

Quantum cryptography - A modern approach

Salabh Rai [‡]

Ayush Kumar Upadhyay [†]

Divyank Sharma [§]

Dharm Raj ^{*}

Department of Computer Science & Engineering

Sharda School of Engineering & Technology

Sharda University

Greater Noida

Uttar Pradesh

India

Ajay Kumar Gupta [@]

Department of Computer Science & Engineering

IIMT College of Engineering

Greater Noida

Uttar Pradesh

India

Danish Ather [#]

Amity University

Tashkent

Uzbekistan

Abstract

In Our daily life we are getting very much dependent on Internet or Virtual Reality. They are nothing but an illusion of a Cyberspace. It has effect on our every aspect of life, like Education, Sports, and Health etc. We are using the term Cryptography which is the science of using mathematics to encrypt and decrypt data. We had used various Encryption

[‡] E-mail: salabh.raai@gmail.com

[†] E-mail: ayush30.up@gmail.com

[§] E-mail: dave06j@gmail.com

^{*} E-mail: dharmraj4u@gmail.com (Corresponding Author)

[@] E-mail: ajayguptagorakhpur@gmail.com

[#] E-mail: danishather@gmail.com

standards in back days namely, DES, AES, RSA, Elliptical AES etc. But nowadays we are using Quantum Cryptography for this. It is nothing but use of Physics (mainly Quantum Physics) for Encrypting the data. In this Research paper we will mainly focus on the new approaches that come in the path of Quantum Cryptography. We will also view some interaction of Quantum Cryptography in future Internet services. Quantum computing is yet to be explored but still the explored part has the capabilities to counter the “alien” hacking protocols if tested over any System. Older System were using protocols like RSA, AES, DES even some of them are more capable than our need, but the use of QC will not only secure the systems but there are major chances that eavesdropper got caught while eavesdropping. Also QC is a pathway to secure communication. This paper includes the review of older state of Quantum Cryptography which will give us information about QKD algorithms and its protocol and we will also overview on its risk and security features. We will also provide a glimpse of current various works going in various Educational Institutions.

Subject Classification: 68M25.

Keywords: Quantum, Cryptography, Encryption, Technology, Internet, Protocols, Standard.

1. Introduction

Cryptography is a Mathematics or Science which make our private information or data safer from the access of unauthorized person, which ensure data integrity and authentication [1]. For this purpose, one uses Encryption: in this a data is mixed according to certain algorithm with some of secret information which will certainly produce Cryptogram. For this purpose, we have used various algorithms over a period of time. Now a day we are using Quantum Cryptography for achieving this goal. Quantum Cryptography's idea comprises of the ideology of Quantum Mechanics to implement a cryptographic system [2][35]. The key problem which was solved by Quantum Cryptography is eavesdropping detection and this is done probabilistically when it occurs. In Quantum Cryptography the bits of data are represented as Qubits, which have been physically modeled by photons, and communicated over a quantum channel. Generally, the state of polarization is same as binary i.e. 0's and 1's [4].

The ideas of QP & QI when applied to data communication which is of long range may be used for attacking the problems of transfer of an absolutely Randomly Generated Key through the help of accessible data channels with more assurance of security. There are two properties of Quantum which is used here [5]

- (1) “To extract info about nonorthogonal states without any disturbance is impossible”.

- (2) “An unknown Quantum state is cannot be cloned (the no-cloning theorem)”.

The very important step taken in Quantum Cryptography data transfer is the test in which researchers check about possibilities of capturing information's those are being transmitted through a Quantum Channel.

2. Some protocols in quantumcryptography

a) *BB84*[7]:

Charles Bennett and Gilles Brassard created a quantum key distribution method for quantum cryptography in 1984. Basically, it was dependent on following things [35].

1. “The quantum features that information gains are only feasible through degrading the signal if the two states one is seeking to differentiate are not orthogonal.”
2. “The presence of a public classical channel that is authenticated.”

