Intuitive Understanding of Quantum Computation and Post-Quantum Cryptography (Chapter 4)

Nguyen Thoi, Minh Quan [*]

4 Hash-based signatures

I won't pretend that I can write better than chapter 14 in Dan Boneh and Victor Shoup's book [1] or Matthew Green [2], Adam Langley [3] excellent blog posts about hash-based signatures, so go there and read them :) Instead, I'll discuss a little bit about their security. Hash-based signature protocol is the safest signature protocol against quantum computers. All signature protocols use hash functions and hence they must rely on hash functions' security. All signature protocols, except hash-based signature protocol, must rely on additional security assumption of other computational hard problems. Hash-based signature protocol, on the other hand, only depends on the security of hash functions. Furthermore, cryptographic hash functions are assumed to act like random oracles and as far as I know, quantum computers have limited success on breaking unstructured functions like random oracles and the best known quantum attack only has quadratic speedup compared to classical attacks.

In terms of applied cryptography, I recommend you never deploy stateful hash-based signatures, instead use stateless hash-based signatures although the latter have lower performance. The chance that you screw up security of stateful hash-based signatures deployment is far higher than the chance of general purpose quantum computers breaking your ECDSA signatures.

References

[1] Dan Boneh and Victor Shoup. *A Graduate Course in Applied Cryptography.*

[2] Matthew Green. Hash-based signatures: An illustrated primer. `https://blog.cryptographyengineering.com/2018/04/07/hash-based-signatures-an-illustrated-primer/`.

[3] Adam Langley. Hash based signatures. https://www.imperialviolet.org/2013/07/18/hashsig.html.

[*] https://www.linkedin.com/in/quan-nguyen-a3209817, https://scholar.google.com/citations?user=9uUqJ9IAAAAJ, msuntmquan@gmail.com