International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT12176101

A Comprehensive study on Quantum Key Distribution

Sagarmoy Ganguly, Asoke Nath
Department of Computer Science, St. Xavier's College (Autonomous), Kolkata, West Bengal, India

Article Info
Volume 7, Issue 6
Page Number : 402-409

Publication Issue :
November-December-2021

Article History
Accepted : 15 Dec 2021
Published : 30 Dec 2021

ABSTRACT

Quantum cryptography is a comparatively new and special type of cryptography which uses Quantum mechanics to provide unreal protection of data/information and unconditionally secure communications. This is achieved with Quantum Key Distribution (QKD) protocols which is a representation of an essential practical application of Quantum Computation. In this paper the authors will venture the concept of QKD by reviewing how QKD works, the authors shall take a look at few protocols of QKD, followed by a practical example of Quantum Cryptography using QKD and certain limitations from the perspective of Computer Science in specific and Quantum Physics in general.

Keywords - Quantum Key Distribution, Traditional Cryptography, Photon Polarization, Qubits, Quantum Entanglement, Quantum Cryptography, Quantum key exchange.

I. INTRODUCTION

Today, people hold a lot of secrets in the form of private information and invariably we must give them away to the internet. For example, debit card / credit card details, personal details etc. But we don't know where such information is kept and how well they are secured. Also, there is the matter of secure communication where transmitted data is only to be viewed by designated sender and receiver and we don't know whether such communications are being protected from outside parties or potential eavesdroppers. This is where cryptography comes to play as it translates the data into a code which can only be read or viewed by the right people. Thus, cryptography and data encryption are crucial when it comes to our daily online communications and data stored on the internet.

A key, in real life, is used to open and close a lock. Similarly in cryptography, a key is a parameter which controls and oversees the cryptographic algorithm. The key dictates the translation of plain text into cipher text during encryption and vice versa during decryption. Traditionally, public keys which are known to all, or private keys were used to ensure data protection and secure transmissions. But, either of them isn't secure enough as third parties and potential eavesdroppers are constantly able to retrieve the key and get a hold of the encrypted data. Thus, classical

cryptography cannot provide unreal and unconditional security of data and communication. The process of data encryption and illegally retrieving data has become an endless loop as cryptographers build more and more secure means of protecting sensitive data while hackers, eavesdroppers are also grinding furiously to crack the system.

Quantum cryptography uses Quantum Key Distribution which enables sharing of keys with unreal levels of security and protection. Unlike classical cryptographical protocols, which are based on mathematical functions and computational complexity, QKD protocols rely on laws of physics and quantum mechanics. This makes security provided by QKD resistant and immune to infinite computational power. In contrast, classical cryptography is vulnerable and easily falls prey to the power of efficient computation. Furthermore, a QKD system adds a new feature to the field of cryptograph in general by making it possible to detect any illegal eavesdropping activity as the presence of a third party or potential eavesdropper adds apparent noise to the transmission taking place in a quantum channel.

II. LITERATURE SURVEY

Quantum Cryptography was first proposed by Stephen Wiesner in early 1970s. Following the creation of QKD, in 1984 was developed by Charles Bennett and Gilles Brassard. This was described using Photon Polarization state to transmit the information. The first experimental prototype based on the BB84 protocol was operated over a distance of 32cm **[1]**. Since then, several other QKD protocols have been developed as well as modified. In 2007, Mohen S.Hooshang proposed a newer and modified version of BB84 protocol which resulted in an increase in the length of the quantum key, but increased the time taken for key generation.

In 2003, a team at the University of Vienna transmitted entangled photons across the river Danube, through free space **[2]**. The first bank transfer using QKD based system took place in 2004. The QKD system was developed using Polarized entangled photon pairs, generated by firing a laser through a crystal to split each photon into two. Two such QKD systems were then installed between the headquarters of an Austrian bank and Vienna City Hall, which were connected by 1.45 Km of optical fibre cable **[3]**. The entangled photon pairs were then sent one by one from the one destination to another using the fibre optic cable.

III. WHAT IS QKD AND HOW DOES IT WORK

A QKD model consists of a sender, receiver, and a quantum channel. QKD enables the sender and receiver to generate a random secret key at the quantum scale. QKD refers to secure key management at the quantum level **[4]**. The working of QKD is based on the transmission of light particles or photons over a quantum channel. The Quantum Channel serves as the medium for transmitting these quantum states (photons) between the sender and receiver. Usually, a fiber optic cable or an optical network is used as a Quantum Channel. Figure 1 shows a QKD Model where Alice is the sender, Bob is the receiver and Eve is an eavesdropper.