If Alice wants to transmit Aman a private key using the BB84 method, she starts with two series of bits called p and q, each of which is n bits long. After that, using a tensor product of n Qubits, she encodes these two strings as follows:

$$|y\rangle = \bigotimes_{i=1}^n |y_{a_i b_i}\rangle,$$

Provided that a_i and b_i , respectively, represents i^{th} bits of p and q. $a_i b_i$ provide us with an index into the four qubit states together, as listed below [6]:

$$\begin{aligned} |y\ 00\rangle &= |0\rangle, \\ |y\ 10\rangle &= |1\rangle, \\ |y\ 01\rangle &= |+\rangle = (1/\sqrt{2})|0\rangle + 1/\sqrt{2}|1\rangle, \\ |y\ 11\rangle &= |-\rangle = (1/\sqrt{2})|0\rangle - 1/\sqrt{2}|1\rangle. \end{aligned} \quad [10]$$

Be aware that the basis a_i is encoded in is determined by the bit b_i (calculated in computational basis or Hamdard basis). Qubits are now present. The state which is certainly not in the states of mutual orthogonality, and therefore without knowing b, it is difficult to distinguish between all of them [6].

Since we all know that BB84 is very powerful protocol, but is one of the very initial step in domain of secure communication with the use of quantum network. After that many of the additional protocols have been developed and many algorithms are still in the research as Quantum is still not very known that enhances the use of cryptography in quantum network. For taking advantage of this protocol for our practical applications, we first need to figure out how we can have built very large- scale quantum networks that can provide Entanglement as a Service (EaaS) more broadly.

There is also a B92 protocol which is a variant of BB84[35] protocol which have major difference form BB84, BB84 protocol works on four different polarization states of photon, while B92 protocol uses only two, in which one state was from the rectilinear basis, which was conventionally H-polarization state and the other from the diagonal basis, conventionally +45 degree – polarization state.

b) 3-Stage protocol for quantum cryptography

Another name for it is Kak's three-stage procedure. and it is a method of encrypting data which is based on random polarization rotation by both the user, here Alice and Aman. It is proposed by Subhash Kak. In its ideology If single photons are employed, it may be used to encrypt data continuously and irreversibly. Although it could also be used for key exchange, it differed from the Quantum Key Distribution-QKD approach in that it could be used for effective data encryption.

The main idea behind this method is actually double lock cryptography. In this method Both user place their lock on the box which contain valuable information. Firstly, Alice locks the box and send it to Aman, who send it back to Alice after putting another lock on it. Then Alice removes her lock and send it back to Aman, who then unlock the box

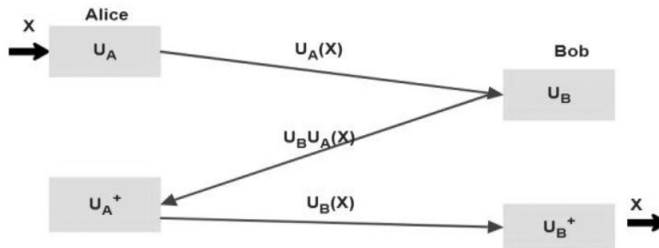


Figure 1
3 Stage Protocol for QC

and get his secret information. [11][12]. Pramode Verma in Oklahoma University's Quantum Optics Lab did the hardware implementation of Basic Polarization Rotation Scheme. In his technique he showed that more than a photon can be used in exchanges between Aman & Alice therefore this open up the possibility of multi photon QC. On the basis of rotational Quantum errors, the three stage protocol was analyzed by Parakh & proposed a modification that can make this free from errors. One interesting feature is that it is invariant to the cost of rotational error and can therefore updated for arbitrary rotations.

c) *KMB09 Protocol*

In this alternate quantum key distribution, Alice and Aman employ two mutually unbiased bases, one of which we encode as "0" and the other as "1." The security of this system is made achievable by the minimal Quantum Bit Error Rate (QBER) and index transmission error rate (ITER) introduced by eavesdroppers. This method's benefit is that it will produce more clamour in the transmission line that will enable Alice and Aman to go farther without the use of an intermediary node [13].

3. Quantum Key Distribution-QKD

It is a method of communicating securely which use the implementation of Cryptographic Protocol which involves the elements that make up quantum mechanics. It enables the communicators to generate a secret key at random that is used to encrypt or decode communications and shared by the users. As it is best known, it is frequently referred to as quantum cryptography for its QC tasks [14].

Advantage of using QKD is that it gives power to both to identify any outsiders who could be attempting to learn the key. This is the outcome of fundamental property of quantum mechanics: every measurement of a quantum system affects it. The key must somehow be accessible to a third party attempting to listen try to measure the key which disturb the quantum system and it is get detected by system. It uses some of technologies like quantum entanglement or superposition and transmitting information in quantum state combine it with communication system that detects eavesdropping. There is certain threshold value for eavesdropping, whenever the value of eavesdropping is above than certain threshold value, the contact is terminated since there is no secure key available.

