From: Moody, Dustin (Fed)
To: Miller, Carl A. (Fed)
Subject: Re: PQC Round 2 report assignments
Date: Friday, June 5, 2020 3:02:48 PM

Sure, that sounds like a good revision.

For the cycle counts, I looked at their recent paper:

https://falcon-sign.info/falcon-impl-20190918.pdf

> New E˙icient, Constant-Time Implementations of Falcon
>
> New E˙icient, Constant-Time Implementations of Falcon ThomasPornin NCCGroup,thomas.pornin@nccgroup.com Abstract. AnewimplementationofFalconispresented ...
>
> falcon-sign.info

From: Miller, Carl A. (Fed) <carl.miller@nist.gov>
Sent: Friday, June 5, 2020 2:54 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: PQC Round 2 report assignments

Hi Dustin –

I checked the factors and they look good to me. Comparing speed between qTESLA and Falcon was harder for me to do directly, because it didn't seem like Falcon gives cycle counts for its operations, but the speed comparison between qTESLA and Dilithium looks right.

One wordsmithing comment: we write:
In particular, the public key sizes of q-TESLA-p-I and qTESLA-p-III are about 15-20 times larger than FALCON and CRYSTALS-DILITHIUM, and the signature sizes are larger as well. In comparing cycle counts required for signing and verifying, qTESLA is roughly 2-5 times slower than the other two lattice-based signature schemes which are moving on.

It may be confusing that we first refer to FALCON and CRYSTALS-DILITHIUM, and then refer to "the other two lattice-based signature schemes which are moving on" (which are the same two schemes). We could replace the latter phrase with "FALCON and CRYSTALS-DITHIUM" also?

-Carl

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Friday, June 5, 2020 at 12:49 PM

To: "Miller, Carl A. (Fed)" <carl.miller@nist.gov>
Subject: Re: PQC Round 2 report assignments

Carl,
I added in some approximate numbers to show qTESLA isn't competitive. Can you double check the relative comparison factors I used? Thanks,

Dustin

From: Miller, Carl A. (Fed) <carl.miller@nist.gov>
Sent: Thursday, June 4, 2020 9:54 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: PQC Round 2 report assignments

Ok, sure, I'll add some details to the end. My impression is that the public keys for qTESLA are significantly worse in size than for Falcon and Dilithium, and that qTESLA isn't better by any other metric. (Not sure about speed – I'll try to find the right comparison chart from our slides.)

-Carl

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Thursday, June 4, 2020 at 9:49 AM
To: "Miller, Carl A. (Fed)" <carl.miller@nist.gov>
Subject: Re: PQC Round 2 report assignments

Carl,
I saw that. It looks good. We may want to add in more detail, but I'm not yet sure. Specifically, it may turn out we want to cite sources for attacks on schemes. In which case we'd cite the forum posts on qTesla. But we may decide that isn't necessary. Let's not worry about it right now.

We should probably expand on the last sentence more, though. We could describe a little bit more the difference in performance between qTesla and its competitors to make it clear why it isn't moving on.

Thanks,

Dustin

From: Miller, Carl A. (Fed) <carl.miller@nist.gov>
Sent: Thursday, June 4, 2020 9:42 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: PQC Round 2 report assignments

Hi Dustin –

Yesterday I added to our draft a comment on qTESLA (clipped in below). If there's any part that you think should be fleshed out, you can let me know. (I did some reading about qTESLA this week and am pretty well caught up on it.) Talk to you later!

-Carl

qTESLA

qTESLA is a structured lattice-based signature scheme (like FALCON and CRYSTALS-DILITHIUM). The public keys in qTESLA consist of LWE samples within a ring over **Z** mod **q,** and signing is performed using hash functions and further arithmetic in the ring.

The second-round version of qTESLA that was submitted to NIST specified twelve different parameter sets (q-TESLA-*, q-TESLA-*-s, and q-TESLA-p-*). After some questions were raised about the security arguments in the specification, the authors retracted ten of the parameter sets and kept the remaining two (q-TESLA-p-I, qTESLA-p-III). Although there is benefit to having a diversity of design among lattice-based candidates, the performance of the two remaining parameter sets q-TESLA-p-I and qTESLA-p-III is not strong enough to remain competitive.

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Wednesday, May 27, 2020 at 11:21 AM
To: internal-pqc <internal-pqc@nist.gov>
Subject: PQC Round 2 report assignments

Everyone,
We need to edit more our round 2 report. It is accessible on sharepoint at:

PQC Report on Round 2.docx

I'd like to give out some assignments as we continue our selection. There are two types:

1) I've already sort of written much of the text, mostly adapted straight from the round 1 report. We need to re-write it for the round 2 report, adding in relevant info. Feel free to propose adding new sections or info.

- Yi-Kai, Section 1 - Introduction
- Ray, Section 2.2.1 - Security
- David, Section 2.2.2 - Performance
- Quynh, Section 2.2.3 - Algorithm and implementation char.

Daniel ST, Section 2.3 - selection of 3rd round candidates

- Angela, Section 4 - Conclusion. Maybe add in something about the on ramp idea (esp. for non-lattice general purpose signatures)

2) The most important part will be section 3, where we discuss each candidate. Please add info, either with bullet points or just writing it out. Address our evaluation criteria. Some schemes already have this started. Here is where we need to justify our decisions.

- Gorjan, Kyber, Frodo, NTRU
- Yi-Kai, LAC
- Daniel A, New Hope, NTRUprime, Saber, 3 bears
- Angela, Round 5, Rollo, HQC
- Ray, Classic McEliece, Bike, LEDAcrypt, RQC
- Carl, qTesla, check falcon and dilithium
- Quynh, GeMSS
- Daniel ST, LUOV, MQDSS
- David, check sphincs+, picnic
- Rene, picnic, check SIKE
- John, (already done some), any you feel like

Of course, please do look at the whole report and make edits/comments any where you wish. Let's see if we can have everybody do this by next Wednesday (one week), so we will have a complete first draft. This is just a first step. Thanks everyone!

Dustin