From: Perlner, Ray A. (Fed)
To: Liu, Yi-Kai (Fed); Moody, Dustin (Fed); Cooper, David (Fed); internal-pqc
Subject: RE: NTRU Prime performance
Date: Monday, March 21, 2022 1:30:34 PM

FWIW, I think the reason both NTRU and NTRUprime have lower core SVP than kyber, when considering similar key sizes is that they are targeting perfect correctness, and therefore have narrower noise distributions.

Ray

-----Original Message-----
From: Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>
Sent: Monday, March 21, 2022 1:21 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Cooper, David A. (Fed) <david.cooper@nist.gov>; internal-pqc <internal-pqc@nist.gov>
Subject: Re: NTRU Prime performance

Thanks! I'll add this to the Overleaf document. Maybe I'd be inclined to say something more vague? It definitely seems useful to compare sntrup761 and ntrulpr761 with Kyber-768. But I'd prefer to be vague about what we should conclude from this, i.e., whether NTRU Prime is similar to Kyber, or worse than Kyber. (Both conclusions seem like fuel for future flame wars.)

--Yi-Kai

_____
From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Monday, March 21, 2022 10:10 AM
To: Cooper, David A. (Fed); internal-pqc
Subject: Re: NTRU Prime performance

David,

The NTRU Prime webpage (security tab) says that the 761 parameter sets have 153 and 155 coresvp. See
https://ntruprime.cr.yp.to/security.html
That is a little less than Kyber 768 which has 183 bits. Saber2 (category 3) claims 189 bits of coresvp.

Dustin

_____
From: Cooper, David A. (Fed) <david.cooper@nist.gov>
Sent: Friday, March 18, 2022 4:04 PM
To: internal-pqc <internal-pqc@nist.gov>
Subject: NTRU Prime performance

Hi all,

I've been thinking about bit about concerns that the NTRU Prime team (DJB) will complain (as they have already done) that we unfairly penalized NTRU Prime by comparing its performance against parameter sets from other schemes with lower security levels due to their "bulletproofing" method of assigning security levels.

According to the numbers that I've computed from the SUPERCOP benchmark results (see table below), whether the cost of key generation is taken into account or not, the cost of NTRU Prime's recommended parameter sets, sntrup761 and ntrulpr761, is comparable to the cost of Kyber768 and Saber2. I can't figure out what the core SVP hardness is for sntrup761 or ntrulpr761, but my guess is that it is significantly lower than for Kyber768 or Saber2.

This could be particularly significant if we end up not including Kyber512 in the standard.

In the NTRU Prime section perhaps we could add a footnote to the end of the following sentence:

This did not invalidate the original parameter sets for NTRU Prime, but it moved them to lower security levels, so that they are roughly comparable to other structured lattice-based cryptosystems, in terms of quantitative security and performance.

that says:

The parameter sets recommended by the NTRU Prime submission team, sntrup761 and ntrulpr761, have performance comparable to {\Kyber}768.

Submission Parameter Set
Key gen encrypt decrypt
Public
Key ciph. Public key + ciph. total cost w/o key gen (1000 cycles/byte) total cost w/ key gen (1000 cycles/byte) total cost w/ key gen (2000 cycles/byte)
CRYSTALS-Kyber 512
25,435 39,888 31,162
800 768 1,568 1,639,050 1,664,485 3,232,485
CRYSTALS-Kyber 512-90s
16,676 25,669 19,874
800 768 1,568 1,613,543 1,630,219 3,198,219
CRYSTALS-Kyber 768
44,178 60,258 47,766
1,184 1,088 2,272 2,380,024 2,424,202 4,696,202
CRYSTALS-Kyber 768-90s
26,536 38,021 29,869
1,184 1,088 2,272 2,339,890 2,366,426 4,638,426
CRYSTALS-Kyber 1024
60,539 83,340 67,488
1,568 1,568 3,136 3,286,828 3,347,367 6,483,367
CRYSTALS-Kyber 1024-90s
39,422 54,143 43,884
1,568 1,568 3,136 3,234,027 3,273,449 6,409,449

Saber LightSaber2
42,504 58,013 57,786
672 736 1,408 1,523,799 1,566,303 2,974,303
Saber Saber2
74,465 95,103 93,596
992 1,088 2,080 2,268,699 2,343,164 4,423,164

Saber FireSaber2
114,216 139,124 138,690
1,312 1,472 2,784 3,061,814 3,176,030 5,960,030

NTRU ntruhps2048677
286,881 37,109 61,550
930 930 1,860 1,958,659 2,245,540 4,105,540
NTRU ntruhrss701
269,191 26,510 63,375
1,138 1,138 2,276 2,365,885 2,635,076 4,911,076
NTRU ntruhps4096821
414,070 44,119 81,114
1,230 1,230 2,460 2,585,233 2,999,303 5,459,303

NTRU Prime ntrulpr653
70,036 72,259 78,215
897 1,025 1,922 2,072,474 2,142,510 4,064,510
NTRU Prime sntrup653
668,114 61,487 58,609
994 897 1,891 2,011,096 2,679,210 4,570,210
NTRU Prime sntrup761
879,472 67,373 61,049
1,158 1,039 2,197 2,325,422 3,204,894 5,401,894
NTRU Prime ntrulpr761
74,597 76,455 82,367
1,039 1,167 2,206 2,364,822 2,439,419 4,645,419
NTRU Prime ntrulpr857
86,601 94,857 103,337
1,184 1,312 2,496 2,694,194 2,780,795 5,276,795
NTRU Prime sntrup857
1,107,741 78,848 80,624
1,322 1,184 2,506 2,665,472 3,773,213 6,279,213