Meta-review of the efficacy of next-generation security protocols against attacks from quantum computers

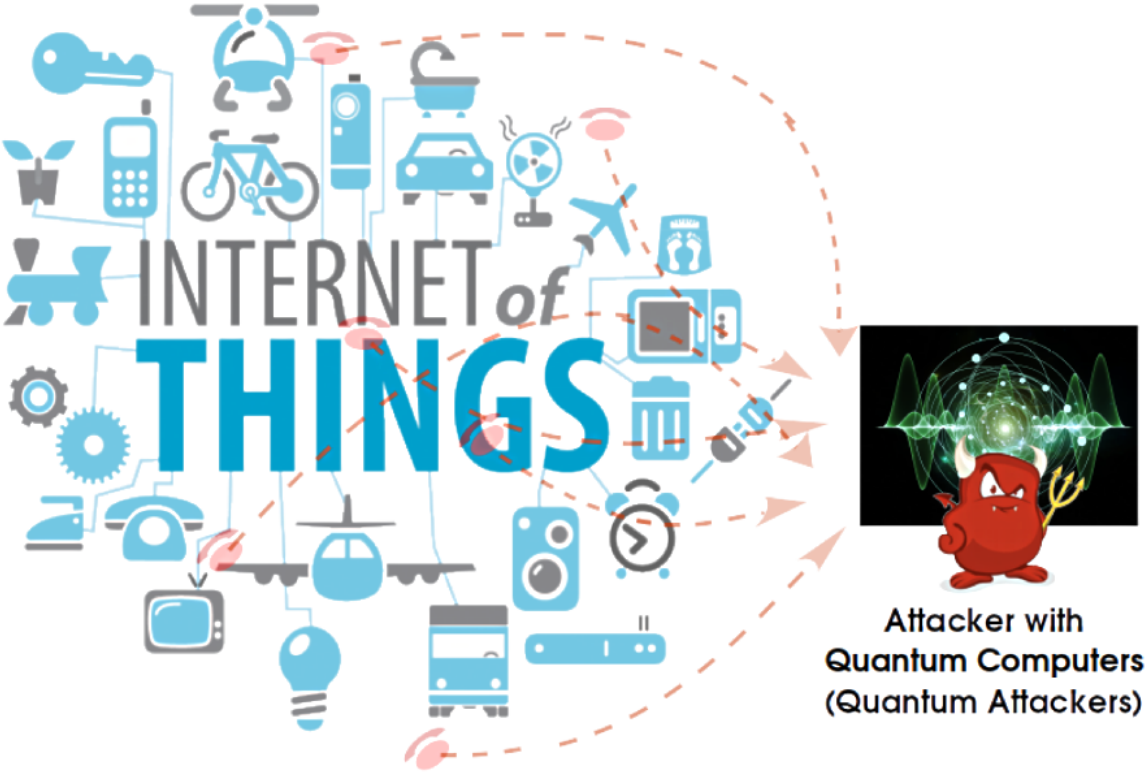

Image source: [Post-quantum cryptography]

Table of Contents:

1. Introduction: Security protocols are in danger because of quantum computers

1.1. Cryptography

Cryptography defines the art of writing and solving codes, and it keeps everything from Wi-Fi to bank accounts secure worldwide. Computers code and decode messages through cryptographic protocols that jumble the secret message using a password. Then, only someone who knows the password can retrieve the secret message from the jumble. This is like speaking in a foreign language with your friend so other people around you can't understand. Every piece of information stored on a computer and communicated between computers is guarded by some form of cryptographic protocol. Without cryptography, your location, identity, history, financial accounts, and anything else you keep on any technology is exposed to anyone who wants it.

The security of current cryptographic protocols relies on algorithms that are difficult for computers to solve, a class of algorithms called "intractable" algorithms. For example, a hacker trying to steal my Wi-Fi password would need thousands of years to calculate it depending on the password. Even with many powerful computers working together, the time required to crack the password stays as long as years.

