From: Mike Hamburg <mike@shiftleft.org>
Sent: Tuesday, January 30, 2018 10:10 PM
To: pqc-comments
Cc: pqc-forum@list.nist.gov
Subject: OFFICIAL COMMENT: Three Bears
Signed By: mike@shiftleft.org

Hello PQCers,

While investigating failure probabilities for various proposed LWE systems, I found typos in the ThreeBears supporting documentation.

I copied the wrong entry from a table for BabyBear's failure probability. The correct (or at least, correctly copied) failure probability is 2^-135, not 2^-148. This doesn't affect the work for CCA attack, which I copied correctly as 2^122.

The text claims that all recommended instances have a failure probability of 2^-133 or less. This is true, but it should say 2^-135 or less. The 2^-133 failure probability is for one of the variants without forward error correction, which was recommended in an earlier draft but not in the final submission.

I am preparing a technical report on the difficulty of CCA attacks based on failures, which should add more nuance to the CCA attack estimates for ThreeBears, Hila5+FO, and maybe other systems.

Cheers,
— Mike

From: Mike Hamburg <mike@shiftleft.org>
Sent: Wednesday, January 31, 2018 2:14 PM
To: pqc-comments
Cc: pqc-forum@list.nist.gov
Subject: OFFICIAL COMMENT: Three Bears

Speaking of typos when copying things into tables, Table 2 lists:

BabyBear, d=2
MamaBear, d=3
PapaBear, d=3.

This should have PapaBear, d=4. The example software, analysis, benchmarks, object sizes etc use d=4.

My apologies to anyone who was doing analysis on these systems. If NIST wants they can remove the PapaBear parameter set for being a moving target, or they can consider this as just a typo correction.

Thanks to Fernando Virdia of the Estimate-All-The-LWE-and-NTRU-Schemes team for pointing out the typo.

— Mike