The Rise of Quantum Cryptography

Aaron J. Henry

University of Louisville

Author Note

Aaron J. Henry, CIS Undergraduate, University of Louisville

Correspondence concerning this article should be addressed to Aaron Henry, CIS Undergraduate, University of Louisville, 2301 S 3rd St, Louisville, KY 40292.

Contact: aaron.henry.1@louisville.edu

Abstract

In recent years, quantum cryptography emerged and with it, the risk of losing secure communication in the quantum age. Current researchers give estimates on how long we have until we must address such risks. By outlining the capabilities of quantum computers and the risks they pose to current mathematical encryption methods, this article will describe what post-quantum cryptography is and its current status in the development process. It includes an analysis of the consequences of failing to maintain secure communications for business and looks at possible quantum-based infrastructure that could be implemented to protect communications.

Keywords: emerging trends, quantum cryptography, quantum resistant, post-quantum cryptography, quantum computers, encryption

The Rise of Quantum Cryptography

After the first concepts of quantum computing emerged, it quickly became clear that it would have a big impact on the future of computing. Quantum computers would offer the ability to solve large mathematical algorithms in a very short time frame. This amazing benefit lead theorists to speculate that some of the current encrypted communication methods would be rendered useless by quantum computers.

As quantum computers have become a reality and the commercial sale began, it's clear that we will need to be able to ensure that encrypted communication is maintained. According to Cheng, Lu, Petzoldt, & Takagi (2017, p. 117), in less than 20 years large scale quantum computing will come into existence and be capable of rending parts of our current communication infrastructure insecure. Cheng et al. (2017) explain that we need to develop new encryption methods that are not based on mathematical problems which are susceptible to attacks from quantum computers.

In 2016, the National Institute of Standards and Technology (NIST) began asking for proposals on new encryption methods that were, for the first time, quantum computer resistant (also known as post-quantum cryptography). The new methods must be capable of running on classical computers which are non-quantum based. According to Chen et al. (2016, p. 1), the most crucial communication protocols rely on three forms of encryption: public key, digital signatures, and key exchanges. These protocols are what make modern internet possible. The source also states that these forms of encryption are no longer secure against quantum attacks, which led to the emergence of a large international community to address the issue of communication security in the quantum age.

In 2019, NIST reported on the results from the international community's proposals for new quantum resistant methods. According to Alagic et al. (2019, p. ii), 82 proposals were submitted to NIST for consideration. 26 of the proposals passed the first stage of testing and are now moving onto the second. As the development trend for quantum computer continues, so will the development trend of quantum cryptography.

If we are not able to come up with a method to handle secure communications in the quantum age, we will find ourselves in a bad situation. According to Saliba (2017, p. 5), transmissions between different parties will no longer be kept confidential, secret, or inaccessible to others. This will introduce major implications for business. Online payments will vanish due to a high risk of fraud and potential lawsuits between customers who become victims of fraud will arise. Retailers will no longer be able to take online orders. Companies will no longer use online information systems for fear of losing highly valued intellectual property or customers' private records. This will have a greater impact on businesses than the emergence of internet itself, since we are now so dependent on it to do business.

Even if quantum computers render mathematical encryption irrelevant, the new quantum technology enables quantum encrypted communications. According to Hughes & Nordholt (2017, p. 456), there are two types of systems that are currently in development: ground base fiberoptic cables and satellite-based optics. These new technologies enable physically unbreakable security, but they may come at a high cost due to their very precise nature. Businesses will forced to change out their existing infrastructure for these new quantum communication systems to maintain online operations.

Over the next 20 years we will have time to adapt to the risks posed by quantum computers. Adapting could mean we have to move away from communicating sensitive information online. We may have to adopt new infrastructure that's required to communicate in the quantum age. It may be as simple as updating to the latest, quantum resistant encryption standard set by NIST.

References

Alagic, G., Alperin-Sheriff, J., Apon, D., Cooper, D., Dang, Q., Liu, Y.-K., … Smith-Tone, D. (2019). Status report on the first round of the NIST post-quantum cryptography Standardization process. *National Institute of Standards and Technology*. doi: 10.6028/nist.ir.8240

Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). Report on Post-Quantum Cryptography. *National Institute of Standards and Technology*. doi: 10.6028/nist.ir.8105

Cheng, C., Lu, R., Petzoldt, A., & Takagi, T. (2017). Securing the Internet of Things in a Quantum World. *IEEE Communications Magazine*, *55*(2), 116–120. doi: 10.1109/mcom.2017.1600522cm

Hughes, R. J., & Nordholt, J. E. (2017). Quantum space race heats up. *Nature Photonics*, *11*(8), 456–458. doi: 10.1038/nphoton.2017.124

Saliba, B. (2017). Backdoor encryption policies: a legal dilemma. Retrieved from https://www.um.edu.mt/library/oar/handle/123456789/29314.