Global Information Assurance Certification Paper

Straddling the Next Frontier Part 2: How Quantum Computing has already begun impacting the Cyber Security landscape.

GIAC (GCFA) Gold Certification

Author: Eric Jodoin, ejodoin@hotmail.com
Advisor: Stephen Northcutt

Accepted: Aug 9 2014

"The irony of quantum computing is that if you can imagine someone building a quantum computer that can break encryption a few decades into the future, then you need to be worried right now."

Dr. Daniel Amihud Lidar, Director and co-founder of the USC Center for Quantum Information Science & Technology(CQIST)

Abstract

Theoretical designs of quantum computing are progressively transmuting into practical applications. But, when will such applications of quantum physics phenomena become available? How will they impact the cyber security landscape? As cyber security professionals, what must we know and what must we start doing today to be ready? Using the foundation developed in my previous paper, part 2 focuses on understanding the threats as well as existing and developing opportunities. The first objective of part two is to help the reader take preemptive steps in a timely fashion and posture defenses appropriately. The second objective is to help readers gain the knowledge that will help ensure they can be ready to take full advantage of quantum computing opportunities as they becomes available.

1. Introduction

Theoretical designs of quantum computing are progressively transmuting into practical applications. News articles announcing breakthroughs are appearing in mainstream media just about every month. Hacking and cyber security conferences have begun offering presentations on the subject. In fact, it was a lecture by Blake Cornell at Quebec City's Hackfest in November 2013 which stirred my curiosity. It set me on the path to researching what quantum computing is and how will it impact the cyber security landscape. Then in December 2013, a posting in the SANS GIAC Advisory Board Discussion mailing list regarding Quantum computing research done by the NSA resulted in over twenty responses. Most of the responses highlighted the absence of consolidated information available to cyber security professionals regarding the subject. Then it became obvious there was an informational need regarding the impact of quantum computing on the cyber security landscape and gold papers could help fill that need.

This gold paper is the second half of a two-part research project on quantum computing. Readers who have not yet read part one are strongly encouraged to do so before continuing as it provides the necessary understanding to accurately contextualize the quantum technologies discussed in this paper.

The advent of quantum computing will be no less revolutionary than classical computing turned out to be. It will also have a profound impact on cyber security professionals from the analyst investigating an incident to the CISO considering mitigation measures in response to a Threat Risk Assessment. In fact, some of the changes are groundbreaking; it behooves cyber security professionals to take them into consideration today.

Some of the threats and benefits emanating from quantum physics in general and quantum computing in particular have already begun to materialize. Areas of cyber security, such as asymmetric encryption, will be dramatically impacted by the proliferation of quantum computers. For example, forensic analysts may be able to re-open cold cases that had ground to a halt because the evidence seized was encrypted but vulnerable to cryptanalysis using Shor's or Grover's quantum algorithms. Of course, this

would require that the investigator understood this possibility and thought of safekeeping the evidence in the first place.

On the flip side, intellectual property believed to be secured using encryption may become accessible to an adversary who had the forethought of having recorded a competitor's communications for some time. This is especially worrisome when considering that some of the countries actively funding quantum computing research were also suspected of funding intellectual property theft in a report to the US Congress titled "Foreign Economic and Industrial Espionage[1]" (The US Office of the National Counterintelligence Director (ONCIX), 2011).

This is but a few examples of how quantum computing should be influencing cyber security decision makers today. There are many other examples that will be presented throughout this paper, some of which are still theoretical while others are already in implementation. This is not to say that this paper has all the answers. Quite the contrary in fact. It is meant as a primer to help security professionals assess the impact quantum technologies have already begun exerting on the cyber security landscape. It also provides a foundation for cyber security professionals to understand the breadth of opportunities and challenges that are being introduced with the advent of the quantum computing era. But in the end, its ultimate goal is to inspire cyber security professionals at-large to start seeking out the implications to their specific sub-area of expertise in cyber security.

2. The Next Frontier: Quantum Applications in Cyber Security

Given the enormous amount of funding and research conducted, there has been much progress making practical use of quantum technologies in recent years. Some applications such as true random number generation are in use today. While others, such as the D-Wave quantum computer, represent a nascent industry poised to grow dramatically as the technology is refined and becomes more widely accessible. Other applications, such as quantum computers capable of factoring large numbers, have yet to

[1] http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf

be realized. However, given the potential windfalls of such applications, a significant amount of brain thrust is currently being applied to solving the associated engineering hurdles.

