International Journal of Research in Engineering and Applied Sciences(IJREAS)
Available online at: http://euroasiapub.org
Vol. 6 Issue 9 September- 2016,
ISSN (o): 2249-3905 ISSN (P): 2349-6525 | Impact Factor: 6.573 | Thomson Reuters ID: L-5236-2015

QUANTUM CRYPTOGRAPHY: ASTEP TOWARDS CHANGE IN COMMUNICATION

Ritika, Assistant Professor,
Department of Physics,
SSM College, Dinanagar.

ABSTRACT

Quantum Cryptography is a way to deal with making sure about correspondences by applying the wonders of quantum material science. Not at all like conventional old style cryptography, which employments numerical procedures to limit spies, is quantum cryptography engaged on the material science of data. Quantum cryptography gives secure correspondence, whose security relies just upon the legitimacy of quantum hypothesis, i.e., it is guaranteed legitimately by the laws of material science. This is a considerable contrast from any old style cryptographic procedures. This article abridges the current condition of quantum cryptography and gives potential augmentations of its practicality as an instrument for making sure about existing correspondence frameworks. The internet has become the most well-known transporter of data trade in each side of our life, which is beneficial for our life in practically all perspectives. With the ceaseless improvement of science and innovation, particularly the quantum PC, the internet security has become the most basic issue for the Internet in not so distant future. Right now, center around dissecting qualities of the quantum cryptography and investigating of the benefits of it later on Internet. It is important that we dissect the quantum key appropriation (QKD) convention in the commotion free channel. In addition, so as to mimic genuine circumstances later on Internet, we additionally search the QKD convention in the loud channel. The results reflect the genuine security of quantum cryptography hypothetically, which is appropriate for the Internet as ever-expanding difficulties are unavoidable later on.

INTRODUCTION

The material science of quantum cryptography makes a way for colossally charming opportunities for cryptography, the craftsmanship and science of conveying within the sight of foes. Intriguing attributes of quantum mechanics incorporate the presence of resolute quanta and of caught frameworks, the two of which lie at the foundation of quantum cryptography (QC). QC

is one of only a handful scarcely any business uses of quantum material science at the single quantum level. With the advancement and fast improvement of the Web, human culture has entered the data age. These days, all strolls of individuals and all parts of life cannot be isolated from the system. In 1990s, the expression "the internet" was utilized to speak to numerous new thoughts and marvels in the Internet, organizing, and computerized correspondence. Cryptography is the training and investigation of encoding and translating mystery messages to guarantee secure correspondences.

There are two principle parts of cryptography: mystery (symmetric-) key cryptography and open (hilter kilter) key cryptography. A key is a bit of data (a parameter) that controls the activity of a cryptographic calculation. In encryption, a key determines the specific change of plaintext into figure content, or bad habit versa during decoding. Keys are additionally utilized in other cryptographic calculations, for example, advanced mark plans also, message validation codes. Practically speaking, due to noteworthy troubles of appropriating keys covertly key cryptography, open key cryptographic calculations are broadly utilized in ordinary cryptosystems.

A cryptographer put forth attempts to manufacture to an ever increasing extent advanced intends to cloud the delicate data which is to be transmitted. Be that as it may, the programmers, code breakers, spies work angrily to split the frameworks. Assuming either cryptographers accomplish security or the code breakers interpret the security the achievement will be transitory. This procedure of making sure about the message utilizing figuring and breaking the framework utilizing interpreting is an interminable procedure. Once, this situation is a pursuit in the race. These days, this term is utilized to portray the area of the worldwide innovation condition by specialists and scientists of specialized procedure, security, government, military, and industry and undertakings. Likewise, this term is utilized to allude to anything related with the Internet. Utilizing this worldwide organize, individuals can take part in a wide range of exercises, for example, conveying thoughts, sharing data, giving social support, leading business, coordinating activities, making creative media, messing around, and taking part in political conversation. Run

of the mill applications dependent on the internet incorporate distributed computing and customized recommender frameworks.

