SECURITY ADVANTAGES OF QUANTUM CRYPTOGRAPHY

JEREMY CLOYD
UNIVERSITY OF TULSA
Department of Computer Science

Address to: Dr. Mark Rideout,
CEO Globe Humanitarian Ventures
1564 Stratford Way Ilyria, OK 74444

The security advantages of quantum cryptography. This paper covers the benefits of quantum cryptography ant it's relation to the limitations of current cryptologic practices, protocols, and technologies. I especially emphasize how the key exchange problem exemplifies the limitations of currently used practices. This research will elaborate on the technology and practices that contribute to the elimination of this longstanding problem. This paper further delves into how quantum Cryptography can be implemented, the wide range of applications of this technology, as well as the possible drawbacks of its adoption. This research is important in order to gain an objective insight into a future characterized by the proliferation of near impenetrable personal encryption. We must strive to make this technology accessible to all interested parties as soon as possible, while also taking great care not to introduce an environment which inhibits the capacity of law and national security agencies to conduct meaningful and fruit-bearing investigations, as the overarching goal of privacy is after-all the common good.

Security Advantages of Quantum Cryptography

Jeremy A. D. Cloyd

University of Tulsa

Department of Computer Science

March 20, 2018

Email: Jec245@utulsa.edu

Abstract

Quantum cryptography is a new method for encoding communications which enables security as infallible as the laws of mechanics. This paper will detail the underlying principles of quantum cryptography as well as the security advantages of quantum cryptography over current cryptologic practices, protocols, and technologies. This paper will elaborate on the technology and practices that contribute to the elimination of the longstanding key exchange problem that exemplifies the limitations of currently used practices. This research aims to detail how quantum Cryptography can be implemented, the wide range of applications of the technology, as well as the possible drawbacks of the its adoption. I believe this research is important in order to gain an objective insight into a future characterized by the proliferation of near impenetrable personal encryption.

"I love strong encryption. It protects us in so many ways from bad people. But it takes us to a place - absolute privacy - that we have not been to before." - James Comey

Page Break

Introduction

Cryptography is the science of encoding communications to protect secrets and communications. Secrecy being intuitively more valuable in times of war has spurred many developments in cryptography to coincide with military necessity to protect and breach the confidentiality of wartime communications. Among those wartime cryptographic developments is Caesar's cipher used to send encoded messages when addressing topics of politics or war. Julius Caesar's eponymous cipher involved shifting each letter of his messages forward by a certain number of letters. Depending on the letter used as the "secret key" the recipient would shift Caesar's message forward by the number of letters represented by the key's place in the alphabet (if the key were "AAAAA…", repeated for the length of the message, then each character would be shifted by a value of 1). Later, in World War II when the Allied forces succeeded in breaking the Enigma cipher, significantly contributing to their ultimate victory and the creation of the first electronic computer. Cryptographic needs have not diminished with time, people currently have greater need for privacy than ever before since the proliferation of digital information systems. The goal of encryption has also remained unchanged, to protect sensitive information from prying eyes, allowing people to communicate and do business as freely and as confidentially as possible. As cryptography has developed throughout history, the sciences of the time have often been coupled with knowledge of encryption to produce favorable advancements (I.e. the German Enigma Machine, which used circular rotors and electrical pins to allow each rotor to complete a full substitution cipher). Currently we possess information and technology from various of schools of science that allow us to again implement a powerful coupling. Employing certain laws of quantum mechanics in the encryption

processes previously and widely adopted, it is now possible to generate a form of encryption that is impervious to “cracking”.

In this paper the theory of quantum cryptography will be detailed, as will its possible implementations and the benefits thereof. I will explain the underlying terms and concepts present in the concept of quantum cryptography, among those being: quantum, key distribution, eavesdropping, and Heisenberg’s Uncertainty Principle. This paper will also satisfy pertinent questions to the necessity of quantum cryptography, among them being: Why is this new form of cryptography needed? what does it do better than what is currently used? What problems that are currently faced does it solve? What type of data can be encrypted using this method?