This paper serves as a repository of existing and nascent applications. It also serves as a compilation of applications whose future potential is likely to be realized within the next decade. All of which should be thoughtfully considered by any cyber security professional with input into their organizations strategic vision.

2.1. True Random Number Generation

Classical computers have always struggled with randomness because of their deterministic nature. At best, a computer can output is a pseudo-random number generated from a series of calculations following a specific algorithm. However, to initiate this calculation, a seed number is required. This seed can come from many sources such as the computer's date and time or mouse movements. The problem with pseudo-random number generation stems from the fact that for any given input, the output will always be the same.

Random numbers are important because they are often used to generate a one-time symmetric key. This key is then used to encrypt a secure communication channel. But, if an attacker knows the algorithm used by his potential victim to generate its random key, he may be able to predict the seed and divine the encryption key. The only guaranteed protection against this type of attack is to use a truly random number generation mechanism. This is where quantum indeterminacy provides a definitive advantage.

ID Quantique[2] is a Swiss company that markets a random number generator that leverages quantum indeterminacy. Although not a quantum computer per se, the technology nonetheless exploits an elementary quantum optics process. Photons are sent one by one onto a semi-transparent mirror and detected. The exclusive events (reflection or transmission) are associated to "0" and "1" bit values respectively (ID Quantique, 2010). Available with USB and PCI interfaces, it is used widely in industries that rely

[2] http://www.idquantique.com/

heavily on true randomness such as cryptography but also lotteries, PIN Number generation, pre-paid cards, and statistical research.

2.2. Pattern Matching Problems

D-Wave quantum computers have the potential to solve certain problems significantly faster than any contemporary classical computer. The Google's binary image classifier introduced in part one of this research project, which is capable of discerning complex characteristics out of images, is a good example. Google's algorithm could be used to match and index the faces of victims in cases of online child exploitation. In an interview following a major child exploitation case, a Royal Canadian Mounted Police (RCMP) constable indicated that five investigators could manually verify approximately 100,000 images a day (Crawford, 2013). By pre-processing the images, a D-wave quantum computer can group them by individual victims. An investigator would only have to look at each potential victims in a single image to decide if it is a minor. Then, all images containing the same child would be automatically entered in the system as containing child pornography. This saves the investigator from having to look at every single images containing the same victim. Furthermore, a database of victims could be kept to accelerate future investigations as images of these victims may be found in other suspect's computers. D-Wave also holds the potential to significantly decrease database search times. Such algorithms could also be used during the forensic analysis of a suspect's hard drive to rapidly find other incriminating data.

Before Google confirmed its purchase of D-Wave Two, it asked Dr. Catherine McGeoch from Amherst College to test it and verify if it was indeed better at optimization type problems. The ensuing results demonstrated that the D-Wave Two was able to come up with the answers to the test environment in half a second, compared with 30 minutes for a top-level IBM Machine (Jones, 2013). Not quite as fast as a super computer yet, but fast enough to justify Google's investments and encourage further research and development.

2.3. Source Code Validation

Another interesting application for security researcher is Source Code Validation. Given the risks introduced by 0-day vulnerabilities, an automated process able to discover

bugs and vulnerabilities before a program is publically released would significantly reduce that program's threat surface. This has long been proven to be impossible for classical computers to accomplish. However, Lockheed Martin and University of Southern California (USC) researchers have developed an algorithm that allows D-Wave computers to tell whether a piece of software code is bug-free (Jones, 2013). The USC's Information Sciences Institute website[3] states that Source Code Validation Research is being conducted. However, it has not yet released any practical findings.

