[1]Rayudu Vinay Kumar,

2Matta Venkata Durga Pavan Kumar,

3Mamatha B,
4Akkisetti Vn Hanuman

Quantum IOT: Security and Communication Aspects

JES Journal of Electrical Systems

Abstract:

Conventional cryptography relies only on the robustness of mathematical principles. Advancements in quantum computing may use reversible logic to calculate keys and easily compromise the security of traditional computers. The examination of the Internet of Things (IoT) network topology reveals that the whole system's backbone would disintegrate if subjected to an assault or hacking attempt. The Internet of Things (IoT) is a wireless technology that links various objects to the Internet. The Internet of Things (IoT) represents a revolution that must be safeguarded from attackers, since breaches might result in significant, perhaps deadly losses. Consequently, ensuring robust protection of user data in IoT is a significant problem. This study aims to explore the principles of Quantum Key Distribution, examine security considerations for the Internet of Things, and discuss the use of QKD in securing IoT systems. The problem faced is to enhance the range and transmission rate of data in Quantum Key Distribution (QKD) systems, while also exploring potential methods to integrate these systems with current information security measures.

***Index Terms*—** Eaves dropping , Internet of Things , Protocols, Quantum Cryptography, Quantum Key Distribution.

INTRODUCTION

The connectivity of several devices communicating over the internet, facilitating data flow among people, machines, and inter-machine interactions, is termed the "Internet of Things." The Internet of Things (IoT) seeks to enhance daily living quality but encounters significant risks to the sensitive and vital data transmitted online [1]. Eavesdropping is a significant issue that cannot be identified by standard cryptography methods. The use of Quantum Mechanics concepts to cryptography has facilitated a remarkable method of secure communication. Quantum cryptography is an emerging field in the history of secure communication. The users generate a collective secret random bit string, applicable as a key in cryptographic contexts. The robust security of Quantum Key Distribution (QKD) is grounded on the basic principles of quantum physics, in contrast to traditional cryptography, which relies on unverified computational assumptions. The security of Quantum Key Distribution (QKD) is based on the principles of quantum physics rather than computing capabilities. This is infuriating because measuring a photon always alters its behavior. Although quantum cryptography may seem to be a concept from future science fiction, several firms are diligently striving to convert the theoretical into a scalable, commercially viable product.

[1] [1,2,3,4]International School of Technology and Sciences for Women, A.P, India.

Quantum key distribution relies on the notion that continuous observation alters the observed entity, making the interception of communication between two nodes impractical. Therefore, Quantum Key Distribution (QKD) is impervious to breaches in accordance with the principles of Quantum Mechanics. Quantum Key Distribution (QKD) employs basic particles, namely photons, to provide unbreakable secure keys for data protection. Numerous cryptographic techniques have been presented in the literature to protect IoT networks; however, improvements in Quantum Computing (QC) represent a danger to these current systems. There is a pressing need for quantum-resistant technologies to safeguard IoT devices.

Related Work

Initially, it started with the One Time Pad developed by Vernam, which required a key as lengthy as the plaintext, presenting significant challenges in implementation. This was succeeded by stream ciphers and several other cryptographic methods, including RSA, till the present day. All these techniques operate on the premise of mathematical or computational security; specifically, if the key length is sufficiently extensive, even supercomputers would need hundreds or thousands of years to decipher a message.

