APPLICATION OF QUANTUM CRYPTOGRAPHY TOWARDS PROTECTION OF DATA

J Component Project

Submitted for the course:

INFORMATION SECURITY ANALYSIS AND AUDIT (CSE3501)

SLOT: F1

Amirth Raj
20BCE0902

Snehil Sinha
20BCE2005

Anshuman Gupta
20BCE2119

B.Tech. Computer Science and Engineering

Submitted to

Dr. Aju D

School of Computer Science and Engineering

Vellore Institute of Technology

Vellore

November, 2022

Abstract

1. Motivation-
   In today's time, one of the major concerns in this digital world is keeping our information safe and secure. For data safety in the future, a time period in which it is anticipated by experts that malicious digital adversaries will have even more access to powerful machines and newer algorithms, information security will be at an all-time risk and therefore would be extremely crucial to protect.

2. Aim-
   The development of various computer communication networks has led to an increase in instances of computer vulnerability and cybercrime. Most firms are therefore under extreme pressure to safeguard their assets. The confidentiality/integrity of traffic transmitted across digital networks can be secured using contemporary cryptosystems**.** This paper concentrates on quantum cryptography which applies the use of quantum mechanics, with the aim of using this technology to contribute toward network security.

3. Methodology-
   Quantum Cryptography is a technology that was born from the usage of contemporary cryptosystems for network security. The most advanced cryptosystems based on mathematical models expose many security weaknesses. For that reason, efforts have been made to establish a new foundation for cryptography science in computer communications networks. One of these efforts has led to the development of quantum cryptography technology, whose security relies on the laws of quantum mechanics. The methods that we aim to apply to our paper based on Quantum Cryptography are Quantum Key Distribution and RSA Algorithm.

4. Expected Outcome-
   Through this project what we expect to achieve is an implementation of quantum cryptography techniques to the current encryption algorithms by usage of quantum key distribution and RSA algorithm. This in turn will give us more protection against attacks that cyber criminals use by utilizing quantum computers and maliciously employing algorithms like Shor's algorithm and Grover's algorithm.

Keywords: — *Quantum computers; Quantum Key Distribution; RSA Algorithm; Post Quantum Cryptography; Shor's Algorithm; Grover's Algorithm*

Introduction

A vulnerability when it comes to computer security is a flaw that an attacker can use to carry out unauthorized operations on a computer system. An attacker needs just one technique or tool that can reach a system's flaw to exploit the vulnerability. The development of quantum computers, which are used to launch effective assaults against established methods like the popular types of public key cryptography, is particularly concerning. In Quantum cryptography, Quantum key distribution (QKD), offers a set of protocols that includes quantum key distribution, quantum random number generation, closed group digital signatures, long-term secure data storage, and multi-party secure computation, that can be resistant to future algorithmic and computational advances which include the emergence of malicious use of quantum computers. As long as the encryption key can be exchanged with complete security assured, quantum cryptography is secure. Quantum cryptography ensures that the act of an eavesdropper intercepting a photon, even if it's merely to see or read it, irrevocably changes the information encoded on that photon by delivering the key encoded at the single photon level on a photon-by-photon basis.

To ensure high security in making sure data cannot be deciphered, encryption would function like a trapdoor, making it easy to move forward but difficult to go back to. RSA algorithm is among the most well-known trapdoors for this purpose. The data is encrypted using a key, and the key is created by multiplying several prime numbers.

But Shor's algorithm gave rise to a brand-new issue in the world of cryptography. A quantum algorithm is employed to decrypt RSA. The following assaults and their corresponding defenses against a common QKD system are as follows: the Trojan-horse attack, multi-photon emission, imperfect encoding, bright-light attack, back-flash attack, efficiency mismatch, and time-shift attack.

The Heisenberg uncertainty principle is heavily utilized in quantum cryptography technology to ensure secure cryptography. Quantum cryptography exploits the laws of quantum physics to guarantee the confidentiality of data transmission.

Latest studies have shown how quantum computers have evolved and are within a realm of reality where we will be able to make one of our own. In fact, there are already a number of these prototypes. Consequently, we now have a new problem. Buchanan and Woodward discuss how almost all of the current encryption algorithms, which were created primarily in the hope that the key couldn't be calculated due to the significant computational power needed, are now rendered obsolete by the advent of quantum computers due to their extremely high computational power.

In this project, we would like to try to implement quantum cryptographic algorithms in addition to the existing encryptions in order to secure the data against malicious attacks that are made possible by utilizing quantum computers and algorithms like Shor's Algorithm and Grover's Algorithm. Some of the methods employed by quantum cryptography are

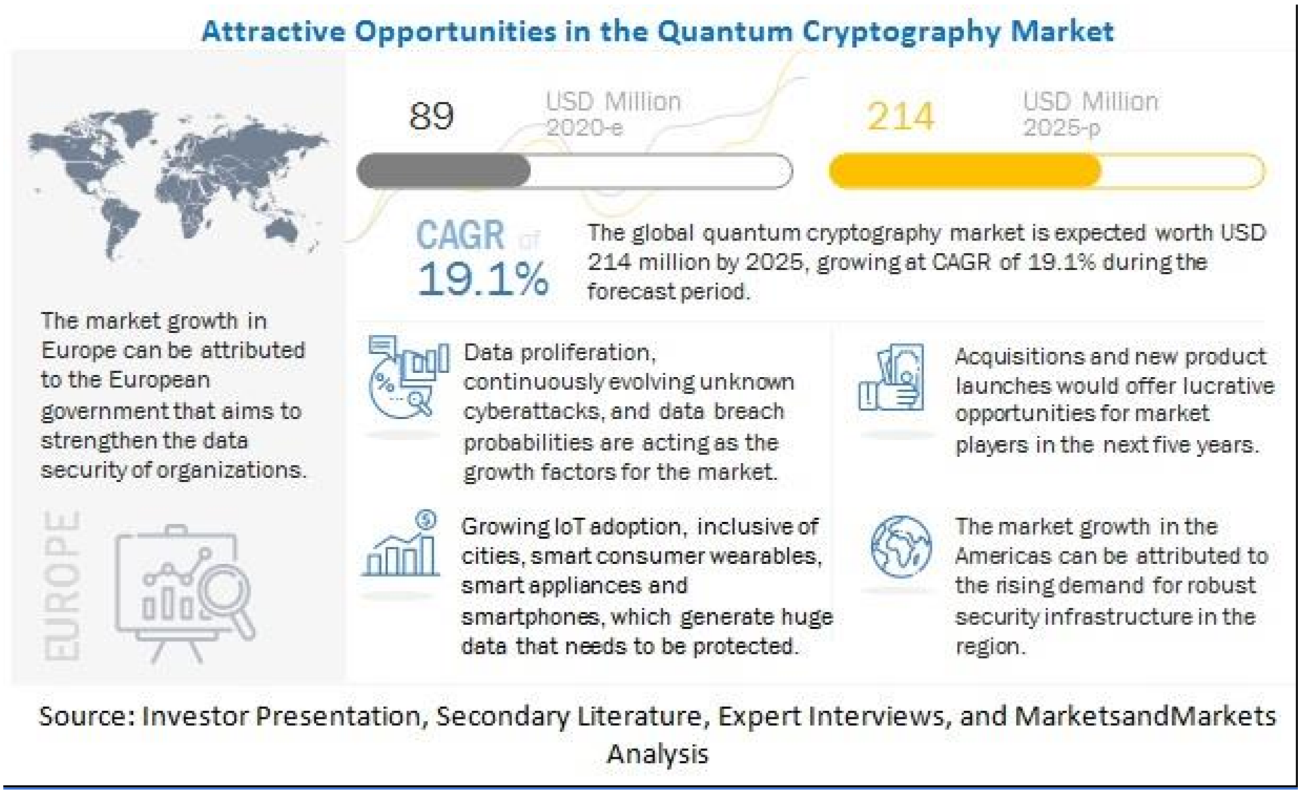
- Post Quantum Cryptography: Quantum computers may become a technological reality; it is, therefore, important to study cryptographic schemes used against adversaries with access to a quantum computer. The study of such schemes is often referred to as post-quantum cryptography.

- BB84 Protocol: The BB84 method is the basis of quantum key distribution methods. Instead of mathematical bits, quantum computers use photons for encryption and decryption and for transferring data.
- Quantum Key Distribution: The best-known method of quantum cryptography is quantum key distribution (QKD), which is the process of using quantum communication to establish a shared key between two parties without a third party.

