From: Moody, Dustin (Fed) <dustin.moody@nist.gov> via pqc-forum <pqc-forum@list.nist.gov>
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: [pqc-forum] 3rd Round Report correction
Date: Thursday, September 29, 2022 12:56:05 PM ET

Everybody,

We wanted to apologize for omitting an important paper from our report. In Section 3.2.3, we provided a brief history of some of the foundational papers in lattice-based cryptography. In doing so, we failed to highlight the contribution of the following paper:

Stehle D, Steinfeld R, Tanaka K, Xagawa K (2009) Efficient public key encryption based on ideal lattices. International Conference on the Theory and Application of Cryptology and Information Security (Springer), pp 617–635.

as introducing a search variant of ring-based LWE, with associated public-key encryption scheme. The report has been updated and can be found at:

https://doi.org/10.6028/NIST.IR.8413-upd1

Again, we apologize for the omission.

Thanks,

Dustin Moody

NIST PQC