1.2. Quantum Computers

A new type of computer, a quantum computer, will crack current cryptographic protocols exponentially faster. The Sycamore quantum processor created by the Google AI Quantum team funded by the NASA Ames Research Center and the U.S. Department of Energy demonstrated the potential by sampling a quantum circuit millions of times in 200 seconds [1]. An equivalent task on a classical state-of-the-art supercomputer would take approximately 10,000 years [1]. Despite the speedup, running a complex protocol-cracking algorithm is not yet attainable as it requires thousands of qubits and quantum computers are currently still within one hundred qubits, as shown in Figure 1 [2].
Once quantum computers are large enough to run them, algorithms like Shor's algorithm will solve a large portion of the formerly intractable problems behind our protocols [3]. The protocols in use globally will be rendered insecure and our computers' information will be vulnerable: emails, financial accounts, passwords, all unveiled and unprotected to a hacker with a quantum computer.

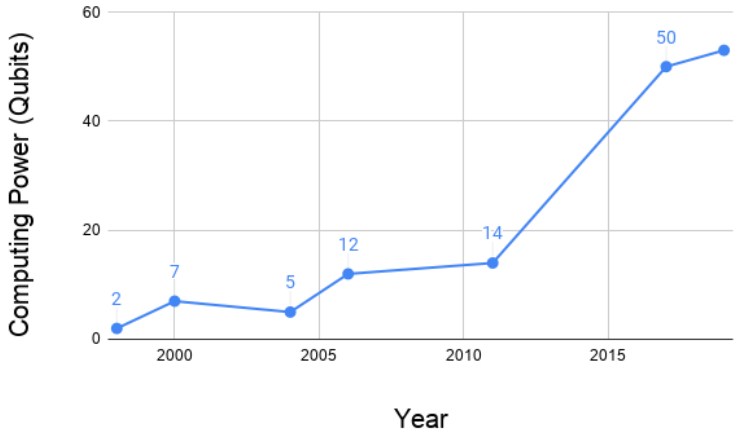

Figure 1: **Growth of quantum computing power (in qubits) over time**. This graph features some breakthroughs. Data from [4]–[10]

1.3. New protocols

Researchers are creating new cryptographic protocols for our computers to combat quantum computers' cracking capabilities. To safeguard against the first quantum attacks, advanced protocols are emerging [11]. Some are upgrades to present-day protocols that make them quantum-resistant [12], [13], while others are newly created protocols [11]–[25]. By upgrading protocols that are still intractable, they stay safe against quantum computers. Meanwhile, new protocols based on new intractable problems replace vulnerable protocols whose problems are solved by quantum computers. Researchers are successfully preparing quantum-resistant protocols.

1.4. Government facilitation

To keep security proactive, the National Institute of Standards and Technology (NIST) has created a competition to find the best protocol [26]. A protocol's success is measured by the following criteria:

- **Secure**: It is hard for quantum computers to crack
- **Efficient**: It quickly encodes and decodes messages and uses little computer memory
- **Feasible**: It replaces protocols that are currently at-risk

The competition finished Round 2, and Round 3 is coming in a few months, with plans to implement the remaining list of protocols [27]. Due to government supervision, security can stay ahead of attackers by preparing for quantum computers.

Will the next-generation of cryptographic protocols sufficiently resist quantum attacks? Through crowdsourcing research, the planned protocols will sustain security into the new age of quantum computers. This report is a meta-review of the current planning for post-quantum cryptography.

2. Quantum computers solve certain types of problems incredibly fast

2.1. Incredibly fast

Quantum computers are incredibly fast because information is stored differently. Classical computers store information using bits but quantum computers store information using qubits. Abstracting away the hardware creating these two, we will focus on the values they can represent. A bit can represent a value of 0 or 1. Qubits can also represent a classical value of 0 or 1, but additionally they can be in a superposition state with a probability of "collapsing" into either a 0 or 1. Imagine a qubit as a particle pointed in a direction, and we can only measure the direction as up or down. A particle pointed sideways would have probabilities of aligning as up or down when we measure it. The unit circle describes these probabilities, where the classical states of 0 and 1 are points on the top and bottom, and the rest of the points in the circle are possible superposition states (Figure 2).

