**From:** abcmint pqc <abcmintpqc@gmail.com> via pqc-forum@list.nist.gov
**To:** pqc-forum <pqc-forum@list.nist.gov>
**Subject:** [pqc-forum] An ABCMint PQC Upgrade Plan ( ABCMint Version 2 )
**Date:** Wednesday, March 23, 2022 07:33:59 AM ET

Abstract

Ward Beullens, a postdoctoral researcher at IBM Research, published a paper entitled "Breaking Rainbow Takes a Weekend on a Laptop" on the "Cryptology ePrint Archive". The paper suggests that the rainbow signatures currently submitted to the NIST POC Round 3 Security Level 1 can be cracked in a short time by a classic computer. (The paper has been tested in practice by the Rainbow Signature team, and the results show that the attack is effective.)

(While the Level 1 parameter sets clearly are clearly broken by the attack, its impact on the larger parameter sets is much more "moderate".)

(Rainbow team proposed to Nist to replace the Rainbow Level 1 parameters with our Level 3 parameters and Level 3 with Level 5 parameters.)

Since the parameters of the Rainbow Signature used by ABCMint (the ABCMint proprietary version of the Rainbow Signature) are similar to the security level 1 submitted to NIST, there are security concerns as well, which is the main reason for this upgrade plan.

Planning

The goal of this project is to update the current core PQC algorithm of ABCMint (the rainbow signature of ABCMint proprietary version) to the new version of rainbow signature with the parameters proposed by Prof. Ding, in order to fix the security vulnerabilities identified in the paper and achieve the goal of persistent security of ABCMint.

The project will officially start raising funds and recruiting developers for the project soon.

BY ABCMint PQC Round 1 Security Upgrade Committee (Third Party Community)
Discord: https://discord.gg/4jQyMDFfmg

--

**From:** andy yi <hy8196695@gmail.com> via pqc-forum@list.nist.gov
**To:** pqc-forum <pqc-forum@list.nist.gov>
**CC:** abcmi...@gmail.com <abcmintpqc@gmail.com>
**Subject:** [pqc-forum] Re: An ABCMint PQC Upgrade Plan ( ABCMint Version 2 )
**Date:** Tuesday, April 19, 2022 12:46:55 AM ET

---

You can't enter after clicking on the link, please notify you when there is a message, and hope that the rainbow signature will become stronger after updating the parameters

在2022年3月23日星期三 UTC+8 19:33:08<abcmi...@gmail.com> 写道：

> Abstract
>
> Ward Beullens, a postdoctoral researcher at IBM Research, published a paper entitled "Breaking Rainbow Takes a Weekend on a Laptop" on the "Cryptology ePrint Archive". The paper suggests that the rainbow signatures currently submitted to the NIST POC Round 3 Security Level 1 can be cracked in a short time by a classic computer. (The paper has been tested in practice by the Rainbow Signature team, and the results show that the attack is effective.)
>
> (While the Level 1 parameter sets clearly are clearly broken by the attack, its impact on the larger parameter sets is much more "moderate".)
>
> (Rainbow team proposed to Nist to replace the Rainbow Level 1 parameters with our Level 3 parameters and Level 3 with Level 5 parameters.)
>
> Since the parameters of the Rainbow Signature used by ABCMint (the ABCMint proprietary version of the Rainbow Signature) are similar to the security level 1 submitted to NIST, there are security concerns as well, which is the main reason for this upgrade plan.
>
> Planning
>
> The goal of this project is to update the current core PQC algorithm of ABCMint (the rainbow signature of ABCMint proprietary version) to the new version of rainbow signature with the parameters proposed by Prof. Ding, in order to fix the security vulnerabilities identified in the paper and achieve the goal of persistent security of ABCMint.

> The project will officially start raising funds and recruiting developers for the project soon.
>
> BY ABCMint PQC Round 1 Security Upgrade Committee (Third Party Community)
> Discord: https://discord.gg/4jQyMDFfmg

--

**From:** abcmint pqc <abcmintpqc@gmail.com> via pqc-forum@list.nist.gov
**To:** pqc-forum <pqc-forum@list.nist.gov>
**CC:** hy81...@gmail.com <hy8196695@gmail.com>, abcmint pqc <abcmintpqc@gmail.com>
**Subject:** [pqc-forum] Re: An ABCMint PQC Upgrade Plan ( ABCMint Version 2 )
**Date:** Thursday, April 21, 2022 08:32:45 AM ET

---

I just had it checked and everything is fine.

--

**From:** abcmint pqc <abcmintpqc@gmail.com> via pqc-forum@list.nist.gov
**To:** pqc-forum <pqc-forum@list.nist.gov>
**CC:** abcmint pqc <abcmintpqc@gmail.com>, hy81...@gmail.com <hy8196695@gmail.com>
**Subject:** [pqc-forum] Re: An ABCMint PQC Upgrade Plan ( ABCMint Version 2 )
**Date:** Friday, June 10, 2022 08:36:18 AM ET

---

The ABCMint Upgrade Committee has opened a new group in the google group, so if you're interested, join us.

https://groups.google.com/g/abcmintversion2
On Thursday, April 21, 2022 at 8:32:34 PM UTC+8 abcmint pqc wrote:

> I just had it checked and everything is fine.

--