2.4. Cryptanalysis using Grover's Quantum Algorithm

There is much debate on quantum computer's ability to break some symmetric encryption algorithms. Johnson in his 2003 book "A Shortcut through time" postulate that Grover's algorithm may be used for breaking symmetric key encryption under certain conditions. However, to succeed, a cryptanalyst would require a sample of cypher text and its original plain text. Making use of two entangled registers, a cryptanalyst would be able to run a laser pulse version of the encryption algorithm at the 1st register, using each of the keys to convert the samples of plaintext into corresponding cypher text. Since this would be a quantum computer, all these calculations would be done simultaneously. Because of the entanglement, the result would be all possible cipher text hovering in superposition in the 2nd register. Then, applying Grover's algorithm, the quantum computer would process the entries simultaneously. The result of which would be a series of probability waves, some canceling each other's while others would combine. Then, a measurement would collapse the superposition as represented by the single remaining probability wave into the correct key (Johnson, 2003).

As Johnson himself pointed out, in the absence of a working quantum computer, inventing algorithms like this is an act of pure abstraction. Despite continued research and much debate, the jury is still out on whether or not a quantum computer could be used to break symmetric encryption. Furthermore, the precise and restrictive conditions described in the previous paragraph that are absolutely necessary for success makes this approach impractical under most circumstances.

[3] http://www.isi.edu/research_groups/quantum_computing/research

2.5. Cryptanalysis using Shor's Algorithm

If cracking the symmetric encryption key is still a problem too hard to break even with quantum computers, perhaps the key could be stolen. Before any encrypted communication can take place, both parties must be in possession of the encryption key. On rare instances, some organizations still use physical key exchange methods such as couriers to deliver encryption keys. However, most key exchange nowadays are done electronically. And, if someone can eavesdrop as the sender and receiver exchange the key, then all future communication using this particular key will be compromised.

Asymmetric encryption, often referred to as Public Key Cryptography, is the most commonly used method for exchanging secret keys. Explaining Public Key Cryptography in details is beyond the scope of this paper. For a more comprehensive explanation, read Thomas Johnson GIAC paper titled "Public-key Cryptography: PGP, SSL, and SSH"[4]. But in short, a sender can use a recipient's widely published public key to encrypt a secret such as a symmetric encryption key to be used in future communications. The secret is sent to the recipient who is the only one able to decrypt it using its private key. Then, both sender and recipient can establish a communication channel using the shared symmetric key. One might ask why asymmetric encryption is not used all the time instead of using it to share symmetric keys. The reasons are twofold. First, asymmetric encryption takes longer to process. Using it for all encrypted communications would measurably slow down the exchange of data. Second, symmetric encryption is still considered the stronger of the two.

Public key cryptography is used to initiate secure (HTTPS) sessions for banking and other sensitive web activity. As the connection is initiated, asymmetric encryption is used to exchange an ephemeral symmetric encryption key that will only be used for this particular session. Each time a new HTTPS session is initiated, a new ephemeral symmetric key is used. If the symmetric key is somehow compromised, only this particular session is compromised. Public key cryptography is also used in countless other applications such as secure emails, Virtual Private Networks (VPNs), and digital signatures.

[4] http://www.sans.org/reading-room/whitepapers/vpns/prime-numbers-public-key-cryptography-969

RSA asymmetric encryption, Diffie–Hellman key exchange, and Elliptic Curve Cryptography (ECC) are the most utilized asymmetric encryption solutions today. The strengths of these asymmetric encryption methods rely on the fact that it is practically impossible for classical computers to solve these discrete logarithm and integer factorization problems. However, as mentioned in part one of this research project, superposition and the manipulation of probability waves offers a new approach to quickly solving factorization problems.

Enter Shor's algorithm, discovered by Bell Labs Scientist Peter Shor in 1994. Taking advantage of a previously undiscovered mathematical connection between factoring and Fourier transform, Shor demonstrated that factoring large numbers could be quickly accomplished using superposition and probability waves. If factoring were of interest only to pure mathematicians, Peter Shor's paper still would have caused a small sensation (Johnson, 2003). But, the fact that Shor's algorithm can be used in a Quantum Computer to crack the most commonly used asymmetric encryption was not lost on cryptanalyst the world over.