In spite of all benefits and preferences of the internet, it is viewed as the biggest unregulated and uncontrolled feldin mankind's history. Therefore, the issue of data security is the essential issue of the internet. On the one hand, data innovation and industry have entered an extraordinary phase of flourishing. Then again, the methods for a wide range of attack rise in a perpetual stream. Attack, similar to programmer attack, malevolent software attack, and PC infections, represent an incredible danger to the internet data security. Additionally, the advancement of science and innovation additionally presents new difficulties to the internet security. Because of the qualities of the quantum PC, many existing open key cryptography (RSA, ELGamal, elliptic bend cryptography (ECC), etc.) will be never again safe in the quantum PC. In particular, the notable discrete logarithm issue (DLP) or the number factorization issue will never again be difficult under quantum PC. Tis proposes that so as to oppose quantum PCs, new cryptosystems that are most certainly not in view of discrete logarithms issue or the enormous factor decay issue ought to be investigated. Just right now can the data security of the internet be guaranteed in the future Internet?

Quantum cryptography is still in its outset. Be that as it may, we cannot disregard the difficulties it brings to the security of existing the internet. In 1994, mathematician Shor has proposed the quantum calculation by which the whole number factorization issue and the discrete logarithm issue can be efficiently explained in polynomial time. Note that so far analysts have not found the traditional calculation to fathom the huge whole number decay and the discrete logarithm issue efficiently under the Turing machine model. Therefore, the test of the rise of quantum PCs to the conventional cryptosystems cannot be disregarded regardless of whether it is still in its outset. Cryptography and system security are the key innovations to guarantee the security of the data framework.

Quantum cryptography is a significant part of cryptography, which is the mix of quantum mechanics and traditional cryptographist security of correspondence can be ensured by

Heisenberg's vulnerability standard and quantum no-cloning hypothesis. The fundamental objective of the investigation of quantum cryptography is to plan cryptographic calculations also, conventions, which is against quantum figuring attack. As expressed already, investigating quantum cryptographic conventions will be a fundamental piece of the internet security issues for future Internet. Right now, concentrate on investigating and investigating the quantum key dispersion convention focus for the internet security for the future Internet.

QUANTUM CRYPTOGRAPHY FUNDAMENTALS

On a more extensive setting, quantum cryptography is a part of quantum data handling, which incorporates quantum processing, quantum estimations, and quantum teleportation. Quantum calculation and quantum data is the investigation of the data preparing assignments that can be cultivated utilizing quantum mechanical frameworks.

Quantum mechanics is a scientific system or set of rules for the development of physical speculations. The guidelines of quantum mechanics are basic yet even specialists discover them strange, and the most punctual forerunners of quantum calculation and quantum data might be found in the long-standing want of physicists to more readily comprehend quantum mechanics. Maybe the most striking of these is the investigation of quantum Entanglement. Trap is an extraordinarily quantum mechanical asset that assumes a key job in a considerable lot of the most fascinating utilizations of quantum calculation and quantum data; Entanglement is iron to the old style world's Bronze Age. As of late there has been an enormous exertion attempting to more readily comprehend the properties of Entanglement considered as a crucial asset of Nature, of equivalent significance to vitality, data, entropy, or some other principal asset. Despite the fact that there is up 'til now no total hypothesis of Entanglement, some advancement has been made in understanding this abnormal property of quantum mechanics. It is trusted by numerous scientists that further investigation of the properties of Entanglement will yield experiences that encourage the advancement of new applications in quantum calculation and quantum data.

As we known, it is fascinating to discover that multi decade before individuals understood that a quantum PC could be utilized to break open key cryptography, they had just discovered an

answer against this quantum assault – quantum key circulation (QKD). In light of the key standards in quantum material science, QKD gives a genuinely secure approach to convey irregular keys through uncertain stations. The safe key created by QKD could be additionally applied in the OTP conspire or other encryption calculations to upgrade data security. Right now, will present the basic standards behind different QKD or QSS and present the cutting edge quantum cryptography advancements.

Entanglement State

The nonsensical expectations of quantum mechanics about connected frameworks were first talked about by Albert Einstein in 1935, in a joint paper with Boris Podolsky and Nathan Rosen. They exhibited a psychological study that endeavored to show that quantum mechanical hypothesis was inconceivable.

In any case, streaming the EPR paper, Erwin Schrodinger composed letter (in German) to Einstein in which he utilized the word Verschrankung (interpreted without anyone else as Entanglement) "to depict the connections between two particles that collaborate and afterward independent, as in the EPR try". He presently distributed an original paper characterizing and talking about the thought, and naming it "entrapment".