- Mistrustful Cryptography: In mistrustful cryptography, the participating parties do not trust each other. Mistrustful quantum cryptography studies the area of mistrustful cryptography using quantum systems.

Some Statistics:

Source:https://www.marketsandmarkets.com/Market-Reports/quantum-cryptography-market-45857130.html#%3A~%3Atext%3D%5B158%20Pages%20Report%5D%20The%20global%2Cat%20a%20CAGR%20of%2019.1%25



Quantum cryptography is expected to have a market size of USD 214 million in 2025, with a CAGR of 19.1%. The global quantum cryptography market is anticipated to grow as a result of the rising number of cyberattacks in the digital age, causing a rise of cybersecurity funding, causing a rising demand for next-generation security solutions for cloud and IoT technologies, and developing next-generation wireless network technologies.

Since 2007, Switzerland has been using quantum cryptography to conduct secure online voting in federal and regional elections. In Geneva, votes are encrypted at a central vote-counting station. Then the results are transmitted over a dedicated optical fiber line to a remote data storage facility. The voting results are secured via quantum cryptography, and the most vulnerable part of the data transaction when the vote moves from counting station to central repository is uninterruptible. This technology will soon spread worldwide, as many other countries face the specter of fraudulent elections.

https://www.networkworld.com/article/2286834/quantum-cryptography-to-secure-ballots-in-swiss-election.html

Literature Survey / Related Works

Title of the paper	Authors	Challenges	Methodology	Applications	Pros	Cons
1) Quantum Cryptography: A New Generation of Information Technology Security System	Mehrdad S. Sharbaf Grad. Sch. of Comput. & Inf. Sci., Nova Southeastern Univ., Fort Lauderdale, FL	One of the challenges for the researchers, is distance limitation. Currently, quantum key distribution distances are limited to tens of kilometers because of optical amplification destroys the qubit state, and also to develop optical device capable of generating, detecting and guiding single photons; devices that are affordable within a commercial environment. Another issue is the lack of a security certification process or standard for the equipment.	BBN, Harvard, and Boston University built the DARPA quantum network, the world's first network that delivers end-to end network security via highspeed quantum key distribution and tested that network against sophisticated eavesdropping attacks [9,10,11].This network is suitable for deployment in metro-size areas via standard telecom (dark) fiber. This network allows users at BBN Technologies, Harvard University, and Boston University	Currently, quantum key distribution distances are limited to tens of kilometers because of optical amplification destroys the qubit state, and also to develop optical device capable of generating, detecting and guiding single photons;	The advances in computer processing power and the threat of limitation for today's cryptography systems will remain a driving force in the continued research and development of quantum cryptography. The technology has the potential to make a valuable contribution to the network security among government, businesses, and academic environment	Realization of practical quantum information technologies cannot be accomplished without involvement of the network research community

		Also users need reassurance not only that QKD is theoretically sound, but also that it has been securely implemented by the vendors. Overall, the theoretical and experimental results will present a main impact, in near future, on the process of commercialization on of the QKD systems.	to tap into a fiber-optic loop secured by a quantum cryptography system. The DARPA security model is the cryptographic virtual private network (VNP). To achieve confidentiality, and authentication/ integrity, the conventional VPNs use public-key and symmetric cryptography. Public key mechanism support key exchange or agreement and authenticate to endpoints. Symmetric mechanism (e.g., 3DES, AES) provide traffic confidentiality and integrity. In DARPA			

			quantum cryptography network, existing VPN key agreement primitives are augmented or completely replaced by keys provided by quantum cryptography.			
2) Quantum cryptography for IoT: A Perspective	Sudhir K. Routray ; Mahesh K. Jha ; Laxmi Sharma ; Rahul Nyamangoud ar ; Abhishek Javali ; Sutapa Sarka	One of the challenges for the researchers, is a hybrid network such as hybrid fiber coax or fiber digital subscriber line combination cannot provide the same level of security. In the wireless domain, the key distributions are done as mentioned. Thus, the implementatio ns of QC at different levels have to be carefully chosen for different network	In QC, a bit of quantum of information is called a ‘qubit’. Here a photon is characterized using its plane of polarization, ranging from 0° to 180°. QC uses the property that if a diagonally polarized photon is passed through a linear polarizer it randomly ‘chooses’ either the horizontal or vertical state of polarization with a probability	Internet of things (IoT) is going to be an integral part of our lives in the next few years and can be used in all iot projects.	QC is a robust security technology. It can handle the security threats which are supposed to emerge from the quantum computers of the future. No other solution is visible currently which can be compared with QC. It is very much suitable for the IoT related applications. IoT will enter in to all critical aspects of	The implementations of QC at different levels have to be carefully chosen for different network configurations

		configurations.	of 0.5. The representation of bits through polarized photons is the foundation of quantum cryptography, known as Quantum Key Distribution (QKD). In QKD the encryption key is transmitted through quantum channel to the end users. In this case, two types of channels are used: (a) Quantum channel: to transmit the secret key and (b) Public channel: used by the end users(usually in literature, Alice, the transmitter and BOB, the receiver) to verify if the transmitted key is distorted		connected living and smart environment. In the future, IoT applications will be pervasive and the security for all these applications will be paramount. Under such intensely secure environment, QC is presumed to be ubiquitous.	

			indicating eavesdropping (presence of EVE). The polarization state of a photon is used to represent the bits.			
3) Quantum Photonic Network: Concept, Basic Tools, and Future Issues	Masahide Sasaki ; Mikio Fujiwara ; Rui-Bo Jin ; Masahiro Takeoka ; Te Sun Han ; Hiroyuki Endo ; KenIchiro Yoshino ; Takao Ochi ; Shione Asami ; Akio Tajima	One of the challenges for the researchers, is Quantum communicatio n and cryptography are to realize communicatio ns with higher capacity than the Shannon limit and unbreakable security, which cannot be possible with conventional technologies. Pursuing high capacity in optical communicatio ns, one has recently reached the quantum limited regime where the signals are densely packed in	WDM encoder and decoder structures. At Alice, optical pulses of 50-pswidth pass through a 2 × 2 asymmetric Mach–Zehnder interferometer of PLC, and are converted into the time-bin pulses with a 400 ps separation. The time-bin pulses are demultiplexed, and each wavelength component is independently encoded with the signal and decoy information. The	Quantum communication and cryptography are to realize communications with higher capacity than the Shannon limit and unbreakable security.	We have presented our recent results on GHz clocked BB84 QKD systems, entanglement QKD technologies, and the theories of QKD key rate bound and physical layer cryptography. Our QKD systems are deployed into practical metropolitical networks, and are integrated into the QKD platform for a new solution for key exchange and key supply.	Eventually the known schemes of QKD and prospective schemes of physical layer cryptography will be integrated on photonic network infrastructures to realize high capacity communications with the provable security. These schemes should cooperate with modern cryptographic technologies which are already operating in the upper layers. This new network paradigm is referred to as quantum photonic network. It indicates a direction to unify optical/ quantum communications with coding and

		the phase space so that quantum indistinguisha bility of the signal states becomes a matter. Further improvement to increase the rate in bits/s/ Hz/photon requires quantum engineering	signals are multiplexed again, together with the clock and frame synchronization signal, and input into a single fiber. At Bob, the clock signal is first separated, and the quantum signals pass through the PLC interferometer. They are then demultiplexed at each of the four ports, and finally detected by the photon detectors.		Entanglement QKD can be put into shorter distance links, such as important intranet works. The point-to-point QKD link performance, however, has the intrinsic limit as shown in Section III-E . Quantum repeater is yet to be met with the criteria for practical application to QKD.	cryptographic technologies, which is indeed an endeavour in information and communications technologies.
4) Quantum Cryptography: An Emerging Technology in Network Security	Mehrdad S. Sharbaf	One of the challenges for the researchers, is to develop optical device capable of generating, detecting and guiding single photons; devices that are affordable within a	The quantum-key distribution hardware box is claimed by MagiQ. to be the first commercially available quantum key distribution (QKD) system Another	The technology has the potential to make a valuable contribution to the network security among government, businesses, and academic environment.	An important and unique characteristic of quantum cryptography is the ability to detect the presence of any third party between two communicating users. The	developing more advanced hardware to enable higher quality and longer transmission distances for quantum key exchange. users need reassurance not only that QKD is theoretically sound, but also that it has been securely

