From: pqc-forum@list.nist.gov on behalf of Yang Bolin <yangbolin@zju.edu.cn>
Sent: Tuesday, August 11, 2020 9:26 AM
To: pqc-forum
Subject: [pqc-forum] ROUND 3 OFFICIAL COMMENT: CRYSTALS-KYBER

Dear editor:
When I was doing some analysis on the reference implementation code from the CRYSTALS-KYBER, I found that the NTT function in this implementation is different from the traditional way. The variant “len”, which also means the distance in NTT, in the last round of their ntt is 2, rather than 1. So I wonder this is written by mistake or on purpose.
--

Kerman, Sara J. (Fed)

From: 'Bas Westerbaan' via pqc-forum <pqc-forum@list.nist.gov>
Sent: Tuesday, August 25, 2020 5:00 AM
To: Yang Bolin
Cc: pqc-forum
Subject: Re: [pqc-forum] ROUND 3 OFFICIAL COMMENT: CRYSTALS-KYBER

This is intended, see lower part of page 6 of the round 2 spec of Kyber.

(The chosen field F does not contain a 512th root of unity. Thus X^256+1 does not split completely, but it does factor into degree two polynomials. So strictly speaking you can't do a regular NTT, but you can do one which is close enough. Instead of an efficient isomorphism from F[x] / (X^256+1) to F^256, you get one from F[x] / (X^256+1) to \prod_i F[x]/(X^2+zeta_i), for some particular zeta_i that are powers of the chosen 256th root of unity, which still allows you to speed up multiplication.)

On Tue, Aug 11, 2020 at 3:26 PM Yang Bolin <yangbolin@zju.edu.cn> wrote:

> Dear editor:
> When I was doing some analysis on the reference implementation code from the CRYSTALS-KYBER, I found that the NTT function in this implementation is different from the traditional way. The variant “len”, which also means the distance in NTT, in the last round of their ntt is 2, rather than 1. So I wonder this is written by mistake or on purpose.
> --