Entanglement is generally made by direct cooperation's between subatomic particles. These communications can take various structures. One of the most generally utilized strategies is unconstrained parametric down-change to create a couple of photons Entanglement in polarization. Different strategies incorporate the utilization of a fiber coupler to limit and blend photons, the utilization of quantum specks to trap electrons until rot happens, the utilization of the Hong-Ou-Mandel impact, and so forth. In the soonest trial of Bell's hypothesis, the trapped particles were created utilizing nuclear falls. It is additionally conceivable to make trap between quantum frameworks that never legitimately associated, using Entanglement swapping.

One-time –pad and Key Distribution Problem

In traditional cryptography, an unbreakable code exists. It is known as the one-time-cushion and was created by Gilbert Vernam in 1918. In the one-time-cushion technique, a message (customarily called the plain content) is first changed over by Alice into a twofold structure (a string comprising of "0"s and "1"s) by a freely known strategy.

The one-time-cushion strategy is unbreakable, yet it has a genuine disadvantage: it guesses that Alice and Bob at first offer an irregular string of mystery that is the length of the message. In this way, the one-time-cushion just moves the issue of secure correspondence to the issue of key dissemination. This is the key dispersion issue. The one of conceivable answer for the key conveyance issue is open key cryptography.

Quantum mechanics can give an answer for the key dispersion issue. In quantum key conveyance, an encryption key is produced arbitrarily among Alice and Bob by utilizing non symmetrical quantum states. In quantum mechanics there is a quantum no-cloning hypothesis, which expresses that it is generally outlandish for anybody including a busybody to make an extra duplicate of an obscure quantum state. In this manner, any endeavor by a busybody to learn data about a key in a QKD procedure will prompt unsettling influence, which can be identified by Alice and Bob who can, for instance, check the bit blunder pace of an arbitrary example of the crude transmission information.

Quantum No-cloning Theorem

The quantum no-cloning theorem was stated by Wootters, Zurek and Dieks in 1982 and has profound implications in quantum computing and related fields.

Theorem (Quantum no-cloning theorem) an arbitrary quantum state cannot be duplicated.

Quantum no-cloning hypothesis is an immediate consequence of the linearity of quantum material science. It is firmly identified with another significant hypothesis in quantum mechanics, which states: if an estimation permits one to pick up data about the condition of a

quantum framework, at that point when all is said in done the condition of this quantum framework will be upset, except if we know ahead of time that the potential conditions of the first quantum framework are symmetrical to one another.

From the start sight, the inconceivability of making ideal duplicates of obscure quantum states is by all accounts a weakness. Shockingly, it can likewise be a bit of leeway. It worked out that by utilizing this inconceivability sagaciously, genuinely secure key dissemination could be accomplished: any endeavors by the meddler to get familiar with the data encoded quantum precisely will upset the quantum state and uncover her reality. Extraordinarily, we can get the accompanying attributes about quantum no-cloning hypothesis:

The no-cloning hypothesis keeps us from utilizing traditional mistake revision procedures on quantum states. For instance, we can't make reinforcement duplicates of a state in a quantum calculation, and use them to address consequent blunders. Mistake rectification is indispensable for handy quantum processing, and for quite a while this was believed to be a deadly impediment. In 1995, Shor and Steane restored the possibilities of quantum processing by freely concocting the primary quantum mistake amending codes, which dodge the no-cloning hypothesis.

Correspondingly, cloning would damage the no teleportation hypothesis, which says old style teleportation (not to be mistaken for snare helped teleportation) is outlandish. At the end of the day, quantum states can't be estimated dependably.

The no-cloning hypothesis keeps us from survey the holographic rule for dark gaps as significance we have two duplicates of data lying at the occasion skyline and the dark gap inside at the same time. This leads us to increasingly extreme understandings like dark opening complementarity.

Heisenberg's Uncertainty Principle

Heisenberg's Uncertainty Principle (condensed HUP) is one of the crucial ideas of quantum material science, and is the reason for the underlying acknowledgment of essential vulnerabilities

in the capacity of an experimenter to gauge more than each quantum variable in turn. Endeavoring to quantify a basic molecule's situation to the most noteworthy level of exactness, for instance, prompts an expanding vulnerability in having the option to gauge the molecule's force to a similarly high level of precision.