In the early 1970s, Stephen Weisner proposed the notion of Quantum Cryptography, and in 1984, scientists Bennett and Brassard introduced the first quantum cryptography protocol known as “BB84,” which was demonstrably safe. In 1991, Ekart introduced the encryption method "E91," which used EPR pairings (Einstein–Podolsky–Rosen). In 1992, Bennett proposed the "BB92" protocol, demonstrating that two non-orthogonal states are enough for Quantum Cryptography. In 1999, the Six State Protocol (SSP) used three orthogonal bases for communication with the BB84 algorithm. The "SARG04" protocol, established in 2004, demonstrated an increase in the Quantum Bit Error Rate (QBER) of BB84 when employing attenuated laser pulses instead of a single photon source. [11] An enhancement in security against Photon Number Splitting attacks was observed. [10] In the same year, the Coherent One Way Protocol (COW) exhibited elevated bit rates for weak coherent pulses, leading to enhanced efficiency of distilling secret bits per qubit. 12

The "KMB09" protocol employs two bases for encoding binary values 1 and 0, rather than using two routes from a single base, resulting in reduced eavesdropping and an increased system error rate, all while maintaining user privacy. [13] Shor's method, which facilitates the factorization of prime numbers, has the potential to compromise the RSA algorithm, generating significant attention among academics due to its implications for computing complexity, therefore demonstrating that quantum computers may surpass their conventional counterparts in capability. [15]

Security Challenges In IOT

The expansion of Industrial IoT is accelerating continuously, along with its weaknesses. According to a report by Techsynt Solutions in November 2017, significant cyberattacks against IoT devices and protocols occurred without exposing users' personal data or credentials; nevertheless, a more damaging incident might transpire in the future. [14] Consequently, there is a need for comprehensive security analysis as a high priority, along with the development of algorithms to protect the network. The problems that security specialists must consider include i) safeguarding user data in accordance with privacy and compliance regulations. ii) Frequently updating all IoT devices iii) Ensuring adherence to embedded technology security regulations by integrating all IoT services iv) Enhancement of consumer impression about the use of IoT devices v) Management of devices.

The primary focus among these issues is preserving the security and confidentiality of data sent over IoT. Optimal security may be attained by integrating all components of an IoT ecosystem for protective measures—utilizing cutting-edge encryption, robust passwords, and the most current iterations of software and hardware on the device. However, with the advancement of quantum computers, classical algorithms like as DES, AES, and ECC will become inadequate. All these methods entail the exchange of keys between end users, which is the primary security vulnerability. The notion of Quantum Key Distribution emerges, relying on Quantum Mechanics to provide unconditional security between communication parties, impervious to eavesdropping techniques [4].

Security Issues In IOT

The advancement of 'IoT-enabled communication' has been propelled by the adoption of innovative technologies across several domains, including smart agriculture, advanced healthcare, and intelligent urban environments. Devices inside the 'Internet of Things (IoT)' that provide these applications transfer huge quantities of data across many contexts. The expansion of IoT applications results in an increase in cyber-attacks. Furthermore, it presents possible risks to the confidentiality and privacy of users. The primary security issues related to the 'IoT' ecosystem include verification, authorization, integrity, and trust management. Figure 2 depicts significant security issues within the layered architecture of IoT. This section examines the potential risks to the IoT infrastructure and the advantages of including the 'Quantum Layer' to enhance IoT security.

‘Sensing Stratum’

This layer integrates many sensing technologies, including Wireless Sensor Networks (WSN), Radio-Frequency Identification (RFID), and Global Positioning System (GPS), to support Internet of Things (IoT) applications. Each of these technologies contributes to the management of IoT actuators and sensors. Sensors are used to gather information from the environment, including ultrasonic, visual, and thermal detection. The sensing layer is vulnerable to several types of attacks, including sensor node acquisition, insertion of fraudulent data codes, eavesdropping, and sleep deprivation attacks.

Network Layer

‘Computational Units’ are essential for processing data obtained from the foundational layer, namely the ‘Sensor Layer’. The primary role of the Network Layer is to transmit data obtained from the Sensor Layer to the processing units.

Processed data is crucial for facilitating IoT applications. Nonetheless, unlimited internet connection renders 'Network Layers' susceptible to significant security vulnerabilities, including access control breaches, Denial of Service attacks, and data transfer assaults. Quantum Layer

Difficulties Associated With Quantum based

Internet Of Things (IOT)

‘Quantum Key Distribution’: It offers a reliable method for transmitting cryptographic keys. Assuming, however, that the detection of an illegal listener on the 'quantum communication' channel occurred. In such cases, the whole method is rendered invalid, and subsequent communication will not resume until all information interception is entirely eliminated from the channel.

