Comment on Post-Quantum Cryptography Requirements and Evaluation Criteria

Vadim Lyubashevsky <VAD@zurich.ibm.com>

Thu 9/15/2016 5:09 AM

To: pqc-comments <pqc-comments@nist.gov>;

Dear NIST,

I have two comments about the draft document.

The first concerns the target security requirements in section 4.A.4. I do not understand the relationship that is drawn between the security of public key primitives and brute-force attacks on SHA/AES. Unlike SHA/AES, the best attacks against public key primitives are not brute force, so there is no reason to assume that the effect of Grover's algorithm on the quantum security of such primitives is analogous to its effect on symmetric ones such as SHA/AES.

Of course, when public key primitives use SHA as a sub-routine, the parameters of SHA should be set appropriately to resist quantum attacks (for example, in Fiat-Shamir constructions, one can use a hash function with 128-bit outputs to have 128 bits of classical security in the random oracle model, but would most likely need to use SHA-256 for 128-bits of quantum security.) But just because one needs to increase the security of the hash function does not imply that anything needs to be increased in the rest of the construction. For example, there are no known quantum algorithms for lattice reduction that outperform classical ones by any significant margin. Thus other than adjusting for a larger output from SHA, there would be no reason to increase the hardness of the lattice problem in the aforementioned Fiat-Shamir example.

Perhaps something reasonable that could be mandated is that if one uses hash functions or block ciphers within the primitive, then they must at a minimum have all the classical/quantum security features of SHA-256 and AES-256 (or one can just use SHA-256 or AES-256). But I believe that it would be very wasteful to set parameters so that the whole public key scheme is 256-bit secure classically when what we really want is that the scheme cannot be broken in 2^128 time on a quantum computer.

My second comment/question is about 4.B.4. Would it be possible for NIST to specify precisely what are the acceptable rates of decryption or key-agreement failures? If these failures lead to attacks, this is of course unacceptable. But if, for example, with probability 2^-30 the key-transport protocol fails and thus needs to be redone, is this something that's acceptable?

Thank you very much and best regards,

Vadim Lyubashevsky

IBM Research - Zurich