Implications of Quantum Information Processing On Military Operations

By MSG Jeffrey Morris | May 29, 2015

INTRODUCTION

This paper discusses the benefits and drawbacks of quantum computing and quantum cryptography, subsets of the field of Quantum Information Processing (QIP). This field uses quantum mechanics for information processing rather than classical mechanics and portends game-changing implications to technologies long-relied on by military organizations, including computing, communication, and cryptographic systems. QIP is an emerging area of research whose complexity and often counterintuitive nature makes it difficult to separate fact from fiction. This paper provides an overview of QIP from the perspective of military operations and proposes estimates when major breakthroughs might occur. As with any attempt at predicting the future, these estimates are just that, estimates, but included to provide a rough approximation.

Quantum mechanics allows a single quantum computer to compute as dozens or even hundreds of classical computers, known as 'quantum parallelism.' This is leading to a new paradigm in computing [1] as these computers undermine current public key infrastructure (PKI) encryption systems, including the Department of Defense (DOD) Common Access Card (CAC) system, as breaking this form of encryption would be a trivial effort [2]. Continuing work in lattice-, code-, hash- and multivariate-based cryptographic systems shows promise for being 'quantum resistant' [3-6], as they do not use the same basis for encryption as PKI.

QUANTUM COMPUTING

Quantum computing uses a fundamental information unit, the quantum bit or 'qubit,'[1] different from classical computers, which use the 'bit', a logical unit based on whether an electrical signal is off or on through a pathway. Unlike classical computing, where each bit contains only one of two possible values [7], each qubit is in a continuous range between '1' or '0' and a system of qubits hold *each* set of values in each qubit. Figure 1 shows a comparison between the values in a bit and a qubit.

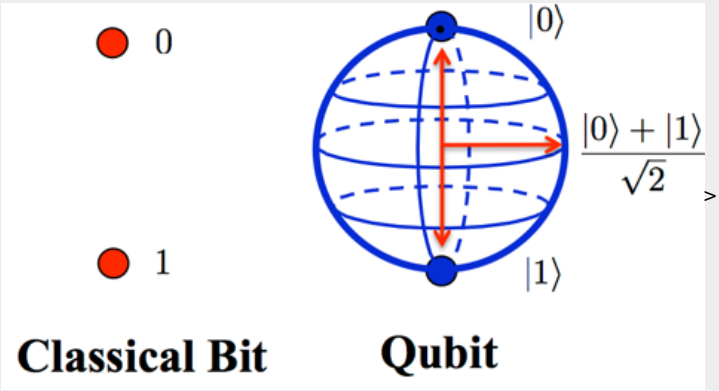

Fig 1. Comparison of classical and quantum bits [8].

For example, a system of three classical bits can hold a single number between 0-7 (2^3) while system of three qubits can hold *all* numbers 0-7 at the same time. While quantum computing provides efficient solutions to some classes of problems due to working on huge number sets at a single time (e.g. factoring large numbers, the basis for current PKI cryptograph), it does no better than existing classical computers on certain problem classes (hashes, multi-variate systems) and on other classes it provides only a small increase in efficiency (e.g. searches of unstructured lists).

Devoret and Schoelkopf created a 'timeline' for quantum computing comparing the complexity necessary for such a computer to the time needed to perfect the complexity. Figure 2 visualizes the seven levels of complexity and shows quantum computing is moving from level three (QND Measurements) to level four (logical memory lifetimes) Devoret says as of yet, scientists have not found any fundamental problems that would prevent building large-scale quantum processors.