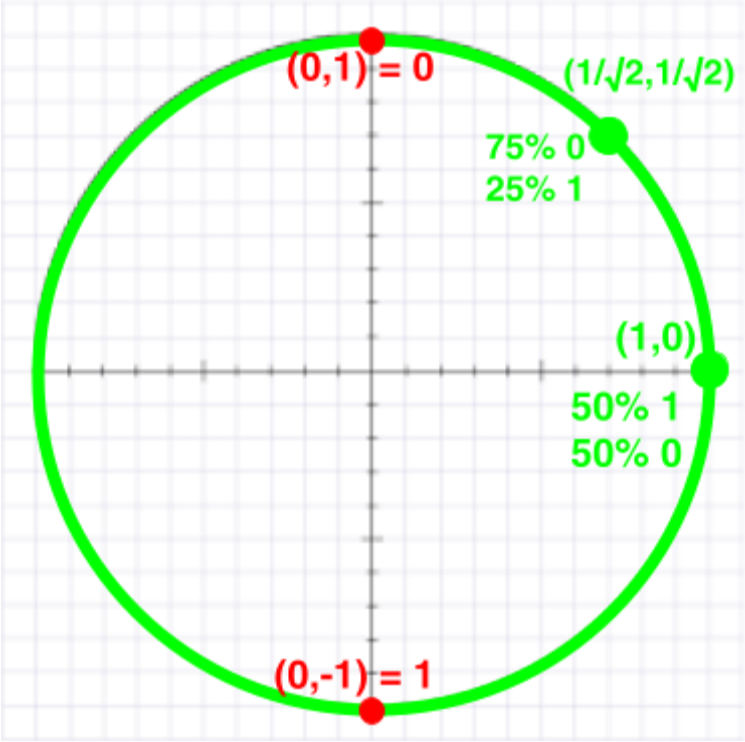

Figure 2: **Bits vs Qubits**. Classical bits are limited to the red points, while qubits can be anywhere on the circle. Illustration by the author

For example, a qubit could be in the superposition state described by the green point on the right at the figure above; when measured, this qubit has a 50% chance of being the value 0 and 50% chance of being the value 1. Before the qubit is measured however, the probabilities are

not real numbers like 75% but instead described by the amplitude of a wave (quantum mechanics probability is different from classical probability). With more qubits, the probability waves interfere, constructively or destructively. With complex math done by an algorithm, the values that are not the correct answer have probabilities that destructively interfere, and the correct values have probabilities that constructively interfere. By choreographing these waves, incorrect answers cancel out and correct answers reinforce each other; this procedure gives quantum computers the immense speedup.

2.2. Only certain types

Framing problems, such as protocol cracking, as problems that are solvable by a quantum computer algorithm is challenging. This is because all calculations on qubits must be reversible. Accordingly, every algorithm computing on qubits has to be built off of only reversible calculations, complicating the creation of functional algorithms. A comprehensive list of algorithms created so far is available at the website Quantum Algorithm Zoo [28]. These algorithms show the vast speedup over their classical algorithm counterparts for the same purpose, highlighting the new computing potential from quantum computers in the coming years.

3. Some modern protocols are cracked by framing them as quantum computer problems

3.1. Below acceptable security

The bits of security for certain protocols fall below the acceptable level. NIST has a standard measure of security for a protocol in bits, where a protocol with 50 bits of security would require 2^50 computer calculations to crack. NIST requires at least 112 bits of security for a protocol to pass into use [29].

As an example of the effect of quantum computers, secure protocol AES and vulnerable protocol RSA are shown in Table 1. Both protocols were considered secure against classical computers (left column). The difference is that the secure protocol AES has its bits of security only halved by quantum computer algorithms, so using AES with a bigger key size keeps it above the secure level. Meanwhile, the vulnerable protocol RSA is easily cracked by Shor's algorithm on a quantum computer and even with a huge key size is still insecure [3].

Table 1. **Bits of security for two protocols against classical vs quantum computers**. Bits of security under 112, the NIST minimum, are highlighted in red. Table modified from [30]

Protocol (key size)	Bits of security against attacks from	
	Classical computers	Quantum computers
Vulnerable RSA (2048)	112	25
Vulnerable RSA (15360)	256	31
Secure AES (128)	128	64
Secure AES (256)	256	128

The difference is because of the intractable problems behind the protocols. RSA is based on the previously intractable problem of factoring large integers; Shor's algorithm on a quantum computer solves this problem, making it tractable. The problem that AES is based on is still intractable even though it is solved faster on quantum computers. The speedup from quantum computer algorithms makes some intractable problems, such as RSA's, solvable. Hence, researchers are on the search for new types of problems intractable for quantum computers.

