From: Bassham, Lawrence E (Fed)
To: Moody, Dustin (Fed)
Subject: Re: Open Quantum-Safe library
Date: Tuesday, August 23, 2016 1:18:56 PM

I got it. Just did a quick look at it, but I image we can make them work together. Seems like the interface between the two might be algorithm specific.

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Tuesday, August 23, 2016 at 11:05 AM
To: "Bassham, Lawrence E (Fed)" <lawrence.bassham@nist.gov>
Subject: FW: Open Quantum-Safe library

Larry,

I haven't heard back from you. Just wanted to check you got this email. Let me know. Thanks,

Dustin

From: Moody, Dustin (Fed)
Sent: Monday, August 15, 2016 10:59 AM
To: Bassham, Lawrence E (Fed) <lawrence.bassham@nist.gov>
Cc: Perlner, Ray (Fed) <ray.perlner@nist.gov>; Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>
Subject: Open Quantum-Safe library

Larry,

At the SAC workshop that Ray and I attended, there was a guy named Douglas Stebila who talked about something he's doing with Mike Mosca for implementing/benchmarking PQC algorithms called "Open Quantum-Safe". Can you take a look at it? I hope our API is compatible with theirs, or if not, that we can coordinate with them to make it work. The part where he talks about it is slides 64 to 67 of the following:

https://s3.amazonaws.com/files.douglas.stebila.ca/files/research/presentations/20160812-SAC.pdf

The github repository is available at:

https://github.com/open-quantum-safe/liboqs

Doug has been doing work in a lattice-based key-exchange protocol that would be suitable for TLS, so I bet his implementation is on the github site.

Let me know. Thanks!

Dustin