From: Moody, Dustin (Fed)
To: (b) (6)
Subject: RE: [Pqc-forum] Feedback on Libraries Likely to Be Used Across Many Different Submissions
Date: Wednesday, July 26, 2017 1:21:00 PM

There were a few requests to include GMP. I talked with Ray, Larry, and John, and they seemed to think that wasn't unreasonable. The conversation extended to the idea that perhaps a few other libraries might be made available. Larry wanted to know what other libraries people would want. He is thinking about setting up a virtual machine where people could check their builds to see if everything will compile correctly when we have to do it here. He wants the headaches to be on the submitters' end, not on his end. We were talking about making the reference version include everything, but the optimized version could call a few standard libraries without needing to include them. What do you think of that idea?

I agree we don't want to have too many libraries. Hopefully we can keep life simple both for us and submitters.

Dustin

From: Daniel Smith (b) (6)
Sent: Wednesday, July 26, 2017 12:18 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: [Pqc-forum] Feedback on Libraries Likely to Be Used Across Many Different Submissions

Do we really want to ask everyone what the must have builds of their favorite libraries are? Are we going to have too many responses with obscure libraries that people claim are standard? I feel like we have discussed this at length before. Has something really changed as we are approaching the last months before the deadline?

Did Larry say anything about this?

On Wed, Jul 26, 2017 at 11:05 AM Alperin-Sheriff, Jacob (Fed) <jacob.alperin-sheriff@nist.gov> wrote:

> All,
>
> In response to the feedback on our initial policy regarding how open-source libraries may be used and included in submissions, we are considering providing a guarantee that specific versions of a few libraries that we expect to be used across many different submissions will already be pre-installed on the reference platform, in order to make submissions packages smaller and easier to create for those not using specialized open-source libraries.
>
> Specifically, we expect that should we end up providing such a guarantee, it will include (version and build TBD):
>
> - gmp
> - NTL

> Are there any others that we are missing?
> Please let us know which exact version and build should be used (both for the above two libraries and any other libraries you feel will be ubiquitous), rather than just the name of the library.
> Thanks!
>
> —Jacob Alperin-Sheriff