Christian Martinez
CST 373
Professor Scott
14 May 2017

Quantum Computing and its Implications on Encryption

Data security is a topic that has become more relevant to internet users over the past few years. Americans are concerned with their data's privacy and how to keep their information safe while still using the internet however they choose. Encryption has provided this sense of user security for years but developing technologies like quantum computing are making current encryption techniques less viable for the future. Quantum computing will have a major impact on our data security in the coming years. I will be discussing if we should continue development on quantum computers if it poses such a high data security risk. I will address the involved parties, possible courses of action, ethical frameworks of those actions, and my opinion.

To begin discussion about quantum computing, we should first address what it is. According to Margaret Rouse (2010), quantum computing can be defined as , "...the area of study focused on developing computer technology based on the principles of quantum theory, which explains the nature and behavior of energy and matter on the quantum (atomic and subatomic) level". This may seem overwhelming at first, but essentially Quantum computers use the ideas of the intrinsic randomness of physics at the subatomic level. The computers are built on a bit type called a "Qubit". Qubits have more possibilities than a binary bit because they can be a 1 or a 0 or in something called a superposition. The University of Waterloo's Institute of Quantum Computing defines superposition as, " ...essentially the ability of a quantum system to be in multiple states at the same time — that is, something can be "here" and "there," or "up" and “down” at the same time.” In terms of computing, this means that a qubit can be in a state where it is a 1 and a 0. When multiple qubits begin to work together the concept of entanglement comes into play. Entanglement creates a situation where observing one qubit tells you the state of other qubits it is entangled with. Due to the fact that only one bit needs to be observed, factorization and other computationally heavy operations become much faster to complete. Now you may be wondering how this ties into encryption.

TechTarget (2014) defines encryption as, “...the conversion of electronic data into another form, called ciphertext, which cannot be easily understood by anyone except authorized parties”. Essentially, encryption is the act of making data that you are passing to some other person or system unreadable until a key is used to decypher it. This is a very widely used way of making sure that the data being transferred is not seen by anyone trying to intercept it. Often times websites will have an “https//” instead of an “http//”. The ‘s’ is what tells the user that the connection is secure and encrypted. Like previously mentioned, The state of data security may be at risk due to the potential power of quantum computers. With the current power of classical computers, the binary bits are not able to perform algorithms to find encryption keys fast enough to consistently be a threat to encryption as a whole. With quantum computing however, qubits are able to be in so many states at once, that the key will theoretically be found much faster. Elliot Williams of Hackaday(2014) stated, “Anyone storing your (or your government’s) data now will likely be able to read it when today’s toddler is enrolling in college”. While this may seem a ways away, William’s fears that with the loss of encryption, all data including government information, passwords, and credit card numbers will be visible to those with a strong enough computer. A multitude of parties are concerned with this possibility and with the odds of this being on the horizon, it is no wonder that people want to act now.

With today's tech centered society, many people can be considered stakeholders in this issue. For the sake of this paper I will be addressing the government, tech companies, and the general public. By addressing these three in broad strokes, the issue will be easier to understand as a whole without getting lost in the nitty gritty.

The government, or more accurately the NSA, is concerned with the current threat that quantum computing poses on national security. The NSA values the security of the country from any form of threat and quantum computing may be the biggest foe they have had thus far. Gizmodo writer Jamie Condliffe (2016), quoted the NSA addressing their concerns about quantum computing's implications on national security, stating, "NSA does not know if or when a quantum computer of sufficient size to exploit public key cryptography will exist... There is growing research in the area of quantum computing, and enough progress is being made that NSA must act now to protect [national security services] by encouraging the development and adoption of quantum resistant algorithms". The NSA is concerned with the computational power being created with quantum computers and is responsible for data security in the government sector as well as of the American people. National security is one of government's core values and it is noted that their main goal is to encourage development of stronger encryption algorithms.

The tech companies that are creating these computers are another major stakeholder. Their values and intentions are not directly to create technology to undermine a government and take over the world, but simply to push the boundaries of technology and provide breakthroughs in the world of computing. D-Wave Systems, one of the first quantum computing companies, has a vision statement that reads, " While we are only at the beginning of this journey, quantum computing has the potential to help solve some of the most complex technical, commercial, scientific, and national defense problems that organizations face. We expect that quantum computing will lead to breakthroughs in science, engineering, modeling and simulation, financial analysis, optimization, logistics, and national defense applications". It is clear from reading their vision that D-Wave Systems is a group of technologist trying to make a difference in computation. Their position on their technology being used to break encryption is currently unknown. The company has not put out an official statement saying how they feel about this possible use of their tech. Seeing as their computer can only be used in an extremely controlled environment as to maintain its computational integrity, the issue has most likely not been one of their concerns.

The last major stakeholder in this issue is the general public. The root of this issue is data privacy which affects not just the government, but the general public as a whole. The general public's interest is to maintain security of their precious data such as credit card information or social security numbers. Their concerns are that data privacy will no longer exist and this will infringe on their right to privacy which is laid out in Article 12 of the Universal Declaration of Human Rights which states, "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks." People value privacy and hold companies and government bodies responsible to value this right.

