From: Moody, Dustin (Fed)
To: Kenney, Craig L. (Fed); clk8@njit.edu
Subject: Re: PQC Constant Time Testing
Date: Monday, August 19, 2019 5:26:16 PM

Craig,

Thank you. I don't think I've met you yet. Most of the PQC team is attending our workshop this week, but we will definitely look at this when we return.

Dustin Moody
NIST PQC team

From: Alperin-Sheriff, Jacob (Fed) <jacob.alperin-sheriff@nist.gov>
Sent: Friday, August 16, 2019 4:54 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Perlner, Ray (Fed) <ray.perlner@nist.gov>; Apon, Daniel C. (Fed) <daniel.apon@nist.gov>
Subject: FW: PQC Constant Time Testing

From: "Kenney, Craig L. (Fed)" <craig.kenney@nist.gov>
Date: Friday, August 16, 2019 at 3:59 PM
To: "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>
Subject: PQC Constant Time Testing

Hello,

This is Craig Kenney, we spoke quite a while ago about my helping out on the PQC project by making sure implementations actually ran in constant time while I was here, and since it is the last day of my internship it's about time I reported. First of all, sorry for not being in contact – I ended up with a bit less time to work on this than I thought I'd have, and this ended up being pushed to the backburner just around the time I was feeling I should check in. Regardless, I do hope what I have put together is useful after I'm gone.

You told me to focus on the submissions with AVX implementations, so that is what I have done. Attached to this email is an excel spreadsheet covering code inspection and sanity check testing (by compiling and running either my own test code or modified existing test code) on roughly half of the AVX implementations (sorry about GeMSS, that one turned into a bit of a nightmare and I wanted to move on rather than keep spending time on it).

Most of the ones I tested do seem to be in constant time with respect to secret information, though sanity checking was of less use than I had thought it would be at first given the abundance of rejection sampling. I had intended to add annotations to use an automated tool like ctgrind/ctverif/dudect to further check my inspections, but lack of time pushed that off; it might be a good idea in the future though. I also discovered some oddities and bugs with several of the implementations, if that is of any use; LWC round 1 didn't really care about the implementations all that much from my experience working on that, but I ran into these things and figured it would be a waste not to note them, and that if you want the code in constant time they matter more for PQC round 2.

Anyway, I hope this is helpful to the PQC project, and I apologize again for basically disappearing for the duration of my internship. If anything needs clarification you can contact me at my academic email address, clk8@njit.edu as I don't believe I will have access to this one anymore after today.

Thanks for the opportunity,
Craig Kenney