# Quantum Computing using Quantum Superposition and Entanglement

Dan Reynolds

20473104

SCI 207

A5

Computing is only beginning to take advantage of the benefits that will come from humanity's growing understanding of quantum mechanics. While it is unlikely a person will be able to go out and buy a quantum computer anytime soon, companies and scientists are investing heavily in exploring the applications of this technology. Normal computers work on the lowest level in the language of binary, combinations 0s and 1s that equate to a circuit being switched on or off. Conventional computers try to incorporate as much circuitry as possible in the form of memory chips that can store and flip these binary states as efficiently as possible. While classical computing has made great strides in optimizing this technology, quantum computing is not limited by bits that are either on or off. A quantum bit, referred to as a qubit, can take advantage of the property of quantum superposition to be in multiple states as once. If a conventional computer had 5-bits of memory and had to try every 5-bit binary password to unlock a door, it would have to go through all 32 binary numbers in a sequence to generate every possible password. A quantum computer, however, can simultaneously represent both a 0 and a 1 in each qubit, allowing it to immediately compute all 32 states [1]. With each additional qubit, a quantum computer doubles the number of states that it can be in simultaneously, allowing it to exponentially perform increasingly complex calculations. A series of 64 qubits provides nearly "one million terabytes" of processing power, while a conventional computer can represent the same number of states, but only one at a time [1].

There are a number of different ways to design machines capable of taking advantage of quantum superposition. One leading approach which has been used by Google, IBM and others is to encode "quantum states as oscillating currents in superconducting loops" [2]. The loop of a superconductor can have current running through that flows both clockwise and counterclockwise at once, creating a superposition state, however, these systems can easily collapse, losing their superposition properties [1]. Physicist John Martinis at Google spent the last decade extending the lifespan of these fragile states, reaching a period of stability of approximately 50-100 microseconds [3].

If scientists can keep these qubits stable for long periods and successfully read their data, then there are a number of powerful uses for this technology.

One of the most important consequences of quantum computing is in computer cryptography. Many of the ways that computers encrypt their communications relies on the difficult conventional computers have with factoring large numbers. Popular encryption methods like RSA public encryption, which is used frequently on the web, uses an encryption key that is the combination of large prime numbers in order to secure data transmissions [4]. Standards like RSA-2048, which has keys that are 2048 digits long, have never been successfully factored and offers a secure encryption system in the modern Internet [5]. A 1994 revelation by MIT mathematician Peter Shor revealed that a quantum computer, using Shor's algorithm, could factor these large numbers very quickly as a result of the superposition properties of a quantum machine, rendering much of modern cryptography vulnerable to attacks [4]. While quantum computers pose a danger to cryptographic techniques founded on the difficult of factoring large numbers, cryptographers have other techniques for keeping data secure. One such method are called One Time Pads (OTP), consisting of a long sequences of binary numbers. A plain message can be combined with an OTP to create an encrypted message that requires the exact OTP used to reverse the process [4]. A quantum machine cannot decrypt an OTP encrypted message, since trying every possible OTP that could have been used to generate the message will yield every possible message, with no way to determine which one is correct. The difficulty in using OTP messages is distributing these large OTP encryption keys. Fortunately, a process called Quantum Key Distribution (QKD) makes use of an additional quantum property called quantum entanglement to effectively transmit keys.

Quantum entanglement is a process by which two entangled particles become "inextricably linked", able to effect each other even after being separated over incredibly large distances. For example, measuring a particular binary property of one particle and measuring it as a 1, one can then measure that same property of a second particle and get a value of 1. If a different binary property is measured on the second particle, then there is no correlation between the two particles and the binary property of the second particle has an equal likelihood of being a 0 or 1 [6]. Scientists are already using quantum entanglement to transfer information. The Institute for Quantum Computing (IQC) in Waterloo has developed a prototype QKD device that can be used to transfer data between two stations at the IQC and the University of Waterloo [4]. Each facility receives have of a number of entangled photons and the binary polarization of these entangled photons can be measured by each side to generate the same random sequence of numbers that can then be used as an encryption key.

Quantum computing, while still in its infancy, will have significant ramifications for computer performance and cryptography. By further exploring the properties of quantum superposition and entanglement, physicists can pursue technology that can potentially leap far ahead of the comparably incremental improvements being made in classical computing and make it possible to perform calculations and encryption methods far more efficient and secure than current approaches.

# References

[1] C. O'Connell, “Quantum computing for the qubit curious,” *Cosmos Magazine*, 07-Aug-2016. [Online]. Available: https://cosmosmagazine.com/physics/quantum-computing-for-the-qubit-curious. [Accessed: 15-Mar-2017].

[2] D. Castelvecchi and N. magazine, “Quantum Computers Ready to Leap Out of the Lab in 2017,” *Scientific American*, 03-Jan-2017. [Online]. Available: https://www.scientificamerican.com/article/quantum-computers-ready-to-leap-out-of-the-lab-in-2017/. [Accessed: 15-Mar-2017].

[3] “Physics: Quantum computer quest,” *Nature News*. [Online]. Available: http://www.nature.com/news/physics-quantum-computer-quest-1.16457. [Accessed: 15-Mar-2017].

[4]“Quantum computing 101,” *Institute for Quantum Computing*, 11-Nov-2013. [Online]. Available: https://uwaterloo.ca/institute-for-quantum-computing/quantum-computing-101. [Accessed: 15-Mar-2017].

[5] “RSA Number,” *RSA Number -- from Wolfram MathWorld*. [Online]. Available: http://mathworld.wolfram.com/RSANumber.html. [Accessed: 15-Mar-2017].

[6] “Entanglement Made Simple,” *Quanta Magazine*. [Online]. Available: https://www.quantamagazine.org/20160428-entanglement-made-simple/. [Accessed: 15-Mar-2017].