Mass communication among Internet of Things (IoT) users via the quantum channel is problematic due to the limited range of Quantum Key Distribution (QKD) for short-distance communication.

‘Quantum Reversible Computing’: The presence of an adversary poses a significant threat to quantum-based reversible computing.

‘Cybersecurity Breach’: Quantum-based communication is susceptible to targeted assaults. In this situation, the assailant establishes a new 'quantum channel' by intercepting a 'quantum signal' sent between Alice and Bob.

Quantum Cryptography Preliminaries

Quantum Cryptography involves the transmission of light waves by photons across a fiber optic cable or open air in a point-to-point manner. Quantum Key Distribution transmits random keys by quantum cryptographic mechanisms, followed by the use of traditional encryption for secure communication. The quantum system processes information using quantum bits, or qubits, which may simultaneously represent 0 and 1 in a condition referred to as superposition. The polarization capability of a photon enables it to function as a secret key. The data associated with photon spin may be used to generate binary information. Photons may be polarized to one of four angular orientations: 0º, 45º, 90º, and 135º. The zero and 90º polarizations are designated as the rectilinear basis, whereas the 45º and 135º polarizations are termed the diagonal basis.

Two ideas of Quantum Mechanics provide this absolute assurance.

1. Superposition principle: A system may simultaneously inhabit all conceivable states. Qubits may exist in two states concurrently, allowing them to store far more information with lower energy consumption compared to traditional bits. The magnitude of the superposition increases exponentially with the quantity of particles.
2. No-Cloning Theorem: Copying an unknown quantum state is impossible. Quantum physics imposes stringent constraints on the accuracy of measurements. The No-Cloning Theorem facilitates secure communications. For instance, assume two individuals, Alice and Bob, transmitting quantum states of light (photons) to one another; an eavesdropper, Eve, is unable to quantify these photons without causing disturbance. Ultimately, they get a cryptographic key composed of shared random bits, yielding flawless encryption.

Quantum Key Distribution

Alice, the sender, picks a random binary value, which is then submitted to a polarizer with randomly chosen bases. The polarized photons, serving as the secret keys, are sent over a quantum channel to the recipient, Bob. Bob transforms the photons into binary digits. A diagonally polarized picture, when transmitted via a rectilinear polarizer, has a 50% possibility of being selected as either horizontally or vertically polarized, and vice versa. Consequently, some bits are altered, omitted, or modified owing to various disruptions during transmission. Alice and Bob converse on a public channel about the procedures used to get the necessary keys and to ascertain the existence of an eavesdropper. Following the debate, some bits are eliminated, and the remaining bits form the shared key. Quantum Key dissemination (QKD) guarantees the safe dissemination of a one-time key exchange.

Results

This section encapsulates the results from the examined system and the feasibility of implementing our proposed approach. As outlined in Section IV, we devised a post-quantum technique that allows IoT devices to produce any post-quantum cryptographic key, irrespective of key size.

We assessed our system based on three criteria: execution time, optimum device count, and submatrix threshold size (i.e., the minimum size at which our method continues to partition a matrix).

A. Influence of Matrix Dimensions on Execution Duration

Given that McEliece's post-quantum cryptography key generation and encapsulation procedures rely significantly on matrix multiplications and inverses, we developed a simulation software to address this aspect. Table I presents the execution computational time on a single IoT device compared to three IoT devices. Table I indicates that the processing time on a single Raspberry Pi is consistently slower than that on three Raspberry Pis. This outcome enables us to assert with confidence that our suggested strategy, Q-SECURE, enhances computation time when using several IoT devices inside a distributed and parallel computing network system. The same conclusion is shown in Fig. 4. The execution duration on a single Raspberry Pi exceeds that of our Q-SECURE environment, which is dispersed over three Raspberry Pi devices.