The major disadvantage of QKD is that it uses a traditional route for communications that is authenticated. Having this channel today denotes

the exchange of a symmetric key with a sufficient length and security level. With this knowledge, everyone can succeed. The security level of Quantum Cryptography without using QKD by using some simpler method such as using the Advanced Encryption Standard's Galois/Counter mode. QKD therefore performs the function of a stream cipher most of time. QKD is the only way to create and distribute keys; it is not utilized to send messages or data over the network. This key can be used to encrypt or decode a message that is conveyed over any communication channel using any acceptable technique. The one-time pad algorithm, which is frequently connected with QKD since it is demonstrably safe when used in conjunction of secret, random key. Also in real time it is combined with Symmetric key algorithms like AES [15].

4. Eavesdropping Strategies

As the Quality of Encryption is increasing over a period of time, on the same basis Eavesdropper are also evolving on behead of technology and physics in case of Quantum Cryptography. Various Eavesdropping strategies were developed, such as Opaque and Translucent Eavesdropping. Let's take brief look over them [16]:

a) *Opaque Eavesdropping* [19]

For this strategy, let's assume a eavesdropper Eve who is trying to steal information from Alice who is communicating with Bob. In this process Eve intercept Alice's message and the send this message to Bob and trying to pretend that nothing happens. It is found that If Alice used only one specific orthogonal quantum alphabet for her communication with Bob, then Eve will go undetected.

For example, if Alice used any quantum alphabet then Eve can measure its every bit with any device which is based on circular polarization or linear polarization operators such as

$$\begin{array}{cccc} \left| \begin{array}{c} \curvearrowright \\ \updownarrow \end{array} \right\rangle & \left\langle \begin{array}{c} \curvearrowleft \\ \updownarrow \end{array} \right| & \left| \begin{array}{c} \curvearrowright \\ \leftrightarrow \end{array} \right\rangle & \left\langle \begin{array}{c} \curvearrowleft \\ \leftrightarrow \end{array} \right| \end{array}$$

b) *Translucent Eavesdropping without Entanglement* [20]

In this method, Eve somehow manage to pass the information or secret of Alice which is getting transmitted to Bob, through her Probe and let it interact it with unitarily, and then let it proceed on to Bob in a slightly

modified state. We can assume the case of B92 protocol here, If Alice is using it the Eve probe with initial state

$$\begin{aligned} &|a\rangle \\ &|q\rangle|a\rangle \rightarrow U|q\rangle|a\rangle = |q'\rangle|aq\rangle \\ &|\bar{q}\rangle|a\rangle \rightarrow U|\bar{q}\rangle|a\rangle = |\bar{q}\rangle|a\bar{q}\rangle \end{aligned}$$

where $|\theta'\rangle$ and $|\theta\rangle$ is denoting the change in the state of message received by Bob.

c) Translucent Eavesdropping With Entanglement [21]

In this method, Eve entangles her Probe and the carrier, and then she sends the carrier to Bob. In the case of protocol which Alice is using (here B92), Eve detection probe with initial state $|\alpha\rangle$ will perform a unitary transformation U of the form

$$\begin{aligned} |q\rangle|a\rangle &\rightarrow U|q\rangle|a\rangle = a|q\rangle|aq\rangle + b|\bar{q}\rangle|a\bar{q}\rangle \\ |\bar{q}\rangle|a\rangle &\rightarrow U|\bar{q}\rangle|a\rangle = b|q\rangle|aq\rangle + a|\bar{q}\rangle|a\bar{q}\rangle \end{aligned}$$

5. Risk Analysis

When in the interception Eve identified all the Qubits, possibility of matching of samples of Alice and Bob is very minute and then through the channel of Eve they try to send unprotected message. Let's estimate the vulnerability of QKD: There is probably more chance that both Alice and Bob picked up a similar basis. On the case of off chance if Eve chooses same premises, she will accidentally block this bit without any detection of error. Will perform a Unitary Transformation U of the form [22]

$$\begin{aligned} &|\uparrow\uparrow\rangle\langle\uparrow\uparrow| \\ &|\leftrightarrow\leftrightarrow\rangle\langle\leftrightarrow\leftrightarrow| \end{aligned}$$

