is
"TqERiKoFpkDEOEUGrq2WfH/
XvTxP8dzbUxUpD1UyTUyLnVUaZcqW9IV+bTLIuamWS+XVKFcslYHLnxNcjcjnCA==" (Base64)

The Abcmint client does offer functionality to verify signatures like these, but the feature was apparently implemented incorrectly and only allows verifying messages signed with a private key in the user's own wallet. Thus, we instead publish code to verify this signature using the Abcmint codebase as well as our own Sage script:

https://github.com/mkannwischer/breaking-abc

We hope this clears up any remaining doubts about the applicability of the attack to the Abcmint blockchain. Please inform us how to collect the promised $400,000.

Cheers,
Lorenz and Matthias

On Thu, Jul 21, 2022 at 9:16 AM ToTheMars ABC <abctot...@gmail.com> wrote:

> abcmint is a post-quantum secure blockchain project led by Mr. Liu Jin and approved by famous cryptographers around the world, not a scam project.
>
> The official website of abcmint coin is http://abcmint.org
>
> Mr. Liu Jin's twitter

在2022年7月21日星期四 UTC 12:29:18<bank...@gmail.com> 写道：

> why this NIST mailing list becomes a bullshit cryptocurrency scammer system?
>
> On Thu, Jul 21, 2022 at 7:52 AM ToTheMars ABC <abctot...@gmail.com> wrote:
>
> > Although the rainbow signature is no longer on the NIST PQC list, Mr. Liu Jin said, the next 20 years, 100 years or more, the shortest signature length and can resist quantum computer cracking digital signature algorithm, or only based on multivariate cryptography (Multivariate cryptography) rainbow signature algorithm, this is a fucking mathematical decision! No one can change it!
> >
> > Mr. Liu Jin's twitter
> >
> > 在2022年7月11日星期一 UTC 09:29:03<ToTheMars ABC> 写道：
> >
> > > You are right, ABC is the first cryptocurrency signed with rainbow, only code. So it's very valuable.
> > >
> > > Legendary cryptographer @claucece sums up all the digital signature algorithms!
> > >
> > > Remember! The shorter the signature length i.e. the signature size (bytes) in the last column, the friendlier it is to cryptocurrency mining miners!
> > > From Mr. Liu Jin's twitter
> > >
> > > 在2022年7月8日星期五 UTC 00:42:28<hy81...@gmail.com> 写道：
> > >
> > > > Even so, I still think it is unique, because the algorithm parameters used in abc are directly provided by Professor Ding, which is different from other cryptocurrencies. It can upgrade the parameters, etc. Rainbow team After submitting the new parameters, abc can complete the upgrade. https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/6bJFzU_h44I
> > > >
> > > > 在2022年7月7日星期四 UTC+8 19:29:34<gmax...@gmail.com> 写道：

> > > > > On Thu, Jul 7, 2022 at 9:39 AM andy yi <hy81...@gmail.com> wrote:
> > > > > > Today may be a historic day. This is the first time in the history of cryptocurrency that a cryptocurrency has been cracked because of its encryption algorithm.
> > > > >
> > > > > Not at all. Just to give an example, IOTA's signature scheme suffered signature forgeries. (https://github.com/mit-dci/tangled-curl/blob/master/vuln-iota.md). Interestingly, that is also an example of a "post quantum" scheme that wasn't classically secure (in that case a lamport like signature constructed out of a usenet-kook-grade adhoc hash function). I can think of other signature scheme vulnerabilities in 'cryptocurrencies' too, though less applicable to this list.
> > > > >
> > > > > It's true that most of the time cryptocurrency cryptographic flaws come from things other than the digital signature algorithm -- but that's merely a result of the fact that there are so many other things their authors can break in their quest to brew novel snake oil flavors. With so many other knobs to twiddle that they usually leave the digital signature part alone.
> > > --
> > > 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/254ae41a-f91c-4472-b3b2-cce76b91006cn%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/e2c3a5f6-4fa1-49c8-acac-32bb5c3e4b38n%40list.nist.gov.

From: s zhang <shezhangth@gmail.com> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
CC: abctot...@gmail.com <abctothemars@gmail.com>, bank...@gmail.com <bankofbsc@gmail.com>, pqc-forum <pqc-forum@list.nist.gov>, hy81...@gmail.com <hy8196695@gmail.com>, gmax...@gmail.com <gmaxwell@gmail.com>, Matthias Kannwischer <m.kannwischer@gmail.com>, Lorenz Panny <lorenz@yx7.cc>
Subject: Re: [pqc-forum] Re: Why rainbow Signature is the strongest cryptocurrency algorithm?
Date: Friday, December 09, 2022 08:02:21 AM ET

Rainbow Signature has been proven to be vulnerable by many parties, but even so, do you still believe that your project is secure? And that is, since the rainbow and abc are cracked, abc project party should not fulfill the promise to pay the $400,000 cracking bonus?
Finally, you ABC project related people should be appropriate to stop it, this is a forum to discuss the pqc algorithm, not you speculators speculate on their own project place.

