From: Dang, Quynh H. (Fed)
To: Cooper, David (Fed)
Subject: Re: Kyber"s core-SVPs in Rd 2 and 3"s versions.
Date: Friday, March 18, 2022 1:56:08 PM

Thank you David.

Quynh.

From: Cooper, David A. (Fed) <david.cooper@nist.gov>
Sent: Friday, March 18, 2022 12:11 PM
To: Dang, Quynh H. (Fed) <quynh.dang@nist.gov>
Subject: Re: Kyber's core-SVPs in Rd 2 and 3's versions.

Hi Quynh,

If you look at Table 10 in the 4rd round report, you'll see the following for core SVP levels for Kyber:

Kyber512: C:118, Q:107
Kyber768: C: 183, Q:166
Kyber1024: C:256, Q: 232

If you look at the results of the Kyber.py script below on the lines that begin "Primal & ", you'll see the above numbers. So, this is where the core SVP numbers are being printed. It also shows core SVP numbers in the same place on the "Dual & " line, but presumably the Kyber team argues that these numbers should be ignored.

On 3/16/22 10:24 AM, David A. Cooper wrote:

```
Kyber512 (light):
--------------------
security:
Primal attacks uses block-size 406 and 486 samples; dim d=999
Primal & 486 & 406 & 118 & 107 & 84
Dual attacks uses block-size 403 and 512 samples; dim d=1024
shortest vector used has length l=3294.02, q=3329, `l<q'= 1
log2(epsilon) = -41.82, log2 nvector per run 83.63
Dual & 512 & 403 & 117 & 106 & 83
params:  {'n': 256, 'm': 2, 'ks': 3, 'ke': 3, 'ke_ct': 2, 'q':
3329, 'rqk': 4096, 'rqc': 1024, 'rq2': 16}
com costs:  (800.0, 768.0)
failure: 0.0 = 2^-139.1

Kyber768 (recommended):
--------------------
security:
Primal attacks uses block-size 626 and 650 samples; dim d=1419
Primal & 650 & 626 & 183 & 166 & 129
Dual attacks uses block-size 620 and 650 samples; dim d=1418
shortest vector used has length l=5003.21, q=3329, `l<q'= 0
log2(epsilon) = -64.32, log2 nvector per run 128.66
Dual & 650 & 620 & 181 & 164 & 128
params:  {'n': 256, 'm': 3, 'ks': 2, 'ke': 2, 'ke_ct': 2, 'q':
3329, 'rqk': 4096, 'rqc': 1024, 'rq2': 16}
com costs:  (1184.0, 1088.0)
failure: 0.0 = 2^-165.2

Kyber1024 (paranoid):
```

```
--------------------
security:
Primal attacks uses block-size 878 and 860 samples; dim d=1885
Primal & 860 & 878 & 256 & 232 & 182
Dual attacks uses block-size 868 and 838 samples; dim d=1862
shortest vector used has length l=5920.11, q=3329, `l<q'= 0
log2(epsilon) = -90.06, log2 nvector per run 180.13
Dual & 838 & 868 & 253 & 230 & 180
params:  {'n': 256, 'm': 4, 'ks': 2, 'ke': 2, 'ke_ct': 2, 'q':
3329, 'rqk': 4096, 'rqc': 2048, 'rq2': 32}
com costs:  (1568.0, 1568.0)
failure: 0.0 = 2^-175.2
```