After careful thought, I have come to two separate courses of action. The first is to allow progress on stronger encryption and quantum computers to be developed simultaneously. This course of action will appease the most stakeholders and and aligns with the Common Good Approach. In order to make the most innovation we would need to not hinder the production of these machines and continued research into quantum computing will help solve Non-Polynomial problems. These problems include factorization which is the core of RSA encryption. The second course of action would be to halt progress on quantum computers until stronger encryption can ensure data security. This course of action is the best for the general public but creates roadblocks for technology companies such as D-Wave Systems. The ethical framework that aligns most with this course of action would be The Rights Approach. The general public is entitled to the right to privacy and with potential to break that right, development should not continue. While both of these courses of action have their merits, I have formulated my own opinion on how this issue should be addressed.

When it comes to my stance on this issue, I feel that there are many things to take into consideration. I believe that many of the positions of the stakeholders are very much justified. The protection of government structure, intellectual property, or personal data are all valid data to be accounted for. That being said, I agree with the Common Good approach of allowing for the two technologies to be developed simultaneously. I do recognize the value in working in tandem and how it will make for better understanding of each other's algorithm. I value this approach because it maintains velocity of innovation while keeping the most stakeholders happy.

Quantum computing is a tool that will be used to make some incredible discoveries in the coming years. From 1981 to 2017, quantum computing's concept has come a long way and is very close to being a force to be reckoned with. These computers have the power of Qubits behind them and can revolutionize the way we conduct computation. While this is all well and good, the fear of this power is very apparent. Encryption is something that can not be easily replaced and a solution needs to come into play before quantum computing's effects become irreversible. Many groups are quite concerned with whether or not these computers see the light of day. The government is concerned with their data security as well as the security of the general public. Companies want to be able to create this technology and bring a new way to compute to life. The general public is concerned with their data and if the internet will be safe after this computer becomes a functional reality. Options are limited when it comes to this breakthrough in technology. Hindering research of quantum computers maintains data security while allowing the research to be conducted in tandem with stronger encryption keeps innovation at full velocity. Although both options have their positives and their negatives, allowing for the encryption algorithm and quantum computers to be researched simultaneously is most beneficial to the future of our nation.

Bibliography

Kurzgesagt. *YouTube*. YouTube, 08 Dec. 2015. Web. 13 Mar. 2017.
<https://www.youtube.com/watch?v=JhHMJCUmq28>.

This source was one of the earlier sources I found and made the concepts of quantum computing seem digestible. The creator of the video uses visuals and simple terms to explain how powerful these computers are. I plan to use this video in my presentation to explain the technology of quantum computing because I think it is a great starting point to get the audience to understand the topic. As for the validity of the information presented in the video, I believe that the source is credible. I have been subscribed to this channel before I found the video on this topic and the creator tends to spend large amounts of time on each video to make sure it is valid. Through further research into the topic I have found that the information holds up.

Kevin Bonsor & Jonathan Strickland "How Quantum Computers Work" 8 December 2000.
HowStuffWorks.com. <http://computer.howstuffworks.com/quantum-computer.htm> 12 March 2017

This source was quite helpful in explaining the history of quantum computing. The page was put online in 2000 but has been updated with more current information since then. I plan to use this source to explain where quantum computing came from and how it differs from regular computers. In terms of validity, I consider this to be a reliable source. The site is called “How Stuff Works” and is geared toward explaining things to its users. I would find it quite odd for them to mislead its readers but I will be hyper aware as I look into more sources to see if they are writing similar information before I use the information in my paper.

D-Wave Systems. (n.d.). Retrieved May 20, 2017, from
http://www.dwavesys.com/our-company/meet-d-wave

D-Wave is one of the biggest companies that is currently researching and creating quantum computers. They have multiple different machines ranging in amounts of qubits available to the machine. This source will be used to explain the current status of commercial quantum computing.

(n.d.). Retrieved May 5, 2017, from http://www.merriam-webster.com/dictionary/utilitarianism
This source will be used to explain one ethical framework that will be recognized in the paper. I have found Merriam-Webster to be a valid academic source when it comes to definitions. The goal is to allow for a neutral definition of the concept to ensure the readers understand what I mean when applying the framework to my topic.

First 'Quantum Computer' No Faster Than Classic PC. (n.d.). Retrieved May 15, 2017, from http://www.livescience.com/46414-first-quantum-computer-no-faster.html

This source talks about D-Waves first quantum computer and tells us that the computer is actually not much faster than a regular PC. I will use this source to question the validity of quantum computers being able to make the impact that other sources in the paper claim. I hope to have both sides represented so that the writing is lacking bias. The validity of this source is questionable as it is not peer reviewed and is not a reputable name in the science community but I hope to find more sources to back up its claims.

Fung, B. (n.d.). How Many Cyberattacks Hit the United States Last Year? Retrieved May 28, 2017, from http://www.nextgov.com/cybersecurity/2013/03/how-many-cyberattacks-hit-united-states-last-year/61775/

To add validity to the threat upon cyber security that quantum computing holds I wanted to pull from this source the numbers of cyber attacks are increasing. With cyber attacks increasing annually and more powerful computing power being introduced to the market place, security of data will be threatened. The source does not feel to be the most official however the numbers are compelling and I feel pertain directly to my topic.