		commercial environment. present that a particular problem for QDK is selling technology based on quantum mechanics to clients who often know little about physics and are used to traditional cryptography. Another issue is the lack of a security certification process or standard for the equipment.	product from MagiQ is QPN8505 to support external, customer supplied encryption engines. The QPN7505 supports the notion of splitting a secure LAN into physically separate network segments by inserting QPN7505s between the SONET Multi Service Switch (MSS) and the Ethernet Switch IDQ's Cerberis solution offers a radically new approach to network security, by combining the sheer power of high-speed layer 2 encryption appliances with the unconditio		security of quantum cryptography depends on the foundation of quantum mechanics, and that can revolutionize the network security QKD techniques can be married to standard internet technology in order to provide highly secure communications for practical use.	implemented by the vendors

			nal security of quantum key distribution (QKD) technology to secure point-to-point backbone and storage networks.			
5) Secure attribute-based data sharing for resource limited users in cloud computing	Jin Li, Yinghui Zhang, Xiaofeng Chen, Yang Xiang	Data sharing becomes an exceptionally attractive service supplied by cloud computing platforms because of its convenience and economy. As a potential technique for realizing fine-grained data sharing, attribute based encryption (ABE) has drawn wide attentions. However, most of the existing ABE solutions suffer from the disadvantages of high computation overhead and weak data	The notion of ABE, known as fuzzy identity-based encryption was proposed and applied in biometrics encryption by Goyal et al. In biometrics encryption application, the key extracted from the biometrics such as fingerprint will always different each time because of the biometric measurement noise during the extraction algorithm. With the technology of fuzzy identity based encryption,	In this section, we summarize the related works on ABE, online/ offline cryptography and outsourcing computation.	Aiming at tackling the computation efficiency and weak data security issues in cloud data sharing, we propose an attribute based data sharing scheme suitable for resource limited mobile users in cloud computing.	The proposed scheme supports online/ offline encryption modes and allows anyone to check the validity of ciphertexts before expensive full decryption. Even the computation task in offline phase is significantly reduced by adding system public parameters. The proposed scheme is proven secure in the proposed selective chosen attribute set and chosen ciphertext security model under the wDBDH assumption. Theoretical analysis and experimental results indicate that the proposed data sharing scheme

		security, which has severely impeded resource constrained mobile devices to customize the service. The problem of simultaneously achieving fine-grained, high efficiency on the data owner's side, and standard data confidentiality of cloud data sharing actually still remains unresolved. This paper addresses this challenging issue by proposing a new attribute-based data sharing scheme suitable for resource limited mobile users in cloud computing. The proposed scheme eliminates a majority of	such problem can be solved by introducing error tolerance in fuzzy identity-based encryption. It allows the private key with slight different from the original one to decrypt the ciphertext for the original biometric identity. The notion is extended into ABE by defining the identity as a set of attributes. In, it introduced two different and complementary notions of ABE called KP-ABE and CP-ABE, to deal with the error tolerance in key generation phase or ciphertext generation phase. A			is extremely suitable for resource limited mobile users. A possible goal for our future research would be to consider direct attribute revocation in data sharing for resource limited users in cloud computing

		the computation task by adding system public parameters besides moving partial encryption computation offline.	secure construction of KP-ABE was given in by dividing the private key according to the access policy.			
6) Towards Post Quantum Blockchain : A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks	TIAGO M. FERNÁNDEZCARAMÉS, AND PAULA FRAGALAMAS	The transition from prequantum to post-quantum blockchains requires to think carefully the involved steps. For such a purpose, different researchers have devised methods. For instance, the authors propose a scheme to extend the validity of past blockchain blocks when the security of a hash function or of the digital signatures is compromised. However, the transition scheme may	The recent progress on quantum computing has sparked interest in researchers and developers that work with DLTs like blockchain, where public-key cryptography and hash functions are essential. This article analyzed the impact of quantum computing attacks (based on Grover's and Shor's algorithms) on blockchain and studied how to apply postquantum cryptosyste	Besides the use of cryptosystems to transition from prequantum to post-quantum blockchain, several researchers proposed quantum computing based blockchains . For instance, in and , the authors propose to migrate Bitcoin to quantum computers, while others described how to accelerate mining by modifying Grover's algorithm. Moreover, some authors have already	Although the analyses carried out in this article are focused on blockchain, since other DLTs work in a similar way, it is quite straightforward to apply to them the provided recommendations and extracted conclusions. Thus, such recommendations and conclusions could be extrapolated to DLTs based on Directed Acyclic Graphs (DAGs) or on	In order to increase security, some post-quantum schemes limit the number of messages signed with the same key. As a consequence, it is necessary to generate new keys continuously, which involves dedicating computational resources and slowing down certain blockchain processes. Therefore, blockchain developers will have to determine how to adjust such key generation mechanisms to optimize the blockchain efficiency

		actually imply a hardfork of the blockchain, but, to avoid it, a soft-fork mechanism may be implemente d. Another mechanism is proposed where it is presented a simple commit–delay–reveal protocol that enables blockchain users to move in a secure way funds from pre-quantum Bitcoin to a version that implements a post-quantum digital signature scheme.	ms to mitigate such attacks. For such a purpose, the most relevant postquantu m schemes were reviewed and their application to blockchain was analyzed, as well as their main challenges. In addition, extensive compariso ns were provided on the characterist ics and performanc e of the most promising postquantu m public key encryption and digital signature schemes. Thus, this article gives a broad view and insights on the quantum threat on blockchain, and provides useful	suggested using quantum cryptograp hy to implement smart contracts. Furthermor e, more research is necessary on key establishm ent physics-based methods that are collectivel y known as Quantum-Key Distributio n (QKD).	Hashgraph s . However, researchers still need to evaluate thoroughly DLT implement ations that have already claimed to be better prepared for the post-quantum era than certain blockchain s	

			guidelines for the researchers and developers of the next generation of quantum-resistant blockchains.			
7) Anonymous and Traceable Group Data Sharing in Cloud Computing	Jian Shen ,Tianqi Zhou, Xiaofeng Chen, Jin Li, and Willy Susilo	Our goal is to achieve anonymous data sharing under a cloud computing environment in a group manner with high security and efficiency. To achieve this goal, the following challenging problems should be taken into consideration.	Firstly, an arbitrary and variable number of group members should be supported. In practical applications, the number of members in each group is arbitrary, and the dynamic joining and exiting of group members is frequent. A desired scheme not only supports the participation of any number of users but also supports efficient key and data updating. Secondly, the	Ateniese et al. proposed a proxy re-encryption scheme to manage distributed file systems that attempt to achieve secure data storage in the semi-trusted party. Based on bilinear maps, the scheme offers improved security guarantees. Although the scheme provides a stronger concept of security compared with, it is still vulnerable under collusion attacks and revoked	In this paper, we present a secure and fault-tolerant key agreement for group data sharing in a cloud storage scheme. Based on the SBIBD and group signature technique, the proposed approach can generate a common conference key efficiently, which can be used to protect the security of the outsourced data and support secure group data sharing in the cloud	Note that algorithms to construct the SBIBD and mathematical descriptions of the SBIBD are presented in this paper. Moreover, authentication services and efficient access control are achieved with respect to the group signature technique. In addition, our scheme can support the traceability of user identity in an anonymous environment. In terms of dynamic changes of the group member, taking advantage of the key agreement and efficient access control, the computational complexity and communication complexity for updating the common

			confidentiality of the outsourced data should be preserved. Since the uploaded data may be sensitive and confidential business plans or scientific research achievements, data leakages may cause significant losses or serious consequences. Without the guarantee of confidentiality, users would not like to be involved in the cloud to share data. Thirdly, the way that data are shared should follow the many to-many pattern, which makes the information sharing more convenient	malicious users.	at the same time.	conference key and the encrypted data are relatively low.

			and efficient.			
8) A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms	TAHER ELGAMAL	New signature scheme is proposed, together with an implementation of the Diffie Hellman key distribution scheme that achieves a public key cryptosystem. The security of both systems relies on the difficulty of computing discrete logarithms over finite fields.	Given m, r, and s, it is easy to verify the authenticity of the signature by computing both sides and checking that they are equal. Note I: As will be shown in Section IV, the value of k chosen in step 1) should never be used more than once. This can be guaranteed, for example, by using as a “k generator” a DES chip used in the counter mode as a stream cipher.	For the signature scheme using the above arguments for the sizes of the numbers in our system and the RSA system, the signature is double the size of the document. Then the size of the signature is the same size as that needed for the RSA scheme, and half the size of the signature for the new signature scheme that depends on quadratic forms published by Ong and Schnorr and also Ong, Schnorr, and Shamir (since both systems are based on the integer factoring problem).	The paper described a public key cryptosystem and a signature scheme based on the difficulty of computing discrete logarithms over finite fields. The systems are only described in GF (p). The public key system can be easily extended to any GF (pm), but recent progress in computing discrete logarithms over GF (p”) where m is large makes the key size required very large for the system to be secure	The subexponential time algorithm has been extended to GF(p2)and it appears that it can be extended to all finite fields, but the estimates for the running time for the fields GF(p”) with a small m seem better at the present time. Hence, it seems that it is better to use GF(p”) with m = 3 or 4 for implementing a cryptographic system. The estimates for the running time of computing discrete logarithms and for factoring integers are the best known so far, and if the estimates remain the same, then, for the same security level, the size of the public key file and the size of the cipher text will be double the size of those for the RSA system.