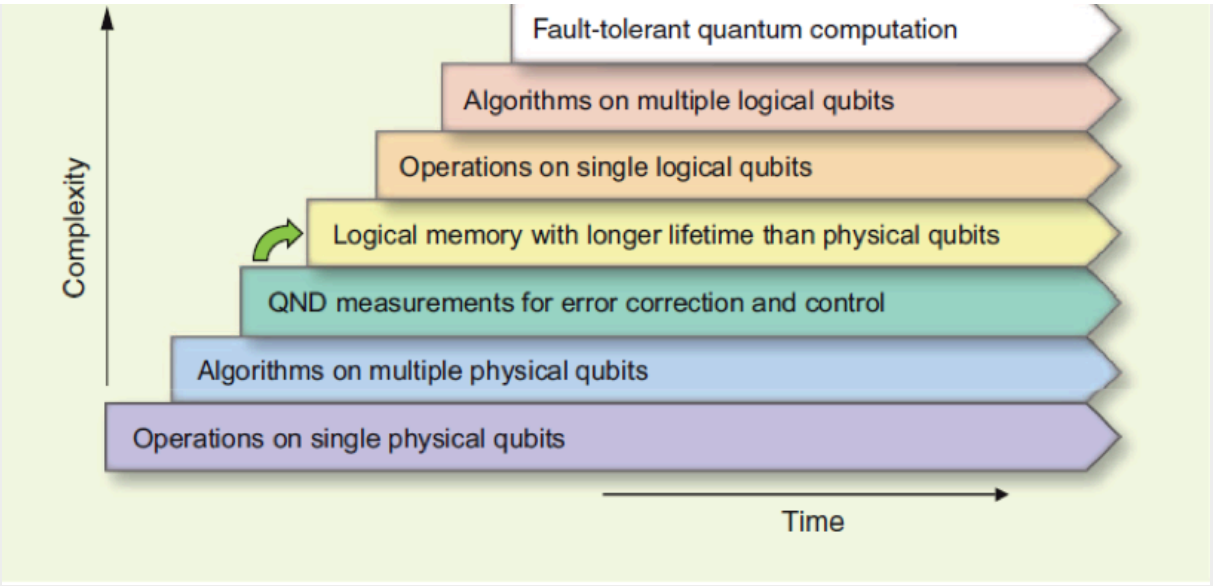

Fig 2. Seven stages in the development of quantum information processing [9].

Prime Factorization Cryptography Will Fall

The strength of many common cryptographic algorithms rely on computational security, meaning the algorithm is secure if there is a negligible chance of discovering the key in a "reasonable" amount of time using current computational technology [10]. Recent developments in quantum computing technology (including supporting algorithms) place certain classes of commonly-used asymmetric cryptographic algorithms (i.e. those that rely on the difficulty of factoring large numbers into their constituent primes, such as the Rivest, Shamir, and Adleman (RSA) algorithm), at risk.

These algorithms are the basis of existing PKI used throughout the world (e.g. e-commerce, digital signatures and token-based authentication systems). The resulting loss of security in commonly used asymmetric public key cryptographic algorithms, such as RSA, will likely increase the use of symmetric cryptographic systems and intensify the need for secure and efficient key distribution [11, 12]. Certain groups of cryptographic systems (lattice & multi-variate) believed hard to solve by quantum systems are rising to the forefront of next-generation PKI systems. Table 1 compares classical and quantum computers factoring different size of numbers.

Table I. Comparison of Classical vs. Quantum computers [2]

Classical Computer	Quantum Computer
Factor 193 digits using a 2.2Ghz machine: 30 CPU years	Factor 193 digits using a 2.2 GHz machine: 0.1 seconds
Factor 232 digits using a 2.2Ghz machine: 2000 CPU years*	No estimate available
Factor 500 digits using a 2.2Ghz machine:10^{12} CPU years	Factor 500 digits using a 2.2 GHz machine: 2 seconds

*Largest number currently factorable; special hardware using a distributed system of computers [13]

Another concern is cryptographic data security in the future. Vast quantities of data encrypted with current technology and stored in computers across the globe will suddenly become at risk once quantum computers become a reality. Any encrypted text captured and stored by adversaries but secure now will become vulnerable in the future. There are certain secrets that need protection into the future, such as nuclear weapon technology, trade secrets or proprietary data and diplomatic traffic. Decryption of this data could have dangerous consequences and this stored data must be re-encrypted with newer technology once the older encryption systems become compromised.

Faster Hardware and Quantum Parallelism

Another expected benefit is increases in hardware speed. Current computer technology increases hardware speed by increasing the density of transistors on a single processing chip, shortening the travel distance for electrons through the trace paths within the chip. This miniaturization is now subject to harmful quantum effects because of the minute distances between electron paths (quantum tunneling). Hardware built to harness these quantum effects, rather than minimize them, may run much faster than current technology [14].