在2022年7月25日星期一 UTC+8 16:43:43<abctot...@gmail.com> 写道：

> If you have any questions about abcmint being cracked, you can ask Jin Liu, the chairman of abcmint, and he will approve the authenticity of the crack instead of talking nonsense here. Here is Jin Liu's contact information:
>
> https://twitter.com/abcardo
>
> https://twitter.com/amisrepresented
>
> https://www.linkedin.com/in/liujinabcardo?trk=org-employees
>
> abcmint Project Official Website:
>
> http://www.abcmint.org
>
> 在2022年7月24日星期日 UTC 11:45:44<bank...@gmail.com> 写道：
>
> > if not scammer, why not keep your promise and pay the $400,000?
> >
> > >>>>>> "Abc Chairman Liu Jin has said "Anyone who cracks Abc's rainbow signature will be awarded a $400,000 bonus", have you heard of anyone getting it so far?"
> >
> > Dear ToTheMars ABC, dear all,
> >
> > On Mon, 4 Jul 2022 at 18:05, ToTheMars ABC <abctot...@gmail.com> wrote:

> In response to your comment that "rainbow algorithm have also been cracked"
> Abc Chairman Liu Jin has said "Anyone who cracks Abc's rainbow signature will be awarded a $400,000 bonus", have you heard of anyone getting it so far?

as has been pointed out before, the level-1 parameter sets of Rainbow are practically broken by https://ia.cr/2022/214.
This obviously also applies to the Rainbow(16,32,32,32) instance used in Abcmint.

We have successfully recovered the secret key corresponding to the public key with address
84cJso7keg6SHW4vbNVbXccimCZrz7WoESXTtw12b5UsWqmm5.
This address is one of the wealthiest on the chain with a balance of 9M ABC. There is only one address with a higher balance, but as it has no outgoing transactions, we don't know the public key.

The private key was recovered within a few hours of wall-clock time using a slightly tweaked version of Ward Beullens' attack software (which in turn makes use of Ruben Niederhagen's XL implementation).

The forged signature for the message
"There is no pot of gold at the end of the Rainbow." (ASCII)
is
"TqERiKoFpkDEOEUGrq2WfH/
XvTxP8dzbUxUpD1UyTUyLnVUaZcqW9lV+bTLIuamWS+XVKFcslYHLnxNcjcjnCA==" (Base64)

The Abcmint client does offer functionality to verify signatures like these, but the feature was apparently implemented incorrectly and only allows verifying messages signed with a private key in the user's own wallet. Thus, we instead publish code to verify this signature using the Abcmint codebase as well as our own Sage script:

https://github.com/mkannwischer/breaking-abc

We hope this clears up any remaining doubts about the applicability of the attack to the Abcmint blockchain. Please inform us how to collect the promised $400,000.

Cheers,
Lorenz and Matthias

On Thu, Jul 21, 2022 at 9:16 AM ToTheMars ABC <abctot...@gmail.com> wrote:

> abcmint is a post-quantum secure blockchain project led by Mr. Liu Jin and approved by famous cryptographers around the world, not a scam project.
>
> The official website of abcmint coin is http://abcmint.org
>
> Mr. Liu Jin's twitter
>
> 在2022年7月21日星期四 UTC 12:29:18<bank...@gmail.com> 写道：
>
> > why this NIST mailing list becomes a bullshit cryptocurrency scammer system?
> >
> > On Thu, Jul 21, 2022 at 7:52 AM ToTheMars ABC <abctot...@gmail.com> wrote:
> >
> > > Although the rainbow signature is no longer on the NIST PQC list, Mr. Liu Jin said, the next 20 years, 100 years or more, the shortest signature length and can resist quantum computer cracking digital signature algorithm, or only based on multivariate cryptography (Multivariate cryptography) rainbow signature algorithm, this is a fucking mathematical decision! No one can change it!
> > >
> > > Mr. Liu Jin's twitter
> > >
> > > 在2022年7月11日星期一 UTC 09:29:03<ToTheMars ABC> 写道：
> > >
> > > > You are right, ABC is the first cryptocurrency signed with rainbow, only code. So it's very valuable.
> > > >
> > > > Legendary cryptographer @claucece sums up all the digital signature algorithms!
> > > >
> > > > Remember! The shorter the signature length i.e. the signature size (bytes) in the last column, the friendlier it is to cryptocurrency mining miners!
> > > > From Mr. Liu Jin's twitter
> > > >
> > > > 在2022年7月8日星期五 UTC 00:42:28<hy81...@gmail.com> 写道：

> > > > > Even so, I still think it is unique, because the algorithm parameters used in abc are directly provided by Professor Ding, which is different from other cryptocurrencies. It can upgrade the parameters, etc. Rainbow team After submitting the new parameters, abc can complete the upgrade. https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/6bJFzU_h44I
> > > > >
> > > > > 在2022年7月7日星期四 UTC+8 19:29:34<gmax...@gmail.com> 写道：
> > > > >
> > > > > > On Thu, Jul 7, 2022 at 9:39 AM andy yi <hy81...@gmail.com> wrote:
> > > > > > > Today may be a historic day. This is the first time in the history of cryptocurrency that a cryptocurrency has been cracked because of its encryption algorithm.
> > > > > >
> > > > > > Not at all. Just to give an example, IOTA's signature scheme suffered signature forgeries. (https://github.com/mit-dci/tangled-curl/blob/master/vuln-iota.md). Interestingly, that is also an example of a "post quantum" scheme that wasn't classically secure (in that case a lamport like signature constructed out of a usenet-kook-grade adhoc hash function). I can think of other signature scheme vulnerabilities in 'cryptocurrencies' too, though less applicable to this list.
> > > > > >
> > > > > > It's true that most of the time cryptocurrency cryptographic flaws come from things other than the digital signature algorithm -- but that's merely a result of the fact that there are so many other things their authors can break in their quest to brew novel snake oil flavors. With so many other knobs to twiddle that they usually leave the digital signature part alone.
> > > > --
> > > > 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/254ae41a-f91c-4472-b3b2-cce76b91006cn%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/35769561-1f00-4ba7-aedb-62aaeba6c62fn%40list.nist.gov.