				The Ong Schnorr Shamir system has been broken by Pollard and new variations are being suggested. Thus, it is not clear at the present time whether a secure system based on modular equations can be found, and hence no further remarks will be made regarding these schemes.		
9) Algorithm s for Quantum Computati on: Discrete Logarithm s and Factoring	Peter W. Shor	A computer is generally considered to be a universal computation al device; i.e., it is believed able to simulate any physical computation al device with a cost in computation time of at most a polynomial factor: It is not clear	The laws of quantum mechanics only permit unitary transformat ions of the state. A unitary matrix is one whose conjugate transpose is equal to its inverse, and requiring state transformat ions to be represented by unitary	Since quantum computatio n deals with unitary transformat ions, it is helpful to be able to build certain useful unitary transformat ions. In this section we give some techniques for constructin	This algorithm does not use very many properties of Z,, so we can use the same algorithm to find discrete logarithms over other fields such as Z,-. What we need is that we know the order of the	If one were to actually program this algorithm (which must wait until a quantum computer is built) there are many ways in which the efficiency could be increased over the efficiency shown in this paper.

		whether this is still true when quantum mechanics is taken into consideration. Several researchers, starting with David Deutsch, have developed models for quantum mechanical computers and have investigated their computational properties. This paper gives Las Vegas algorithms for finding discrete logarithms and factoring integers on a quantum computer that take a number of steps which is polynomial in the input size, e.g., the number of digits of the integer to be factored. These two problems are generally considered	matrices ensures that the probabilities of obtaining all possible outcomes will add up to one. Further, the definitions of quantum Turing machine and quantum circuit only allow local unitary transformations, that is, unitary transformations on a fixed number of bits. Perhaps an example will be informative at this point. Suppose our machine is in the superposition of states	g unitary transformations on quantum machines, which will result in our showing how to construct one particular unitary transformation in polynomial time. These transformations will generally be given as matrices, with both rows and columns indexed by states. These states will correspond to representations of integers on the computer; in particular, the rows and columns will be indexed beginning with 0 unless otherwise specified	generator, and that we can multiply and take inverses of elements in polynomial time	

		hard on a classical computer and have been used as the basis of several proposed cryptosystems. We thus give the first examples of quantum cryptanalysis				
10) Quantum Cryptography using Quantum Key Distribution and its Applications	N.Sasirekha, M.Hemalatha	Another problem is that for distances beyond 50 kilometers or so, the noise becomes so great that error rates also increases drastically. This leaves the channel very vulnerable for eavesdroppers and makes the channel virtually impossible to send information. However, in future, it is possible for quantum keys to be exchanged through the air. Small telescopes may be aligned to	Quantum cryptography does not depend on difficult mathematical problems for its security. Quantum cryptography accomplishes these remarkable feats by exploiting the properties of microscopic objects such as photons. The photons have three chosen bases of polarization and the probable results of a measurement according to the	With political upheaval and accusations of voter fraud rampant in developed and developing countries alike, it’s clear that making the voting process more secure is a necessity. Since 2007, Switzerland has been using quantum cryptography to conduct secure online voting in federal and regional elections. In Geneva, votes are encrypted	It is concluded that to transmit sensitive information between two or more points, some stronger technique is needed. It’s sure that Quantum key distribution and other quantum encryption methods will allow us to secure sensitive information more effectively in the future. Quantum encryption is a powerful and positive	In case of entangled photons, which seems to be safe, there is also a practical problem not only with the cost, but also with keeping them entangled long enough to meet the needs of the real world. QKD is the first practical application of the foundations of quantum mechanics, and as such it indicates to the value of basic science research. If Quantum Key Distribution is to ever be used in practice its security must be certified, and hence the thorough examination is necessary with the aspects of quantum

		detect the signal. Some calculations even suggest that photons could be detected by a satellite, which allows communication between any part of the world.	bases are: *Rectilinear (horizontal or vertical) *Circular (left-circular or right-circular) *Diagonal (45° or 135°) [2]. Although there are three bases, only two bases are used in any given protocol for quantum cryptography. Photons can be measured to determine their orientation relative to one of these bases of polarization at a time. Classically, one would expect the photon to have a certain polarization, which can be measured but which is not changed by the measureme	at a central vote-counting station. Then the results are transmitted over a dedicated optical fiber line to a remote data storage facility. The voting results are secured via quantum cryptography, and the most vulnerable part of the data transaction when the vote moves from counting station to central repository is uninterruptible. This technology will soon spread worldwide, as many other countries face the specter of fraudulent elections.	step in the right direction, toward a future in which we can feel more secure about how and what we share. Thus, we can also expect a considerable feedback from QKD into basic physics, which leads to a new perspective on the foundations of quantum mechanics. The perspective can be more “practical” than “philosophical.” It has been speculated that the American power grid is one of the most vulnerable targets for a cyber attack. In fact, some major U.S. utilities are under	mechanics on which its security is based. To validate these security concepts new experiments should be performed based on the foundations of quantum mechanics.

			nt. Photons, however, are quantum objects, which are considered to have a property only after it is measured. The type of measurement impacts the property of the object. This implies that a photon can only be considered to have a particular polarization after it is measure, and that the basis chosen for the measurement will have an impact on the polarization.		“constant” attack by cyber enemies. A small encryption device helps the workers to send totally secure signals using public data networks to control smart electricity grids. Smart grids are essential for balancing supply and demand for efficiency. Additionally, with proper precautions in place, they are significantly more secure than traditional grids.	
12) Privacy Preserving and Lightweight Key Agreement Protocol for V2G in the Social Internet of Things	Jian Shen, Member, Tianqi Zhou, Fushan Wei, Xingming Sun and Yang Xiang	Lightweight: Many existing complicated and powerful cryptographic algorithms and primitives cannot be	In this subsection, the functionality and features of the proposed protocol are compared with those	The results of the computational cost analysis presents the computational costs of the client (e.g, EV, user) and	The communication complexity of our protocol is analysed in terms of the number of exchanged messages.	In this paper, we propose a lightweight key agreement protocol that features strong privacy and security. Our protocol is more efficient compared with ECC-based

		implemented in V2G networks, due to their resource consumption and computational overhead. To solve this problem, we designed a lightweight protocol for V2G that employs only oneway hash functions and bitwise XOR operations. Note that the proposed protocol reduces resource consumption and computational overhead without impairing security. • Self synchronization: If EVs use the same pseudonyms all the time, attackers can acquire their real identities by analyzing pseudonyms in the same way as real identities. In	of Turkanovic ́ et al.s' protocol, Choi et al.s' protocol, Wang et al.s' protocol and Abdallah et al.s' protocol. None of these four protocols can withstand a desynchronization attack. Neither Turkanovic ́ et al.s' protocol nor Choi et al.s' protocol offer the property of anonymity and they cannot resist replay or impersonation attacks as well as the proposed protocol. In addition, Turkanovic ́ et al.s' protocol does not offer the property of perfect forward security, while Choi	the server (e.g, AGT, sensor) when using the relevant protocols. In this comparison, Th, TXOR, Tm and Tp are the times required to perform a one-way hashfunction, a bitwise XOR operation, a modular exponentiation and a point multiplication on an elliptic curve, respectively. The times required to perform Th, Tm and Tp are approximately 0.0005 seconds, 0.063075 seconds and 0.072311 seconds, respectively. The time required to perform TXOR is ignored in the comparison because	In others, in addition to two messages for registration, the user needs to exchange six messages with the gateway node (GWN) and a corresponding regular sensor node. The communication costs of the two protocols are 2 + 12n and 2 + 5n, respectively. Here, n is the number of EVs.	protocols, which makes it both applicable and practicable for resource constrained environments. Moreover, the proposed protocol addresses the dark aspects of smart grids, such as security and privacy issues. Specifically, security during communications is ensured by the negotiated session key, while privacy is protected by the self synchronization mechanism of the proposed. protocol. Performance and security analyses demonstrate that our protocol is more efficient and safer compared with other relevant existing protocols.

