From: Perlner, Ray A. (Fed)
To: Cooper, David (Fed); internal-pqc
Subject: RE: NTRU key generation
Date: Friday, October 29, 2021 4:01:51 PM

I strongly suspect no one bothered to optimize NTRU key generation for M4. The NTRUprime specification reports that sNTRUprime761 keygen takes 10,777,811 cycles on an m4 processor, which is pretty much inline for what I'd expect for NTRU given the Haswell numbers. I find it pretty close to inconceivable that the differences between the specification of NTRU and sNTRUprime are significant enough to make sNTRUprime key generation 15 times faster than NTRU if both implementations have been optimized.

From: Cooper, David A. (Fed) <david.cooper@nist.gov>
Sent: Friday, October 29, 2021 2:56 PM
To: internal-pqc <internal-pqc@nist.gov>
Subject: NTRU key generation

Hi all,

I've been looking into the cost of key generation for NTRU. On the Haswell processor, the cost in clock cycles seems reasonable, even though it is about 10 times as expensive as Kyber or Saber. According to https://bench.cr.yp.to/results-dh.html#amd64-hiphop, key generation for P-256 is about 273,000 cycles, and ECC key generation is generally considered fast enough for ephemeral use.

What puzzles me is the key generation on the M4, where the numbers are very slow for NTRU. The table below shows the clock cycles for both Haswell and M4 for various operations on Kyber, Saber, and NTRU, along with the ratio of the ratio of the cost in cycles between the processes. Note that all of the ratios are less than 17 except for NTRU key generation where the ratios are well over 400!

Does anyone have a guess as the to reason for the M4 numbers? Are there instructions on Haswell that are useful for NTRU key generation (but not for any other operations), where the same calculation is very expensive to calculate without, or could this be an indication that NTRU key generation simply hasn't been optimized for the M4 and a better implementation might be 10 to 20 times faster?

Thanks,

David

	key Gen			Encap			Decap		
	Haswell	M4	ratio	Haswell	M4	ratio	Haswell	M4	ratio
Kyber512	33,856	457,126	13.50	45,200	551,681	12.21	34,572	511,970	14.81
Kyber768	52,732	744,136	14.11	67,624	898,630	13.29	53,156	838,939	15.78
Kyber1024	73,544	1,190,374	16.19	97,324	1,373,614	14.11	79,128	1,295,290	16.37
LightSaber	45,232	352,196	7.79	62,236	481,006	7.73	62,624	452,654	7.23
Saber	80,340	645,222	8.03	103,204	820,799	7.95	103,092	774,055	7.51

FireSaber	126,220	994,446	7.88	153,832	1,204,260	7.83	155,700	1,151,016	7.39
NTRUhrss701	340,823	149,737,679	439.34	50,441	375,948	7.45	62,267	867,921	13.94
NTRUhps204877	309,216	143,750,608	464.89	83,519	820,054	9.82	59,729	812,608	13.60
NTRUhps4096821	431,667	208,835,960	483.79	98,809	1,027,338	10.40	75,384	1,031,141	13.68