D-Wave Systems offers their version of a 'quantum computer.' They have stirred controversy with their D-Wave Two computer, which they claim contains 512 qubits. While scientists debate whether the machine performs quantum computations [15, 16], last year Time magazine featured an article on D-Wave and noted several

While scientists debate whether the machine performs quantum computations [15, 16], last year Time magazine featured an article on D-Wave and noted several companies and agencies have bought these machines (Lockheed-Martin, NASA, Google and an unnamed U.S. intelligence agency) [17]. This machine is specifically built to solve optimization problems and cannot factor large numbers, leading scientists to debate if it is the quantum computer envisioned by the early pioneers [18-20].

Quantum parallelism allows a single quantum computer to do the work of a distributed system of classical computers, enabling better brute force attacks on cryptographic systems by using this technique along with efficient quantum algorithms [21]. Classical computational power scales *linearly* as processing speed, memory speed and number of processors increase. Quantum computational power scales *exponentially* with the number of qubits added to the system. Table II, from a recent paper on quantum computers, shows the comparison between classical and quantum computers needed to factor a 2048-bit number of the type used for RSA encryption.

Table II. Factoring a 2048-bit Number [22].

Metric	Classical Computers	Quantum Computer
Time to Run:	10 years	24 hours
Size of hardware:	Server farm covering ¼ of North America	100K logical qubits and 200M physical qubits, in less than a small room
Power Usage:	10^{12} megawatts (10^5 times world output, consuming the world's entire amount of fossil fuels in one day)	<10 megawatts (less than the power consumed for a house for a year)[23]
Cost:	$$10^9$ billion (17,000 x 2014 US GDP)[24]	$100 billion (0.6% of 2014 US GDP)[24]

Faster Search

Quantum computing leads to faster searches for certain classes of structured lists, such as large databases and the results of analytic programs and processes. While the increase is small,[2] it been proven faster than any classical approach [25]. Matched with an increase in computation speed, this could lead to better and faster simulations, real-time process searches and fast n^{th} dimensional data searches.

Quantum Computing Issues

While quantum computers have many expected benefits, there are several hurdles to overcome. The first is the greatest challenge: manipulating qubits is hard. Quantum systems disturb easily, causing the qubits to collapse into unusable or error states, the phenomenon of *decoherence*[3] [26]. The difficulty is isolating the qubits from the surrounding environment but still be able to manipulate them for computational purposes. Most of the effort in resources in a quantum computer will go into error correction of the qubits, countering the decoherence effects [9].

A common solution is to cool the machine to temperatures approaching absolute zero, an expensive and technically difficult solution. This problem currently limits the size of quantum computers to less than tens of qubits, a chip size of 2^{10} bits of processing power. As of yet, there has not been a 'Moore's Law'[4] growth in the complexity of quantum computers [9]. Even these small achievements need massively-cooled systems or exotic hardware such as nuclear magnetic resonance (NMR) systems the size of rooms [25].

Even solving these problems will not make quantum computers an everyday device. While providing increases in speed and quickly solving problems considered infeasible for classical computers, there are entire classes of problems where quantum computers are not better, such as post-quantum cryptographic systems, and certain kinds of math problems. The quantum search algorithm mentioned earlier was shown to be optimal, meaning these searches cannot improve through better quantum computers, meaning regardless of computer improvements, the problem does not become easier to solve.

Certain other results suggest the limited nature of quantum algorithms (beyond the scope of this paper). These problems, with hardware costs and scaling issues, limit quantum machines to specialized applications such as decryption, massive database searching and complex modeling and simulation, much like the "super-computers" of earlier decades. Referring back to Figure 2, there are further development stages that need solving before QIP becomes reality [9]. Table III provides estimates when quantum technology may become generally available.

Table III. Quantum Technology Deployment Estimates

Technology	Time to Deployment	Notes
QKD	Now	Systems improving rapidly
Quantum Computer (adiabatic)*	Now	D-Wave systems 512-qubit system

Quantum Computer (gated)**	10-20 years	Dependent on solving many other technology issues

*specialized system for optimization problems

**general design using quantum equivalents of classical computing gates

QUANTUM KEY DISTRIBUTION (QKD)

Cryptography is a centuries old battle between code maker and code breaker [11]. Today much of modern society depends on cryptography to provide security services including confidentiality, integrity, authentication, and non-repudiation [27]. Unfortunately, only the One-Time-Pad (OTP) symmetric key algorithm is "information-theoretically secure" [28, 29]. All other cryptographic systems are breakable if the adversary has enough cipher text, computational resources, and time [10], a significant issue at the dawn of the quantum computing. Despite its security, the OTP is not in common use because of its requirement that its keys are random, equal in length to the message, and are never reused. These requirements impose significant limitations on use of the OTP in most applications because of the problems involved with secure key generation and distribution.