Let's assume a case that if Eve choses a different basis, for example alternate of that of Alice and Bob, there is still chance of 50% that Bob will gauge the message that Alice was attempting to send. So, for the proposed attempt of block it was undetected. For the same above scenario, that is if Eve take the alternate basis that of the Alice and Bob, there is probably 50% chance that Eve get detected by the Bob because this will introduce error in keys. [33]

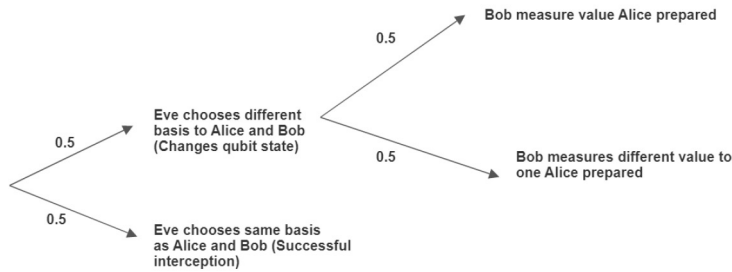


Figure 2
Risk Analysis

On the off-chance that researchers used at 15 bits as given, it was received that 1.3% possibility Eve will be undetected, on the off-chance it was unreasonably hazardous, and the author proposed to look at 50 bits, and had a 0.00006% possibility of being spied upon accidentally [24].

6. Quantum Cryptography Forfuture Internet [32]

If we assume that Alice and Bob is communicating over a public channel and Eve is an eavesdropper. For the sake of ensuring privacy Alice will encrypt the data and send it to Bob, even if their information is encrypted they cannot prevent eavesdropper to attack on their channel. If they are communicating with help of cable the Eve can monitor with an oscilloscope or a multimeter. From the portion of a light signal eavesdropper can obtain information in Optical Fiber Communication. Keep in mind that environmental elements like temperature and pressure are to blame for the fiber loss etc. But in the case of Quantum computing, the quantum no cloning hypothesis ensures that the eavesdropper will be discovered. Eavesdropper will measure the quantum channel with the same base as the sender with a 50% chance if he watches the quantum channel to obtain Qubits. Therefore, there is a 50% chance of catching an eavesdropper. It should be noted that the likelihood of an eavesdropper being discovered is $1-(1/2)^n$ for quantum information of n bits [25].

7. Security of QKD [31]

In this part of this paper we will analyze the real situation of future internet, in the channel of both noisy and noise free quantum channel. In advance there is agreement between both the parties that if there is vertical

and oblique upward polarization then it indicates “1”, while if there is horizontal and oblique downward polarization then it represent “0”.

$$\Pr = \Pr\{\text{Base}_A = \text{Base}_B \wedge \text{Measure}_A \neq \text{Measure}_B\}.$$

This is the probability formula for getting the existence of a eavesdropper on the QKD protocol. In the Figure 1 it is channel with 0 noise and we can observe here that the probabilities increase to 100% if there is the number of transmission is increase to 40. But in Figure 2, this is quantum channel with 30% noise, and here we can observe that when the no. of transmitted photon reaches 80 then the probabilities of eavesdropper is close to 100%. So from both of this graph we can say that in Quantum channel detection of eavesdropper is 100% as the no. of transmitted bits is rising (as shown in Figure 3 and 4).