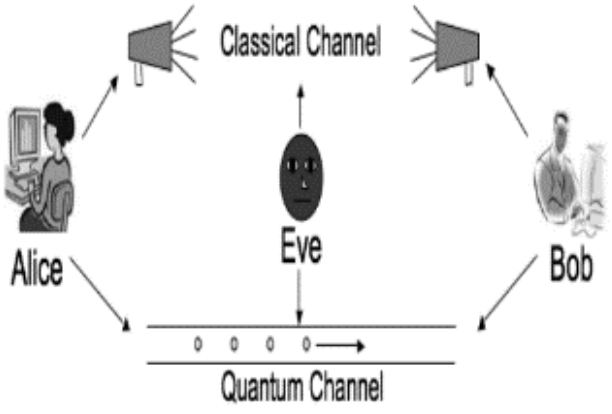

Fig1: Quantum Key Distribution Model [2].

Quantum Key Distribution works in 3 stages:

A. Key Exchange

This stage, also known as the Raw Key Exchange, leads to the generation of the raw key. The sender generates random quantum bits (qubits) which are then exchanged between the two parties in the form of photons / light particles over the quantum channel. Each photon has 4 different polarization states (vertical, horizontal, +45°, -45° diagonal) and associated bit values. Figure 2 shows the types of polarizations and orientations. The process of photon polarization is used to attach these bit values (0 or 1) to each state, ex. bit value 0 can be associated with horizontal or -45° diagonal state and similarly bit value 1 can be associated with vertical or +45° diagonal state. Therefore, each bit value is represented either orthogonally or diagonally and this takes place at random. Each polarized photon is the encryption of each bit of information in the plain text. Thus, the sequence of polarized photons represents the entire encrypted bit sequence/plain text. This sequence is then sent to the receiver. The receiver uses a filter (beam splitter) of random orientation (orthogonal / vertical) to distinguish between the polarization states and detect the deflection of each photon, in order to decrypt the encrypted text and obtain the original bit of information. This process is repeated by the receiver for decrypting the entire secure key. The sender and receiver maintain records of the orientations and the receiver also maintains a record of the outcomes. Figure 3 shows how polarization randomly encodes a quantum state to a bit value which is then decrypted by the receiver using a filter of random orientation.

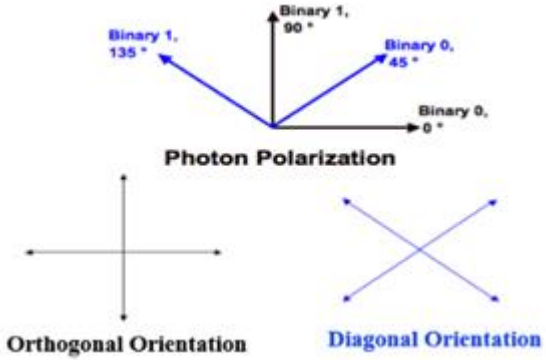

Fig2: Types of photon polarizations and orientations [5].

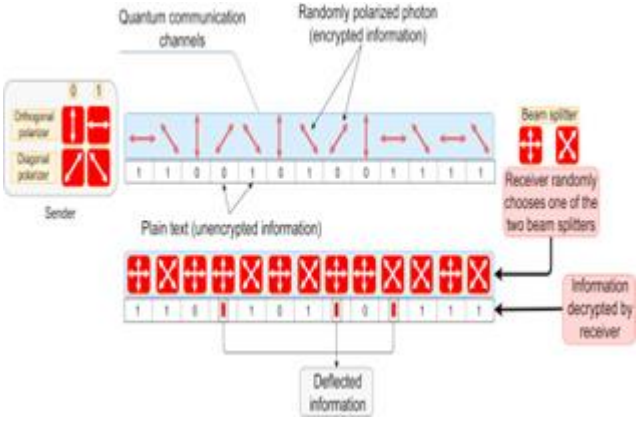

Fig3: Simple presentation of Key Exchange [4].

