**From:** Dang, Quynh H. (Fed)
**To:** Cooper, David (Fed); (b) (6)
**Subject:** Re: Not asking for a level 5 option for NTRU Primes.
**Date:** Friday, June 12, 2020 8:37:44 AM
**Attachments:** Untitled.png

Hi Dave,

Thank you for pointing out many good points.

The reason is that quantum computers don't find collisions easier than classical computers. So, under the quantum world, level 4 has significant more security strength.

Quynh.

---

**From:** David A. Cooper <david.cooper@nist.gov>
**Sent:** Friday, June 12, 2020 8:27 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:

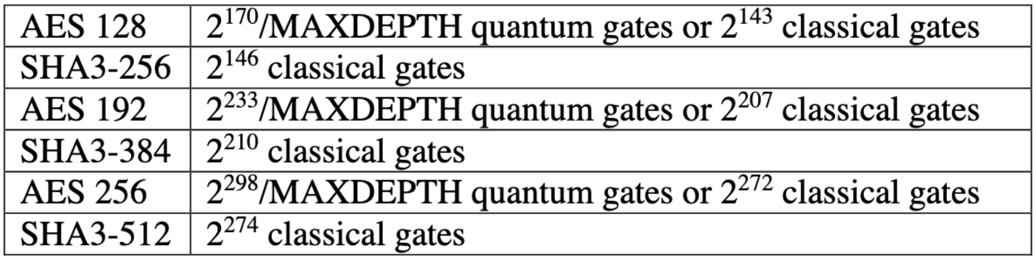
> Hi Daniel,
>
> I don't think we should say this " Finally, while NTRU Prime has considerable strength in its proposed level 1 parameters, NIST encourages the NTRU Prime team to provide a level 5 parameter set going into the 3rd round. ".

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