From: (b) (6)
To: Apon, Daniel C. (Fed)
Cc: Perlner, Ray A. (Fed); Cooper, David (Fed); Dang, Quynh H. (Fed); internal-pqc
Subject: Re: Not asking for a level 5 option for NTRU Primes.
Date: Friday, June 12, 2020 10:26:22 AM
Attachments: image001.png

I agree, Daniel. Don't see why we can't ask for all schemes. (Even outside of their sections we can make a blanket statement that now we want level 5.)

On Fri, Jun 12, 2020 at 10:08 AM Apon, Daniel C. (Fed) <daniel.apon@nist.gov> wrote:

> I'm not sure I understand at all the problem with asking for a high security parameter set (that's totally independent from the other parameter sets).
>
> ---
>
> **From:** Perlner, Ray A. (Fed) <ray.perlner@nist.gov>
> **Sent:** Friday, June 12, 2020 10:07 AM
> **To:** Cooper, David A. (Fed) <david.cooper@nist.gov>; Dang, Quynh H. (Fed) <quynh.dang@nist.gov>; Daniel Smith (b) (6)
> **Cc:** internal-pqc <internal-pqc@nist.gov>
> **Subject:** RE: Not asking for a level 5 option for NTRU Primes.
>
> Hi David
>
> The reason level 4 is stronger than level 3 primarily has to do with quantum attacks. Key search on a 192 bit key is subject to Grover's algorithm, while collision search on SHA3-384 is not. To give an idea of the number of quantum gates involved in the Grover attack (on somewhat optimistic assumptions for quantum computation), plug in something like 2^64 in for MAXDEPTH. You'll find the attack on AES-192 uses about a trillion times fewer quantum gates than the attack on SHA3-384 uses classical gates.
>
> Now for sieving-type lattice attacks, the situation regarding quantum speedup is much more like collision search than key search, so a parameter set targeting category 4 should not be very much above one targeting category 3. For something like BIKE, where the best attacks have a near full Grover speedup, the situation should be reversed (meeting category 5 with BIKE isn't much harder than meeting category 4.)
>
> So the question is, is category 4 good enough. The reasons for saying it's good enough include:

1. 2^192 classical SHA3 operations is really beyond anything remotely plausible. Even if you posit reversible computing (i.e. computation speed inversely proportional to energy consumption using hbar as the proportionality constant) powered by the full output of the sun with a Jupiter sized atomic-scale memory it would still take a few years. If you scale that down to the solar energy reaching earth, and the number of atoms in the earth's crust, it would take a few billion years. This suggests that by the time we reach category 4 we should primarily be worried about quantum attacks. If we're primarily concerned about quantum attacks, category 4 and category 5 are basically the same.
2. We basically said category 4 was good enough in the CFP.

The reasons for saying it's not good enough include:

1. If what we're actually worried about is cryptanalysis improvements, category 5 means bigger parameters for lattices, and therefore more safety margin if there's a bit improvement in lattice attacks. Category 4 parameters are much closer to category 3 parameters
2. Kyber and Saber did give category 5 parameters (although NTRU didn't, except on pessimistic assumptions regarding the cost of RAM)
3. NSA asked for category 5 parameters in passing in a phone call.

I think at present, I'm leaning against explicitly asking for category 5 parameters where we're comfortable saying schemes have at least category 4 parameters, since that's what we asked for in the CFP. I do think we need to note somewhere that by the standard metrics, the highest security level offered by Kyber, Saber, and Falcon is higher than that of NTRU, NTRUprime, and Dilithium. Likewise, the lowest security parameters proposed by NTRU and Dilithium are on the low end compared to NTRUprime and Saber (with Kyber and Falcon somewhere in between. – Looking at the Falcon spec, I think 114 is the core SVP figure, not 103, which is labeled "quantum security.")

From: David A. Cooper <david.cooper@nist.gov>
Sent: Friday, June 12, 2020 8:28 AM
To: Dang, Quynh H. (Fed) <quynh.dang@nist.gov>; Daniel Smith (b) (6)
Cc: internal-pqc <internal-pqc@nist.gov>
Subject: Re: Not asking for a level 5 option for NTRU Primes.

On 6/12/20 6:32 AM, Dang, Quynh H. (Fed) wrote:

> Hi Daniel,

> I don't think we should say this " Finally, while NTRU Prime has considerable strength in its proposed level 1 parameters, NIST encourages the NTRU Prime team to provide a level 5 parameter set going into the 3rd round. ".

I think that Quynh may have a point, although I don't really understand the relevant information. The call for proposals says:

> when considering algorithms claiming a high security strength (e.g. equivalent to AES256 or SHA384)....
>
> NIST recommends that submitters primarily focus on parameters meeting the requirements for categories 1, 2 and/or 3, since these are likely to provide sufficient security for the foreseeable future. To hedge against future breakthroughs in cryptanalysis or computing technology, NIST also recommends that submitters provide at least one parameter set that provides a substantially higher level of security, above category 3. Submitters can try to meet the requirements of categories 4 or 5, or they can specify some other level of security that demonstrates the ability of their cryptosystem to scale up beyond category 3.

So, the call for proposals seems to suggest that providing a level 4 parameter set is sufficient to meet the recommendation, which could imply that we should not now be asking for a level 5 parameter set. On the other hand, the call for proposals includes the following table:

AES 128	2^{170}/MAXDEPTH quantum gates or 2^{143} classical gates
SHA3-256	2^{146} classical gates
AES 192	2^{233}/MAXDEPTH quantum gates or 2^{207} classical gates
SHA3-384	2^{210} classical gates
AES 256	2^{298}/MAXDEPTH quantum gates or 2^{272} classical gates
SHA3-512	2^{274} classical gates

In terms of classical gates, level 4 seems only negligibly higher than level 3. The reason that level 4 is considered meaningfully higher than level 3 escapes me.

I see that our report does say "The [NTRU Prime] parameters targeting the higher levels, however are more aggressive and it will need to be determined whether they actually meet their claimed security targets." So, perhaps we are not convinced that they actually have provided us a level 4 parameter set. But, if that is the reason for encouraging the NTRU Prime team to provide new parameter sets, then perhaps the text should be reworded to indicate that we encourage them to provide new, stronger parameter sets in case it turns out that their current parameter sets do not meet their claimed security targets.

Thanks,

David