		our protocol, the EV and AGT can update the pseudonym for each session. Therefore, the real identity of a EV can be protected in our scheme. • Communication security: In key agreement protocol, two communicating entities can agree on a common conference key, thus ensuring the security of their subsequent communications. Note that in our paper the security model and security definitions are clearly defined with regard to V2G networks. Moreover, both informal and formal security analyses show that the	et al.s’ protocol cannot withstand the stolen smart card attack. Compared with the more recent and well-designed and proven protocols which cannot resist the stolen smart card and desynchronization attacks, our protocol performs well. Note that the security of the proposed protocol has been formally proven under the random oracle model.	it is negligible compared to the others. The same is for the string concatenation operation, which is also ignored in the comparison. Protocols that employ the ECC have a higher computational cost, while lightweight protocols and our protocol require only about one hundredth of the time cost of protocols.		

		proposed protocol is secure under the security model and the given security definitions.				
13) Quantum Cryptography using Quantum Key Distribution and its Applications	N.Sasirekha, M.Hemalatha	Cryptography is the practice and study of encoding and decoding secret messages to ensure secure communication s. There are two main branches of cryptography: secret-(symmetric-) key cryptography and public-(asymmetric) key cryptography. A key is a piece of information (a parameter) that controls the operation of a cryptographic algorithm. In encryption, a key specifies the particular transformati	Many algorithms of encoding and decoding information using a given key have been created already, many years before quantum cryptography came into existence. Quantum cryptography is not replacing traditional cryptography but it allows for a more secure transfer of the keys used in encoding and decoding. The maximum speed, scale and security of the transfer is achieved by sending the secret	Quantum encryption already protects both sensitive national security information in the public sector and financial information in the private sector. Its security is tested and proven. Here are some current and near-future applications of quantum cryptography.	In case of entangled photons, which seems to be safe, there is also a practical problem not only with the cost, but also with keeping them entangled long enough to meet the needs of the real world. Another problem is that for distances beyond 50 kilometers or so, the noise becomes so great that error rates also increases drastically. This leaves the channel very vulnerable for eavesdrop	It is concluded that to transmit sensitive information between two or more points, some stronger technique is needed. It's sure that Quantum key distribution and other quantum encryption methods will allow us to secure sensitive information more effectively in the future. Quantum encryption is a powerful and positive step in the right direction, toward a future in which we can feel more secure about how and what we share. Thus, we can also expect considerable feedback from QKD into basic physics, which leads to a new perspective on the foundations of quantum mechanics. The

		on of plaintext into cipher text, or vice versa during decryption. Keys are also used in other cryptographic algorithms, such as digital signature schemes and message authentication codes. In practice, due to significant difficulties of distributing keys in secret key cryptography, public-key cryptographic algorithms are widely used in conventional cryptosystems.	key using quantum coding, but encoding and sending the data itself using traditional methods and algorithms.		pers and makes the channel virtually impossible to send information. However, in future, it is possible for quantum keys to be exchanged through the air. Small telescopes may be aligned to detect the signal. Some calculations even suggest that photons could be detected by a satellite, which allows communication between any part of the world. QKD is the first practical application of the foundations of quantum mechanics, and as such it indicates to the	perspective can be more “practical” than “philosophical.

					value of basic science research. If Quantum Key Distribution is to ever be used in practice its security must be certified, and hence the thorough examination is necessary with the aspects of quantum mechanics on which its security is based. To validate these security concepts new experiments should be performed based on the foundations of quantum mechanic	
14) Quantum Cryptography: An Emerging Technology in Network Security	Mehrdad S. Sharbaf, Loyola Marymount University California State University , Northridg	One of the challenges for the researchers, is to develop optical device capable of generating, detecting and guiding	An important and unique characteristic of quantum cryptography is the ability to detect the presence of any third	IDQ's Cerberis solution offers a radically new approach to network security, by combining the sheer	The quantum cryptography allows a bit string to be agreed between two communications parties	The other vulnerability is susceptible to the future of quantum computation protocols. For example: Shor’s Algorithm , allows for factoring large

	e Sharbaf & Associates	single photons; devices that are affordable within a commercial environment. Particular problem for QDK is selling technology based on quantum mechanics to clients who often know little about physics and are used to traditional cryptography	party between two communicating users. The security of quantum cryptography depends on the foundation of quantum mechanics, and that can revolutionize the network security. QKD techniques can be married to standard internet technology in order to provide highly secure communications for practical use. The scope of this research paper is to cover the weaknesses, and the security pitfalls in modern cryptography, fundamental concepts of quantum cryptography, the real –world	power of high-speed layer encryption appliances with the unconditional security of quantum key distribution (QKD) technology to secure point-to point backbone and storage networks	without having two parties to meet face to face two parties can be sure with a high confidence that the agreed bit string is exclusively shared between them.	numbers on a quantum computer in polynomial time, theoretically breaking RSA encryption. The same argument demonstrate that classical cryptosystem provides no mechanism for detecting eavesdropping Moreover, once scholars able to build a feasible quantum computer, Shor's algorithm could beak RSA easily in polynomial time.

			application implementation of this technology, finally the future direction in which the quantum cryptography is headed forwards.			
15) A Survey on Quantum Key Distribution	Mr. Abhishek Sharma1 , Dr Amit Kumar2 1SRM Institute of Science and Technology, Delhi – NCR Campus, 2KIET, Ghaziabad	With the development of Quantum Cryptography, the challenges have also increased. QKD, which is the most important component of QC, is also one of the important components of secure quantum communication. It has passed through the fear that quantum computer will use the Shor secure algorithm to nullify the existing public key cryptography Quantum Computing is also a measure	The review of Quantum Computing including different application fields like Quantum public key cryptography, QKD, Quantum Authentication. - Quantum key distribution is a catchword among industry specialist now a day.It is arising an alarming situation to all the current network security techniques. These are the basic properties of Quantum Mechanics,	With the advancement in the field of quantum computing, it has created a question mark on current cryptographic system. So to solve this issue a new approach is being developed known as Post Quantum Cryptography. Theoretically it ensures the safety of information against Quantum attacks . Quantum A.I. is the implementation of Quantum processing in	The main advantage of Digital signature is to ensure the purity of the data and the validity of the sender in the communication. This is the combination of the asymmetric key encryption technology with digital abstract technology	quantum mechanics states that a Qubit can hold multiple states in parallel. In simple words we can say that without measuring the state of a qubit we cannot say it is holding what state, as to determine the state of qubit is known as qubit measurement. So before performing measurement on qubit its states cannot be determined so at present it is in a super position of all its possible states.

		issue. Here we have listed few of they which are worth of discussion. These issues are true random number, light source, detection, postprocessing, authentication, repeater, etc. QKD experimental systems are also improved a lot with its time span. As we are having many QKD protocols based on physical properties to apply and observe on recent cryptographic applications. Few categories of our QKD protocols are listed as here. • Discrete variable Quantum Key Distribution (DVQKD) • Continuous Variable Quantum Key Distribution	which makes a combination with network security	implementation of Artificial Intelligence. It is a research effort of Google Corporation. Quantum AI by google is dedicated to improve quantum computing by developing quantum processors and novel quantum algorithms. It will help researchers and developers to solve near-term problems.		