Given a quantum computer able to run a customized version of Shor's algorithm, a cryptanalyst could take a target's public key and compute its corresponding private key. As long as the cryptanalyst is able to intercept the target's communication, he will be able to read its content which will include any symmetric key used to encrypt further communications. Then it is only a matter of running the symmetric encryption algorithm on a classical computer using the decoded symmetric key to reveal the target's communications be it HTTPS, SSH, VPN, or otherwise. The same can also apply to emails encrypted using PGP[5] or GPG[6]. An attacker having broken the private key using a quantum computer could read all email correspondence sent to its victim. It could even impersonate its victim and send signed emails on its behalf. Finally, if encrypted communication that relies on asymmetric encryption is recorded today, it could easily be decrypted in a not so distant future when such a quantum computing device is made available to the attacker.

[5] Pretty Good Privacy
[6] The GNU Privacy Guard

2.6. Quantum Key Distribution

If quantum physics renders the most widely used Public Key Cryptography methods obsolete, it also opens up new possibilities for distributing symmetric keys and other secrets. Quantum Key Distribution (QKD) is fundamentally different from its classical cousin. Traditional key distribution relies on computational limitations such as factoring large numbers to assure security. QKD relies on unique properties of quantum physics including superposition, entanglement, and indeterminacy to detect or elude eavesdropping attempts. As such, QKD is used to securely distribute a symmetric key that will subsequently be used to encrypt communications using classical methods.

2.6.1. The BB84 protocol

QKD can be separated into two categories. First is the BB84 protocol invented by Charles H. Bennett and Gilles Brassard in 1984 (Bennett & Brassard, 1984). In this implementation, an emitter and a receiver exchange a series of photons through a pre-configured quantum communication channel such as a fiber optic cable or free space. For this method to work, a second, independent communication channel such as the Internet is required. The BB84 protocol requires this separate communication channel over which the actual encrypted communication will take place after the symmetric key has been exchanged over the quantum channel. This separate communication channel is always assumed to be insecure. Therefore all data transmitted over it must either be of no value to a potential eavesdropper or it must be encrypted.

As photons are transmitted through the quantum communication channel from the sender to the recipient, each end randomly applies polarization filters that represent 1 or 0. After the exchange, the receiver reveals the sequence of filter he used without divulging the actual results of his measurements. This information is exchanged over the unsecure communication channel. In return, the sender announces to the receiver in which cases the polarization were compatible without revealing which filter it used. Now, both the sender and the receiver have enough information to reconstruct a series of random bit which are the same on both side and represent the shared key. This is called the sifting of keys. Some fault tolerance is built into the sifting of keys to allow for normal interference in the quantum communication channel. However, if an eavesdropper attempted to

measure a sizeable number of photons, the resulting quantum indeterminacy would introduce errors that would be readily apparent to both the sender and receiver. In such a case, the quantum communication channel would be considered compromised. It is important to note that the interception of the communications over the unsecure communication channel by the eavesdropper does not constitute a vulnerability, as they take place after the transmission of photons over the quantum channel has already occurred (ID Quantique, 2012).

This form of QKD is already in use today. Four companies offer variations of QKD based on the BB84 protocol. They are ID Quantique[7], MagiQ Technologies[8], QuintessenceLabs[9], and SeQureNet[10]. In addition to a classic communication channel such as the Internet, each require a dedicated fiber optic link as the quantum communication medium. This limits the distance between the sender and recipient to no more than 100 kilometers (60 miles) because repeaters would alter the quantum state of photons. However, the obvious costs and distance limitation has not deterred some practical applications. The Austrian's Secure Communication based on Quantum Cryptography (SECOQC) project lays claim to the first commercial application of QKD. According to a press release it issued on 21 April 2004, Bank Austria Creditanstalt, on behalf of the City of Vienna, performed the World's first bank transfer encoded via quantum cryptography (Secure Communication based on Quantum Cryptography (SECOQC), 2004). The fact that today, four companies' offers QKD solutions is a testament of the growing market penetration this technology has experienced since 2004.

The science behind QKD based on the BB84 protocol is sound. Further improvements in the technology will likely open up new opportunities for practical uses beyond 100 kilometers. Shedding fiber optic cables in favor of free space could significantly reduce cost while increasing range. Especially if the free space quantum communication medium can leverage satellites for over the horizon communications. In February 2014, an Italian research team presented a workable QKD approach through

[7] http://www.idquantique.com
[8] http://magiqtech.com
[9] http://quintessencelabs.com
[10] http://www.sequrenet.com

free-space (Vallone, et al., 2014). Although practical experiments were over short distances, there is little doubt refinements will permit QKD well over the 100 km limits.