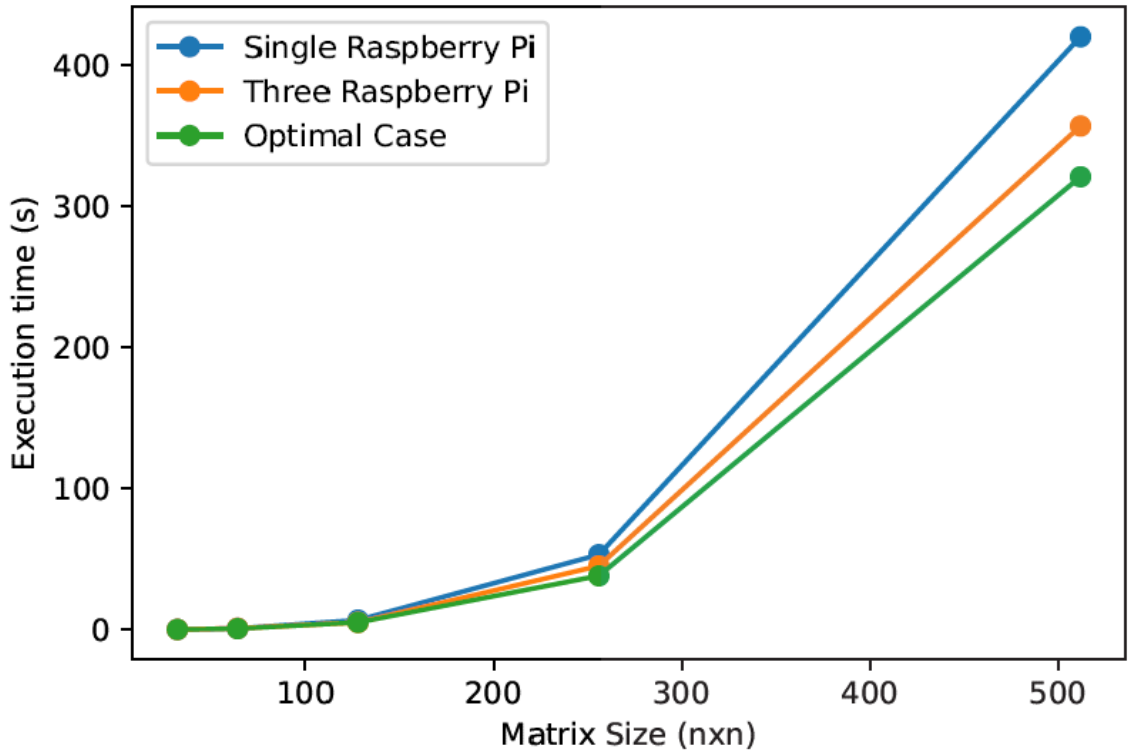

Fig. 1. The execution time at different number of devices (Raspberry Pis).

B. Influence of Device Quantity on Execution Duration

The last phase of our assessment involves determining the ideal quantity of IoT devices required to do a designated job in the minimum time frame. To do this, we established a network of various devices, including Raspberry Pis and virtual computers. The virtual machines are designed with reduced CPU power and little memory to closely resemble those of Raspberry Pis. Our investigation indicates that for a certain matrix size, a predetermined quantity of IoT device assistants must be solicited by the client to optimize execution time. The outcome is seen in Fig. 5.

We defined a square matrix M of dimension 256. Figure 5 illustrates that four devices (three IoT assistants and one client) are required to calculate a key generation of size 256 in about 40.2 seconds.

Our experimental findings in Fig. 5 reveal the appropriate quantity of IoT devices corresponding to various matrix sizes that provide the minimal execution time. Figure 6 illustrates that the ideal quantity of IoT devices required escalates with the augmentation of the matrix size.