RELATE WORKS

Quantum cryptography originates from the idea of quantum cash, which was proposed by Wiesner in 1969. Restricted by the degree of innovation ever, this novel and imaginative thought can't be acknowledged, which causes it to stay unpublished until 1983. Thefirst useful QKD convention was proposed by Bennett and Brassard, in 2011. By utilizing single photon polarization, they spearheaded the execution of the quantum key conveyance convention.After that, a ton of effort was put into QKD so as to improve security and efficiency.

In 1991, Ekert proposed the convention that depends on Chimes hypothesis. Note that utilizes a couple of quantum bits (i.e., an EPR pair), which is basically equivalent to. Thusly, in 1992, the improvement of the conspire was advanced by Bennett. Utilizing any two nonorthogonal states, the improvement is more efficient and basic. Afterthat, numerous QKD conventions utilizingthe basic standards of quantum mechanics have been proposed progressively.

As a significant cryptographic fundamental convention, the neglectful exchange convention is one of the key advancements for security assurance in cryptography. The neglectful exchange convention is, where the sender sends numerous potential data to the beneficiary, yet the sender itself is not mindful of the specific substance of the transmission. The idea of quantum careless exchange (QOT) was first set forward by Crepeau in 1994. After that, numerous works have ' been dedicated to the QOT convention. In 1994, the "unmindful move" security of against any individual estimation permitted by quantum mechanics was demonstrated by Mayers and Salvail in. In 1998, the convention was proposed, which demonstrates the security of the QOT convention under an spy. Different conventions were proposed to improve QOT convention to differing degrees.

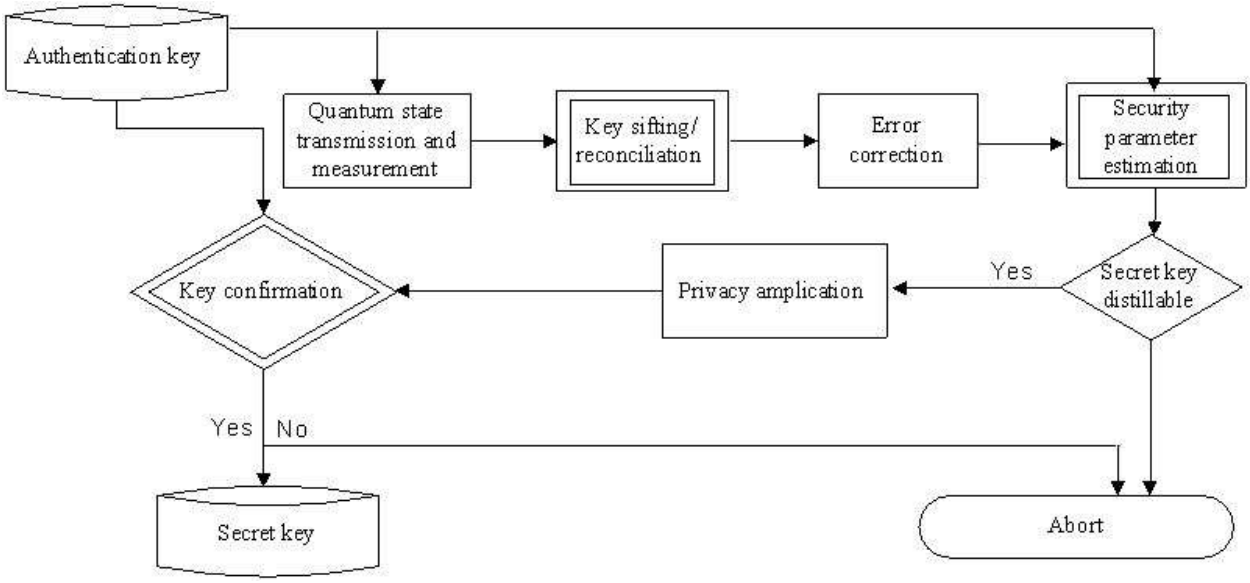
Quantum verification (QA) convention is additionally one of the quantum cryptographic conventions. It was proposed in in 2001. After that, numerous QA conventions have been proposed one after another. The quantum cryptography convention has created numerous branches now. Notwithstanding the conventions (i.e., QKD convention, QOT convention, and QA convention) we talked about above, quantum cryptography conventions likewise incorporate quantum bit responsibility (QBC) conventions and quantum signature (QS) conventions.