Quantum Key Distribution (QKD) is a technology that offers the means for two geographically separated parties to create a shared secret key [30]. QKD allows for detecting eavesdropping on the key exchange, assuring the secrecy of the key. This is possible because of the fundamental laws of quantum mechanics, which ensures any third-party eavesdropping on the quantum channel introduces detectable errors.

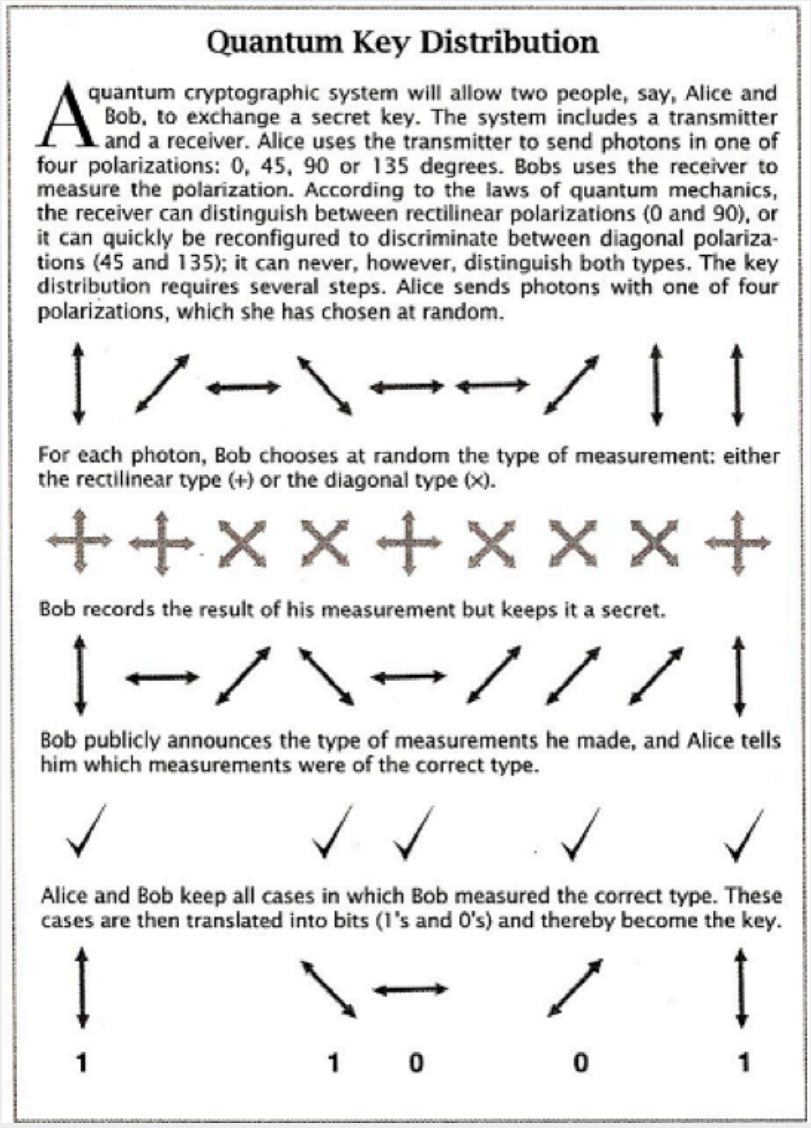

Fig 3. Quantum Key Distribution, shown in Bennett's 1992 paper [31].

The genesis of Quantum Key Distribution (QKD) traces back to Stephen Wiesner, who developed the idea of quantum conjugate coding in the late 1960s [32]. He described an application for quantum coding to broadcasting multiple messages in such a way that reading one of the messages destroys the others (quantum

multiplexing). Wiesner's quantum multiplexing uses photons polarized in conjugate bases as qubits to pass information. If the receiver measures the photons in the correct polarization basis, he or she receives a correct result with high likelihood. However, if the receiver measures the photons in the wrong (conjugate) basis, the measured result is random, and because of the measurement, all information about the original basis is destroyed [33]. These ideas lead Charles Bennett and Giles Brassard to describe a cryptographic system based on the laws of quantum mechanics [31].