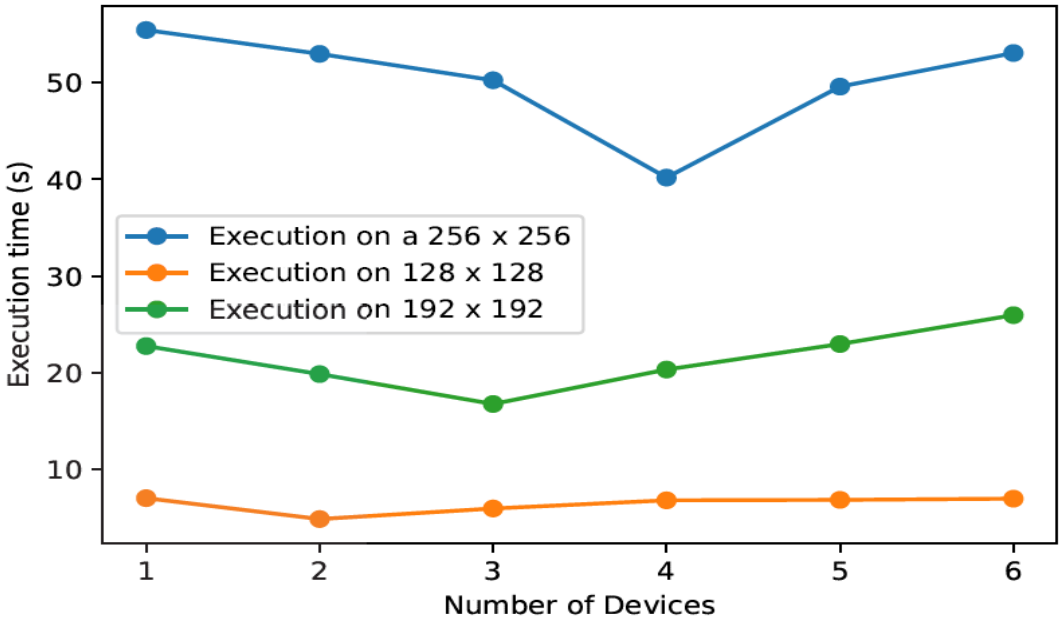

Fig. 2. The key generation time in different numbers of devices.

C. Influence of Submatrix Size Threshold on Execution Duration

The ideal submatrix size, referred known as the threshold, is the dimension M of the input matrix that activates our program's divide and conquer method. A threshold is a variable parameter that may vary based on the hardware and the dimensions of the matrices for which the determinant and inverse are calculated. The threshold should be calibrated to ensure that, for smaller matrices, the recursive computation is more efficient than the factorization of a lower triangular matrix (L) and an upper triangular matrix (U), often referred to as LU decomposition. Nonetheless, it is not sufficiently huge to impede memory or processing time for bigger matrices.