P., & Condliffe, J. (2016). NSA Plans to 'Act Now' to Ensure Quantum Computers Can't Break Encryption. Retrieved May 21, 2017, from http://gizmodo.com/nsa-plans-to-act-now-to-ensure-quantum-computers-cant-b-1757038212

This source talks of the NSA taking precautions due to quantum computers threat to encryption. This is one of the strongest sources to reference due to the fact that a large organization for America's security is recognizing the threat quantum computing holds. While this may be a very early reaction or the USA being late to the game the source is going to show how real the threat is becoming. I hope to use this to really drive home the validity of the threat.

Quantum computing 101. (2013). Retrieved May 20, 2017, from https://uwaterloo.ca/institute-for-quantum-computing/quantum-computing-101

The University of Waterloo has an institute of Quantum Computing which has a great resource for learning the basic workings of Quantum computers. This source has the best explanation of superposition and will be useful when trying to explain how the tech works so people can understand why certain groups are concerned with its power. I consider this to be a credible source because it is provided from a place of higher education whose goal is to teach these types of cutting edge information.

Shanks, T. (n.d.). Approaches to the Study of Ethics. Retrieved May 23, 2017, from http://aggie-horticulture.tamu.edu/syllabi/315/ethics/study.html

This source will be where I take the ethical approaches and frameworks that will be applied to the arguments for and against quantum computing. The source is from a school again but it has many different ethical approaches that can be taken which makes it quite helpful. The information aligns with what we have discussed in class so it seemed more appropriate to cite the website.

Velasquez, M. (n.d.). Thinking Ethically. Retrieved May 20, 2016, from https://www.scu.edu/ethics/ethics-resources/ethical-decision-making/thinking-ethically/

This source talks about the thought process that should go into ethical decision making. It is a supporting source for the ethical frameworks and will show the process of understanding why each side thinks the way they do on my topic. I found this source helpful in having me understand what goes into ethical decision making. Most people would think that the decisions they make are ethical but it becomes more difficult as the decisions effect bigger bodies like national security or bank account information. As for the validity, it is an academic source and was made by the ethics department of Santa Clara University.

What is encryption? - Definition from WhatIs.com. (n.d.). Retrieved May 20, 2016, from http://searchsecurity.techtarget.com/definition/encryption

This source will be used to define encryption. It is a great overview of the ways that different encryption algorithms work and how not all encryption works the same. This will be used to explain encryption as a technology and will help to have the reader understand it in its current state. The source is rather old (last updated in 2014) so I hope to come across another source with more up to date information on the subject. As for its validity, It is a tech website whose goal is to teach its readers about technological concepts. I will have to cross validate but it seems to be sound information on the page.

Williams, E. (n.d.). Quantum Computing Kills Encryption. Retrieved May 20, 2016, from http://hackaday.com/2015/09/29/quantum-computing-kills-encryption/

The goal of this source is to talk about the threat of quantum computing directly from the encryption standpoint. This article talks about the encryption side of the issue and essentially states that the within 10-30 years, current encryption will be obsolete. While this maybe the best case scenario, the writer says that we should be making steps toward a stronger form of encryption because D-Day is coming. This sources validity is questionable due to the sites branding and clear bias. I do think that the information relayed in the article is true but the predictions are all speculative. I will try to only use the objective parts of the article to avoid quoting a journalist with no academic backing.

Chu, Jennifer. "The beginning of the end for encryption schemes?" MIT News. N.p., 03 Mar. 2016. Web. 4 Apr. 2017.

This is MIT's most recent attempts in the Quantum Computing space. They are using a form of Quantum computer that is using a 5 atom scheme that is far more scalable than earlier iterations. I will use this source to explain how higher learning institutions are working to make quantum computing a reality sooner rather than later. MIT is one of the most respected institutions for engineering and is well respected as a valid source for such content.

Kobie, Nicole. "The quantum clock is ticking on encryption – and your data is under threat." WIRED UK. WIRED UK, 20 Mar. 2017. Web. 15 Apr. 2017.

This wired article talks about how the timeline for when quantum computers become a threat to encryption keeps changing. They ask experts on how encryption will recover after these computers make the older styles of encryption trivial. Wired is a credible tech news site and is not peer-reviewed.

Hutchinson, Alex. "HACKING, CRYPTOGRAPHY, AND THE COUNTDOWN TO QUANTUM COMPUTING." The New Yorker. The New Yorker, 26 Sept. 2016. Web. 15 Apr. 2017.

This article from the New Yorker uses recent hacking scandals to show the true threat that the average hacker with a classical computer can bring to the marketplace. They then mention that these hackers are often very brilliant individuals and speculates that these hackers could be the ones working on the next big thing, Quantum computing. I found this article to be far to speculative however I decided to include it in the bibliography as it may serve to be a strong source in showing that not all people reporting on this issue are as valuable. I do hope to come across more article similar to this but with a bit more information brought to the table to make the argument more sound.