From: D. J. Bernstein <djb@cr.yp.to>
Sent: Sunday, January 13, 2019 8:20 PM
To: pqc-comments
Cc: pqc-forum@list.nist.gov
Subject: OFFICIAL COMMENT: NTRU-HRSS-KEM
Attachments: signature.asc

Regarding NTRU Prime, I wrote:
> I expect further speedups in Streamlined NTRU Prime and in various
> other submissions relying on Euclid-type algorithms. For example, it
> should be very easy to adapt the inversion-mod-3 part of the new
> software to save
> 60000 cycles in NTRU-HRSS key generation.

This adaptation is now online as part of supercop-20190110; ntruhrss701 keygen is now just 238128 cycles on titan0 (Haswell), where previously it was 299684 cycles on the same machine.

(The submission said 294874 cycles on another Haswell. Presumably the gap between 294874 cycles and 299684 cycles comes from differences in how well different gcc versions optimize some auxiliary C functions. The earlier inversion-mod-3 code was in asm, and the new code is in C with intrinsics, with noticeable differences in vectorization from gcc 5 through gcc 8. SUPERCOP 2 will show these effects more systematically.)

---Dan