RE: Comment on Post-Quantum Cryptography Requirements and Evaluation Criteria

Perlner, Ray (Fed)

Wed 9/7/2016 12:04 PM

To: damien.stehle@ens-lyon.fr <damien.stehle@ens-lyon.fr>; pqc-comments <pqc-comments@nist.gov>;

Thanks for your comment Damien.

Regarding your questions:

1)Our reason for primarily considering attacks involving fewer than 2^64 decryption/signature queries is that the number of queries is controlled by the amount of work the honest party is willing to do, which one would expect to be significantly less than the amount of work an attacker is willing to do. Any attack involving more queries than this looks more like a denial of service attack than an impersonation or key recovery attack. That said, as noted in the proposed call for algorithms, we are open to considering attacks involving more queries. We would certainly prefer algorithms that did not fail catastrophically if the attacker exceeds 2^64 queries.

As a side note, if we do consider 2^64 online queries to be a realistic attack model, one of the first things we would need is a block cipher with a larger block size than 128 bits.

2)The issue of security strengths is discussed in some detail in our FAQs: http://csrc.nist.gov/groups/ST/post-quantum-crypto/faq.html , but to summarize: Our target security strengths are designed so that, if we need to transition to higher security strengths, as we did when moving from 80 bits to 112 bits of security, starting around 2010, we can time transitions for the new algorithms to coincide with those for algorithms we have already standardized (in particular AES, SHA2, and SHA3.) We would like the timing of these transitions to make sense given as wide a variety of assumptions as possible, regarding the progress in classical and quantum computing

In particular, we think it makes sense to explicitly consider security levels against classical attacks. The best quantum attack against most proposed postquantum schemes seems to either be the classical attack or something similar to Grover's algorithm. Given the poor parallelization of Grover-like attacks, the difficulty of constructing quantum computing hardware, and the overhead associated with reversibility and fault tolerance, it seems likely that in practice, the security of postquantum schemes will still be limited by the best classical attack.

It is also possible, however, that progress in quantum computing will bring the cost of quantum computing components to near parity with classical computing components. Even under this more "optimistic" scenario, though, Grover's algorithm will still parallelize poorly, and we would still expect this to be practically important, since current cryptanalytic efforts (e.g. attacks on RSA challenges) involve a high degree of parallelism. When claiming security equivalent to, say AES-128, we'd like to make sure that the attacker still has all the disadvantages he would have when attacking AES. This leads us to define quantum security a little strangely -- For example, when we say "80 bits quantum security" we mean "as hard to break as a 160 bit block cipher, even if your quantum computing architecture is highly parallel." As a result, assuming that the best classical attack parallelizes reasonably well (twice as many processors will make it twice as fast, up to say, the square root of the serial time complexity.), it will be very hard to claim quantum security more than about 2/3 of the classical security.

Hopefully the above discussion, and our FAQs help explain why our security strengths look like they are targeting equivalence with a hash function or block cipher. If a submitted algorithm has a different ratio of quantum to classical security than would be expected for a hash function or block cipher, we would suggest setting the parameters so that both quantum and classical security exceed the appropriate target security strength. We will certainly not penalize an algorithm for having more security than required in one of the two metrics.

Let us know if you have any further questions, comments or concerns.

Thanks again,
Ray Perlner

-----Original Message-----
From: Damien Stehlé [mailto:damien.stehle@ens-lyon.fr]
Sent: Sunday, September 04, 2016 3:58 AM
To: pqc-comments <pqc-comments@nist.gov>
Subject: Comment on Post-Quantum Cryptography Requirements and Evaluation Criteria

Dear Madam/Sir,

I have a few of comments on the document "Proposed Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process".

In Sections 4.A.2 and 4.A.3, you set the number of decryption (resp.
signature) queries, that an attacker against a proposed encryption (resp. signature) scheme can make, to at most 2^64.
I find this very low compared to the targets of security mentioned in Section 4.A.4. What is the rationale for not letting the adversary make essentially as many queries as the target security?

I am a bit confused by Section 4.A.4. Clearly, the classical and quantum bit security of a given scheme can differ. But why are the ratios 1/2 and 2/3 put forward as targets? This seems driven by search and collision-search, but these algorithms may not be so relevant for the schemes that will be proposed.
We could very well imagine that for some proposed schemes, the ratio will be 1, and for others it will be 1/10. As the focus is on quantum security, it may be tempting to focus on quantum bit-security targets, possibly with an additional requirement of not getting below a certain (and higher) classical bit security.

Best regards,
Damien Stehlé