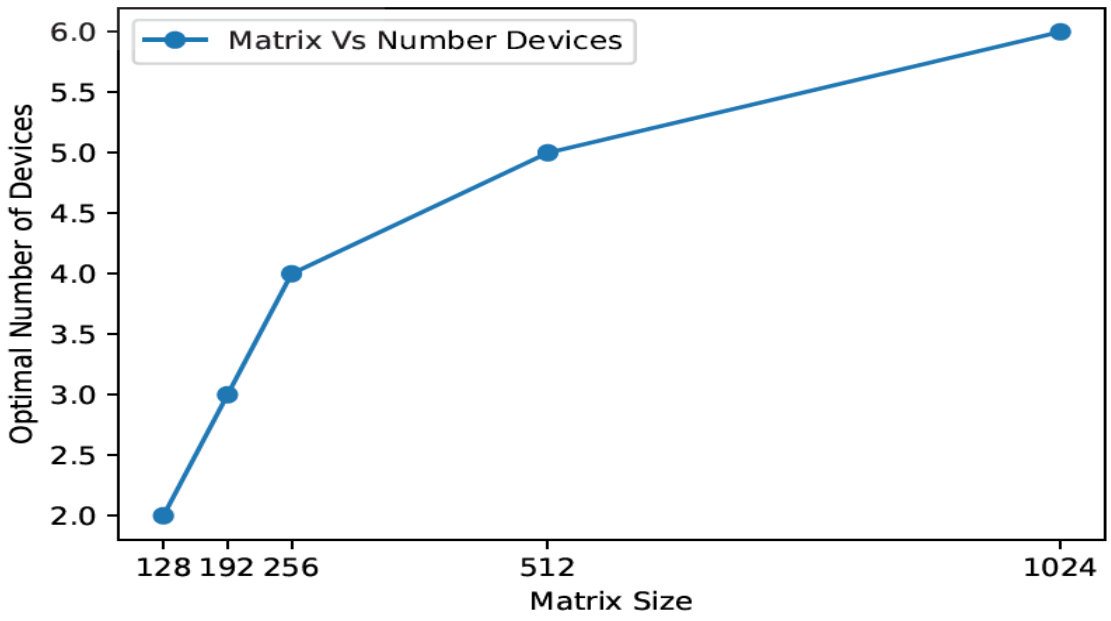

Fig. 3. The optimal number of devices for different matrix sizes.

Conclusion

IoT is going to be a major utility with a vision to facilitate sensing, actuation, communications, control of vast amounts of data from varied applications and sources. Quantum communication forms the core idea for a universal secured IOT.[9] This idea of a highly secure network opens doors to many future possibilities. QKD is a viable solution to counter the threats that may appear in future from quantum computers thereby securing all IOT related applications. Also QKD is an essential element for building a quantum safe infrastructure including quantum-resistant classical algorithms and quantum cryptographic solutions.

Based on the preceding section, it can be inferred that scholars have conducted studies in several domains utilizing a range of techniques and algorithms. The researchers presented key aspects pertaining to the assessment of their proposed methodologies. The IoT is the interconnectedness of various devices, allowing them to communicate with one other. This connection offers several benefits to customers by simplifying decisionmaking processes. It is imperative that such technology, which encompasses vital information in areas such as healthcare, smart cities, and military applications, is fortified with robust security measures. There are several traditional cryptographic primitives that guarantee secure communication by depending on ‘complex mathematical structures’. The security offered by ‘traditional cryptographic architecture’ is no longer dependable due to its susceptibility to 'Quantum Computing' assaults. Hence, connectivity provided by IoT necessitates the implementation of quantumbased security measures in order to withstand potential quantum attacks in the future. Our survey focused on examining quantum-based cryptographic protocols designed to enhance the security of IoT connectivity. This article provides a thorough analysis of ‘security attacks’ on ‘Internet of Things (IoT)’ applications. The paper explores strategies that can resist quantum assaults in order to safeguard IoT communication, quantum authentication techniques, quantum key distribution (QKD), and the difficulties encountered in deploying quantum-enabled IoT communication. Therefore, this work provides significant suggestions for future ‘IoT’ researchers to include ‘quantum-resistant technologies’.

References

1. Ashvini Kamble, Sonali Bhutad, “ Survey on IOT Security Issues and Solutions” IEEE Xplore compliant , ICISC2018,ISBN : 97-1-5386-0807-4.
2. Z. L. Yuan, A.W. Sharpe, A. J. Shields, “Unconditionally secure quantum key distribution using decoy pulses,” Appl. Phys. Lett. 90, 011118, 2007.
3. C.H. Bennett, G. Brassard, Quantum cryptography: public key distribution and coin tossing, in: Proc. of International Conference on Computers, Sys-tems, and Signal Processing, Bangalore, India, 1984, pp.175–179.
4. Aysajan Abidin , Jan-˚ake Larsson “Vulnerability Of “A Novel Protocol-Authentication Algorithm Ruling Out A Man-In-The-Middle Attack In Quantum Cryptography” Int.Journal of Quantum Information , 2009, pp 1401-1407.
5. Bennett, Ch., and Brassard, G.: Quantum Cryptography Using Any Two Non-Orthogonal States. Physical Review Letters, Vol. 68, Issue 21, pp. 3121—3124 (1992).
6. D. Mayers, Unconditionalsecurity in quantum cryptography, J. ACM 48 (2001) 351; eprint arXiv:quant-ph/9802025.