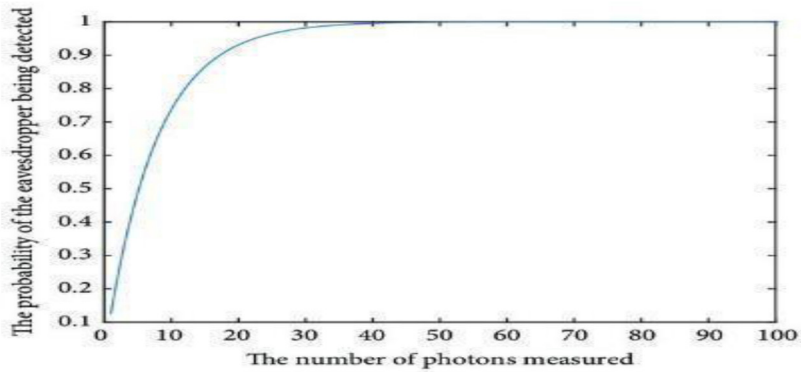


Figure 3

Detecting eavesdropper on less noise

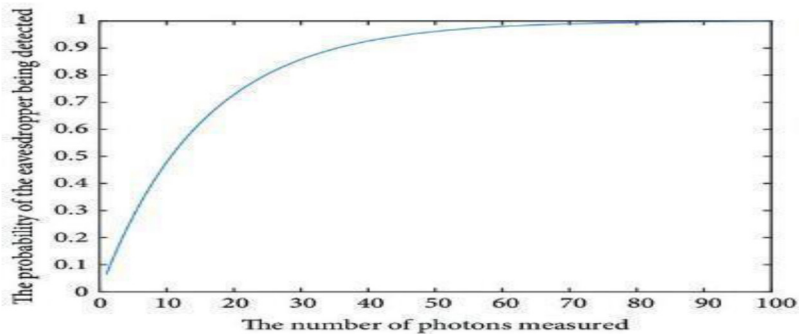


Figure 4

Detecting eavesdropper on more noise

Here we can also say that chance of detecting eavesdropper is more in the case of noise-free channel than in the case of noisy channel. As the noise increase more transmitted bits are required to detect the eavesdropper.

From both the graph it is clear that the use of Quantum Cryptography is better than use of any Cryptographic algorithms because the act of getting catch on the eavesdropper is much more powerful and easy and fast. If the noise is greater than the eavesdropper can be found on very low no of transmission which shows that it can act more efficiently on noisy channel which is one of the biggest problems for any other cryptographic algorithms.

8. Quantum Product Comparison

Product	Features	Category	Authentication	Protocols used
Cerberis [34]	Secure P-P Backbone Latency is less than 15us. It is highly secure, scalable, resourceful 10GBPS bandwidth. There is also dual key agreement up to 100 km transmission	Server	Control over access role is based upon identification.	BB84, SARG RSA which is dual key, AES-256 CFB etc.
QPN[28]	It is compatible with DWDM Latency which is less than 10 us. There is remote monitoring which is Integrated with PKI and in transit security Of access of data to SAN upto 40 km of transmission	Gateway	DSS Authentication	BB84 3DES AES IPsec
QKD GHz System [29]	Management of Keys and also there is distribution Side channel attacks counter measures. >100km transmission	Point to point	Decoy Pulses	AES with OTP SDC

Contd...

Cygnus[30]	On the basis of LDPC, there is Error Correction Low SNR. In the range of 80 KM WDM is compatible for transmission privacy Amplification	Peer to Peer	HMAC based Digital Signature authentication which is of 256 bits	AES with OTP E91 SHA-1 RSA
Clavis ^[26]	Concept of key reconciliation and privacy amplification up to 50 km	External Connector	Universal hashing with one time pad	BB84 SARG04
Q-Box ^[27]	Symmetric Key Distribution for Person to Person single photon based Upto transmission of 50 km	Peer to Peer	DSS Authentication	BB84 Diffie Helmen,

9. Quantum Research Group

Following are the some of the top scientific and research organizations in the area of quantum computing [31].

1) The Mcgill University

At this University, a group of scientists and researchers are working on projects in the areas of QC, quantum information and mechanics, quantum cryptography, algorithms, and complexity theory.

2) The Michigan University

The University of Michigan's research focuses on modeling the quantum circuits which will model any faults and error in it, there is some discovery in quantum and classical reversible circuit, and circuit equivalence checking. It also examines simulations of quantum circuits on classical computers, quantum computer architecture, and quantum design automation. The study is carried out in association with MIT, NIST, and Columbia University

3) The Norwegian Quantum Hacking Group

Quantum hacking group Norway is primarily interested in finding flaws in the quantum system, as well as eavesdropping and complete security. Quantum Hacking Group is receiving assistance from Id Qu antique and the University of Waterloo Canada for their study. Their primary focus is identifying weaknesses in quantum hardware.

4) Victoria of Quality Communication

In the field of Quantum computation, Quantum technology, Quantum communication device and photon sources there is a major research being conducted by Quantum Communication Victoria research group. There are various organization giving fund for this research like University of Melbourne, MagiQ Technologies, Silicon Graphics Inc. all provide funding for research efforts in QCV.

5) SEECS, NUST

Currently, Pakistan's National University of Science and Technology has a School of Electrical Engineering and Computer Science. is working in the field of quantum cryptography and non- locality. It was to develop a method or algorithm which will share quantum secret via entanglement and teleportation mechanism. Moreover, there one of the researches is focused on "Quantum Secure Positioning". It is a simple method to validate user and its location as claimed by them.