Encryption has always aimed at converting sensitive information to a form that is more difficult or impossible for an unauthorized third party to intercept and interpret. Thwarting attempts at interception in the past involved the routes your courier would take to the intended recipient without enemy detection, now the routes that our communications travel by are digital. Having our messages traverse to their destination uninterrupted depends upon proper enforcement of network security protocols. Where encryption historically focused on sufficiently obfuscating the content of messages through the usage of ciphers, more recently, computer algorithms have allowed for messages to be encrypted in a much more sophisticated manner. Although sophisticated, the current protocol for encryption is only as infallible as the method used to establish the “secure” channel. Advancements in the field of cryptology have battled those of cryptanalysis (deciphering coded messages without knowledge of the key) closely, each field’s advancement contributing to the obsolescence of some of the other’s techniques. An example of this interaction is the development of the Vigenère cipher, which was a strict improvement upon the Caesar cipher, and considered unbreakable for hundreds of years. Where the Caesar cipher used only one letter as the shift-key, the Vigenère cipher shifted each letter by a different amount, resetting after *n* letters (the key to a “*n = 3”* Vigenère cipher would be something similar to “BACBACBACBAC…” repeating the length of the message). The alternating key of the Vigenère cipher would definitively stump anyone accustomed to cryptanalysis of the more straight-forward Caesar cipher. Though this relationship between cryptography and cryptanalysis seems balanced at first glance, cryptography has always suffered a major disadvantage: the key exchange problem. In the case of the “Key exchange problem” it is impossible to verify that the original communication used to establish a secure channel for future communication with another party was not compromised. In Caesar’s case this problem was not as pronounced as it is now, because he could always whisper the key to decode his messages to his future recipients in person. The current state of communication is rarely physical, with messages traversing great distances in seconds, often between parties whom have never met. How would Caesar go about relaying the instructions of

how to decipher all of his coded messages without the privacy of a whisper, to a person he doesn't know? This is the essence of the key exchange problem, how do two unfamiliar entities come to share a common secret without a third stranger being privy. If an eavesdropper is able to access the secret that one party sends to the other to encode future transmissions, that eavesdropper may easily undermine the entire endeavor. Quantum Cryptography seeks to eliminate this problem by securing the initial distribution of the private key(s) with quantum data so that an eavesdropper cannot access the "secure" channel with an intercepted key. This inviolable method of key exchange is referred to as quantum key distribution or QKD.

QKD offers the enticing promise of impenetrable communication encryption, an unparalleled notion in information security. This promise is delivered on the back of QKD's resistance to the common method of intercepting a transmission, altering or copying it, and retransmitting it to its intended recipient. Quantum key distribution achieves this feat of security through the employment of several laws of quantum mechanics governing interaction with quantum states. Werner Heisenberg states in his 1927 paper, "At the instant at which the position of the electron is known, its momentum therefore can be known only up to magnitudes which correspond to that discontinuous change; thus, the more precisely the position is determined, the less precisely the momentum is known, and conversely". This principle states that the way quanta are observed dictates their behavior; namely attempting to observe the details of a quantum system alters that system's properties in such a way that the data recorded is corrupted. When the intended receiving party in the communication receives the corrupted data, usually the key being distributed, they will be made aware of the presence of the eavesdropper, making it obvious that the communication channel has been compromised. It would then follow as only logical to attempt to copy the quantum data without attempting to view it to avoid corrupting its state and thereby detection. Copying in this manner is demonstrably impossible in quantum mechanics due to the "No-Cloning Theorem" which details that an unknown quantum state possesses too much variability to ever be blindly copied. In short, quantum cryptography greatly assures privacy of communication by first transmitting data in a state that is altered if observed in transmission and cannot be copied without observation. This technology allows for QKD to be verifiably more secure than PKI (public key infrastructure), the current standard.

Cryptography

Asymmetric cryptography uses secret keys which are then stored as random sequences of bits. The Keys are relatively short when compared to the message (with the notable exclusion of the "one-time pad"). In Asymmetric cryptography, party A or "Alice" employs an Algorithm, A which is used in part with a secret key, K to encode a message, M. The algorithm can and should be public; K, should remain entirely private, however. The now encrypted message [E=

$A_k(M)]$ is transmitted to party B or "Bob". In order to extract the message *M,* Bob must decrypt *E* using the inverse of the encryption method, $[M = A_{k^{-1}}(E)]$. This method of key distribution encounters the previously detailed problem distributing a shared secret to the parties.