Meanwhile, flaws in the BB84 protocol implementation can still offer an avenue of attack. For example, security researchers published a paper in 2011 where they demonstrated their ability to override ID Quantique receiver's ability to detect a breach of security (Centre for Quantum Technologies in Singapore, 2011). Therefore, today's QKD technology does not necessarily equate to absolute security as other implementation flaws are likely to be discovered. But then again, the same can be said of any implementation as the recent hearthbleed[11] OpenSSL implementation flaw clearly illustrated.

Finally, it is important to note that this approach is vulnerable to certain forms of Denial of Service. If an attacker is not as interested in eavesdropping as he is at preventing any communication, then consistently measuring photons on the quantum communication channel would invariably result in a failed attempt at creating a shared key. That is, until such time that the sender and receiver switch to a different quantum communication channel that is inaccessible to the attacker. This also highlights a shortcoming in the quantum communication channel. There is no way to authenticate the incoming photons and validate their origin. All photons are assumed to have been sent by the sender. This could provide an opportunity for a Man-in-the-Middle attack by an adversary present in both the quantum communication channel and the independent communication channel (IEEE Spectrum, 2008).

2.6.2. The E91 protocol

In a variation on the BB84 protocol, Arthur Ekert proposed in 1991 an approach that would see a pair of entangled photons split up between a sender and a receiver. Known as the E91 protocol, it uses quantum entanglement to allow both parties to read its own photon's state and predict the state of the other's photon using a variation on the polarization technique used in the BB84 protocol (Winkler, 2010).

This approach offers three significant advantages. First of all, there is no maximum distance after which the entanglement effect dissipates. Therefore, both parties could be right next to each other or at opposing ends of the earth. Secondly, there is

[11] http://heartbleed.com/

absolutely no detectable communication between the two particles, making this quantum communication channel impervious to eavesdropping. Finally, any attempts by a 3rd party to observe correlation between both particles would immediately destroy the correlation between them and be readily detectable by the legitimate participants.

Recent developments have even opened the door to multi-party quantum communication. In March 2014, researchers at the IQC have demonstrated the distribution of three entangled photons at three different locations (IQC Press Release, 2014). In effect, suggesting that three, and potentially more, separate parties could exchange information using quantum entanglement. This is still in the experimental stage but, it opens up possibilities unequaled in the classical Public Key Cryptography domain.

Unlike the E84 protocol, QKD using the E91 protocol is still in the research and development stage and is unlikely to become available in the next decade.

2.7. Preparing for the Quantum Computing Revolution

Advancements in quantum computing technology are both cause for concern and for celebration. The power of quantum computers is still probably decades away from being accessible to everyday users. However, as was the case with classical computers, this power is much closer at hand to some governments and select corporations. Therefore, some institutions will be uniquely positioned to take advantage of advances in quantum computing early on.

2.7.1. Quantum based Cryptanalysis in support of Network Defenders and Forensic Investigations

The Source Code Validation techniques developed by Lockheed Martin could be used for both offensive and defensive purposes. There is a significant amount of open source software used in commercial applications. OpenSSL is such an example which made the news recently because of a software bug. Such source code could be scanned by anyone with access to a D-Wave computer and an algorithm such as the one developed conjointly by Lockheed-Martin and the USC. Whether the findings are used to exploit vulnerabilities or to fix them depends entirely on the intent of the operator.

Researchers have developed an approach to machine learning and anomaly detection via quantum adiabatic evolution. This approach consists of two quantum phases, with some amount of classical preprocessing to set up the quantum problems (Pudenz & Lidar, 2013). It was specifically designed to work on D-Wave quantum computers. The anomaly detection method for discovering malware using classical computers is widely used on hosts and networks alike. The approach proposed by this research could be adapted to service this type of anomaly detection and potentially increase detection speed and rate in the defense of networks and hosts.

