Quantum Cryptography and its Consequences

Joseph Patrick C, Galvez

American Military University

ISSC266: Cryptography Concepts

Mr. Joel Stewart

6/22/2025

Quantum Computing is a type of computation that utilizes concepts from quantum physics, such as superposition, entanglement, and quantum interference, instead of logical binary or analog operations. Superposition is a concept that allows a quantum computer to use Qubits instead of regular bits, these qubits can simultaneously represent a 0 or 1 which gives quantum computers an exponential advantage in some calculations. Entanglement is when two or more particles are linked in ways that correlate to each other but the outcome is random. Lastly there is quantum interference which affect Qubits in predictable ways, which allows it to act as its equivalent to logic gates. These new computational methods give quantum computing an advantage in the large computational needs needed to crack cryptographic security methods.

Current methods of cryptography largely rely on their difficulty to solve, which is a result of the sheer number of possibilities resulting from logical operators and changing states used by algorithms. Critical communication applications that rely on this are public key encryption, digital signatures, and key exchange, these are also the applications most at risk of becoming insecure as a result of quantum computing as proven by Peter Shor in 1994 (Kuhn & Tracy, 2016). Of these, the most at threat are algorithms that rely on public key exchange such as RSA, ECC, and DSA likely due to the fact that there exists a publicly available key as is presented in Table 1 as claimed by Kuhn and Tracy (2016). These threats to the security of web communications have warranted an effort to adapt to these new conditions.

In an effort to preserve the security of public key algorithms some solutions have been presented which offer resistance to the threat of quantum computing-based cryptographical cracking. Code-based cryptography suggests that making structural changed to algorithms and increasing key sizes can provide more security; the McEliece cryptosystem was introduced in 1978 and has not been broken since (Kuhn & Tracy, 2016). Multivariate polynomial cryptography is a possible solution due to its sheer difficulty. Hash-based signatures offer proven security against quantum attacks, but they require a record of each message that was sent otherwise the security is compromised; furthermore, they produce a limited number of signatures before key length must be increased (Kuhn & Tracy, 2016). There are known countermeasures to quantum cryptanalysis but they all require an increase in key size which make them more cumbersome which increases the difficulty of mass adoption. To fully counter the threat, however, there must be a transition to post-quantum cryptosystems.

In conclusion, Quantum Computing is a form of computing that utilizes the properties of matter on the quantum level; primarily superposition, entanglement, and quantum interference. Quantum Computing has achieved a level of reliability and development to the point of threatening current cryptographic algorithms. As a result of this threat current countermeasures exist but a transition to post-quantum cryptosystems is needed to maintain the security of information and communication.

References

Kuhn, D. R., & Tracy, M. (2016). *NISTIR 8105: Policy considerations for the Internet of Things (IoT)*. National Institute of Standards and Technology. <https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf>

*For additional information on APA Style formatting, please consult the* [*APA Style Manual, 7th*](https://apastyle.apa.org/style-grammar-guidelines) *Edition.*