

From: D. J. Bernstein <djb@cr.yp.to>
To: pqc-comments@nist.gov
CC: pqc-forum@list.nist.gov, authorcontact-mceliece-merged@box.cr.yp.to
Subject: ROUND 4 OFFICIAL COMMENT: Classic McEliece
Date: Tuesday, October 25, 2022 08:14:20 AM ET
Attachments: [smime.p7m](#)

The round-4 Classic McEliece submission is available here:

<https://classic.mceliece.org/nist/mceliece-20221023.tar.gz>

As before, KATs have been split into a separate file:

<https://classic.mceliece.org/nist/mceliece-kat-20221023.tar.gz>

—D. J. Bernstein, on behalf of the Classic McEliece team

From: Wrenna Robson <wren.robson@gmail.com> via pqc-forum@list.nist.gov
To: pqc-forum@list.nist.gov, authorcontact-mceliece-merged@box.cr.yp.to, pqc-comments@nist.gov
Subject: Re: [pqc-forum] ROUND 4 OFFICIAL COMMENT: Classic McEliece
Date: Tuesday, October 25, 2022 08:31:02 AM ET

Thanks for this, Dan.

Obviously I've just had a quick glance, and will read in detail in the fullness of time, but I just want to say that I love the restructuring of the supporting documentation and the separation of content into the different documents for different purposes, and the rewriting and clarification of the content that I've seen already. It looks really great.

Best,

Wrenna

On Tue, 25 Oct 2022 at 13:01, D. J. Bernstein <djb@cr.yp.to> wrote:

>

> The round-4 Classic McEliece submission is available here:

>

```
> https://gcc02.safelinks.protection.outlook.com/?
url=https%3A%2F%2Fclassic.mceliece.org%2Fnist%2Fmceliece-20221023.tar.gz&data=05%
7C01%7C%2F%2Fclassic.mceliece.org%2Fnist.gov%7C6f776255708f404d8b0c08dab6840b2b%7C2ab5d82fd8fa4
797a93e054655c61dec%7C1%7C0%7C638022978625129943%7CUnknown%7CTWFpbGZsb3d8eyJWljoImC4w
LjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Iik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=p59I
EfuXmLUSyCeBdg4vMBN0x2BGeRylJXwvEDN88qI%3D&reserved=0
```

>

> As before, KATs have been split into a separate file:

>

```
> https://gcc02.safelinks.protection.outlook.com/?
url=https%3A%2F%2Fclassic.mceliece.org%2Fnist%2Fmceliece-
kat-20221023.tar.gz&data=05%7C01%7Cclawrence.bassham%40nist.gov%7C6f776255708f404d
8b0c08dab6840b2b%7C2ab5d82fd8fa4797a93e054655c61dec%7C1%7C0%7C638022978625129943%7CUn
known%7CTWFpbGZsb3d8eyJWIjojMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Iik1haWwiLCJXVCI6Mn0%3
D%7C3000%7C%7C&sdata=Kp0vlgEaR%2B11mhLH5iX5mptv%2FIfwA1X1dDdes%2F2b1WY%3D&
reserved=0
```

>

> —D. J. Bernstein, on behalf of the Classic McEliece team

>

> --

> 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/20221025120034.160285.qmail%40cr.yp.to>.

--

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/CANuKc3im%2B80APrZdFY1hoY2-cuZYV5cv_yxK_tfPFYxgTP7BuQ%40mail.gmail.com.