Quantum computing could do even more than just help find malware in the future. The presence of malware, especially if capable of exfiltrating intellectual property, is considered by many as an existential threat to various governments and corporations. However, in order to obfuscate what is being pilfered and therefore delay any containment and remediation efforts, most threat actors will use encryption to send commands to their malware and to trickle out data. This way, if the traffic is discovered, the incident responder may know that data was likely exposed but not exactly what it contained or what else the malware was told to do, even if extensive forensic analysis is conducted on the compromised hosts(s). And, to prevent reverse engineering from revealing a symmetric encryption key hidden deep within the malware, most malware writers will use commonly available public key cryptography instead of hardcoding a symmetric key. If the incident responder is able to obtain a full packet capture starting with the asymmetric key exchange, then extracting the symmetric encryption key becomes trivial using quantum computing. In turn, this will reveal everything that has been extracted, and any commands employed to operate the malware.

Finally, a forensic analyst who has been stopped cold in an investigation because of encryption may be able to leverage quantum computing to break the case. Provided the case involves the use of public key cryptography by the suspect such as a recorded HTTPS session or emails sent between accomplices. All that would be needed is a few minutes of quantum computation to reveal the encrypted symmetric keys and other secrets such as emails. Then, traditional forensics could take over and continue the investigation. The case does not even need to be recent. As long as all the encrypted evidence has been

collected and preserved, decryption of previously inaccessible data could tip the balance in favor of the investigators.

2.7.2. Defense against Quantum based Cryptanalysis

If a specific organization's intellectual property is the envy of competitor(s). And if they have been or suspect they may be targeted by illicit attempts at stealing their intellectual property. Then the ability by an adversary to develops or acquires a quantum computer capable of breaking the public key cryptography used by the organization is cause for serious concerns today.

At some point, measures will need to be taken to prevent intercepted communications from quantum computer aided cryptanalysis. When and to what extent this protection must be applied depends entirely on the usable life of the data being encrypted. Individual banking transactions may not hold much value a few days after they have been completed. However, sources of income, bid preparation, strategic outlook, or loss of other types of intellectual property could strip an organization from its competitive advantage. In situations where this data is intended to remain private for several years, now is the time to consider new encryption methodologies.

Quantum Key Distribution (QKD) is one approach that is possible today. However, as discussed in section 2.6, it suffers from serious limitations including cost and distance. But, perhaps QKD is not the only approach able to resist quantum computer aided cryptanalysis. Other public key cryptography algorithms are believed to be impervious to known quantum attacks. And they have the added benefit of not requiring a dedicated quantum communication channel. The following solutions are strong contender believed to be capable of resisting both classical and quantum computer attacks (IEEE Spectrum, 2008):

1. Lattice-based cryptography;
2. Hash-based signatures;
3. Multivariate cryptography; and,
4. Elliptic Curve Isogenies cryptography.

Various algorithms have been developed for each approach but few have made it beyond the theoretical realm and into practical applications thus far. Although advancements in quantum computing may spur renewed interest in the near future, there has not been much effort made toward implementing any of these algorithms but for one exception.

In 2008, the NTRU encryption algorithm, a lattice-based cryptography solution, was standardized by IEEE Std 1363.1-2008. Then in 2010, it was approved by the Accredited Standards Committee X9 as a new encryption standard for data protection. The ANSI X9.98 standard specifies how to use Lattice-based public key cryptography like NTRU to protect data for financial transactions through a public/private-key crypto system (Robinson & Mann, 2011). Java and C implementations of the NTRU encryption algorithm are available on the NTRU Project web page[12]. In addition, benchmarks posted on this web site suggest that the NTRU algorithm is significantly faster than RSA. This makes NTRU ideal for mobile devices with limited processing power and for high volume servers.

Forward leaning financial institutions are not the only one making use of NTRU. The NTRU Algorithm is patented and owned by SecurityInnovation[13]. The algorithm is available under two licensing options, a free Open Source GNU GPL v2 license and a Commercial license. StrongSwan has a plugin that integrates the Open Source GNU license (StrongSwan UserDocumentation, n.d.). SecurityInnovation also offer several software libraries for implementing NTRU including SSL and ARM7/9 libraries. Although payment is required for a commercial NTRU license, at $2 or less per licenses (Security Innovation, 2013), it is likely to cost much less than a QKD system especially when considering deployment, operation, and maintenance costs.

