

From: [Moody, Dustin \(Fed\)](#)
To: [Kerman, Sara J. \(Fed\)](#)
Subject: RE: revise a couple of PQC FAQ's
Date: Monday, August 7, 2017 9:55:40 AM
Attachments: [A16.docx](#)

Q3 and A3 are pretty much 100% different. So I don't think we'd need to do a track changes, but just archive the old question and answer.

A16 basically has two new paragraphs added. (In the email below, the first two paragraphs are completely new. The rest basically says the same as our previous answer, but Jacob removed the list with 1. 2. and 3.

I've attached a word doc that has the changes for A16 changed. It doesn't look very pretty!

From: Kerman, Sara J. (Fed)
Sent: Monday, August 07, 2017 9:39 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: RE: revise a couple of PQC FAQ's

Hey Dustin,
Previous archives, when the answer was changed, we showed it with track-changes.
<http://csrc.nist.gov/groups/ST/post-quantum-crypto/archive/faq-historical.pdf>

Can you let me know what changed?

Sara

From: Moody, Dustin (Fed)
Sent: Thursday, August 03, 2017 3:35 PM
To: Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Subject: revise a couple of PQC FAQ's

Sara,
We'd like to revise two of our FAQ's. See the new ones below. I guess we should put the old answers in the archive. Again – no rush. Thanks!

Dustin

Revised Text

Q3: What exceptions, if any, are there to the requirement for ANSI C source code? In particular, may C++ code or assembly optimizations be used?

A3:

For both the mandatory reference implementation and the mandatory optimized implementations, all new code written by submitters for the submission should be written in as ANSI C-like a manner as possible, subject to some caveats.

In particular, implementations that use NTL (see Question and Answer 16 for details on the use of third-party open source libraries) are necessarily allowed to be written in C++. However, the original and new code in this submission must still be as ANSI C-like as possible, and should only use C++ functionality where absolutely required in order to use NTL. In particular, as with code using any other third-party open source code, the submission must contain build scripts for both Windows and Linux that compile properly on the Intel x64 reference platform using version 6.4.0 of the GNU Compiler Collection (GCC).

Furthermore, while submitters may not write their own new and original assembly (including inline assembly) code for either the mandatory referenced implementation or the mandatory optimized implementation, we are allowing the use of third party open-source libraries that themselves rely on assembly optimizations, subject to the constraints described in Question and Answer 16.

Any optional additional implementations that submitters wish to include are subject to no constraints at all regarding the language and platform.

Q16: [Can third party open-source code be used in submissions?](#)

A16:

In both the mandatory reference implementation and the mandatory optimized implementation, submissions may use NTL Version 10.5.0 (<http://www.shoup.net/ntl/download.html>), GMP Version 6.1.2 (<https://gmplib.org>), and OpenSSL Version 1.10f (<https://www.openssl.org/source>). Submitters may assume that these libraries are installed on the reference platform and do not need to provide them along with their submissions.

If a submitter wishes to use a third-party open source library other than the ones specified above, they must send a request to NIST at pgc-comments@nist.gov by September 1st, 2017, with the name of the library and a link to the primary website hosting it from which it may be downloaded. NIST will either approve or deny this request within 2 weeks of receiving it. Should a request be approved, it will be added to the above list of acceptable third-party open source libraries provided in this FAQ.

All submission packages using third-party open source code should contain build scripts which will allow for seamless “one-stop” building of the submissions.

For example, on a Linux platform, it should require no more work to build the than running the standard

```
> ./configure [--options]
```

```
> make
```

```
> make install
```

succession of commands. In particular, the build process should be able to find the versions of these

libraries specified above that will be pre-installed on the reference platform.

Separate build scripts should be included for the reference Windows platform and reference Linux platform that work using the GNU Compiler Collection version 6.4.0 and related tools as well as any platform-specific commands required.

In addition, as part of the written submission, the submitter shall describe in their own words the functionalities provided by any algorithms from third-party open-source libraries that are used in the implementations.