From: ducas <L.Ducas@cwi.nl>
Sent: Thursday, July 30, 2020 9:49 AM
To: pqc-comments
Cc: pqc-forum
Subject: ROUND 3 OFFICIAL COMMENT: NTRU

Dear all,

following valuable comments and references from John Schanck, we have updated our report:

LWE with Side Information: Attacks and Concrete Security Estimation
Dana Dachman-Soled and Léo Ducas and Huijing Gong and Mélissa Rossi
https://eprint.iacr.org/2020/292

This updates now also considers the symmetries in the NTRU problem in Section 6.3, and discuss the (known) ways of exploiting it in a primal attack. In particular, we found that the technique of May and Silverman is in fact slightly counter-productive, if one accounts the accumulated probabilities of finding each rotation of the secret key.

The quantitative gain from this analysis remains low (e.g. from 379 bikz to 368 bikz for ntruhps2048509, improving the attack by about 3-4 bits).

This does *__not__* contradict the claims of the NTRU Specifications document, which only claimed 359 bikz because of conservative simplifications. We hope this clarify certain details of NTRU's cryptanalysis.

Best regards,

Dana, Léo, Huijing and Mélissa

From: Simone Dutto <simone.dutto@polito.it>
Sent: Friday, July 31, 2020 10:49 AM
To: pqc-comments
Cc: pqc-forum
Subject: ROUND 3 OFFICIAL COMMENT: NTRU
Attachments: fixed-sample.patch

Dear NTRU team,

while working with the C implementations found in the ZIP file attached to your submission (2nd round), we found a minor error in the code.
Specifically, in all files sample.c, line 86 should be

```
s[4*i+3] =  (u[15*i+11] & 0xfc)      + (u[15*i+12] << 8) + (u[15*i+13] << 16) + (u[15*i+14] << 24);
```

instead of

```
s[4*i+3] =  (u[15*i+11] & 0xfc)      + (u[15*i+12] << 8) + (u[15*i+13] << 15) + (u[15*i+14] << 24);
```

This is not a mandatory correction but, without it, the implemented sampling is not the one described in the documentation.

We saw that this correction is also necessary in the current version of the implementation at
https://github.com/jschanck/ntru/blob/master/ref-common/sample.c
Attached to this email there is the related github patch.

Hoping this comment will help, we thank you for your great work.

Best regards,
Simone Dutto