From: Alagic, Gorjan (Assoc)
To: Cooper, David (Fed); Regenscheid, Andrew R. (Fed); internal-pqc
Subject: Re: PQC
Date: Monday, June 29, 2020 12:50:33 PM

I agree that predictability (from the point of view of the greater community) is important.

One comment about Frodo: if we end up standardizing Frodo as a replacement for structured lattices, this will not be just a surprise, but a huge shock. Depending on the details of how this happened, we might want to sit down and completely rethink the entire process. In any case, I view this as an extremely low probability event, so there is probably not a need to spend a lot of time thinking in detail about how to handle it now.

For the other potential "alternate gets standardized next round" scenarios, I don't have such a strong opinion, and I can definitely see this ambiguity leading to people wondering what they should be working on and which schemes they should be implementing (or preparing to implement.) So more clarity from us, if possible, does seem like a good idea. Do we only see alternates getting standardized in the next round in a "cryptanalysis catastrophe" scenario? Or are there other, more plausible routes to them getting standardized? If yes, what are these routes and how likely do we think they are?

Gorjan

From: David A. Cooper <david.cooper@nist.gov>
Sent: Monday, June 29, 2020 12:41 PM
To: Regenscheid, Andrew R. (Fed) <andrew.regenscheid@nist.gov>; internal-pqc <internal-pqc@nist.gov>
Subject: Re: PQC

I agree entirely. When we were talking about the two track approach, I thought there was to be clear distinction: decisions about finalists would be made in the third round and decisions about alternates would not be made until the fourth round. This would make it clear to those who would be looking at all of the candidates, e.g., groups developing hardware implementations, that it would be okay to just work on the finalists during round three, and that work on the alternates could wait until later.

Our current text isn't so clear. By merely saying that we are "unlikely" to standardize an alternate at the end of round three, that creates confusion. If my goal is to implement all algorithms that might be standardized before the standardization decision is made, can I implement just the seven finalists during the third round or do I need to implement all 15 remaining candidates since any of the alternates "could" be standardized at the end of the third round.

If we aren't going to impose a strict rule of "no selecting alternates at the end of the third round," then I think we should at least say that we won't select an alternate for standardization at the end of the third round unless we make an announcement about it at some point during the third round of evaluation. The amount of time between the announcement and the end of the third round needs to be long enough that people feel they have been given a fair chance to review the algorithm.

David

On 6/29/20 12:12 PM, Regenscheid, Andrew R. (Fed) wrote:

> One of the main things you want in these processes is predictability. It's not enough to say we might do something- people have to expect it. We learned that one in SHA-3.
>
> I've been somewhat concerned that we're sending mixed messages the alternates. In general, we're saying we don't plan to standardize any of them right away (until after a 4th round) except that we want to carve out some leeway so that we could if we really wanted to. The main case for that would probably be SPHINCS+, which we allude to in the report. Perhaps you could imagine Frodo being another case for that.
>
> I don't think we want there to be any surprise if we get to the end of round 3 and we decide we're going to standardize SPHINCS+, Frodo, or one of the other four examples John cited. I think we'd want to signal that clearly, and somewhat formally, in advance. That's where the idea of "elevating" an alternate to a finalist came in.
>
> -Andy
>
> **From:** Kelsey, John M. (Fed) <john.kelsey@nist.gov>
> **Sent:** Monday, June 29, 2020 12:03 PM
> **To:** Moody, Dustin (Fed) <dustin.moody@nist.gov>; internal-pqc <internal-pqc@nist.gov>
> **Subject:** Re: PQC
>
> It seems weird to phrase it that way. I think the point of Andy's sentence there is that we may decide to standardize one of the alternates at the end of the third round, right? But I don't think that would change the fact that we had already named some things as finalists and others as alternates. I mean, if all the structured lattice KEMs get broken or dented and we decide to standardize Frodo at the end of the third round, it wouldn't mean that Kyber and Saber and NTRU got demoted to being alternates—it would mean that we just decided to standardize one of our alternates instead of one of our finalists.
>
> That's a plausible outcome, as far as I can tell, for five or six alternates: SPHINCS+,

GeMSS, HQC, SIKE, Frodo, and maybe BIKE. For example, imagine that over the next 18 months, we get a bunch of results that make us uneasy about the parameter selection for structured lattice schemes, and at the same time, there's a very clear upper bound on error rate for BIKE that lets them get CCA security. It seems very plausible to me that we standardize Frodo and BIKE as KEMs in that world. Then maybe we standardize a structured lattice KEM in another couple years when we feel like we know how the parameters should be selected.

But I don't think that would change the fact that Frodo and BIKE were both alternates instead of finalists. I can't imagine that we'd want to, say, announce that we'd demoted Saber to an alternate and Frodo to a finalist, six months from now.

--John

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Monday, June 29, 2020 at 11:49
To: internal-pqc <internal-pqc@nist.gov>
Subject: PQC

Everyone,
I don't have any plans for a meeting tomorrow. Let me know if you think we need one. The reviews for the report are still on going, and I'll make changes to suggestions we get back. Here's one Andy recommended we add in:

"It is possible that new analysis could result in an alternate candidate being elevated to being a finalist, in the case that NIST's confidence in the security of any of the finalists is greatly reduced."

Seems reasonable to me. It doesn't tie our hands and keeps our options open in case of an unexpected advance that breaks a finalist.

Dustin