From: EL HASSANE LAAJI <e.laaji@ump.ac.ma>
Sent: Saturday, May 25, 2019 8:34 PM
To: pqc-forum
Subject: [pqc-forum] ROUND 2 OFFICIAL COMMENT: NTRUEncrypt & NTRU

Hello NTRU team
Can you say me, why you didn't keep the NTRUencrypt-1024 release, is it because of speed performance or security performance.
Best regards.
--

From: John Schanck <jschanck@uwaterloo.ca>
Sent: Tuesday, May 28, 2019 4:31 PM
To: EL HASSANE LAAJI
Cc: pqc-forum
Subject: Re: [pqc-forum] OFFICIAL COMMENT: NTRUEncrypt & NTRU

Dear El Hassane Laaji,

* EL HASSANE LAAJI <e.laaji@ump.ac.ma> [2019-05-26 00:34:09 +0000]:
> Can you say me, why you didn't keep the NTRUencrypt-1024 release, is
> it because of speed performance or security performance.

Thanks for your question. To clarify for others, the "NTRUencrypt-1024"
parameter set was proposed in the first round NTRUEncrypt submission for use with the ss-ntru-pke and ss-ntru-kem schemes. I'll split your question into two parts:
- Why didn't we recommend ss-ntru?
- Why didn't we recommend an NTRU variant that uses Z[x]/(x^1024 + 1)?

Regarding ss-ntru:

At a fixed security level, NTRU and LWE schemes have a trade-off triangle between
1. the correctness of the decryption procedure,
2. the width of the coefficient distributions,
3. the compactness of public keys and ciphertexts.

The second round NTRU team wanted a compact scheme with a correct decryption procedure. The coefficient distribution used in ss-ntru is not compatible with that goal.

Regarding Z[x]/(x^1024 + 1):

It's not clear to us that there's a real need for an NTRU parameter set with such a large n. The largest n that we recommend is 821.

Best,
John (on behalf of the NTRU team)