**From:** Dang, Quynh H. (Fed)
**To:** Cooper, David (Fed); Moody, Dustin (Fed); internal-pqc
**Subject:** Re: Kyber768 vs Ntruhps2048677.
**Date:** Monday, March 7, 2022 12:23:57 PM

---

The traffic protected by AES256 and curve384 and curve521 is tiny comparing with the traffic protected by Curve256 and Curve25515 and AES128.

Commonly, users choose secure functions which have the best performance for them.

I think that performance on AVX2 is more important than performance on pqm4. TLS servers do encap. Ntruhps677's encap (83,519) is faster than Kyber768's encap (83,748). One can say the difference is small and that is correct but better is better.

Overall performance differences are (4,792,796 - 4,176,464)/4,176,464 = 14.75% or (4,760,448 - 4,176,464)/4,176,464 = 13.98%.

Likely that the matrix A is saved in TLS for decap, but I don't know what most people would do.

Likely that TLS or Ipsec is going to be a real first adopter of a PQKEM.

Quynh.

---

**From:** Cooper, David A. (Fed) <david.cooper@nist.gov>
**Sent:** Monday, March 7, 2022 10:35 AM
**To:** Moody, Dustin (Fed) <dustin.moody@nist.gov>; Dang, Quynh H. (Fed) <quynh.dang@nist.gov>; internal-pqc <internal-pqc@nist.gov>
**Subject:** Re: Kyber768 vs Ntruhps2048677.

Setting aside the security and IP issues (since I have no basis for forming an opinion on those), it doesn't seem that NTRU is a clear win in terms of performance over Kyber.

While it is true that the overall cost of Kyber768 is more than for ntruhps2048677, it is only 13% faster, which seems rather insignificant. In addition, the NTRU team recommends the ntruhrss701 parameter set, and that one has a higher overall cost than Kyber768. While the difference between Kyber768 and ntruhrss701 is negligible, Kyber768 has a much higher core SVP number, so one is getting a much bigger security margin for either slightly more or slightly less cost than the NTRU alternatives.

In addition, the above only applies to the AVX2 numbers. With the PQM4 benchmark numbers, mostly as a result of key generation times, Kyber768 is faster than either

ntruhps2048677 or ntruhrss701. Without key generation, all three seem to have about the same overall cost on the M4. Notably, however, the Kyber768 implementation requires only 2,824 bytes of RAM and 14,528 bytes of flash, whereas ntruhps2048677 (ntruhrss701) implementation requires 19,728 (20,560) bytes of RAM for decapsulation (more for key generation) and 281,696 (264,688) bytes of flash. While I believe NTRU could be implemented with fewer resources than used by the current PQM4 implementation, the result could be even slower. In addition, while we know that Kyber768 can be implemented on the M4 with a small amount of RAM and flash, we can only speculate about NTRU.

So, Kyber768 offers performance that is either better than or almost as good as NTRU, while using fewer resources and offering substantially more security. If we had only chosen Kyber over NTRU for performance reasons, then perhaps some reconsideration would be necessary, if Kyber512 were dropped, but it doesn't seem that performance by itself provides a compelling reason to switch.

David

On 3/7/22 9:14 AM, Moody, Dustin (Fed) wrote:

> Quynh,
>
> We can certainly discuss, however, we do not have to pick the parameter sets right now. In my mind, that is one of the decision's we'll make while writing the standard.
>
> It's not quite an even comparison to compare NTRU level 1 to Kyber level 3 and then judge the performance. But I get why you're comparing them. Anybody else want to comment?
>
> Dustin
>
> ---
>
> **From:** Dang, Quynh H. (Fed) <quynh.dang@nist.gov>
> **Sent:** Monday, March 7, 2022 9:00 AM
> **To:** internal-pqc <internal-pqc@nist.gov>
> **Subject:** Kyber768 vs Ntruhps2048677.
>
> Hi all and Dustin,
>
> As we discussed on Friday, if we don't standardize Kyber512, I think I would have to rethink about our KEM decision. Below are AVX2 numbers where each byte is treated as 2k cycles.
>
> Kyber768: 62,396 + 83,748 + 102,652 + (pk:1184 + ct:1088)x2000 = 4,792,796.

Kyber768: 62,396 + 83,748 + 70,304  + (pk:1184 + ct:1088)x2000 = 4,760,448 when matrix A is saved, not generated from a seed in decapsulation.

Ntruhps2048677: 309,216 + 83,519 + 59,729  (pk:931 + ct:931)x2000  = 4,176,464.

Ntruhps2048677 is a better choice in performance.

In security, we prefer MLWE over NTRU. However, this preference is not a big factor in our decision I think.  There are strong arguments for both.

People would likely even argue that with the 2 patents resolved, the ip risk for Kyber and Saber would be still higher than NTRU.

I am not sure how people would think about the money we spend on the 2 patents in this situation when Kyber512 is out.

Quynh.