		(CVQK D) • Prepare and Measure Quantum Key Distribution (PMQKD) • Entangleme nt Based Quantum Key Distribution (EBQK D) • Measureme nt Device Independent Quantum Key Distribution (MDIQ KD) Each category is a large set of protocols to experimente d and observe to find new results. So the overall output of this fields is very satisfactory till now but still there is a long distance to be travelled along with it.				
16) Embedded security framework for integrated classical and quantum cryptograp hy services in optical	Yuhua Chen1, Pramode K. Verma2 and Subhash Kak3	Disparate and heterogeneo us networks will be a growing reality in the future. Additionally , some of the regulatory,	Quantum cryptograp hy allows one to go beyond the classical paradigm and, therefore, overcome the fundament	Note that burst assembly/ disassembl y functionalit y is only provided at OBS edge routers. There is no burst	Optical burst switching (OBS) is the most promising optical switching technology for the future Internet,	This paper has proposed an approach to embed a security framework in the native OBS network architecture, providing a means to secure the

burst switching networks		national interest, and security requirements. Entities can cooperate to provide high speed, high performance, and cost effective service, on demand, to their customers. We obtain the highest level of interconnection at the optical level. Optical switching technologies can be categorized into optical circuit switching, optical packet switching, and optical burst switching (OBS). Optical circuit switching, also known as lambda switching, can only switch at the wavelength level, and is not suitable for busty Internet traffic.	al limitations that the classical techniques suffer from. However, it also faces new challenges related to performance in the presence of noise and certain limitations of the single-photon generators. Our proposed integrated secure OBS architecture is fully compatible with the well-known BB84 protocol. However, to deal with the technical challenge of siphoning attack on the practical multi-photon sources in the BB84 protocol, we propose to use a new 3-	reassembly in the OBS core network. There is a one-to-one correspondence between the burst header and its associated burst. Burst headers are responsible for setting up optical data paths for their data bursts. Data bursts will simply follow the light paths set up by burst headers and are transparent to OBS core routers.	but it suffers from security vulnerabilities. In this paper, we propose to embed a security framework which incorporates the strengths of classical and the emerging quantum cryptography techniques in the native OBS network architecture, providing a means to make the future Internet secure from the ground up. The proposed embedded security architecture allows the best suited classical and quantum cryptography techniques to be deployed, making it	future Internet from the ground up. The proposed embedded security architecture allows the most suited classical and quantum cryptography techniques to be deployed, making it possible to offer robust security. While the proposed integrated security framework is fully compatible with the well-known BB84 quantum cryptography protocol, we recommend a new 3-stage quantum cryptography protocol based on random rotations of the polarization vector for the OBS security framework. Compared to the BB84 protocol, the 3-stage quantum cryptography protocol for security services in OBS networks has the following advantages: (1) it does not require single

			stage quantum cryptography protocol for the secure OBS framework. Unlike BB84 and its variants, the 3-stage quantum cryptography protocol is immune to siphoning attacks and therefore, multiple photons can be safely used in the quantum key communication. The 3- stage quantum cryptography protocol is based on random rotations which can better protect duplicate copies of the photons than in non-single qubit transmissions of the BB84 protocol. This also means that the new protocol		possible to offer robust security. The security of quantum cryptography is based on the inherent randomness in quantum phenomena. The application of quantum techniques to optical networks is ideally suited to the problem because photons, which carry information in optical modality, are quantum objects. Since the well known BB84 quantum cryptography protocol is susceptible to siphoning attacks on the multiple photons emitted by practical	photon sources as required in the BB84 protocol (since practical photon sources produce many photons some of which may be siphoned off to break the protocol). Instead, multiple photons can be used in communication, increasing potential transmission distances, and reducing the protocol's sensitivity to noise; (2) while the BB84 protocol has one hop quantum communication followed by two hops of communications through classical channels, all three hops of communication in the new protocol are quantum, providing more security; (3) the new protocol never reveals the actual quantum state of the key on the communication link, allowing the protocol to be extended

			can use attenuated pulse lasers rather than single-photon sources in the quantum key exchange, which Step 1: Alice applies a unitary transformation UA on quantum information X and sends the qubits to Bob. Step 2: Bob applies UB on the received qubits UA(X), which gives UBUA(X) and sends it back to Alice. Step 3: Alice applies U† A (transpose of the complex conjugate of UA) on the received qubits to get U† AUBUA(X) = U† AUAUB(X) = UB(X)		sources, we propose to use a new 3-stage quantum cryptography protocol which is immune to siphoning attacks, as it is based on random rotations of the polarization vector. This would allow multiple photons to be used in the quantum key exchange and make it feasible to extend quantum cryptography services beyond trusted routers. Copyright © 2009 John Wiley & Sons, Ltd.	beyond trusted routers.
17) Quantum	Richard J. Hughes*,	We believe that the	We have designed	Satellite QKD	Our knowledge	However, many of the

Cryptography For Secure Satellite Communication	William T. Buttler, Paul G. Kwiat, Steve K. Lamoreaux,R ichard J. Hughes*, William T. Buttler, Paul G. Kwiat, Steve K. Lamoreaux, George L. Mokgari; Jane E. Nordholt, and Charles G. Peterson	development of QKD for re-keying of satellites on orbit would be prudent, so as to have an alternative to traditional key distribution methods that can potentially become vulnerable to unanticipated algorithmic or computational advances. Furthermore, with the use of QKD potential adversaries would have to contemplate high-risk active attacks as opposed to the purely passive attacks that are possible with conventional methods of key distribution.	our QKD system to operate at a wavelength near 770 nm where the atmospheric transmission from surface to space can be as high as 80%. Furthermore, at optical wavelengths the polarized QKD photons .can be faithfully transmitted because the depolarizing effects of Faraday rotation in the ionosphere are negligible. Because the atmosphere is only weakly dispersive, a bright timing pulse (which carries no key informatio n) of - 100-ps duration can be used to set a short time	could also be used to provide secure key distribution to two ground based users (Alice and Bob) who do not have access to optical fiber communications and who are not within line-of-sight: they could each generate independent quantum keys with the same satellite, which would then transmit the XOR of the keys to Bob. Bob would then XOR this bit string with his key to produce a key that agrees with Alice's. Alice and Bob could then use their shared key for encrypted communications over any	the primary physics requirements for this application of QKD, namely the transmission and detection of single photons between a ground station and an orbital asset, have never been demonstrated.	optical acquisition, pointing, tracking and adaptive optics techniques developed for laser communications with satellites can be directly applied to this problem. Therefore, we believe that a surface-to satellite QKD demonstration experiment would be a logical and realistic next step in the development of this new field

			window (-1 ns) within which to look for the QKD photon. A single QKD photon arriving - 100 ns after the bright pulse would find that the satellite had moved by less than 1 mm.	convenient channel.		
18) PROTOCO L AND APPLICATIONS FOR SHARING QUANTUM PRIVATE KEYS	Han- Wei Wang', Thren-Sheng Lin"1,2, IMing Tsai and Sy- Yen Kuo'	One of the main challenges is that :An important issue to protect our entanglement against a person is that we do not want these quantum EPR pairs to be intercepted or copied or even destroyed during the transmission .	Entanglement can be used as a secure channel to transmit information with absolute secrecy. From this perspective , quantum entanglement pairs are equivalent to a quantum private key. In this a protocol is proposed that can be used to distribute such entanglement pairs securely, so they can be subsequent	After the establishment of these entanglement pairs, they can be used to transmit classical or quantum information secretly. Here we give an example of transmitting classical messages using these entanglement pairs. It takes one entanglement pair and one classical bit to transmit a classical bit secretly, and one	We take the advantage of entangled state during information transmission , because the qubits become relational, and they can affect the others jump to the special quantum state after measurements. Therefore, if the quantum state of one qubit of the quantum EPR pair	The security of the algorithms depends on the assumption that there is no fast algorithm to find out the answer of the one-way function.

			ly used to transmit messages with perfect security. The security of this protocol is based on the laws of nature, instead of unproven mathematical hard problems.	entanglement pair and two classical bits to transmit a quantum state secretly. Transmit quantum information using entanglement pairs. Transmit classical information using entanglement pairs.	has been measured, then the other qubit will also be determined according to the result of the former qubit. And no other people will be aware of that variance, let alone to steal the changed quantum information. This and so we can make up some communicate on protocol according to these special properties.	
19) Quantum Cryptography using Quantum Key Distribution and its Applications	N.Sasirekha, M.Hemalatha	Cryptography is the practice and study of encoding and decoding secret messages to ensure secure communication s. There are two main branches of cryptography: secret-(symmetric-) key	Many algorithms of encoding and decoding information using a given key have been created already, many years before quantum cryptography came into existence. Quantum	Quantum encryption already protects both sensitive national security information in the public sector and financial information in the private sector. Its security is tested and proven.	In case of entangled photons, which seems to be safe, there is also a practical problem not only with the cost, but also with keeping them entangled long enough to meet the	It is concluded that to transmit sensitive information between two or more points, some stronger technique is needed. It’s sure that Quantum key distribution and other quantum encryption methods will allow us to secure sensitive information more effectively in

