A Summary of Quantum Computing’s Impact on Modern Cryptographic Algorithms

CSIS 463

Professor Schall

James Riley Dorough

Liberty University

March 2nd, 2021

**Introduction**

Quantum computing is a complex topic that has found renewed interest in the modern-day. It is often considered a buzzword in many industries and is assumed to be a hyper-powerful solution to nearly all computing problems. However, this is not exactly the case. Quantum computing can be used to operate on problems that lie within the realm of quantum physics. This means to unlock the full potential of a quantum computer; you must understand where its limitations lie. Understanding the indirect connections between classical problems and quantum problems allows us to work toward new perspectives for both new and previously impossible solutions to problems. This paper provides a summary of quantum computing with a focus on how it plays a factor in cryptographic security as it exists today.

**An overview of Quantum Computing**

As previously stated, the potential of quantum lies in its limitations. Quantum problems differ vastly from classical problems based on the physics in which they exist. Quantum mechanics is not a new field of study. However, semi-recent technological advancements have allowed humanity to use these mechanics to build quantum circuits and test quantum-related theories. Quantum computers operate by utilizing the superposition probability of particles referred to as Q-bits (Knill, 2010). The operation of Q-bits is reliant on the probability or *amplitude* of an outcome based on a quantum calculation (Brassard et al., 1998). The outputs of these binary Q-bits can be read as a percentage of probability for a specific outcome of an algorithm (1998). This paired with quantum error correction (QEC) allow for fault-tolerant circuits that can handle error rates of upwards of 1% (Franke et al., 2019). This is a major improvement and can speed up the processing of algorithms and begin to minimize the need to restart due to any type of interference. Because of these factors, algorithms that are quantum solvable can produce an output within a reasonable time. However, this does not apply to classical problems. If you were to attempt to use a classical searching algorithm on a quantum computer, you may never reach an output within a reasonable time.

My previous work on the topic of quantum computing focused on its application to real-world physical problems. Specifically, the problem of optimizing ammonia production at an industrial level. The root of the issue is that we can not yet easily model molecular structures well enough to account for uncommon events, such as quantum tunneling (Dorough, 2021). If we take that thought process and delineate between what we currently know about physics and focus on moving toward an understanding of where quantum physics can be completely separated, we can begin to build frameworks for solving these quantum problems.

Of these problems, not all are strictly physical. Logical and mathematical standards we rely on and are comfortable with today may begin to shift as we realign our problem solving to include a quantum perspective. We are rapidly discovering and designing new technologies. Many of which are hardly new, but a rehash and reconfiguration of understood methods and utilities that have already been discovered (Inglesant et al., 2021). With the advent of quantum computing arriving on the scientific stage, we have a new element to begin experimenting with and combining into existing infrastructure. However, some people express concern about such new advances in computing and problem-solving. Much like the creation of the internet, information security and privacy are now objectives we strive to hold onto (Khan, 2021). Regardless of the argument that privacy or security has weakened or just taken a new form, quantum computing has allowed for a new wave of adaptation to digital security tactics techniques and procedures (TTPs).

**Quantum Computing’s Role in Cryptography**

As of today, it is nearly possible to break some encryption algorithms using quantum computers. Because of this, additional security measures have been developed to hinder quantum computing’s progress toward breaking traditional block cipher encryption. For clarification, this can be referred to as the post-quantum cryptography era. Quantum computing’s ability to break traditional encryption is contingent on an algorithm completing its process without the circuity experiencing any interference (Dong et al., 2020). As mentioned previously, QEC allows for up to 1% error correction. The more fault-tolerant that quantum computers become, the closer we come to brute forceable encryption protocols.

There are two ways of categorizing quantum security to protect encryption from the inevitable evolution of quantum computers. Standard security is where a quantum analysis algorithm can not determine the block cipher using classical queries (Dong et al., 2020). Quantum security varies from standard security wherein a block cipher can not be determined using quantum queries (2020). The logic to break standard encryption exists. We still have a few obstacles to clear to truly break security procedures in the wild.

**Conclusion**

Quantum computing is readily understood as a common buzzword for powerful computing. However, we understand that quantum computing has some very strict limitations in its realm of physics. To include limitations of the hardware used. A quantum computer is incredibly precise. Due to this precision, the hardware is incredibly sensitive. Exact temperatures and stability from vibrations much be maintained to ensure the machine can complete an algorithm. The superposition of the super-chilled atoms can be collapsed, and the probability of outcome can be measured to determine the result of an algorithm. We continue to grow closer to being able to break some standard encryption protocols as quantum computers continue to evolve. Some methods of additional security have been created to combat encroaching quantum cyber-attacks.

**References**

Brassard, G., Chuang, I., Lloyd, S., & Monroe, C. (1998). Quantum computing. *Proceedings of the National Academy of Sciences*, *95*(19), 11032–11033. <https://www.pnas.org/content/95/19/11032>

Dong, X., Dong, B., & Wang, X. (2020). Quantum attacks on some feistel block ciphers. *Designs, Codes and Cryptography*, *88*(6), 1179–1203. https://link.springer.com/article/10.1007/s10623-020-00741-y#citeas

Dorough, J. R. (2021). A Study of Quantum Computing and its Application on Industrial Production of Ammonia [Unpublished paper]. School of Business – Cyber Security, Liberty University

Franke, D., Clarke, J., Vandersypen, L., & Veldhorst, M. (2019). Rent’s rule and extensibility in quantum computing. *Microprocessors and Microsystems*, *67*, 1–7. <https://www.sciencedirect.com/science/article/pii/S014193311830293X?via%3Dihub>

Inglesant, P., ten Holter, C., Jirotka, M., & Williams, R. (2021). Asleep at the wheel? Responsible Innovation in quantum computing. *Technology Analysis & Strategic Management*, *33*(11), 1364–1376. <https://www.tandfonline.com/doi/full/10.1080/09537325.2021.1988557>

Khan, I. (2021, February 17). *Will Quantum Computers Truly Serve Humanity?* Scientific American. Retrieved March 20, 2022, from [https://www.scientificamerican.com/article/will-quantum-computers-truly-serve-humanity/#](https://www.scientificamerican.com/article/will-quantum-computers-truly-serve-humanity/)

Knill, E. (2010). Quantum computing. *Nature*, *463*(7280), 441–443. <https://web.s.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=3&sid=19032407-f42d-4590-af82-10d3a4c46bf6%40redis>