B. Key Sifting

The sequence of bits that the receiver decodes in the previous stage might not be entirely identical to the original plain text. If the orientation of the filter (beam splitter), used by the receiver, matches the orientation of the polarizers, used by the sender, then the decrypted bit will be identical to the original bit and if the orientations do not match then there is fifty percent probability that the decrypted bit will be identical to the original bit. The randomness in the selection of the orientation deflects certain bits and makes the measured bit unidentical to the original bit. In this stage, the receiver shares the orientations of the filter with the sender over a classical channel. The sender then compares the filter orientations with the orientation of the polarizers which were used for encryption. The sender then tells the receiver about

the filters which have orientation similar to that of the polarizers. The receiver keeps the bits associated with these filters having identical orientations and discards the rest. The remaining sequence of bits is called the Sifted Key. As the receiver only shares the sequence of the filters, no compromises are made to the privacy of data. Absence of any eavesdropper will result in identical sifted keys, but the sifted keys of sender and receiver will not be the same in the presence of an eavesdropper. Figure 4 shows an example of key sifting where the sifted key is identical between sender (Alice) and receiver (Bob) when there is no eavesdropper, but the sifted key is not identical when a potential eavesdropper (Eve) is present.

Alice's selected orientation	+	x	x	+	x	+	+	+	x	+	x	x
Alices's selected states	↑	↗	↗	→	↘	→	↑	↑	↗	→	↘	↘
Alice's raw-key	1	0	0	0	1	0	1	1	0	0	1	1
Bob's selected orientation	+	+	x	+	x	X	+	+	x	+	+	x
Without eavesdropping												
Bob's measured states	↑	→	↗		↘	↘	↑	↑	↗	→		↘
Bob's raw-key	1	0	0		1	1	1	1	0	0		1
Alice's sifted-key	1		0		1		1	1	0	0		1
Bob's sifted-key	1		0		1		1	1	0	0		1
With eavesdropping												
Bob's measured states	↑	→	↗		↙	↘	↑	↑	↗	↥		↘
Bob's received bits	1	0	0		0	1	1	1	0	1		1
Alice's sifted-key	1		0		1		1	1	0	0		1
Bob's sifted-key	1		0		0		0	1	0	1		1

Erroneous bits

Fig4: Key Sifting Example [6].

C. Secret Key Distillation

When the sifted key is not identical due to presence of an eavesdropper, the sifted key is further processed to generate a secret-key and this process is called Secret Key Distillation. This process itself takes place in three stages.

The first stage is called error estimation and in this stage the amount of quantum bit error is estimated by publicly sharing a minute random subset of the bits.

The second stage is called reconciliation. In this stage the sender and receiver agree on a random permutation of bits in the key, the key is then divided into blocks of length 'L' and compute parities of their blocks and the parity of each block is compared **[6]**. In case of similar parity, the blocks are considered correct and in case of indifferent parity, binary search is used to find the erroneous bit. The last bit of the block with announced parity is then removed. This process is repeated until all permutations are correct which, in the end, generates a reconciliation key.

The next and last stage is known as Privacy Amplification. Privacy amplification is the process whereby Alice and Bob reduce Eve's knowledge of their shared bits to an acceptable level by compressing the reconciled key by an appropriate factor **[7,8,9]**. As a result of this stage, the eavesdropper's knowledge about the key reduces to $2^{-s/\ln 2}$ and the length of the final key is reduced to n-m-s bits, where s is a constantly chosen security parameter **[10]**. Figure 5 shows the reduction in size of raw key after each stage

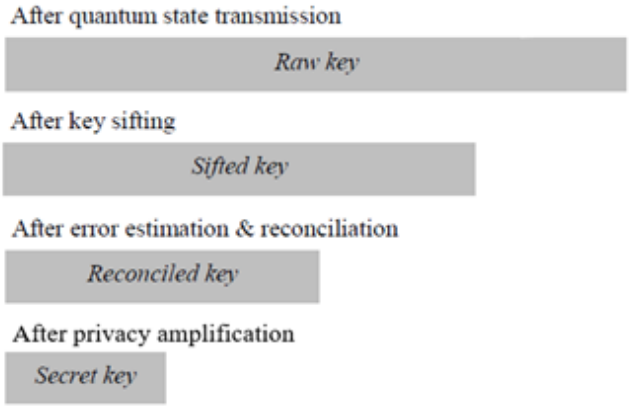

Fig 5: Change in size of raw key after each stage [6].

IV. QKD PROTOCOLS

These protocols consist of the governing rules for securely exchanging encryption keys between two parties for facilitating a well-protected and private communication. These protocols are based on certain

quantum principles. The most renowned BB84 protocol is based on the Heisenberg's Uncertainty Principle (HUP). Another important quantum principle on which QKD is often based is the principle of quantum entanglement. We shall take a deeper look at the HUP based BB84 protocol and Quantum Entanglement based Eckert's Protocol.