(Provably) Secure Key Distribution

QKD is suitable for use in any key distribution application that has high security requirements. Existing documented applications include financial transactions and electoral communications [34, 35], but there are numerous potential applications in law enforcement, government, and military applications. The commercial systems typically use QKD as a means to produce shared secret keys for use in bulk symmetric encryption algorithms, such as the Advanced Encryption Standard (AES). In this case, the QKD-generated key updates the encryption key frequently (e.g., once a minute) reducing the needed QKD-key generation rate, which is inversely related to the distance between the QKD systems. While not unconditionally secure[5], users consider this an improvement when compared with updating the key less frequently (e.g., daily or monthly) [33].

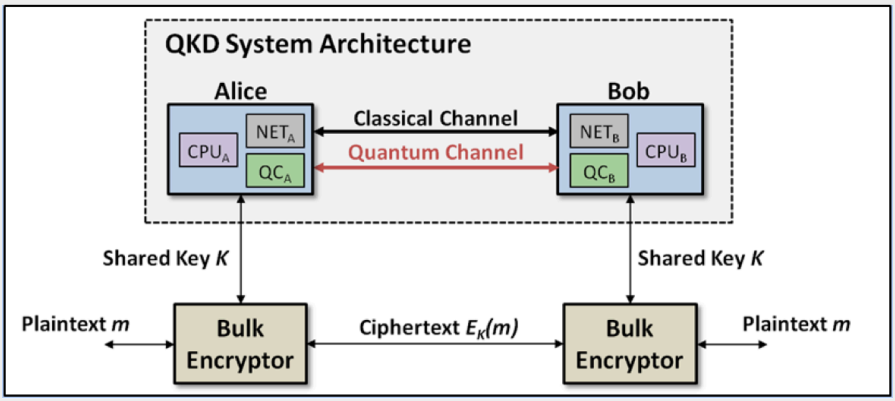

Fig 4. Reference QKD architecture [36].

Since developing the first QKD protocol there have been many new QKD-related protocols, technologies, and architectures developed which provide the ability for unconditionally secure key distribution. In 2001, ID Quantique SA offered and sold the first commercially available QKD system [37]. This was a significant development as anyone could buy an unconditionally secure cryptosystem costing less than half a million dollars, depending on the type of system and the provider. Commercial QKD systems are available from sellers in Europe (ID Quantique; SeQureNet), Australia (Quintessence Labs),North America (MagiQ) and Asia (Quantum Communication Technology Co., Ltd.) and used in applications needing high security such as financial and electoral communications [34, 35]. In 2014, Los Alamos National Laboratory licensed the results of their 20 years of quantum cryptography research to Whitewood Encryption Systems, Inc. to create quantum-based random number generators and encryption systems [38].

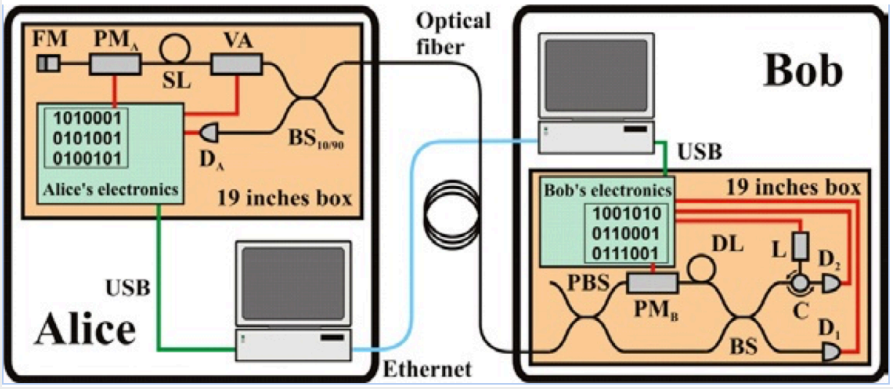

Fig 5. "Plug & Play" system architecture for the Swiss QKD system [39].

Pictured in Fig 4 Is the design for a "plug & play" [40] system proposed and built by Swiss scientists in the early 2000's. This system was successfully deployed under a lake in Switzerland and connected two research centers for many months. Many follow-on QKD systems use a variant of this architecture.