However, along with increased market penetration comes increased scrutiny. It was discovered that Lattice-Based Cryptosystems such as NTRU are not without shortcomings. They are known to be vulnerable to broadcast attacks where a single message is encrypted by the originator numerous times for several recipients who have

[12] http://tbuktu.github.io/ntru/
[13] https://securityinnovation.com/products/encryption-libraries/ntru-crypto/

different public keys. By mathematically superposing ciphertexts intended for different recipients, an attacker can derive the plaintext without requiring any knowledge of any recipient's secret key. The obvious solution to this problem is not to use the broadcast functionality of NTRU, especially since researchers from Tsinghua University in Beijing have demonstrated an algorithm that can efficiently accomplish a broadcast attack against NTRU's highest security parameters (Li, Pan, Liu, & Zhu, 2011). Implementing NTRU in a manner that will not permit broadcasts is an absolute necessity for any deployment.

Other Chinese researchers have also developed an attack against NTRU, this time leveraging quantum computing. Their method combines the advantages of meet-in-the-middle attack and the Grover algorithm. They have demonstrated, in theory at least, that their attack dramatically dropped the time complexity of the cryptanalysis (Xiong, Wang, Wang, Zhang, & Chen, 2012). But even with this attack, NTRU still provides roughly the same security against a quantum computer as AES-128 does today against a classical computer (Jenney, 2014).

At this time, NTRU is probably the most sensible and economical option for enterprises concerned with surviving a classical and/or quantum computers aided cryptanalysis attack. Other solutions based on Hash-based signatures, Multivariate cryptography, or Elliptic Curve Isogenies cryptography may offer viable solutions in the future. However much research and analysis remains to be done to verify their ability to resist classical and quantum cryptanalysis.

3. Conclusion

Recent applications issued from quantum physics research and development such as true random number generators, quantum key distribution, and even D-Wave's quantum computer can serve as good indicators of things to come. With over a billion dollars invested this last decade alone, more advanced quantum computers are bound to make their entrance within the next decade or so. As was the case with classical computers, quantum computers will at first be the exclusive domain of large government agencies and corporations like Lockheed Martin and Google. But how soon before these

institutions begin offering their quantum computer's processing time as a service either to smaller federal/state/local government agencies or the public sector?

Whether this represents an opportunity or a threat depends on how we posture ourselves. Much can be accomplished today to take advantage of quantum computing applications once they become available to us. But without a doubt, the greatest threat is in regard to public key cryptography. If data within encrypted communications going on today can still be of value when quantum computing cryptanalysis becomes a reality, then steps must be taken today to counter this threat.

QKD is one approach available today but with limited practical applications. However, further research is bound to solve its current limitations although it may come too late. Other Public Key Cryptography algorithms may also offer solutions but more research is required to fully transform these potential solutions into practical application. NTRU is the exception with a fully developed and accredited approach that can be implemented today. Although attacks against it have been developed, none have demonstrated a fatal flaw and it remains the most robust public key cryptography solution available.

It is our role as a cyber-security professional to anticipate and counter current and emerging threat. Therefore, our work dealing with quantum computing has just begun. Beyond the questions answered by this paper lies more complex and time-consuming engineering, implementation, deployment, and policy challenges that must be overcome to turn advancements in quantum computing from potentially fatal threats into overwhelming advantages.

4. References

Bennett, C., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. *IEEE International Conference on Computers, Systems and Signal Processing.* Bangalore, India. Retrieved from http://www.cs.ucsb.edu/~chong/290N-W06/BB84.pdf

Centre for Quantum Technologies in Singapore. (2011, June 15). *Making quantum cryptography truly secure: paper in Nature Communications.* Retrieved from http://www.quantumlah.org/: http://www.quantumlah.org/highlight/110615_hacking.php

Eric Jodoin, ejodoin@hotmail.com

Crawford, A. (2013, June 19). *Child porn arrests: Investigators must track moving targets*. Retrieved from CBC News: http://www.cbc.ca/news/politics/child-porn-arrests-investigators-must-track-moving-targets-1.2664765

D-Wave Systems. (2014, April 28). *Meet D-Wave*. Retrieved from www.dwavesys.com: http://www.dwavesys.com/our-company/meet-d-wave

Ford, K. W. (2011). *101 quantum questions: what you need to know about the world you can't see.* Cambridge, Mass.: Harvard University Press.

