From: Tanja Lange <tanja@hyperelliptic.org> via pqc-forum@list.nist.gov
To: pqc-comments@nist.gov
CC: pqc-forum@list.nist.gov, authorcontact-mceliece-merged@box.cr.yp.to
Subject: [pqc-forum] ROUND 4 OFFICIAL COMMENT: Classic McEliece
Date: Friday, September 30, 2022 04:55:51 PM ET
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> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
CC: Tanja Lange <tanja@hyperelliptic.org>, pqc-...@list.nist.gov <pqc-forum@list.nist.gov>, authorcontact-...@box.cr.yp.to <authorcontact-mceliece-merged@box.cr.yp.to>, pqc-co...@nist.gov <pqc-comments@nist.gov>
Subject: [pqc-forum] Re: ROUND 4 OFFICIAL COMMENT: Classic McEliece
Date: Friday, September 30, 2022 05:45:47 PM ET

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: Tung Chou <blueprint@crypto.tw> via pqc-forum@list.nist.gov
To: Michael Lyons <mlyons3@gmu.edu>
CC: pqc-forum <pqc-forum@list.nist.gov>, pqc-co...@nist.gov <pqc-comments@nist.gov>
Subject: Re: [pqc-forum] Re: ROUND 4 OFFICIAL COMMENT: Classic McEliece
Date: Friday, September 30, 2022 09:07:06 PM ET

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) <dustin.moody@nist.gov> via pqc-forum <pqc-forum@list.nist.gov>
To: Tanja Lange <tanja@hyperelliptic.org>
CC: pqc-forum <pqc-forum@list.nist.gov>, authorcontact-mceliece-merged@box.cr.yp.to
Subject: [pqc-forum] Re: ROUND 4 OFFICIAL COMMENT: Classic McEliece
Date: Monday, October 03, 2022 09:29:13 AM ET

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