QUANTUM KEY DISTRIBUTION

The primary endeavor of utilizing quantum mechanics to accomplish missions unthinkable in traditional data began in the mid 70's. Stephen Wiesner proposed two correspondence modalities not permitted by old style material science: "quantum multiplexing" station and fake free certified receipt. Tragically, his paper was dismissed and couldn't be distributed until 10 years after the fact. In 1980's, Charles H.Bennett and Gilles Brassard expanded Wiesner's thought and applied it to take care of the key circulation issue in traditional cryptography. In 1984, the notable BB84 QKD convention was distributed. QKD is another instrument in the cryptographer's tool stash: it takes into account secure key understanding over an untrusted channel where the yield key is altogether free from any info esteem, an undertaking that is outlandish utilizing old style cryptography. QKD doesn't wipe out the requirement for other cryptographic natives, for example, verification, however it very well may be utilized to fabricate frameworks with new security properties.

To vanquish the mistakes made by commotion and wiretapping in the quantum channel, unequivocally secure mystery key understanding over an open channel was planned, data compromise and protection intensification can be utilized to quantum key dissemination, or something else, quantum snare sanitization ought to be utilized. The primary general albeit rather complex verification of unqualified security was given by Mayers, which was trailed by various different evidences. In Mayers' evidence, the BB84 plot proposed by Bennett and Brassard was end up being unequivocally secure. Expanding on the quantum protection enhancement thought, Lo and Chau, proposed an adroitly easier confirmation of security.

In QKD, two gatherings, Alice and Bob, get some quantum states and measure them. They convey (all correspondence structure this point onwards is traditional) to figure out which of their estimation results could prompt mystery key bits; some are disposed of in a procedure called filtering in light of the fact that the estimation settings were inconsistent. They perform mistake adjustment and afterward gauge a security parameter which portrays how much data a busybody may have about their key information. On the off chance that this sum is over a specific edge, at that point they prematurely end as they can't ensure any mystery at all. On the off chance that it is underneath the limit, at that point they can apply security enhancement to press out any residual data the meddler may have, and show up at a mutual mystery key. A portion of this traditional correspondence must be confirmed to keep away from man-in-the-center attack. A few bits of the convention can fall flat with irrelevant likelihood.



A flow chart describing the stages of quantum key distribution is given in Figure

THE SECURITY OF QKD

Security proofs are significant in light of the fact that a) they give the establishment of security to a QKD convention, b) they give an equation to the key age pace of a QKD convention and c) they may even give a development to the old style post-preparing convention (for blunder

rectification and protection intensification) that is vital for the age of the last key. Without security proofs, a genuine QKD framework is inadequate on the grounds that we can never make certain about how to create a safe key and how secure the last key truly is.

After the qubit trade and premise compromise, Alice and Bob each have a filtered key. In a perfect world, these keys are indistinguishable. In any case, all things considered, there are in every case a few blunders, and Alice and Bob must apply some traditional data handling conventions, similar to mistake adjustment and security intensification to their information. The main convention is important to get indistinguishable keys and the second to get a mystery key. Basically, the issue of listening in is to discover conventions which, given that Alice and Bob can just quantify the QBER, either furnish Alice and Bob with an evidently secure key or stop the convention and advise the clients that the key dissemination has fizzled. This is a sensitive issue at the crossing point of quantum material science and data hypothesis. As a matter of fact, it involves a few spying issues, contingent upon the exact convention, the level of admiration one concedes, the innovative force one expect Eve has, and the accepted loyalty of Alice and Bob's gear.

Eavesdropping Attack

So as to disentangle the issue, a few listening stealthily systems of constrained sweeping statement have been characterized and broke down. Specifically noteworthy is the presumption that Eve appends autonomous tests to each qubit and measures her tests in a steady progression. They can be delegated follows:

Singular attack: In an individual assault, Eve plays out an assault on each sign autonomously. The capture resend assault is a case of an individual assault. Let us consider the basic case of a catch resend assault by a spy Eve, who gauges every photon in an arbitrarily picked premise and afterward resends the subsequent state to Bob. For example, if Eve plays out a rectilinear estimation, photons arranged by Alice in the corner to corner bases will be upset by Eve's estimation and offer irregular responses. At the point when Eve resends rectilinear photons to Bob, in the event that Bob plays out a corner to corner estimation, at that point he will find

irregular solutions. Since the two bases are picked arbitrarily by each gathering, such a capture resend assault will give a piece blunder pace of 0.5×0.5+0.5×0 = 25%, which is promptly distinguishable by Alice and Bob. Modern attack against QKD does exist. Luckily, the security of QKD has now been demonstrated.

