From: vadim1980@gmail.com on behalf of Vadim Lyubashevsky <vadim.lyubash@gmail.com>
Sent: Friday, December 22, 2017 6:26 AM
To: pqc-comments
Cc: pqc-forum@list.nist.gov
Subject: OFFICIAL COMMENT: qTESLA

Dear Authors,

In Table 1, should |\Delta L| be ~ 2^{(d+1)n} instead of just 2^(d+1)? In Equation 7, the numerator is |\Delta L| and it's correctly stated as 2^{(d+1)n} there.

In the long equation in the middle of page 14, it looks as if you are correctly using |\Delta L|= 2^{(d+1)n}, but then it also looks as if you forgot to multiply by |\Delta S| because I don't see any B in there.

The main implication of having an incorrect |\Delta L| or forgetting to multiply by |\Delta S| is that it doesn't look that the condition needed for the qROM reduction from plain Ring-LWE can be satisfied (and so I don't think that Theorem 6 is correct ... I am not claiming that the scheme is insecure, though).

If I misunderstood something, I would be interested in seeing a more precise version; because having a Fiat-Shamir signature with a qROM reduction from plain Ring-LWE for such a small value of q would be a very interesting theoretical result.

Best,
-Vadim