From: Kelsey, John M. (Fed)
To: internal-pqc
Subject: Re: PQC Round 2 report assignments
Date: Thursday, June 4, 2020 12:19:49 PM

Would it make sense to specifically call out the large key, small ciphertext/signature thing as a separate performance profile? Classic McEliece, Rainbow, and GeMSS all fit this profile. There's a little test in the document now, but I wonder if it makes sense to call this out as its own thing

--John

From: "David A. Cooper" <david.cooper@nist.gov>
Date: Thursday, June 4, 2020 at 10:11
To: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>, "Dang, Quynh H. (Fed)" <quynh.dang@nist.gov>, internal-pqc <internal-pqc@nist.gov>
Subject: Re: PQC Round 2 report assignments

As I noted in a comment in the document, I think we also discussed:

> It is straightforward to customize the scheme's parameters to meet a range of security targets and performance goals.

When discussing the structured lattice candidates and their CoreSVP strength, we discussed how difficult it would be to tweak the parameters of the different schemes in order to bump up their level of security.

We also very briefly talked about whether the KEM schemes could be used in other ways, such as password-based authenticated key exchange (e.g., the PAKE):

> The scheme can be modified to provide additional functionalities that extend beyond the minimum requirements of public-key encryption, KEM, or digital signature (e.g., asynchronous or implicitly authenticated key exchange, etc.).

I'm not sure whether either of these items warrant a mention (perhaps as things that could impact our final decisions), but if so, then Section 2.2.3 would be the place for that.

On 6/4/20 10:00 AM, Moody, Dustin (Fed) wrote:

> Quynh,
>
> In our CFP we identified 3 main evaluation areas: security, performance, and algorithm and implementation characteristics. I think we should have this section still. It doesn't need to be long. See below for what we wrote about this in the original CFP for algorithm and implementation characteristics. Just write a short summary of this. Relative to round 2 we could add that we have seen some experiments looking into whether the schemes can be incorporated into existing protocols.
>
> For IPR, I don't want much about this in the report, certainly not specific details.

Just a sentence mentioning that this topic is a factor in our decision making process.

Is that alright?

Dustin

4.C.1 Flexibility Assuming good overall security and performance, schemes with greater flexibility will meet the needs of more users than less flexible schemes, and therefore, are preferable.

Some examples of "flexibility" may include (but are not limited to) the following:

a. The scheme can be modified to provide additional functionalities that extend

   beyond the minimum requirements of public-key encryption, KEM, or digital signature (e.g., asynchronous or implicitly authenticated key exchange, etc.).

2. It is straightforward to customize the scheme's parameters to meet a range of security targets and performance goals.
3. The algorithms can be implemented securely and efficiently on a wide variety of platforms, including constrained environments, such as smart cards.
4. Implementations of the algorithms can be parallelized to achieve higher performance.
5. The scheme can be incorporated into existing protocols and applications, requiring as few changes as possible.

4.C.2 Simplicity The submitted scheme will be judged according to its relative design simplicity.

4.C.3 Adoption Factors that might hinder or promote widespread adoption of an algorithm or implementation will be considered in the evaluation process, including, but not limited to, intellectual property covering an algorithm or implementation and the availability and terms of licenses to interested parties. NIST will consider assurances made in the statements by the submitter(s) and any patent owner(s), with a strong preference for submissions as to which there are commitments to license, without compensation, under reasonable terms and conditions that are demonstrably free of unfair discrimination.