Aggregate attack: An increasingly broad class of attack is aggregate assault where for each sign; Eve autonomously couples it with an auxiliary quantum framework, regularly called an ancilla, and advances the consolidated sign/ancilla unitarily. She can impart the subsequent signs to Bob, yet keep all ancillas herself. In contrast to the instance of individual attack, Eve defers her decision of estimation. Simply in the wake of hearing the open conversation among Alice and Bob, does Eve settle on what estimation to perform on her ancilla to remove data about the last key.

Joint attack: The most broad class of attack is joint assault. In a joint assault, rather than cooperating with each sign autonomously, Eve regards all the signs as a solitary quantum framework. She at that point couples the sign framework with her ancilla and advances the joined sign and ancilla framework unitarily. She hears the open conversation among Alice and Bob before settling on which estimation to perform on her ancilla.

For joint and aggregate attack, the standard supposition that will be that Eve quantifies her test simply after Alice and Bob have finished all open conversation about premise compromise, blunder adjustment, and security intensification. For the more sensible individual attack, one accepts that Eve stands by just until the premise compromise period of the open conversation. With the present innovation, it may even be reasonable for accept that in singular attack Eve must gauge her test before the premise compromise. The inspiration for this supposition that will be that one barely observes what Eve could pick up by holding up until after the open conversation on mistake revision and security intensification before estimating her tests, since she is going to gauge them autonomously in any case.

International Journal of Research in Engineering and Applied Sciences(IJREAS)
Available online at: http://euroasiapub.org
Vol. 6 Issue 9 September- 2016,
ISSN (o): 2249-3905 ISSN (P): 2349-6525 | Impact Factor: 6.573 | Thomson Reuters ID: L-5236-2015

QUANTUM CRYPTO NETWORK DEBUTS

Quantum cryptography can possibly ensure impeccably secure correspondences, however as of recently the whole model frameworks have been pointcryptography arrange that pera y. An act use y end e sepulcher p o (IPsec) and makes a kind of virtual e quantum encryption hypothetically difficult to split - more d inside Magiq's servers and systems administration sheets - to-point interfaces instead of systems that share associations. BBN Technologies, Harvard University and Boston University scientists have fabricated a sixnode quantum crypto consistently to give an approach to trade secure keys among BBN and Harvard, which is around 10 kilometers away The scientists will before long move one of the organize hubs across town to interface Boston College into the system. The system is flexible on the grounds that any hub in the system canas a hand-off to associate two different hubs. Becathere are numerous associations with and from an given hub, "disappointment of a connection or hub doesn't imply that we have lost quantum cryptography. The quantum organize utilizes secure highlight point associations between hubs a permits an offered hub to transfer secure organic keys between two different hubs. Since the quantum properties of photons are lost on the off chance that they are watched, they can't be duplicated, be that as it may, making duplicates of light signals is the way signals are helped along conventional media communications lines.

Quantum repeaters, which are under advancement at a few research labs around the world, would rather move the quantum state of new photon to another through cooperation with molecules or through the bizarre quantum wonder of ensnarement, which permits characteristics of at least two particles to be connected despite the separation between them. The system's photon sources are as of now intensely sifted lasers, which are amazingly diminish furthermore, once in a while produce more than one photon at a time. The quantum cryptography arrange works with Web conventions including the safe Internet Convention private system, which gives secure interchanges over unbound systems like the Internet on the loose. The thought is that regardless of whether an meddler can tune in on a line, he would be not able to find out much about the interchanges crossing it. The system is prepared for handy applications today.

CONCLUSION

As this quantum cryptography is another science in a cryptosystem innovation and numerous analysts from around the globe are finding a method for fusing a few gadgets and have just made a leap forward looks quantum cryptography will be a progressed code-production innovation which is hypothetically uncrackable. This is a result of the laws of quantum material science that direct an eavesdroppedcouldn't gauge the properties of a solitary photon without the danger of changing those properties. At the end of the day, regardless of whether an spy can tune in on could be not able to find out much about the interchanges navigating it.

