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 :)

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