Symmetric cryptography, also known as "public key cryptography" allows unfamiliar parties to communicate without need of a shared secret using one-way functions which are simple to calculate but difficult to reverse. Instead of using a shared secret, a complementary "key pair" is generated, one public and one private. So instead of one key being shared between two people, one person has two keys: a public key used to encrypt messages, and a private key used to decrypt them. Using asymmetric cryptology, you would broadcast your public key publicly, and anyone wishing to communicate privately with you would encrypt their messages with your public key. This version of AC ensures confidentiality, as you would be the only person capable of decrypting messages sent this way. If communication integrity is desired, you would need only broadcast your public key as usual, then send a message that is encrypted with your private key to the party you wish to communicate with, that party will then decrypt a message using your public key, that could have only been sent by you.

Diffie-Hellman key exchange was the first public-key algorithm that enabled secure symmetric key exchange between unfamiliar or untrusting parties. Instead of each party generating a public/private key pair, they cooperate to generate a shared secret. The Common example of this version of key exchange involves Alice who would like to communicate with Bob. Alice and Bob agree upon a modulus *M,* and a random generated public prime number, *G*. Alice and Bob select arbitrary integer values *A* and *B,* as secret keys which they keep private. Alice computes $A_{A} = G^{A} \bmod M$ *to* ascertain her "public key" A_{A} (Bob does the same with *B* to generate B_{B}). Alice and Bob then exchange their public keys (the secrecy of these keys is not essential). After receiving each other's public keys, both parties are able to arrive at a shared secret value *K* by respectively calculating the public value they were sent raised to the power of their secret value modulo *M.* In Bob's case he would attain the shared key *K* by computing $[K=A_{B} \mid M]$, Alice would arrive at the same value for *K* through $[K=B_{A} \mid M]$. Both parties attain the same value *K* because under the modulus *M*, because:

$A_{B} \mid M = G^{AB} \mid M = B_{A} \mid M.$

After Alice and Bob obtain the secret key, they can use that value as an encryption key for their communications, without having to know each other or meet. This method is especially secure against eavesdropping for prime number modulus *M* larger than 600 digits, as even modern super computers cannot solve such a large discrete logarithm problem quickly. DHKE has a major failing, in that it does not inherently authenticate the communicating parties, making man-in-the-middle attacks possible. The Man-in-the-middle attack involves the attacker positioning themselves between two communicating parties in the hopes of

intercepting their transmissions. This attack is difficult to detect using DHKE because the two parties are most likely strangers and do not possess the ability to authenticate each other. This inability to authenticate leaves an opening for a third party to masquerade as Alice to Bob and inversely, decoding and recoding messages sent through them.

The One Time Pad is the name given to a type of cryptography that is implemented through two parties having identical sequences of unique cipher pages which are each used only once. Party A would communicate a message using page 1 as the key and party B would decrypt the message with the same page; what is most important however, is that each party should destroy used pages, never communicating again using that page as a key. The one-time pad is the crowning achievement of cryptology, when used correctly, it is impossible to decipher their communications with cryptanalysis. This invulnerability was proved by Claude Shannon in his now declassified World War II research where he went on to posit that if any other unbreakable cipher were to exist it must possess the characteristics of the OTP, namely: a truly random key that is at least as long as the text, which is never reused or shared in any way [9]. The OTP is still employed currently by government agencies worldwide due to the infallibility associated with its inherent lack of cryptanalytic patterns, patterns which led to the eventual downfall of both the Caesar and Vigenère ciphers. The one-time pad is however, only theoretically infallible, as the possibility for misuse exists, as does a version of the key exchange problem. The one-time pad system familiarly requires that pads be distributed securely to the communicating parties in advance, this being often impossible. More recently, there has come to exist another issue with transmitting keys as long as the text being encrypted, as text packets are usually very large, this method of encryption can be resource taxing.

Quantum key exchange solves the problems present in traditional key exchange outright, allowing for simple public key encryption to then be employed for all future communications between the active parties. QKD as a key exchange protocol can be combined with any form of cryptography to increase the security through elimination of the key exchange problem. QKD also removes the reliance on possession of comparatively sophisticated means of obfuscating private key data, instead relying on natural laws that cannot be broken by yet to be developed technologies and techniques.