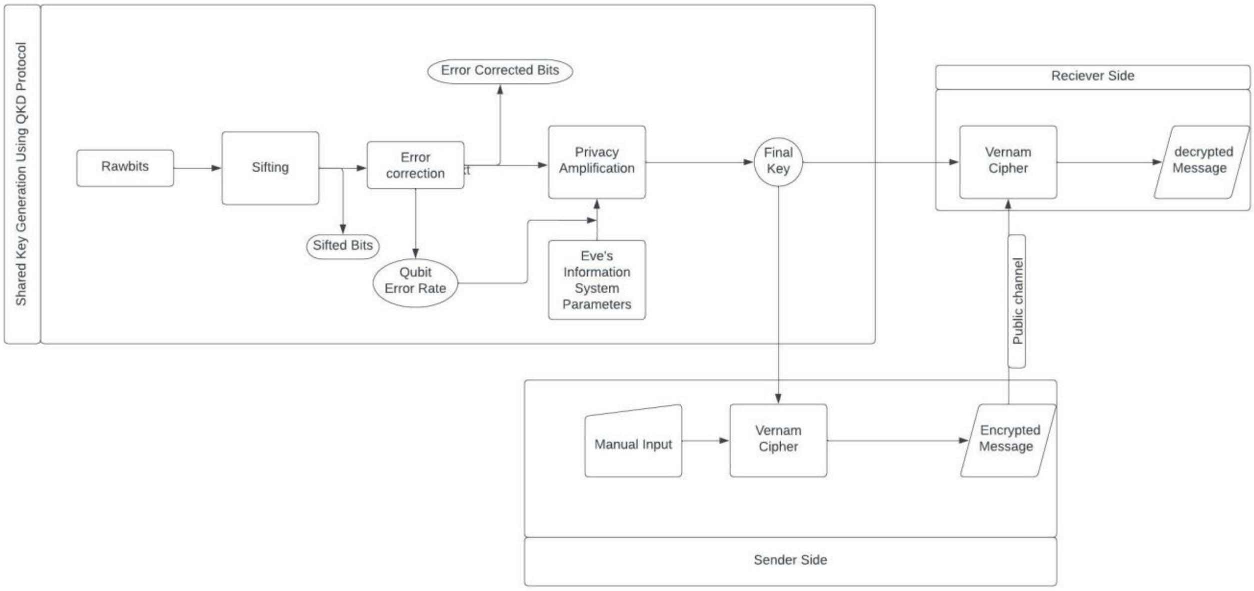
		cryptography and public- (asymmetric) key cryptography. A key is a piece of information (a parameter) that controls the operation of a cryptographic algorithm. In encryption, a key specifies the particular transformation of plaintext into cipher text, or vice versa during decryption. Keys are also used in other cryptographic algorithms, such as digital signature schemes and message authentication codes. In practice, due to significant difficulties of distributing keys in secret key cryptograph	cryptography is not replacing traditional cryptography but it allows for a more secure transfer of the keys used in encoding and decoding. The maximum speed, scale and security of the transfer is achieved by sending the secret key using quantum coding, but encoding and sending the data itself using traditional methods and algorithms.	Here are some current and near-future applications of quantum cryptography.	needs of the real world. Another problem is that for distances beyond 50 kilometers or so, the noise becomes so great that error rates also increases drastically. This leaves the channel very vulnerable for eavesdroppers, and makes the channel virtually impossible to send information. However, in future, it is possible for quantum keys to be exchanged through the air. Small telescopes may be aligned to detect the signal. Some calculations even suggest that photons	the future. Quantum encryption is a powerful and positive step in the right direction, toward a future in which we can feel more secure about how and what we share. Thus, we can also expect a considerable feedback from QKD into basic physics, which leads to a new perspective on the foundations of quantum mechanics. The perspective can be more “practical” than “philosophical.

		y, public-key cryptographic algorithms are widely used in conventional cryptosystems.			could be detected by a satellite, which allows communication between any part of the world. QKD is the first practical application of the foundations of quantum mechanics, and as such it indicates to the value of basic science research. If Quantum Key Distribution is to ever be used in practice its security must be certified, and hence the thorough examination is necessary with the aspects of quantum mechanics on which its security is based. To validate these	

					security concepts new experiments should be performed based on the foundations of quantum mechanics	
20) A Secure Cryptocurrency Scheme Based on Post Quantum Blockchain	Xiu-Bo Chen	The authors conduct a survey of Blockchain applications using Blockchain technology and the challenges this faces. Blockchain technology can also be used in various fields of business. One interesting implementations of Blockchain technology is in the healthcare system.	Entanglement can be used as a secure channel to transmit information with absolute secrecy. From this perspective, quantum entanglement pairs are equivalent to a quantum private key. In this a protocol is proposed that can be used to distribute such entanglement pairs securely, so they can be subsequently used to transmit messages with perfect security. The security of this	Unspent Transaction Output (UTXO) is used to prevent double spending. Every transaction consists of transaction inputs and transaction outputs, and these transactions constitute a chain structure. Transaction inputs have to be unspent transaction outputs, that is to say, outputs of previous transactions that have not yet been spent. CRYPTOCURRENCY SCHEME BASED ON PQB : firstly	User’s private key has the advantage of resisting quantum computing attack. In other words, cryptocurrency is more secure in this cryptocurrency scheme signature scheme has the advantage of provably security in the standard model	The main drawback is that the size of its signature output increases linearly with the number of signatures. However, one can mitigate this by using a combined PQ approach or by utilizing existing graph structures in blockchain applications.

			protocol is based on the laws of nature, instead of unproven mathematical hard problems.	present the definition of postquantum blockchain. Then we introduce our proposed signature scheme based on lattice. Finally, we provide a secure cryptocurrency scheme based on PQB that can resist quantum computing attacks. PQB is a secure blockchain technology which combines postquantum cryptography and blockchain technology together. This means that PQB not only has the advantages of blockchain but also can resist attacks by quantum computer effectively.		

Overall Architecture:



The following architecture can be described as an implementation of **QKD (Quantum Key Distribution) Protocol.** The architecture is meant to act as a safeguard against any third-party tampering of data shared between two respective parties by generating a **quantum key**.

The concept of QKD protocol implementation is based on key distillation. **Sifting** is the process whereby two parties, say Ram and Shyam, window away all the obvious "failed qubits" from a series of pulses. Sifting allows Ram and Shyam to reconcile their **"raw" secret bit streams** to remove the errors (if any). **Error detection and correction** allows Ram and Shyam to determine all the "**error bits**" among their shared, **sifted bits**, and correct them so that Ram and Shyam share the same sequence of error-corrected bits. The process of error detection allows Ram and Shyam to estimate the current **Quantum Bit Error Rate (QBER**), a probability of the undesired change in our qubit state, on the quantum channel between them, which can then be used as input for **privacy amplification.** Privacy Amplification is the process whereby Ram and Shyam reduce the third party's knowledge of their shared bits to an acceptable level, in accordance with **Eve's Information System Parameters.**

With this we get our **Final Key** generated, which is **encrypted** and **decrypted** respectively using a **Vernam Cipher**, a symmetrical stream cipher in which the plaintext is combined with a random or pseudorandom stream of data (the "keystream") of the same length, to generate the ciphertext, using the Boolean "exclusive or" (XOR) function.

Therefore, in this architecture, two parties can send each other messages that are secure as the **Sender's side** does a **manual input** that the Vernam Cipher deciphers into ciphertext, stored as our Final Key generated by the QKD protocol to form an **Encrypted Text**, which is then shared through the **Receiver's side** through a **public channel** where they use Vernam Cipher as well to get their secure, untampered **Decrypted Message.**

To go more in detail about our Architecture's workings, we elucidate our methodology further below.

Proposed Methodology :

The following methods that we used in our project is:

Quantum Key Distribution:

The best- known method of quantum cryptography is quantum key distribution (QKD), which is the process of using quantum communication to establish a shared key between two parties (John and James, for example) without a third party (Joe) learning anything about that key, even if Joe can eavesdrop on all communication between John and James. If Joe tries to learn information about the key being established, discrepancies will arise causing John and James to notice. Once the key is established, it is then typically used for encrypted communication using classical techniques. For instance, the exchanged key could be used for symmetric cryptography.