3.2. Not large nor stable enough yet

Quantum computers are on the rise thanks to recent breakthroughs at IBM and Google [1], [9], [31]. However, the number of qubits required for computing protocol-cracking algorithms are still far off. Even for any useful calculations on one qubit, the error rate in measuring its value and the stability for keeping it in superposition are too prone for error in current systems. Nevertheless, there is progress and predictions range from a few years to a few decades before we can solve problems with quantum computers [32]. The theoretical algorithms remain ahead of the physical implementations, which keeps us prepared for when the algorithms are realizable.

4. Researchers are creating new cryptographic protocols with quantum computers in mind

4.1. Upgrading protocols

Some protocols only need upgrading to achieve security against quantum computers. This is because they depend on problems that quantum computers offer a speedup for, but are still intractable, so the protocols can simply expand to become quantum-resistant. One example is

doubling the key length for AES, like having a longer password, as shown in Table 1. Another expansion involves encoding the input twice and decoding twice, thereby taking more time but achieving security against quantum computer hacking [12]. Compared to finding new intractable problems and creating a new protocol, upgrades to protocols are relatively simple solutions.

4.2. Creating protocols

For protocols with problems that became tractable, researchers create new replacement protocols by searching for problems that are intractable for both classical and quantum computers. The main types of protocols in planning are Lattice, Code-based, Hash-based, and Multivariate [17]. The type describes the problem that the protocol is based on. Recently, the most focus is on Lattice problems [17], but some researchers are attempting to promote an emerging type of problem, Supersingular Isogeny problems [20]. Researchers focus on these main problem types because they anticipate these types to remain intractable for quantum computers to solve. Whether they will stay intractable we will see in the future, but currently no algorithms solve these problems. Hence, they are worthy contenders for new, secure protocols.

5. Conclusion: Cryptography researchers' proactive planning secures our future for the coming years

5.1. Most secure protocols to date

There were 69 complete protocols submitted to the NIST competition for post-quantum protocols. The strongest 26 protocols made it to Round 2, announced on January 30, 2019 [33], and NIST expects Round 3 to begin around June 2020 [27]. Their competitions have had success in the past [34], including a competition to find the best standard measure of security for a protocol [35]. With the resulting protocols implemented, global security will be preserved even with quantum computers around.

5.2. Takeaways

- All protocols will be implemented and scrutinized, then replaced as we find improvements. The cycle will continue and security will stay ahead.
- Summary reports such as NIST's standardization project and the Quantum Algorithm Zoo are a useful gauge of the current state of protocols and attack algorithms.
- Quantum computers are not far away from changing the world, but whether within a few years or a few decades is still uncertain.

Appendix

Table 2 categorizes the 26 protocols that made it to Round 2.

Table 2. **A Count of the Top 26 Protocols According to NIST, Categorized** by type of problem. Data from [23]

Type	Count
Lattice	12
Code-based	7
Multivariate	4
Hash-based	1
Supersingular Isogeny	1
Zero-knowledge proofs	1

Current research is mostly focused on the types of protocols shaded more green [17], because these types of problems will hopefully remain intractable for quantum computers to solve.

References

[1] F. Arute *et al.*, “Quantum supremacy using a programmable superconducting processor,” *Nature*, vol. 574, no. 7779, pp. 505–510, Oct. 2019, doi: 10.1038/s41586-019-1666-5.

[2] dougfinke1, “Applying Moore’s Law to Quantum Qubits,” *Quantum Computing Report*. https://quantumcomputingreport.com/our-take/applying-moores-law-to-quantum-qubits/ (accessed Feb. 23, 2020).

[3] W. C. Peng *et al.*, “Factoring larger integers with fewer qubits via quantum annealing with optimized parameters,” *Sci. China Phys. Mech. Astron.*, vol. 62, no. 6, 2019, doi: 10.1007/s11433-018-9307-1.

[4] “12-qubits Reached In Quantum Information Quest,” *ScienceDaily*. https://www.sciencedaily.com/releases/2006/05/060508164700.htm (accessed Feb. 23, 2020).