Quantum key exchange

Quantum key distribution's ensured infallibility is a product of several characteristics of quantum mechanics. The first implemented versions of QKD (prepare and measure protocols) rely on the impossibility of simultaneous certainty of any two inverse properties of a quantum system. This quantum indeterminacy is protected by The Heisenberg Uncertainty Principle. The No Cloning Theorem further secures quantum key exchange by

preventing the intuitive circumvention of HUP through the means of copying the quantum state in transit and evaluating the inverse properties of the quantum state separately. The no cloning theorem states that it is impossible to copy unknown quantum information [12]. There exist protocols relying on quantum entanglement which I will not be discussing that allow for similar security benefits.

BB84 is the first quantum key distribution protocol, it was developed in 1984 by Charles Bennett and Gilles Brassard. Using this protocol "Alice" communicates a long stream of photons, the polarization states of each corresponding to a binary encoded bit to be received by Bob. In the BB84 distribution each photon can have one of two unique orientations on one of two unique axes, the direction of the photon's polarization encodes a binary bit. A binary value 0 is traditionally encoded for either a 0° horizontally oriented photon on a rectilinear basis or a 45° orientation on a diagonal basis. while a binary 1 is encoded for either a rectilinear 90° orientation, or a 135° diagonal orientation. Interpreting a photon using the rectilinear basis yields a horizontal or vertical result (0° or 90°). If the photon was encoded with horizontal or vertical orientation (rectilinear) then this measures the correct state, if it was encoded at 45° or 135° (diagonal) then rectilinear interpretation yields a 0° or 90° orientation at random. Upon interpreting the photon in any given orientation (horizontal or vertical), all information about its original polarization orientation is lost forever. When Bob receives these photons, he will not know whether the orientation of each individual photon corresponds to a diagonal or rectilinear basis. Bob will have to use something of a coinflip to decide how to interpret the quantum data of each photon; he will use the rectilinear basis half of the time and the diagonal basis for the other half. Bob will record the output he receives from interpreting each photon, choosing the correct basis about 50% of the time, and thereby obtaining the accurate binary number half of the time. When Bob chooses he incorrect basis half of the time, a resulting random binary number will be output; this random bit is either a 0 or a 1 and therefore is also 50% likely to be correct. This leaves Bob with the correctly interpreted half of his photons producing correct bits and the incorrectly interpreted photons half likely to produce correct bits, for an overall accuracy of around 75%. If an eavesdropper " Eve " is to intercept Alice's communication of photons with the hopes of interpreting them and then relaying them to Bob so as to conceal her presence, a problem arises. After interpreting Alice's photon's, Eve will attain the aforementioned 75% photon interpretation rate, then use the basis she assumed for interpreting each photon to send what she believes are exactly the same order of precisely the same photon orientations to Bob. Unlike Alice's original stream of photon's, Eve's output stream is now only 75% accurate, which means when Bob attempts to decode them, he will have a decreased accuracy. Eves intermediary coin-flip has rendered some of Alice's original quantum data lost forever. Bob is now still required to guess which basis to use for each photon, but now he has fewer chances to

guess correctly. Half of Bob's basis assumptions will no longer yield correct bits, and fewer of his incorrect basis assumptions will result in correct bits.

For example:

Alice sends 100 photons which are intercepted and recorded by Eve and retransmitted, 50 of them should be sent to bob intact and 50 will be randomized totaling 75% correct binary representations. When Bob interprets the half that is intact, he will correctly assume their bases and yield correct bits half of the time. When he incorrectly assumes the bases of the intact photons the other half of the time, he will receive a coin-flipped bit that is half likely to be the correct one. When Bob encounters the 50 photons that were randomly re-encoded by Eve, he has the chance to get 25 of them correct. Bob's coin-flips will only arrive at the correct binary number 75% of that possibility, with him being correct only 18.75% of the time.

Coinflip choose orientation bases of 50 photons transmitted by Eve intact.

0.5 * (50) + 0.5 * (25) = 37.5

+

Coinflip choose orientation bases of 50 photons randomly re-encoded by Eve.