QKD-secured systems could connect command and control nodes throughout the communication channels, connecting commanders with their leadership through terrestrial and ground to space circuits. Satellites with onboard QKD devices could communicate globally, and distribute new keys to friendly systems located anywhere in the line of sight to the platforms. Changing the key several times a second could make it almost impossible for cyber adversaries to decrypt the communications traffic.

QKD Limitations

Though QKD provides many benefits, it has several limitations. The first is the most critical, as current technology and hardware does not meet the conditions specified in the QKD protocol. These hardware 'non-idealities' include on-demand single photon emitters, lossless photonic channels between sender and receiver, perfect photonic detectors, and perfect alignment of bases throughout the system. Current QKD systems cannot meet the theoretical security of the original QKD protocol, leading to security issues with the systems, called 'quantum hacking,' with much work with these issues being done at the Quantum hacking lab, led by Dr. Vadim Makarov [41-43].

Other issues with current QKD systems are their slow key generation rate and limited range. The "unconditionally secure" system needs one bit of key for each bit of data, but current QKD systems generate key material far too slowly for this form of encryption, so current implementations generate key for other encryptors, such as a bulk AES network encryptor [34, 37]. Current ranges for QKD systems are less than 100km because of quantum effects with the transmission channels and issues with current-generation photon detectors. The communication range and key generation rate are inversely linked, as the range increases between sender and receiver, the key rate decreases, effectively reaching zero key transmission [37, 44].

IMPLICATIONS

Quantum information processing, specifically quantum computing and QKD, may provide advantageous to Army operations in two areas: massive parallel processing and secure key distribution. As noted before, quantum computing could bring the ability to break widely-used current encryption systems in almost real-time, forcing both friendly and adversaries to invest in developing encryption protocols that are quantum computing resistant [3, 6, 45]. This may require fielding a new generation of cryptographic hardware and systems throughout the Army. The ability of quantum computers to search efficiently large data lists may allow any system that uses databases or data storage to decrease response time and evaluate greater amounts of data efficiently, an important ability in the dawning world of cloud data storage. Any system or process that requires large amounts of computing time or data searching may benefit from quantum computers.

QKD may provide defense against the decryption abilities of quantum computers. If QKD systems increase key generation rates to enable OTP encryption, this would defeat decryption by quantum computers. This requires QKD systems fielded to senders and receivers throughout the Army, and even key distribution by satellites in low earth orbit to ground stations. Even if key rates continue to be slow, using QKD-generated keys to rapidly change keys on quantum-computing resistant cryptosystems may provide secure encryption without using OTP.

REFERENCES

[1] A. Kott, A. Swami and P. McDaniel, "Security outlook: six cyber game changers for the next 15 years," *Computing Edge,* pp. 36-38, January. 2015.

[2] Institute for Quantum Computing, "John preskill – introduction to quantum information (part 1) – CSSQI 2012," 2012.

[3] V. G. Umana. Post-quantum cryptography. *Post-Quantum Cryptography* [Online]. 2011. Available: http://orbit.dtu.dk/services/downloadRegister/6426368/ThesisValerieGauthier.pdf.

[4] A. Nemes. Quantum resistant cryptography. *Post-Quantum Cryptography* [Online]. 2012. Available: http://www.cs.elte.hu/blobs/diplomamunkak/msc_mat/2012/nemes_antal.pdf.

[5] D. Micciancio and O. Regev. "Lattice-based cryptography," in *Post Quantum Cryptography* (1st ed.), D. Bernstein, J. Buchmann and E. Dahmen, Eds. 2009, Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.142.4862&rep=rep1&type=pdf.

[6] J. Buchmann. Post-quantum cryptography. Presented at Second International Workshop on Post-Quantum Cryptography. 2008, Available: https://www-old.cdc.informatik.tu-darmstadt.de/lehre/WS09_10/vorlesung/pqc_files/PQC.pdf.

[7] E. Rieffel, "Quantum computing," in *The Handbook of Technology Management, Vol III*, 1st ed., H. Bidgoli, Ed. Wiley, 2009, .

[8] (2012, January 01). *Quantum optics and quantum many-body systems: quantum computing.* Available: http://qoqms.phys.strath.ac.uk/research_qc.html.

[9] M. H. Devoret and R. J. Schoelkopf. Superconducting circuits for quantum information: An outlook. *Science* [Online]. *339(6124),* pp. 1169-1174. 2013. Available: http://qulab.eng.yale.edu/documents/papers/Superconducting%20Circuits%20for%20Quantum%20Information%20-%20An%20Outlook.pdf. DOI: 10.1126/science.1231930 [doi].