A. BB84

This protocol is the first QKD protocol and is named after its authors, Charles Bennett and Gilles Brassard, and the year,1984, in which it was made. It can be vaguely said that all other HUP based protocols are variants of this protocol, which makes the BB84 one of the most prominent Protocols till date.

The above discussed QKD method follows this protocol. Thus, the basic idea is to encode every bit of secure key in the polarization states of photons [11]. These polarized photons are then sent to the receiver for decryption and the sifted key is obtained by both parties. In case of non-identical keys, further processing is performed for error correction which finally generates the secret key. It is also noticed that the size of the raw key reduces after each stage.

Another important feature of this protocol is that it can announce the presence of a third party or eavesdropper. According to the no cloning theorem, the polarization state of a photon cannot be measured without destroying the photon [12]. Thus, if the security is breached and the photons are somehow obtained by an eavesdropper then the originally sent photons will be destroyed if the eavesdropper tries to decrypt the bits. Now the eavesdropper can either exit with the randomly decrypted bits (which are surely not correct) and the receiver won't receive any more photons, or the eavesdropper can try to send photons to the receiver on its own which will not match the sequence of bits sent by the sender. In both cases, the eavesdropper will be exposed.

B. Eckert's Protocol

This protocol is based on the principle of Quantum Entanglement. This principle states that two quantum particles can become entangled and start carrying properties opposite to each other.

The Eckert's protocol describes a quantum channel with a single source that continuously emits pairs of entangled polarized photons. The sender and receiver each receive one photon from the pair and then they would randomly select orientations to measure the photons. The process of measurement of photons is exactly same as in BB84. If both sender and receive select same orientations then, based on principle of quantum entanglement, they would have exact opposite results. If this repeats for the whole sequence, then each of them will end up having a sequence of bits which is the complement of the other. To detect the presence of an eavesdropper, those photons are considered for which the sender and receiver selected different orientations. They will have to measure these photons in a third orientation and then share the results [13]. Then, this result is tested with Bell's Inequality which should not hold for entangled particles and if the inequality does hold then this would indicate that the photons were not truly entangled, thus exposing the presence of an eavesdropper [14]. Figure 6 shows an entangled QKD model where Alice is the sender, Bob is the receiver and Eve is the eavesdropper.

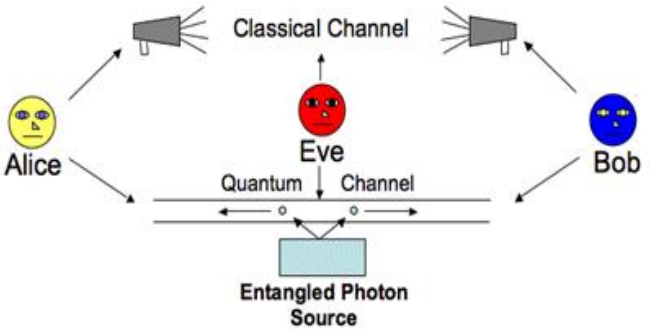

Fig 6: Entangled QKD Model [12].

V. QKD EXAMPLE

For an example of QKD, we shall consider the BB84 protocol-based quantum channel with no potential eavesdropper. So, our model consists of X (sender) and Y (receiver). Let's say X wants to send this 8-bit message 01101001. First, each bit will be encoded to polarization state of each photon. Figure 7 shows the types of basis/orientations. The rectilinear / orthogonal basis encodes 1 for horizontal polarization and 0 for vertical polarization. The diagonal basis encodes 1 for anti-diagonal 135° polarization and 0 for diagonal 45° polarization. X will randomly select the basis for the bits. If bit value is zero and selected basis is rectilinear, then it will result in a vertical polarization and so on.

In this way all the bits are encoded to polarization states and this sequence of polarized photons is sent to Y. Y then randomly selects basis for each photon to measure the polarized states and decrypt each bit. Based on the selected basis, Y gets his photon polarization signal result and respective decrypted bits. Then Y shares his sequence of selected basis with X over a public / classic channel. The bits associated with same basis and polarizations are kept while the rest are discarded. These remaining bits then form the sifted key and, in this case, the secret key (0 1 0 1). Figure 8 shows the entire above-described process.