[5] T. Monz *et al.*, “14-Qubit Entanglement: Creation and Coherence,” *Phys. Rev. Lett.*, vol. 106, no. 13, p. 130506, Mar. 2011, doi: 10.1103/PhysRevLett.106.130506.

[6] Z. Zhao, Y.-A. Chen, A.-N. Zhang, T. Yang, H. J. Briegel, and J.-W. Pan, “Experimental demonstration of five-photon entanglement and open-destination teleportation,” *Nature*, vol. 430, no. 6995, pp. 54–58, Jul. 2004, doi: 10.1038/nature02643.

[7] I. L. Chuang, N. Gershenfeld, and M. Kubinec, “Experimental Implementation of Fast Quantum Searching,” *Phys. Rev. Lett.*, vol. 80, no. 15, pp. 3408–3411, Apr. 1998, doi: 10.1103/PhysRevLett.80.3408.

[8] W. Knight, “IBM announces a trailblazing quantum machine,” *MIT Technology Review*. https://www.technologyreview.com/s/609451/ibm-raises-the-bar-with-a-50-qubit-quantum-computer/ (accessed Feb. 23, 2020).

[9] S. Shankland, “IBM’s biggest-yet 53-qubit quantum computer will come online in October,” *CNET*. https://www.cnet.com/news/ibm-new-53-qubit-quantum-computer-is-its-biggest-yet/ (accessed Feb. 23, 2020).

[10] “Los Alamos Scientists Shed New Light On Quantum Computation,” *ScienceDaily*. https://www.sciencedaily.com/releases/2001/01/010105075630.htm (accessed Feb. 23, 2020).

[11] N. Chikouche, P.-L. Cayrel, E. H. M. Mboup, and B. O. Boidje, “A privacy-preserving code-based authentication protocol for Internet of Things,” *J. Supercomput.*, vol. 75, no. 12, pp. 8231–8261, 2019, doi: 10.1007/s11227-019-03003-4.

[12] G. Brassard, P. Høyer, K. Kalach, M. Kaplan, S. Laplante, and L. Salvail, “Key Establishment à la Merkle in a Quantum World,” *J. Cryptol.*, vol. 32, no. 3, pp. 601–634, 2019, doi: 10.1007/s00145-019-09317-z.

[13] J. Sepulveda, S. Liu, and J. M. B. Mera, “Post-Quantum Enabled Cyber Physical Systems,” *IEEE Embed. Syst. Lett.*, vol. 11, no. 4, pp. 106–110, 2019, doi: 10.1109/LES.2019.2895392.

[14] J. Chen, J. Ning, J. Ling, T. S. C. Lau, and Y. Wang, “A new encryption scheme for multivariate quadratic systems,” *Theor. Comput. Sci.*, vol. 809, pp. 372–383, 2020, doi: 10.1016/j.tcs.2019.12.032.

[15] P. Zeng, S. Chen, and K.-K. R. Choo, “An IND-CCA2 secure post-quantum encryption scheme and a secure cloud storage use case,” *Hum.-Centric Comput. Inf. Sci.*, vol. 9, no. 1, 2019, doi: 10.1186/s13673-019-0193-6.

[16] B. Wang, F. Hu, H. Zhang, and C. Wang, “From Evolutionary Cryptography to Quantum