REFERENCES

1. Wiesner, Stephen., 1983. "Conjugate coding." ACM Sigact News 15.1: 78-88.
2. Henle, F., 2002. BB84 Demo. http://www.cs.dartmouth.edu/~henle/Quantum/cgi-bin/Q2.cgi
3. Ford, James., 1996. "Quantum cryptography tutorial." http://www.cs.dartmouth.edu/~jford/crypto.html
4. Harrison, David M., 2001. "Quantum Teleportation, Information and Cryptography." http://www.upscale.utoronto.ca/GeneralInterest/Harrison/QuantTelep ort/ QuantTeleport.html.
5. Knight, Will., 2004. "Entangled photons secure money transfer." Newscientist.com. http://www.newscientist.com/news/news.jsp?id=ns99994914.
6. "Quantum cryptography." Wikipedia, the free encyclopedia. http://en.wikipedia.org/wiki/Quantum_cryptography. Modified 17 September 2004.
7. "The BB84 Quantum Coding Scheme", June 2001. http://www.cki.au.dk/experiment/qrypto/doc/QuCrypt/bb84coding.ht ml [8]. Gisin, N., Ribordy, G., Tittel, W., Zbinden, H., "Quantum Cryptography", Reviews of Modern Physics, vol. 74, January 2002, pp. 146 - 195. http://www.gap-optique.unige.ch/Publications/Pdf/QC.pdf

8. T. Zhou, L. Chen, and J. Shen, "Movie Recommendation System Employing the User-Based CF in Cloud Computing," in Proceedings of the 2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC), pp. 46–50, Guangzhou, China, July 2017.
9. R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, vol. 21, no. 2, pp. 120–126, 1978.
10. J. Shen, T. Zhou, X. Chen, J. Li, and W. Susilo, "Anonymous and Traceable Group Data Sharing in Cloud Computing," IEEE Transactions on Information Forensics and Security, vol. 13, no. 4, pp. 912–925, 2018.
11. T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," IEEE Transactions on Information Teory, vol. 31, no. 4, pp. 469–472, 1985.
12. Y.-M. Tseng, "An efficient two-party identity-based key exchange protocol," Informatica, vol. 18, no. 1, pp. 125–136, 2007.
13. J. Shen, T. Miao, Q. Liu, S. Ji, C. Wang, and D. Liu, "S-SurF: An Enhanced Secure Bulk Data Dissemination in Wireless Sensor Networks," in Security, Privacy, and Anonymity in Computation, Communication, and Storage, vol. 10656 of Lecture Notes in Computer Science, pp. 395–408, Springer International Publishing, Cham, 2017.
14. P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in Proceedings of the 35th Annual Symposium on Foundations of Computer Science (SFCS '94), pp. 124–134, IEEE, 1994.
15. J. Shen, T. Zhou, F. Wei, X. Sun, and Y. Xiang, "PrivacyPreserving and Lightweight Key Agreement Protocol for V2G in the Social Internet ofTings," IEEE Internet of Tings Journal, pp. 1-1.
16. D. Bruß, "Optimal eavesdropping in quantum cryptography with six states," Physical Review Letters, vol. 81, no. 14, pp. 3018– 3021, 1998.
17. P. Li, J. Li, Z. Huang, C.-Z. Gao, W.-B. Chen, and K. Chen, "Privacy-preserving outsourced classifcation in cloud computing," Cluster Computing, pp. 1–10, 2017.