0.5 * (25) + 0.5 * (12.5) = 18.75

= 56.25% overall accuracy

Bob then communicates on an open channel which basis he used for each photon and the binary values he observed from decoding it to Alice. Alice will inform Bob if he chose the correct basis for the photons, which should have yielded an identical polarization orientation. If the photons were tampered with in transit, some number of photons that were encoded and decoded using the same basis will be represented by bits that disagree, alerting Alice and Bob to the presence of Eve. If no tampering occurs. If no tampering takes place, Alice and Bob will disregard the bits which bob measured with the wrong basis and form an identical string of bits that will become their encryption key for their verifiably secure channel. From this point Bob and Alice may use this Key to communicate with any of the previously discussed encryption techniques. Although after solving the key exchange problem, symmetric key encryption is usually secure enough for real-world situations, the one-time pad method is more provably secure. As observed in this example, this protocol relies heavily on the laws of mechanical physics that are represented by Heisenberg's uncertainty principle to ensure that the communicated photons cannot be evaluated in transit and sent to Bob without corrupting their quantum state, thus alerting the authorized parties to the presence of an eavesdropper.

Alice's Bit	**1**	**1**	**0**	**1**	**0**	**1**
Alice's Basis	Rectilinear	Rectilinear	Rectilinear	Diagonal	Diagonal	Rectilinear
Alice's orientation	0°	90°	90°	45°	135°	0°
Bob's Basis	Rectilinear	Diagonal	Rectilinear	Diagonal	Rectilinear	Diagonal
Bob's orientation	0°	135°	90°	45°	0°	135°
Compare Step						

Secret Key	1	disregard	0	1	disregard	disregard

Security Concerns

QKD is provably secure because Bob and Alice do not have to assume they are safe from Eve based on any evaluation of her capabilities because she *cannot* violate the laws of physics. This communication protocol is however still susceptible to the man-in-the-middle where her behavior in the eavesdropping scenario is replaced instead with mere impersonation. Here, Eve will pretend to be Alice to Bob and vice versa, and without some method of authentication, is impossible to insulate against with sophisticated key distribution alone. There is also cause to believe that use of suboptimal equipment could cause QKD to be less effective. When communicating on a noisy channel the potential arises for that noise to alter some photons in transit, falsely alerting the participating parties to the presence of an eavesdropper.

As previously detailed, in the BB84 protocol bob receives quantum states from Alice via single photons; however, in practice a weakened laser pulse is usually employed to transmit a small number of photons. Pulsing photons in this manner usually yields a Poisson distribution of actual photon emission (e.g. at 0.3 photons per pulse will result in some pulses being empty, some having a desired transmission of exactly one photon, while others have two or more). Herein lies the most significant threat to quantum key distribution; if more than one photon is pulsed, it becomes possible for an eavesdropper to 'split' off and store the superfluous photon(s). The eavesdropper then transmits the remaining to Bob as originally intended, where he then begins the communication with Alice, revealing the encoding basis. Once the encoding basis is revealed, the eavesdropper can measure the split-stolen photons, ascertaining information about the key, undetected.

Applications and implementation

In practice Quantum Cryptography faces some difficulties not present in its theoretical climate, among them being noise, delineation of noise and eavesdropping errors, and PNS attacks stemming from the inability to transmit single photons. The implementation of QC technologies must negotiate these obstacles if ever to see wide stream usage and adoption.

Noise is classified in the field of quantum cryptography as the undesired interaction between transmitted photons, measuring equipment, and the environment. Noise is present in every stage of the QKD process, as such it must be dealt with to maintain the stability and feasibility of the system as a whole. As previously detailed, on an especially noisy channel it is particularly difficult to distinguish between classical noise related errors and those introduced by the presence of an active eavesdropper, this is the true threat of noise. While the amount of transmitted data that is disturbed by noise is negligible, concerns arise when a QKD must have no chance of compromise, and therefore there can be no possibility of an eavesdropper using noise to conceal their presence. Privacy amplification strives to

fully reduce a potential eavesdropper's information about a transmitted key attained either from monitoring the public or private channel. The upper limits of possible information an eavesdropper could have acquired (due to errors detected as previously detailed) are used to create a shorter key, to which the eavesdropper's data about will be insignificant. Using a randomly chosen and publicly available universal hash function, a binary input of the original key's length is given, and a smaller key of predesignated size is rendered. This method eliminates the impact of eavesdropping on quantum channels, ensuring the security of QKD.