Artificial Intelligent Cryptography," *Jisuanji Yanjiu Yu FazhanComputer Res. Dev.*, vol. 56, no. 10, pp. 2112–2134, 2019, doi: 10.7544/issn1000-1239.2019.20190374.
[17] Y.-T. Yang, B.-Y. Liu, Y.-F. Sun, and Z.-C. Li, "Fully Homomorphic Masking Defense Scheme Based on NTRU," *Jisuanji XuebaoChinese J. Comput.*, vol. 42, no. 12, pp. 2742–2753, 2019, doi: 10.11897/SP.J.1016.2019.02742.
[18] L. Zhou, X. Sun, C. Su, Z. Liu, and K.-K. Raymond Choo, "Game theoretic security of quantum bit commitment," *Inf. Sci.*, vol. 479, pp. 503–514, 2019, doi: 10.1016/j.ins.2018.03.046.
[19] S. D. Galbraith, C. Petit, and J. Silva, "Identification Protocols and Signature Schemes Based on Supersingular Isogeny Problems," *J. Cryptol.*, vol. 33, no. 1, pp. 130–175, 2020, doi: 10.1007/s00145-019-09316-0.
[20] C. Peng, J. Chen, S. Zeadally, and D. He, "Isogeny-Based Cryptography: A Promising Post-Quantum Technique," *IT Prof.*, vol. 21, no. 6, pp. 27–32, 2019, doi: 10.1109/MITP.2019.2943136.
[21] T. Espitau, P.-A. Fouque, B. Gerard, and M. Tibouchi, "Loop-Abort Faults on Lattice-Based Signature Schemes and Key Exchange Protocols," *IEEE Trans. Comput.*, vol. 67, no. 11, pp. 1535–1549, 2018, doi: 10.1109/TC.2018.2833119.
[22] Y. Tian, H. Zhang, S. Xie, and F. Zhang, "Post-Quantum Privacy Preserving Smart Metering System," *Jisuanji Yanjiu Yu FazhanComputer Res. Dev.*, vol. 56, no. 10, pp. 2229–2242, 2019, doi: 10.7544/issn1000-1239.2019.20190402.
[23] I. T. L. Computer Security Division, "Round 2 Submissions - Post-Quantum Cryptography | CSRC," *CSRC | NIST*, Jan. 03, 2017. https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions (accessed Mar. 15, 2020).
[24] I. T. L. Computer Security Division, "Round 1 Submissions - Post-Quantum Cryptography | CSRC," *CSRC | NIST*, Jan. 03, 2017. https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions (accessed Mar. 15, 2020).
[25] H. Xie and L. Yang, "Witness indistinguishability and witness hiding against quantum attacks," *IET Inf. Secur.*, vol. 13, no. 6, pp. 579–590, 2019, doi: 10.1049/iet-ifs.2018.5460.
[26] I. T. L. Computer Security Division, "Post-Quantum Cryptography Standardization - Post-Quantum Cryptography | CSRC," *CSRC | NIST*, Jan. 03, 2017. https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization (accessed Mar. 08, 2020).
[27] "Some announcements - Google Groups." https://groups.google.com/a/list.nist.gov/forum/#!topic/pqc-forum/-rKSOqFAQeI (accessed Mar. 15, 2020).
[28] "Quantum Algorithm Zoo." https://quantumalgorithmzoo.org/ (accessed Mar. 08, 2020).
[29] E. B. Barker and A. L. Roginsky, "Transitioning the Use of Cryptographic Algorithms and Key Lengths," Mar. 2019, Accessed: Mar. 16, 2020. [Online]. Available: https://www.nist.gov/publications/transitioning-use-cryptographic-algorithms-and-key-lengths.
[30] K. Martin, "Waiting for quantum computing: Why encryption has nothing to worry about," *TechBeacon*. https://techbeacon.com/security/waiting-quantum-computing-why-encryption-has-nothing-worry-about (accessed Feb. 15, 2020).
[31] E. Gibney, "Hello quantum world! Google publishes landmark quantum supremacy claim," *Nature*, vol. 574, no. 7779, pp. 461–462, Oct. 2019, doi: 10.1038/d41586-019-03213-z.

[32] D. Moody, “Update on the NIST Post-Quantum Cryptography Project,” p. 25.
[33] robin.materese@nist.gov, “NIST Reveals 26 Algorithms Advancing to the Post-Quantum Crypto ‘Semifinals,’” *NIST*, Jan. 30, 2019. https://www.nist.gov/news-events/news/2019/01/nist-reveals-26-algorithms-advancing-post-quantum-crypto-semifinals (accessed Mar. 08, 2020).
[34] “Review on fifteen Statistical Tests proposed by NIST.” http://journaldatabase.info/articles/reviewonfifteenstatisticaltestsproposedbynist.html (accessed Mar. 09, 2020).
[35] J. Nechvatal *et al.*, “Report on the development of the Advanced Encryption Standard (AES),” *J. Res. Natl. Inst. Stand. Technol.*, vol. 106, no. 3, p. 511, May 2001, doi: 10.6028/jres.106.023.