10. Conclusion

The development of quantum computing and quantum based technology appears to be a step forward for information security. Quantum Computers are anticipated to be the most potent computers and be capable of resolving any challenging computational issue this seriously jeopardizes traditional cryptography. According to consumer needs a no. of quantum goods are available on the market with a variety of characteristics. For many reasons, researchers are working to build a quantum computer. According to information provided by Edward Snowden, the NSA [24] is a striving to decode the transmission and has already begun several initiatives in this regards. Google and Microsoft are simultaneously working to build a Quantum Computer that will protect public channels to maintain an individual's privacy. Similar to this, NASA is seeking a Quantum Computer to advance its study of exoplanets. Overall, things are still under control at this point because the Quantum Computer is not fully operational, but the problem has to be carefully handled. Furthermore, the Quantum Hacking Group in Norway use Quantum Hardware to identify vulnerabilities and suggest techniques to do eavesdropping with the goal of obtaining total security through quantum systems.

References

- [1] M. Sasaki, "Quantum Key Distribution and Its Applications, in *IEEE Security & Privacy*, vol. 16, no. 5, pp. 42-48 (September/October 2018), doi: 10.1109/MSP.2018.3761713.
- [2] Aihong Chen, Weimin Peng and Tian Gui, "A variant of BB84 Protocol based on quantum phase," 2013 International Conference on Information and Network Security (ICINS 2013), Beijing, 2013, pp. 1-5, doi: 10.1049/cp.2013.2465..
- [3] V. Padamvathi, B. V. Vardhan and A. V. N. Krishna, "Quantum Cryptography and Quantum Key Distribution Protocols: A Survey," 2016 IEEE 6th International Conference on Advanced Computing (IACC), Bhimavaram, India, pp. 556-562 (2016), doi: 10.1109/IACC.2016.109.
- [4] A. M. Sofy, M. Shalaby, H. M. Dahshan and A. Rohiem, "Modeling One-way and Two-way quantum key distribution protocols," 2019 Ninth International Conference on Intelligent Computing and Information Systems (ICICIS), Cairo, Egypt, pp. 239-244 (2019), doi: 10.1109/ICICIS46948.2019.9014729.
- [5] I. Giroti and M. Malhotra, "Quantum Cryptography: A Pathway to Secure Communication," 2022 6th International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS), Bangalore, India, pp. 1-6 (2022), doi: 10.1109/CSITSS57437.2022.10026388.
- [6] P. G. Kwiat, A. G. White, C. G. Peterson, D. S. Naik and A. J. Berglund, "Entangled-photon quantum cryptography," Quantum Electronics and Laser Science Conference (QELS 2000). Technical Digest. Postconference Edition. TOPS Vol.40 (IEEE Cat. No.00CH37089), San Francisco, CA, USA, pp. 225- (2000).
- [7] 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*, vol. 81, no. 3, pp. 1301-1350 (2009).
- [8] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, "Gaussian quantum information," *Reviews of Modern Physics*, vol. 84, no. 2, pp. 621-669 (2012).
- [9] X.-B. Wang, "Beating the photon-number-splitting attack in practical quantum cryptography," *Physical Review Letters*, vol. 94, no. 23, pp. 230503-1-230503-4 (2005).

- [10] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, pp. 175-179 (1984).
- [11] "A Three-Stage Mutual Authentication Protocol for RFID Systems" by Zhe Liu, Hui Li, and Li Xu, published in the Proceedings of the 2016 International Conference on Networking and Network Applications.
- [12] "A Three-Stage Protocol for Privacy-Preserving Social Network Data Publication" by Jiaojiao Jiang, Jianliang Xu, and Xiaohui Liang, published in the Proceedings of the 2018 IEEE International Conference on Data Mining.
- [13] Kim, J., Moon, D., & Lee, S., New efficient ID-based key agreement protocol secure against clock synchronization attack. *Information Sciences*, 179(7), 883-890 (2009).
- [14] Bennet, C. H., & Brassard, G., Quantum cryptography: Public key distribution and coin tossing. Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, 175-179 (1984).
- [15] Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H., Quantum cryptography. *Reviews of Modern Physics*, 74(1), 145- 195 (2002).
- [16] Brassard, G., & Salvail, L., Secret-key reconciliation by public discussion. *Advances in Cryptology – CRYPTO '93*, 410-423 (1994).
- [17] Acin, A., Gisin, N., & Masanes, L., From Bell's theorem to secure quantum key distribution. *Physical Review Letters*, 97(12), 120405 (2007).
- [18] Scarani, V., & Renner, R., Quantum cryptography with finite resources: Unconditional security bound for discrete- variable protocols with one-way postprocessing. *Physical Review Letters*, 100(20), 200501 (2008).
- [19] Patel, K., & Joshi, A., Security analysis of a novel password-based authenticated key exchange protocol using honey encryption. *Journal of Ambient Intelligence and Humanized Computing*, 9(4), 1227-1240 (2018).
- [20] Vinay Pathak, Karan Singh, Sudhanshu Aggarwal & Anshita Dhoot. Ensuring security framework for WBANs, *Journal of Discrete Mathematical Sciences and Cryptography*, 24:3, 697-710 (2021), DOI: 10.1080/09720529.2020.1822542.