ID Quantique. (2010, April). *Random Number Generation using Quantum Physics.* Retrieved from idquantiqe.com: http://www.idquantique.com/images/stories/PDF/quantis-random-generator/quantis-whitepaper.pdf

ID Quantique. (2012, March). *ID Quantique White Paper: Understanding Quantum Cryptography.* Retrieved from IDQuantique.com: http://www.idquantique.com/images/stories/PDF/network-encryption/white-paper-understanding-qkd.pdf

IEEE Spectrum. (2008, November 2008). *Q&A With Post-Quantum Computing Cryptography Researcher Jintai Ding*. Retrieved from spectrum.ieee.org: http://spectrum.ieee.org/computing/networks/qa-with-postquantum-computing-cryptography-researcher-jintai-ding

IQC Press Release. (2014, March 23). *Experiment opens the door to multi-party quantum communication*. Retrieved from University of Waterloo News: https://uwaterloo.ca/news/news/experiment-opens-door-multi-party-quantum-communication

Jenney, P. H. (2014, MAy 19). personal communication.

Johnson, G. (2003). *A Shortcut Through Time: The path to the Quantum Computer.* New York: Alfred A. Knopf.

Jones, N. (2013, June 19). *Computing: The quantum company*. Retrieved from nature.com: http://www.nature.com/news/computing-the-quantum-company-1.13212

Li, J., Pan, Y., Liu, M., & Zhu, G. (2011, November 24). *An Efficient Broadcast Attack against NTRU.* Beijing: Key Laboratory of Mathematics Mechanization. Retrieved from https://eprint.iacr.org/2011/590.pdf

Pudenz, K., & Lidar, D. (2013, May). Quantum adiabatic machine learning. *Quantum Information Processing, 12*(5).

Robinson, M., & Mann, L. (2011, April 11). Security Innovation's NTRUEncrypt Adopted as X9 Standard for Data Protection. Wilmington, Massachusetts. Retrieved from http://www.businesswire.com/news/home/20110411005309/en/Security-

Eric Jodoin, ejodoin@hotmail.com

Innovation%E2%80%99s-NTRUEncrypt-Adopted-X9-Standard-Data#.U2bGpVfRbdw

Secure Communication based on Quantum Cryptography (SECOQC). (2004, April 21). *World Premiere: Bank Transfer via Quantum Cryptography Based on Entangled Photons.* Retrieved from http://www.secoqc.net: http://www.secoqc.net/downloads/pressrelease/Banktransfer_english.pdf

Security Innovation. (2013, October 4). *NTRU Commercial License.* Retrieved from securityinnovation.com: https://github.com/NTRUOpenSourceProject/ntru-crypto/blob/master/COMMERCIAL%20LICENSE.doc?raw=true

Siegfried, T. (2000). *The bit and the pendulum. From quantum computing to M theory-the new physics of information.* New York: Wiley.

StrongSwan UserDocumentation. (n.d.). *NTRU Encryption as an IKE Key Exchange Mechanism*. Retrieved from StrongSwan User Documentation, PluginList, NTRU: http://wiki.strongswan.org/projects/strongswan/wiki/NTRU

The US Office of the National Counterintelligence Director (ONCIX). (2011). *ONCIX Reports to Congress: Foreign Economic and Industrial Espionage.* Washington, DC: ncix.gov. Retrieved from http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf

Vallone, G., D'Ambrosio, V., Sponselli, A., Slussarenko, S., Marrucci, L., Sciarrino, F., & Villoresi, P. (2014, February 11). Free-space quantum key distribution by rotation-invariant twisted photons. Retrieved from http://arxiv.org/pdf/1402.2932.pdf

Winkler, J. (2010). *Entanglement and Quantum Key Distribution.* Retrieved from University of Rochester Institute of Optics: http://www.optics.rochester.edu/workgroups/lukishova/QuantumOpticsLab/2010/OPT253_reports/Justin_Essay.pdf

Xiong, Z., Wang, J., Wang, Y., Zhang, T., & Chen, L. (2012). An Improved MITM Attack Against NTRU. *International Journal of Security and Its Applications*. Retrieved from http://www.sersc.org/journals/IJSIA/vol6_no2_2012/36.pdf

Eric Jodoin, ejodoin@hotmail.com