From: Moody, Dustin (Fed)
To: internal-pqc
Subject: Fw: Core-SVPs for Kyber and Saber ?
Date: Tuesday, October 26, 2021 11:23:51 AM

From: Dang, Quynh H. (Fed) <quynh.dang@nist.gov>
Sent: Friday, October 22, 2021 9:50 AM
To: internal-pqc <internal-pqc@nist.gov>
Subject: Core-SVPs for Kyber and Saber ?

Hi all,

Kyber used block size 413 for their core-SVP estimates.

After accounting for "dimensions for free", the sieving dimension went down 38. So, the real sieving block size in the coreSVP is b = 375.

Saber used different numbers: block size (BKZ block) is 404 and the "dimensions for free" is 42. So, the real block size for sieving is only 362 (375 - 42) dimensions.

Kyber's spec seemed to say that progressive BKZ gains most comparing to fixed SVP block size at dimension 413 (even though smaller block sizes, the rates of improvement are bigger).

I dont know why Kyber chose # 413 and Saber chose # 404 for their dimensions. Also intuitively, the bigger the dimension, the bigger "dimensions for free" number should be. However, it is opposite for the claimed numbers from Saber and Kyber.

CoreSVP is 2^(constant. blocksize), so the blocksize increases, the number gets bigger. So, why is that at levels 3 and 5 Saber has more coreSVP bits then Kyber does ?

Comments will be appreciated.

Quynh.