From: Nigel Smart <nigel.paul.smart@gmail.com>
Sent: Wednesday, January 17, 2018 12:33 PM
To: pqc-forum@list.nist.gov
Cc: Nigel Smart
Subject: [pqc-forum] LIMA
Attachments: signature.asc

Hi

Here is an update from the LIMA team. For those who have not read our submission I give a brief summary. It is a Ring-LWE scheme which is very conservative and has/had three differing features.

a) It has tight ROM based proofs of security (which other submissions also simultaneously came up with)
b) It has options to use safe-prime ring degrees to avoid issues with power-of-two cyclotomics if people are worried about them.
c) It uses rejection sampling on encryption to avoid decryption errors.

It is point c) that we want to address in this email.

Leixiao Cheng and Yunlei Zhao have pointed out to us a mistake in the analysis of point c, which seems hard to correct.

A simple fix is as follows

i) Delete the function RandCheck from the scheme
ii) Replace the rejection sampling on encryption with a "standard" analysis of decryption errors. Indeed in doing that we believe our parameters will become smaller (but a decryption error probability will come into the advantage statements).

So overall the "fix" will make our scheme faster, but will involve additional analysis, and more complex advantage statements.

If LIMA survives until the second round we will make these changes. But as changes are now "closed" for the first round we will leave as is.

We end this email by thanking Leixiao and Yunlei for their work in looking at the LIMA submission.

Yours

Nigel
(On behalf of the LIMA team)

--