From: Jan-Pieter D'Anvers <janpieter.danvers@esat.kuleuven.be>
Sent: Wednesday, January 17, 2018 7:27 AM
To: pqc-comments
Cc: pqc-forum@list.nist.gov
Subject: OFFICIAL COMMENT: CRYSTALS-KYBER

Dear all,

In the security proof of the IND-CPA security of Kyber [1] the values u'=A^T r+e_1 and v'= t^T r + e_2 in game G1, are substituted with uniform random values in game G2. The values (A,u) and (t,v') in game G1 are considered as samples from a Module-LWE distribution. In the definition of Module-LWE (section 2.3 of [1]) you state that the samples of a_i (in this case A and t), are sampled from a uniform distribution.
However, after compressing and decompressing t, its coefficients are not uniformly distributed in Z_q, and therefore it is not an MLWE sample. So I'm wondering how you arrive at the statement that |Pr[b=b' in game G1]−|Pr[b=b'in game G2]| ≤ Adv^mlwe_{k+1,k,mu}(B), since the last sample
(t,v') does not seem to be a valid Module-LWE sample.

If proving this step would be a problem, you could add a small error to t after decompression, to make its coefficients uniformly distributed in Z_q. Of course, this would result in a (slightly) bigger error and a
(small) increase in computational complexity.

Regards,

Jan-Pieter D'Anvers

[1] Joppe Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M. Schanck, Peter Schwabe, and Damien Stehlé.
Crystals – Kyber: a cca-secure module-lattice-based kem. Cryptology ePrint Archive, Report 2017/634, 2017.
https://eprint.iacr.org/2017/634

From: 赵运磊 <ylzhao@fudan.edu.cn>
Sent: Tuesday, January 23, 2018 3:50 AM
To: pqc-comments
Cc: pqc-forum@list.nist.gov
Subject: OFFICIAL COMMENT: CRYSTALS-KYBER

Dear All:
We also noticed this problem. There are sevrral approaches to deal with it.
The first is of couse to set $t_1=0$, as is done with the analysis of KCL; The second approach is to set $t_0\neq 0$, i.e., without changine protocol structure, then we need to use Renyi divergence technique for provable arguments. The third approach is as proposed by Jan-Pieter to add a new noise. We may prefer to the first approach, as it can further reduce the size of the ciphertext.

Best regards
Yunlei