- [21] Deng, F. G., Long, G. L., & Liu, X. S., Two-step quantum secure direct communication protocol using the Einstein- Podolsky-Rosen pair block. *Physical Review A*, 71(2), 022317 (2005).
- [22] "Quantum key distribution with realistic devices: Security analysis and experimental demonstrations" by J. F. Dynes, H.-K. Lo, M. Lucamarini, B. Fröhlich, A. W. Sharpe, and Z. L. Yuan (Physical Review A, 2016).
- [23] "Risk analysis of quantum key distribution with detector control" by P. Jouguet, S. Kunz-Jacques, and A. Leverrier (Physical Review A, 2013).
- [24] "Quantum key distribution with active phase randomization: Risk analysis and experimental demonstration" by S. Sajeed, S. M. Assad, and M. Lucamarini (Physical Review A, 2017).
- [25] Jiangsu Engineering Center of Network Monitoring, Nanjing University of Information Science & Technology, Nanjing, China.
- [26] Branciard, C., Gisin, N., & Lamas-Linares, A., Security of two distributed-phase-reference protocols for quantum key distribution. *Physical Review A*, 77(2), 022301 (2008).
- [27] Zhang, L., Zhu, Y., & Chen, Y., Experimental investigation of an integrated quantum key distribution system using a novel Q-Box. *Chinese Physics B*, 25(10), 100308 (2016).
- [28] Xu, F., Ma, X., Qi, B., Lo, H. K., & Qian, L., Experimental demonstration of phase-encoding quantum key distribution system with GHz key rate over a 100 km fiber. *Optics Express*, 18(9), 8587-8594 (2010).
- [29] Stucki, D., Legré, M., Buntschu, F., Clausen, A., Felber, N., Gisin, N., ... & Thew, R., High-rate, long-distance quantum key distribution over 250 km of ultra low loss fibres. *New Journal of Physics*, 13(12), 123001 (2011).
- [30] Yan, L., Jiao, Y., Liu, X., Zhang, X., Li, Y., Wang, T., & Zhang, J., Experimental verification of a polarization- encoded quantum key distribution system over 100 km in the presence of turbulence. *Optics Communications*, 457, 124561 (2020).
- [31] Ankit Kumar, Pankaj Dadheech, Vijander Singh, Linesh Raja & Ramesh C. Poonia. An enhanced quantum key distribution protocol for security authentication, *Journal of Discrete Mathematical Sciences and Cryptography*, 22:4, 499-507 (2019), DOI: 10.1080/09720529.2019.1637154.

- [32] Ajay Kumar Gupta, Devendra Singh, Karan Singh & Lal Pratap Verma. An adaptive congestion control algorithm, *Journal of Discrete Mathematical Sciences and Cryptography*, 24:5, 1273-1282 (2021), DOI: 10.1080/09720529.2021.1932912.
- [33] Ankit Kumar, Pankaj Dadheech, Vijander Singh, Ramesh C. Poonia & Linesh Raja. An improved quantum key distribution protocol for verification, *Journal of Discrete Mathematical Sciences and Computer* (2019).
- [34] Noor-ul-Ain, W., Atta-ur-Rahman, M., Nadeem, M., Abbasi, A.G., Quantum Cryptography Trends: A Milestone in Information Security. In: Abraham, A., Han, S., Al-Sharhan, S., Liu, H. (eds) Hybrid Intelligent Systems. HIS 2016. Advances in Intelligent Systems and Computing, vol 420. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-27221-4_3.
- [35] C. H. Bennett and G. Brassard. "Quantum cryptography: Public key distribution and coin tossing". In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, volume 175, page 8. New York (1984).

Received September 2023