[10] B. Schneier. *Applied Cryptography: Protocols, Algorithms, and Source Code in C* (2nd ed.) 1995.

[11] S. Singh, *The Code Book: The Secret History of Codes and Code-Breaking.* London: Fourth Estate, 1999.

[12] S. Loepp and W. K. Wootters. *Protecting Information: From Classical Error Correction to Quantum Cryptography* (1st ed.) 2006.

[13] J. Matson, "Record 232-digit number from cryptography challenge factored," *Scientific American,* Jan. 2010.

[14] E. G. Rieffel and W. H. Polak. *Quantum Computing: A Gentle Introduction* 2011.

[15] S. Boixo, T. F. Rønnow, S. V. Isakov, Z. Wang, D. Wecker, D. A. Lidar, J. M. Martinis and M. Troyer. Evidence for quantum annealing with more than one hundred qubits. *Nature Physics 10(3),* pp. 218-224. 2014. Available: http://arxiv.org/pdf/1304.4595.

[16] T. F. Rønnow, Z. Wang, J. Job, S. Boixo, S. V. Isakov, D. Wecker, J. M. Martinis, D. A. Lidar and M. Troyer. Defining and detecting quantum speedup. *Science* [Online]. *345(6195),* pp. 420-424. 2014. Available: http://arxiv.org/pdf/1401.2910.

[17] L. Grossman, "The Quantum Quest for a Revolutionary Computer," *Time,* Feb. 2014.

[18] D. Deutsch. Quantum theory, the church-turing principle and the universal quantum computer. *Proc. R. Soc. Lond* [Online]. *400(1818),* pp. 97-117. 1985. Available: http://www.cs.princeton.edu/courses/archive/fall06/cos576/papers/deutsch85.pdf.

[19] D. Deutsch. Quantum computation. *Phys World 23(22),* pp. 57-61. 1992. Available: https://inis.iaea.org/search/search.aspx?orig_q=RN:23079965.

[20] R. P. Feynman. Simulating physics with computers. *International Journal of Theoretical Physics 21(6),* pp. 467-488. 1982. Available:

http://mengquantumalgorithm.googlecode.com/svn/tags/release1.1/Report/papers/Simulating%20Physics%20with%20Computers.pdf.

[21] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing* [Online]. *26(5),* pp. 1484-1509. 1997. Available: http://arxiv.org/pdf/quant–ph/9508027.

[22] J. Martinis, “Design of a superconducting quantum computer,” Dec, 2014.

[23] (2015, February 20). *How much electricity does an american home use?* [Online]. Available: http://www.eia.gov/tools/faqs/faq.cfm?id=97&t=3.

[24] (2015, April 10). *GDP (official exchange rate)* [Online]. Available: https://www.cia.gov/library/publications/the-world-factbook/fields/2195.html.

[25] E. Rieffel and W. Polak. An introduction to quantum computing for non-physicists. *ACM Computing Surveys* [Online]. *32(3),* pp. 300-335. 2000. Available: http://arxiv.org/pdf/quantph/9809016.

[26] V. Scarani, *Quantum Physics: A First Encounter: Interference, Entanglement, and Reality.* Oxford, UK: Oxford University Press, 2006.

[27] E. B. Barker, W. C. Barker and A. Lee. NIST special publication 800-21 guideline for implementing cryptography in the federal government. 2005. Available: http://csrc.nist.gov/publications/nistpubs/800-21-1/sp800-21-1_Dec2005.pdf.

[28] C. E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal 28(4),* pp. 656-715. 1949. Available: http://dm.ing.unibs.it/giuzzi/corsi/Support/papers-cryptography/Communication_Theory_of_Secrecy_Systems.pdf.

[29] C. E. Shannon. A mathematical theory of communication. *The Bell System Technical Journal 27*pp. 379-423. 1948. Available: http://www.inf.ed.ac.uk/teaching/courses/com/handouts/extra/shannon-1948.pdf.

[30] M. R. Grimaila, J. D. Morris and D. Hodson, “Quantum key distribution, a revolutionary security technology,” *The ISSA Journal,* vol. 27, pp. 20-27, 2012.

[31] C. H. Bennett, G. Brassard and A. K. Ekert, “Quantum Cryptography,” *Sci Am,* vol. 1, pp. 50-57, 1992.