Solutions to the problem represented by the photon splitting attack include using a true single photon transmission instead of the laser, which is albeit more difficult, has been accomplished (13). There exists a method of laser pulsing that aids in the detection of photon splitting attacks called decoy state protocol. In this protocol Alice would pulse transmit randomly lower averaged number of photons; the eavesdropper on the other hand is incapable of determining which pulses are decoys and which are data. This protocol has been proven to increase secure key rate against all contemporary threats in several experiments including its inaugural attempt at the University of Toronto (14).

With the correct implementation, the uses of QKD are limited only by any given entity or person's desire for security. Establishment of provable secure private channels of communication over very large distances has various commercial, martial, and personal merits. In fields where data is not just data, there is an inherent and violent need for channels of communication to be secured far past what is normally reasonable. One employment of such a manner of secure transmissions is in the field of banking, where it is vital that the information being transmitted is actual money in some cases. Another pertinent application of QC technology is in the theatre of war, where it is absolutely necessary to maintain the security of military intelligence at every step of decision making processes. Here we have possibility of not only fiscal loss but loss of personnel, personnel whom have reasonable expectation that their safety not be jeopardized further than what is necessary. Finally, there is a growing necessity for strong personal encryption; people face greater cyber threats to their privacy every day and must have some reliable means to combat them. Loss of control of confidential data in personal endeavors could allow for among other harms: identity theft, robbery, extortion, leaked medical or other private information. The uses for encryption of this level are definitely present, as are the means for implementing it. What is missing is the drive, governmental support, and infrastructure to accommodate its wide application.

Possible Implications

Among the possible usages of strong encryption, illicit implementations exist for the purposes of crime, terrorism, and or the obstruction of justice. It is necessary for law

enforcement entities to be able to conduct thorough investigations in order to supply courts with evidence to be used in criminal trial; However, it is the belief of many law enforcement agencies that this is becoming increasingly difficult given the speed of advancement in cryptologic technology. At the US Naval Academy in October of 2017, United States Deputy Attorney General Rod Rosenstein stated,

The advent of 'warrant-proof' encryption is a serious problem. The law recognizes that legitimate law enforcement needs can outweigh personal privacy concerns. Warrant-proof encryption defeats the constitutional balance by elevating privacy above public safety. When encryption is designed with no means of lawful access, it allows terrorists, drug dealers, child molesters, fraudsters, and other criminals to hide incriminating evidence. Today, thousands of seized devices sit in storage, impervious to search warrants. Over the past year, the FBI was unable to access about 7,500 mobile devices submitted to its Computer Analysis and Response Team, even though there was legal authority to do so. (12)

Currently, as posited by Rod Rosenstein, Law enforcement and agencies focused on the preservation of national security face significant difficulties with the current strength of encryption. The case that best elaborates this difficulty is when Apple Inc. opposed a federal judge's ruling ordering the company to comply with the FBI's request to have an iPhone unlocked belonging to a shooter in the December 2016 San Bernardino, California attack. Apple CEO Tim Cook stated after the ruling, “The government is asking Apple to hack our own users and undermine decades of security advancements that protect our customers [...]including tens of millions of American citizens from sophisticated hackers and cybercriminals.” Undeterred by Apple's defiance, the FBI hired a third party to break the iphone's encryption in an attempt to retrieve any valuable data from the device before it lost significance. The topic of current encryption as being unnecessarily robust is controversial; on one hand law enforcement agencies must gather evidence needed to enforce laws that protect people from criminal harm, but on the other, it is the responsibility of providers of digital goods and services to safeguard their customers from criminality in the form of information security. This dichotomy of law versus privacy is believed to soon heavily favor privacy with the advent of quantum cryptography. If law enforcement cannot reliably extract or intercept data for their investigations given the current state of cryptography, QC will render future evidence gathering nearly impossible. There is definitely a balance that needs to be struck in regard to these concerns; privacy simply for the sake of privacy is not feasible if it degrades the public good.