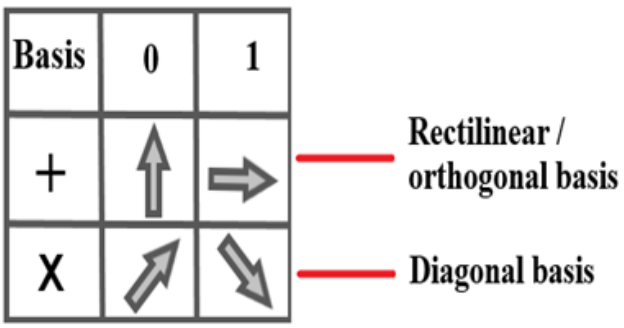

Fig7: Types of Basis.

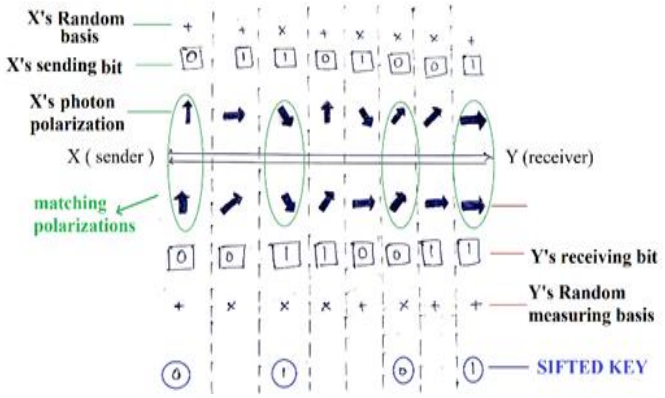

Fig 8: QKD Process

VI. QKD LIMITATION

Quantum computing using the laws of quantum mechanics is a new field of research and development and QKD is its first application. Several limitations exist at the moment such as hardware development, implementation, distance coverage, high cost, etc.

Implementing an efficient but low-cost QKD system is quite challenging. It is important to keep security analysis in mind as QKD is perfectly secure in theory, but in practice, imperfections in tools like single-photon detectors create many security vulnerabilities [15]. QKD systems protocols are vulnerable to attacks over the quantum channel, including authentication failures, intercept/resend (measuring and replacing photons), photon number splitting (stealing photons), and blinding optical receivers (unauthorized laser sources) [16]. Current hardware technologies are still lacking when it comes to using features of QKD, in specific, and Quantum Computing, in general, to their full potential.

When it comes to increasing the distance that can be covered or the communication range of a QKD model, the results are not exactly satisfactory. For distances beyond 50kms (approx.), the noise becomes so great that error rates also increase drastically which leaves the channel very vulnerable to eavesdropping

and makes the channel virtually impossible to send information **[2]**.

For QKD systems to be used in real world applications, low cost and robustness are indispensable features alongside high performance **[17]**. Unfortunately, the implementation of QKD models is far from being low-priced. The hardware requirements are quite advanced and are neither easily available nor they are cheap. In summary, the current hardware limitation serves as the anchor when it comes to QKD systems being used more widely and frequently.

VII. CONCLUSION

This paper started by mentioning how classical cryptography is vulnerable to several security breaches and potential eavesdropping while QKD models deliver unconditional security. Thus, observing the need for Quantum Cryptography using Quantum Key Distribution when it comes to secure communication. The authors further covered the working mechanism of QKDin details and a few QKD protocols in brief. Finally, the authors shed some light on the current limitations of QKD. In conclusion, it can be said that although it is a positive step towards secure and future-proof communications, it is highly limited by current technologies. Only with technological advancements in the future, can QKD systems become more feasible and practical as the hardware requirements will be readily available and moderately priced.

VIII. REFERENCES

[1]. Hitesh Singh, D.L. Gupta, A.K Singh, "Quantum Key Distribution Protocols: Review", 2014. Online].Available:https://www.researchgate.net/publication/269750731_Quantum_Key_Distribution_Protocols_A_Review

[2]. N.Sasirekha, M.Hemalatha, "Quantum Cryptography using Quantum Key Distribution and its Applications", issn: 2249=8958, Volume -3, Issue-4, 2014.