7. E. Biham, M. Boyer, P.O. Boykin, T. Mor, V. Roychowdhury, A proof of the security of quantum key distribution, in: Proceedings of the Thirty Second Annual ACM Symposium on Theory of Computation, 2000, pp.715–724; arXiv:quant-ph/9912053.
8. P.W. Shor, J. Preskill, Simple proof of security of the BB84 quantum key distribution protocol, Phys. Rev. Lett. 85 (2000) 441–444; eprint arXiv:quant-ph/0003004.
9. John A. Stankovic ”Research Directions for Internet of Things”, IEEE Internet Of Things Journal, Vol. 1, No. 1, February 2014
10. V. Scarani, A. Acin, G. Ribordy, N. Gisin, “Quantum cryptography protocols robust against photon number splitting attacks for weaklaser pulse implementations”, *Physical review letters*, vol. 92, pp. 057901, 2004. [Online]. Available: http://dx.doi.org/10.1103/PhysRevLett.92.057901
11. Chi-Hang Fred Fung, Kiyoshi Tamaki, and Hoi-Kwong Lo, “On the performance of two protocols: SARG04 and BB84”, arXiv:quant-ph/0510025v2 12 Oct 2005.
12. Mhlambululi Mafu, Adriana Marais, Francesco Petruccione “Towards the unconditional security proof for the Coherent-One-Way protocol”
13. Syed.S.Hussain, Muhammed M.Khan, Mirza M.Baij, G.Wang, “ Numerical Modelling of Quanutum Key Distribution Ssytem for KMB09 Protocols”, International Journal of Computer science and Information Security, Vol.14, No Aug 2016.
14. Ashvini Kamble, Sonali Bhutad, “Survey On Internet Of Things (Iot) Security Issues & Solutions “,Proceedings of the Second International Conference on Inventive Systems and Control (ICISC 2018) IEEE Xplore Compliant - Part Number:CFP18J06-ART, ISBN:978-1-5386-0807-4
15. Eleanor Rieffel , Wolfgang Polak, “An Introduction to Quantum Computing for Non-Physicists”, arXiv:quant-ph/9809016v2 19 Jan 2000.
16. Anindita'Banerjee, Anil'Prabhakar, Mark'R'Mathias, “ Quantum Key Distribution – A Technology Review” , Journal on Defence Information and Communication Technology Vol 3 No 1 2017
17. Valerio Scarani, Helle Bechmann, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus, “ The Security of Practical Quantum Key Distribution”, Reviews Of Modern Physics, Volume 81, July–September 2009.
18. Mhlambululi Mafu and Makhamisa Senekane , “ Security of Quantum Key Distribution Protocols”, http://dx.doi.org/10.5772/intechopen.74234
19. Akshata Shenoy, Anirban Pathak, Srikanth Radhakrishna, “ Quantum Cryptography: Key Distribution and Beyond”, arXiV:102:05517v1 [quant-ph] 15 Feb 2018.
20. Sayanta Gupta, Chayan Dutta, “ Internet of Things Security Analysis of Networks Using Quantum Key Distribution” , Indian Journal of Science and Technology, Vol 9 (48), Dec 2016.
21. Krithika.S, “Quantum Key Distribution (QKD): A Review on Technology, Recent Developments and Future Prospects”, Research J. Engineering and Tech. 8(3): July-September 2017.