Summary

Parties wishing to communicate a secret without fear of having it interpreted and retransmitted have the option of using a quantum channel to secure their transmission. The channel will not only prevent eavesdropping on the private key exchange, but also alert the parties involved

to the presence of any eavesdropping. Access to encryption of this magnitude raises the concern, do the benefits of the general use of strong encryption outweigh the drawbacks associated with anonymizing criminal activity and communication. This paper detailed terminology and useful history of general cryptography as well as elaborated on the classical implementation of cryptography and the major security threat to all forms of coded message transmission, the "key exchange problem". This paper discussed the principles that govern security in cryptography in general as well as those that apply specifically to quantum cryptography. These principles included the no cloning theorem, the Heisenberg's Uncertainty Principle, and the BB84 quantum distribution protocol which relies on them. Contemporary concerns about the implications of personally accessible strong encryption protocols were also evaluated. It is necessary to introduce this technology immediately in fields where security is absolutely cardinal, such as military and financial sectors; however, it is also necessary to gauge how best to pass the benefits of this technology onto the general population without undermining the effectiveness of justice everywhere.

Page Break

Bibliography

1. A. Hodges, “Alan Turing: The Enigma,” (Hutchinson, London, 1983).
2. Abelson, Harold, Ken Ledeen, and Harry R. Lewis. Blown to Bits: Your Life, Liberty, and Happiness After the Digital Explosion. Upper Saddle River, NJ: Addison-Wesley, 2008.
3. Schneier, Bruce. Applied Cryptography: Protocols, Algorithms, and Source Code in C Edition 20th Anniversary Edition. Wiley, 2015.
4. Young, Hugh D, Roger A. Freedman, A L. Ford, and Francis W. Sears. Sears and Zemansky's University Physics: With Modern Physics. San Francisco: Pearson Addison Wesley, 2004.
5. Parakh, A. (2013) 'A probabilistic quantum key transfer protocol', *Security and Communication Networks*, Vol. 6, No. 11, pp. 1389-1395
6. Bennett, C. and Brassard, G. (1984) 'Quantum cryptography: public key distribution and coin tossing', *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India, pp. 175-179.
7. Schenker, Jennifer L. "A quantum leap in codes for secure transmissions." The IHT Online. 28 January 2004.
8. Poppe, A., et al. "Practical quantum key distribution with polarization entangled photons." Optics Express 12.16 (2004): 3865-3871.Barnum, Howard, et al. "Authentication of quantum messages." Foundations of

Computer Science, 2002. Proceedings. The 43rd Annual IEEE Symposium on. IEEE, 2002.

9. CE Shannon, ‘‘Communication theory of secrecy systems’’, in *Bell Systems Technical Journal* v 28 (1949) pp 656–715

10. Bennett, C. H. and Brassard, G., "Quantum Cryptography: Public key distribution and coin tossing.", International Conference on Computers, Systems & Signal Processing, Bangalore, India, 10-12 December 1984, pp. 175-179. http://www.research.ibm.com/people/b/bennetc/bennettc198469790513.pdf

11. Bennett, C., "Quantum cryptography using any two non-orthogonal states.", Phys. Rev. Lett. 68, 1992, pp. 3121-3124. http://prola.aps.org/pdf/PRL/v68/i21/p3121_1[Wooters82] Wooters, W., Zurek, W., "A single quantum cannot be cloned." Nature 299, 1982, pp. 802-803. http://www.nature.com/nature/journal/v299/n5886/abs/299802a0.html

12. Kim, Matthew. “Deputy Attorney General Rod Rosenstein Remarks on Encryption.” Internet:https://www.lawfareblog.com/deputy-attorney-general-rod-rosenstein-remarks-encryption, [Oct. 10, 2017].

13. P. M. Intallura, M. B. Ward, O. Z. Karimov, Z. L. Yuan, P. See, A. J. Shields, P. Atkinson, and D. A. Ritchie, Appl. Phys. Lett. 91, 161103 (2007)

14. X.-B. Wang, "Beating the photon-number-splitting-attack in practical quantum cryptography", Physical Review Letters, 94, 230503 (2005)

15. Bennett, C. H., Bessette, F., Brassard, G., Salvail, L., and Smolin, J., "Experimental Quantum Cryptography", Journal of Cryptology, vol. 5, no.1, 1992, pp. 3-28.