[32] S. Wiesner. Conjugate coding. *ACM SIGACT News 15(1),* pp. 78-88. 1983.

[33] J. D. Morris, M. R. Grimaila, D. D. Hodson, D. Jacques and G. Baumgartner, “A survey of quantum key distribution (qkd) technologies,” in *Emerging Trends in ICT Security*, 1st ed., B. Akhgar and H. R. Arabnia, Eds. Waltham, MA: Elsevier, 2013, pp. 141-152.

[34] ID Quantique SA, “Redefining Security Geneva government secure data transfer for elections,” 2011.

[35] H. Weier. European quantum key distribution network. *European Quantum Key Distribution Network* 2011. Available: http://edoc.ub.uni-muenchen.de/13320/1/Weier_Henning.pdf.

[36] J. D. Morris, L. O. Mailloux, M. R. Grimaila, D. D. Hodson, D. R. Jacques, C. McLaughlin and J. Holes, “Reference architecture for the analysis of quantum key distribution systems,” *IEEE Transactions on Emerging Topics in Computing,* pp. 1-15, 2014.

[37] (2015, January 01). *Cerberis quantum key distribution (qkd) server.* Available: http://www.idquantique.com/network-encryption/products/cerberis-quantum-key-distribution.html.

[38] (2014, September 02). *Quantum computing goes to market in tech transfer agreement with allied minds.* Available: http://www.lanl.gov/discover/news-release-archive/2014/September/09-02-secure-computing.php.

[39] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy and H. Zbinden. Quantum key distribution over 67 km with a plug&play system. *New Journal of Physics 4*pp. 41-48. 2002. Available: http://arxiv.org/pdf/quantph/0203118.

[40] A. Muller, T. Herzog, B. Huttner, H. Zbinden and N. Gisin. “Plug and play” systems for quantum cryptography. *Appl. Phys. Lett. 70(7),* pp. 793-795. 1997. Available: http://arxiv.org/pdf/quant-ph/9611042.

[41] N. Lütkenhaus. Security against individual attacks for realistic quantum key distribution. *Physical Review A 61(5),* pp. 052304. 2000. Available: http://arxiv.org/pdf/quant-ph/9910093.

[42] J. M. Myers, T. T. Wu and D. S. Pearson. Entropy estimates for individual attacks on the BB84 protocol for quantum key distribution. Presented at Proceedings of SPIE. 2004.

[43] V. Scarani, A. Acin, G. Ribordy and N. Gisin. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Phys. Rev. Lett. 92(5),* pp. 57901. 2004. Available: http://arxiv.org/pdf/quant-ph/0211131.

[44] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus and M. Peev. The security of practical quantum key distribution. *Reviews of Modern Physics 81(3),* pp. 1301. 2009. Available: http://arxiv.org/pdf/0802.4155.

[45] M. A. Barreno. The future of cryptography under quantum computers. Dartmouth College. New Hampshire. 2002[Online]. Available: http://borax.polux-hosting.com/madchat/crypto/papers/marco.pdf.

[46] (2014, August 15). *Moore’s law* [Online]. Available: http://www.merriam-webster.com/dictionary/moore’s%20law.

[47] R. Renner, N. Gisin and B. Kraus. Information-theoretic security proof for quantum-key-distribution protocols. *Physical Review A 72(1),* pp. 012332. 2005. Available: http://arxiv.org/pdf/quant-ph/0502064.

Endnotes

[1]A qubit contains a continuous set of possible values expressed by unit vectors within a complex state space with a fixed basis. These systems describe things such as photon polarization, electron spin, and other orthogonal pairs.

[2] √N steps for a quantum computer vs. N steps for a classical computer.

[3] Decoherence is the errors introduced into a quantum state by interaction with the surrounding environment (heat, light, sound or any other form of energy) .Technically, decoherence leads to an error state for a combination of errors [25].

[4] Moore’s Law – “an axiom of microprocessor development usually holding that processing power doubles about every 18 months especially relative to cost or size”

[4] Moore's Law – an axiom of microprocessor development usually holding that processing power doubles about every 18 months especially relative to cost or size [46].

[5] Unconditional security exists when the potential adversary is limited by the only assumption that the laws of physics are correct. Generally, this leads to an adversary with unlimited computing power, time and storage [47].