From: Tanja Lange <tanja@hyperelliptic.org>
Sent: Friday, September 30, 2022 4:55 PM
To: pqc-comments
Cc: pqc-forum; authorcontact-mceliece-merged@box.cr.yp.to
Subject: ROUND 4 OFFICIAL COMMENT: Classic McEliece
Attachments: mods3.pdf

The attached document "modifications for round 4" specifies the Classic McEliece tweaks for round 4. We will provide updated documentation and software matching this.

Tanja, on behalf of the Classic McEliece team

From: Michael Lyons <mlyons3@gmu.edu>
Sent: Friday, September 30, 2022 5:46 PM
To: pqc-forum
Cc: Tanja Lange; pqc-forum; authorcontact-...@box.cr.yp.to; pqc-comments
Subject: Re: ROUND 4 OFFICIAL COMMENT: Classic McEliece

On page 2 in the sentence [SECDED means “single error correction, double error correction”.]
I believe the last word should be "detection".

Regards,
Mike Lyons
Cryptographic Engineering Research Group
George Mason University

From: pqc-forum@list.nist.gov on behalf of Tung Chou <blueprint@crypto.tw>
Sent: Friday, September 30, 2022 9:07 PM
To: Michael Lyons
Cc: pqc-forum; pqc-comments
Subject: Re: [pqc-forum] Re: ROUND 4 OFFICIAL COMMENT: Classic McEliece

Hi Mike,

You are right. Thank you for pointing this out.

Tung Chou

On Sat, 1 Oct 2022 at 05:45, Michael Lyons <mlyons3@gmu.edu> wrote:

> On page 2 in the sentence [SECDED means “single error correction, double error correction”.]
> I believe the last word should be "detection".
>
> Regards,
> Mike Lyons
> Cryptographic Engineering Research Group
> George Mason University

From: 'Moody, Dustin (Fed)' via pqc-forum <pqc-forum@list.nist.gov>
Sent: Monday, October 3, 2022 9:29 AM
To: Tanja Lange
Cc: pqc-forum; authorcontact-mceliece-merged@box.cr.yp.to
Subject: [pqc-forum] Re: ROUND 4 OFFICIAL COMMENT: Classic McEliece

Thanks Tanja (and team),

When do you think you can send us the updated specs and software?

Dustin

From: Tanja Lange <tanja@hyperelliptic.org>
Sent: Friday, September 30, 2022 4:54 PM
To: pqc-comments <pqc-comments@nist.gov>
Cc: pqc-forum <pqc-forum@list.nist.gov>; authorcontact-mceliece-merged@box.cr.yp.to <authorcontact-mceliece-merged@box.cr.yp.to>
Subject: ROUND 4 OFFICIAL COMMENT: Classic McEliece

The attached document "modifications for round 4" specifies the
Classic McEliece tweaks for round 4. We will provide updated
documentation and software matching this.

Tanja, on behalf of the Classic McEliece team

--

From: D. J. Bernstein <djb@cr.yp.to>
Sent: Tuesday, October 25, 2022 8:01 AM
To: pqc-comments
Cc: pqc-forum; authorcontact-mceliece-merged@box.cr.yp.to
Subject: ROUND 4 OFFICIAL COMMENT: Classic McEliece
Attachments: signature.asc

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>
Sent: Tuesday, October 25, 2022 8:17 AM
To: pqc-forum; authorcontact-mceliece-merged@box.cr.yp.to; pqc-comments
Subject: Re: [pqc-forum] ROUND 4 OFFICIAL COMMENT: Classic McEliece

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:
>