[3]. YoshitoKannamori, Seong-Moo Yoo, Frederick T.Sheldon, "Bank Transfer over Quantum Channel with Digital Checks". Online]. Available:https://www.csm.ornl.gov/~sheldon/public/KanamoriYooSheldon-GlobeCom06.pdf

[4]. HajirPourbabak, WencongSu, "Quantum Channel", 2019. Online]. Available: https://www.sciencedirect.com/topics/engineering/quantum-channel

[5]. Hitesh Singh, D.L. Gupta, A.K Singh, "Quantum Key Distribution Protocols: A review", e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. XI, 2014. online]. Available: https://www.semanticscholar.org/paper/Quantum-Key-Distribution-Protocols%3A-A-Review-Singh-Gupta/86a29ccc18f226ad8e153b714f78736d4f3e6365

[6]. Riaz Ahmad Qamar, MohdAizainiMaarof and Sobariah Ibrahim, "First Tour to Quantum Cryptography", Volume -2, Number -2, 2011. Online]. Available: https://www.researchgate.net/publication/268354440_First_Tour_to_Quantum_Cryptography

[7]. David Deutsch, Artur Ekert, Richard Jozsa, Chiara Macchiavello, Sandu Popescu, Anna Sanpera1, "Quantum Privacy Amplification and the Security of Quantum Cryptography over Noisy Channels," Physical Review Letters, Vol. 77, No. 13, 1996.

[8]. Charles H. Bennett, Gilles Brassard, Claude Crkpeau, Ueli M. Maurer, "Generalized Privacy Amplification," IEEE Transactions on Information Theory, Vol. 41, No. 6, pp. 1915-1923, 1995.

[9]. Yodai Watanabe, "Privacy Amplification for Quantum Key Distribution," Publishing Journal of Physics A: Mathematical and Theoretical 40, 2006.

[10]. Ergun Gumus, G.Zeynep Aydin, M.Ali Aydin, "Quantum Cryptography and Comparison of Quantum Key Distribution Protocols," Journal of Electrical & Electronics Engineering, Istanbul, 2008.

[11]. D.Bouwmeester, A. Ekert, A. Zeilinger (Eds), "The Physics of Quantum Information", Lec - 12. Online]. Available: https://mpl.mpg.de/fileadmin/user_upload/Chekhova_Research_Group/Lecture_4_12

[12]. Valerio Scarani, SofyanIblisdir, Nicolas Gisin, Antonio Acin, "Quantum Cloning", 2005. online]. Available: https://arxiv.org/abs/quant-ph/0511088

[13]. Mart Haitjema, "A survey of the prominent Quantum Key Distribution Protocols", 2007. online]. Availabe: https://www.cse.wustl.edu/~jain/cse571-07/ftp/quantum/#bb84

[14]. Gisin, N., Ribordy, G., Tittel, W., Zbinden, H., "Quantum Cryptography", Reviews of ModernPhysics, vol. 74, January 2002, pp. 146 - 195. online]. Available: http://www.gap-optique.unige.ch/Publications/Pdf/QC.pdf

[15]. Alexander S. Gillis, "Quantum Key Distribution", last updated 2020. online]. Available: https://www.techtarget.com/searchsecurity/definition/quantum-key-distribution-QKD

[16]. Logan O. Mailloux, Michael R. Grimaila, Douglas D. Hodson, Colin V. McLaughlin, Gerald B. Baumgartner, "Quantum Key Distribution: Boon or Bust?", 2016. online] Available: https://scholar.afit.edu/cgi/viewcontent.cgi?article=1168&context=facpub

[17]. Eleni Diamanti, Hoi-Kwong Lo, Bing Qi , Zhiliang Yuan, "Practical challenges in quantum key distribution", Article no- 16025, 2016. online]. Available: https://www.nature.com/articles/npjqi201625

Cite this article as :

Sagarmoy Ganguly, Asoke Nath, "A Comprehensive Study on Quantum Key Distribution ", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 7 Issue 6, pp. 393-401, November-December 2021. Available at doi : https://doi.org/10.32628/CSEIT12176101
Journal URL : https://ijsrcseit.com/CSEIT12176101

AUTHOR PROFILE

Mr. Sagarmoy Ganguly is currently a student at St. Xavier's College, pursuing his M.Sc. degree in Computer Science. His interests lie in the field of Quantum Computing, Machine Learning, Coding, Cyber Security, AI, Computer Hardware, and real-world implementation of said fields.

Dr. Asoke Nath is working as Associate Professor in the Department of Computer Science, St. Xavier's College (Autonomous), Kolkata. He is engaged in research work in the field of Cryptography and Network Security, Steganography, Green Computing, Big data analytics, Li-Fi Technology, Mathematical modelling of Social Area Networks, MOOCs, Quantum Computing etc. He has published 257 research articles in different Journals and conference proceedings.