18. C. Crep´ eau, "Quantum oblivious transfer," Journal of Modern Optics, vol. 41, no. 12, pp. 2445–2454, 1994
19. C. H. Bennett, G. Brassard, C. Crepeau, and M.-H. Sku- ´ biszewska, "Practical quantum oblivious transfer," in Annual International Cryptology Conference, pp. 351–366, Springer.
20. D. Mayers and L. Salvail, "Quantum oblivious transfer is secure against all individual measurements," in Proceedings of the Workshop on Physics and Computation. PhysComp '94, pp. 69– 77, Dallas, TX, USA.
21. D. Mayers, "On the security of the quantum oblivious transfer and key distribution protocols," Lecture Notes in Computer Science (including subseries Lecture Notes in Artifcial Intelligence and Lecture Notes in Bioinformatics): Preface, vol. 963, pp. 124–135, 1995.
22. S. Winkler and J. Wullschleger, "On the efciency of classical and quantum oblivious transfer reductions," Lecture Notes in Computer Science (including subseries Lecture Notes in Artifcial Intelligence and Lecture Notes in Bioinformatics): Preface, vol. 6223, pp. 707–723, 2010.
23. Chailloux, I. Kerenidis, and J. Sikora, "Lower bounds for quantum oblivious transfer," Quantum Information & Computation, vol. 13, no. 1-2, pp. 0158–0177, 2013.
24. M. Curty and D. J. Santos, "Quantum authentication of classical messages," Physical Review A: Atomic, Molecular and Optical Physics, vol. 64, no. 6, 2001.
25. B.-S. Shi, J. Li, J.-M. Liu, X.-F. Fan, and G.-C. Guo, "Quantum key distribution and quantum authentication based on entangled state," Physics Letters A, vol. 281, no. 2-3, pp. 83–87, 2001.
26. D. Zhang and X. Li, "Quantum authentication using orthogonal product states," in Proceedings of the 3rd International Conference on Natural Computation, ICNC 2007, pp. 608–612, China, August 2007.
27. G. Brassard and C. Crepeau, "Quantum bit commitment and ´ coin tossing protocols in," in Proceedings of the Conference on the Teory and Application of Cryptography, pp. 49–61, Springer.

28. N. K. Langford, R. B. Dalton, M. D. Harvey et al., "Measuring entangled qutrits and their use for quantum bit commitment," Physical Review L

29. J. Shen, T. Zhou, X. Chen, J. Li, and W. Susilo, "Anonymous and Traceable Group Data Sharing in Cloud Computing," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 4, pp. 912–925, 2018.View at: Publisher Site | Google Scholar

30. T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 469–472, 1985.View at: Publisher Site | Google Scholar | MathSciNet

31. Y.-M. Tseng, "An efficient two-party identity-based key exchange protocol," *Informatica*, vol. 18, no. 1, pp. 125–136, 2007.View at: Google Scholar

32. J. Shen, T. Miao, Q. Liu, S. Ji, C. Wang, and D. Liu, "S-SurF: An Enhanced Secure Bulk Data Dissemination in Wireless Sensor Networks," in *Security, Privacy, and Anonymity in Computation, Communication, and Storage*, vol. 10656 of *Lecture Notes in Computer Science*, pp. 395–408, Springer International Publishing, Cham, 2017.

33. C. Bennett and G. Brassard, "Quantum Cryptography:Public Key Distribution and Coin Tossing," International Conference on Computers, Systems, and Signal Processing, Bangalore, India, 1984.

34. Ekert, "Quantum Cryptography Based on Bell's Theorem," Phys. Rev. Lett. 67, 661 (5 August 1991).

35. Ekert, Artur. "What is Quantum Cryptography?" Centre for Quantum Computation – Oxford University.Conger., S., and Loch, K.D. (eds.). Ethics and computer use. Commun. ACM 38, 12 (entire issue).

36. Johnson, R. Colin. "MagiQ employs quantum technology for secure encryption." EE Times. 6 Nov. 2002..

37. Mullins, Justin. "Quantum Cryptography's Reach Extended." IEEE Spectrum Online. 1 Aug. 2003.

38. Bienfang, J., et al. "Quantum key distribution with 1.25 Gbps clock synchronization." Optics Express 12.9 (2004): 2011-2016.
39. Inoue, Kyo, Edo Waks, and Yoshihisa Yamamoto. "Differential phase-shift quantum key distribution." Photonics Asia 2002. International Society for Optics and Photonics, 2002.
40. Barnum, Howard, et al. "Authentication of quantum messages." Foundations of Computer Science, 2002. Proceedings. The 43rd Annual IEEE Symposium on. IEEE, 2002.
41. Elliott, Chip, David Pearson, and Gregory Troxel. "Quantum cryptography in practice." Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications. ACM, 2003.
42. Buttler, W. T., et al. "Fast, efficient error reconciliation for quantum cryptography." Physical Review A 67.5 (2003): 052303.
43. Poppe, A., et al. "Practical quantum key distribution with polarization entangled photons." Optics Express 12.16 (2004): 3865-3871.
44. Lütkenhaus, Norbert. "Estimates for practical quantum cryptography." Physical Review A 59.5 (1999): 3301.