The quantum cryptography allows a bit string to be agreed between two communications parties without having two parties to meet face to face, and yet that two parties can be sure with a high confidence that the agreed bit string is exclusively shared between them. BB84 allows two parties, conventionally “Ram” and “Shyam”, to establish a secret common key sequence using polarized photons. Each of these photons is in a state denoted by one of the four following symbols:

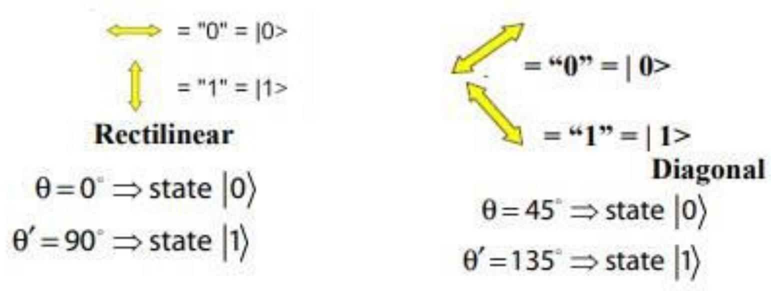


Fig1

—, |,⁄, \,. According to [1], the first two photon states are emitted by a polarizer which is set with a rectilinear orientation and the other two states are emitted by a polarizer which is set with a diagonal orientation. For example: +(0)= — , +(1)= | , x(0)=⁄ , x(1)= \ )= \

If Ram sends random sequence of photons: ++xx++xxx++xx the binary number represented with these states is 1110010110010 Now, if Shyam wants to obtain a binary number sent by Ram, he needs to receive each photon in the same basis (as shown in the Fig.2)

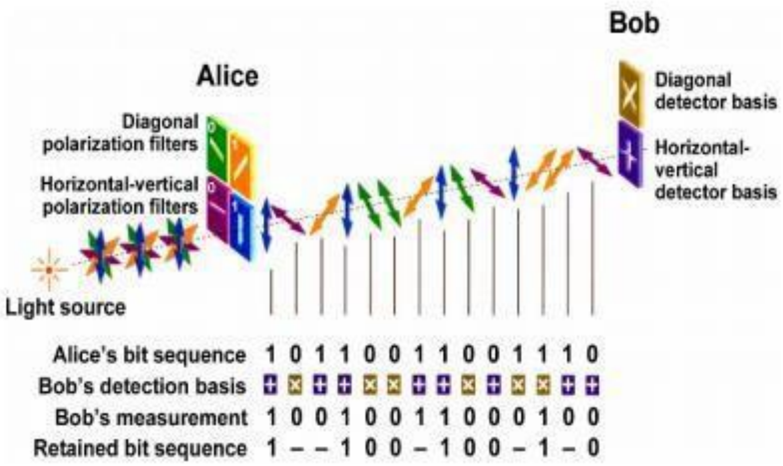


Fig2

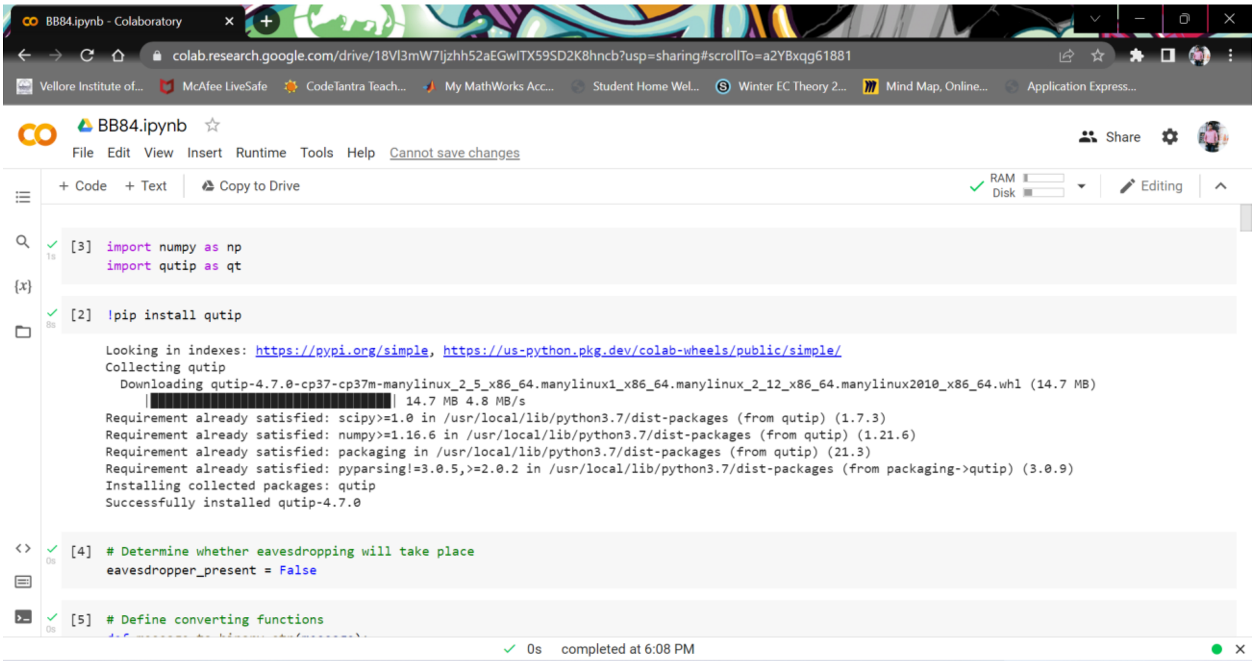
For each conventional bit to be transmitted in the QKD protocol Ram will set differently oriented polarizes + or x uniformly random stated that because a photon is an indivisible elementary particle, the QKD communications cannot be passively tapped in the conventional sense so adversaries

would need to undertake far more risky active attacks. However, the Heisenberg Uncertainty Principle ensures that any active attack will not permit an attacker to faithfully read the key transmission, in another word, as a third party, say Sita, intercepts Ram's photons, she has to measure them with a random basis and send new photons to Shyam.
Sita's presence is always detected: measuring a quantum system irreparably alters its state (The Heisenberg Uncertainty principle). For that reason, if an eavesdropper Sita tries to tap the channel, this will automatically show up in Shyam's measurements. In those cases where Ram and Shyam have used the same basis, Shyam is likely to obtain an incorrect measurement (Error Rate). Sita's measurements are bound to affect the states of the photons, leading to an obvious detection of tampering of data being shared between Ram and Shyam.

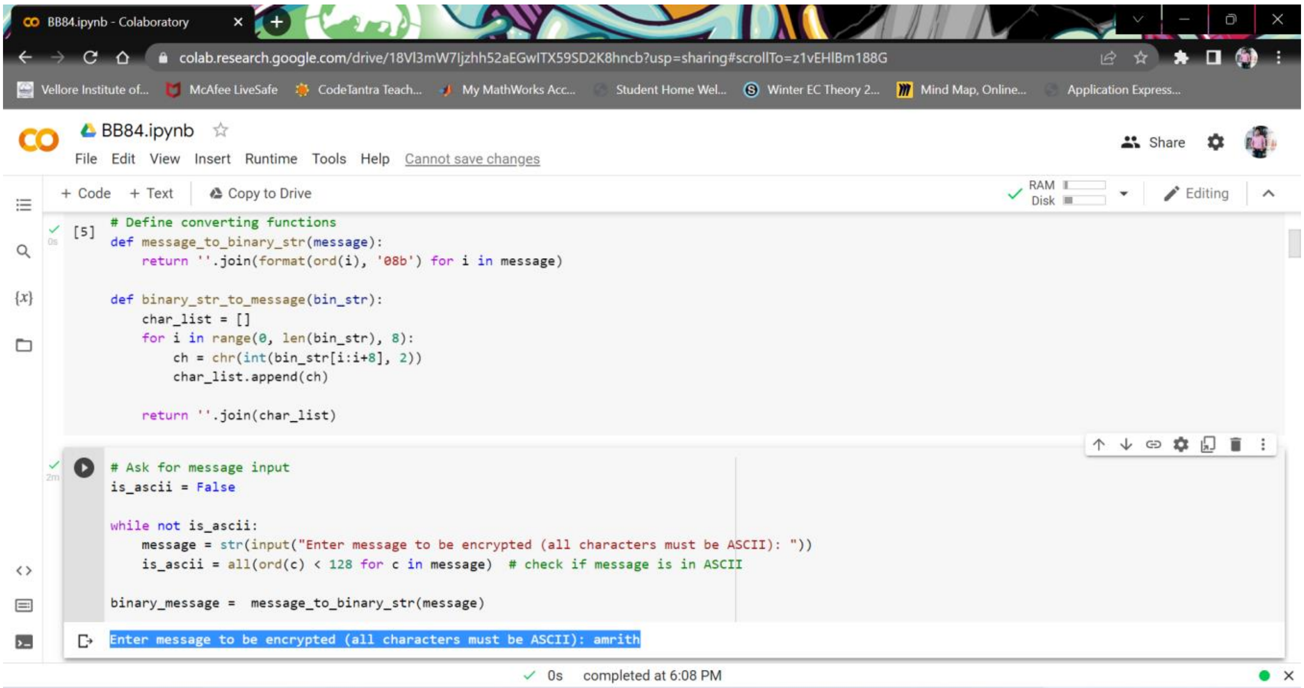
Results

Code-

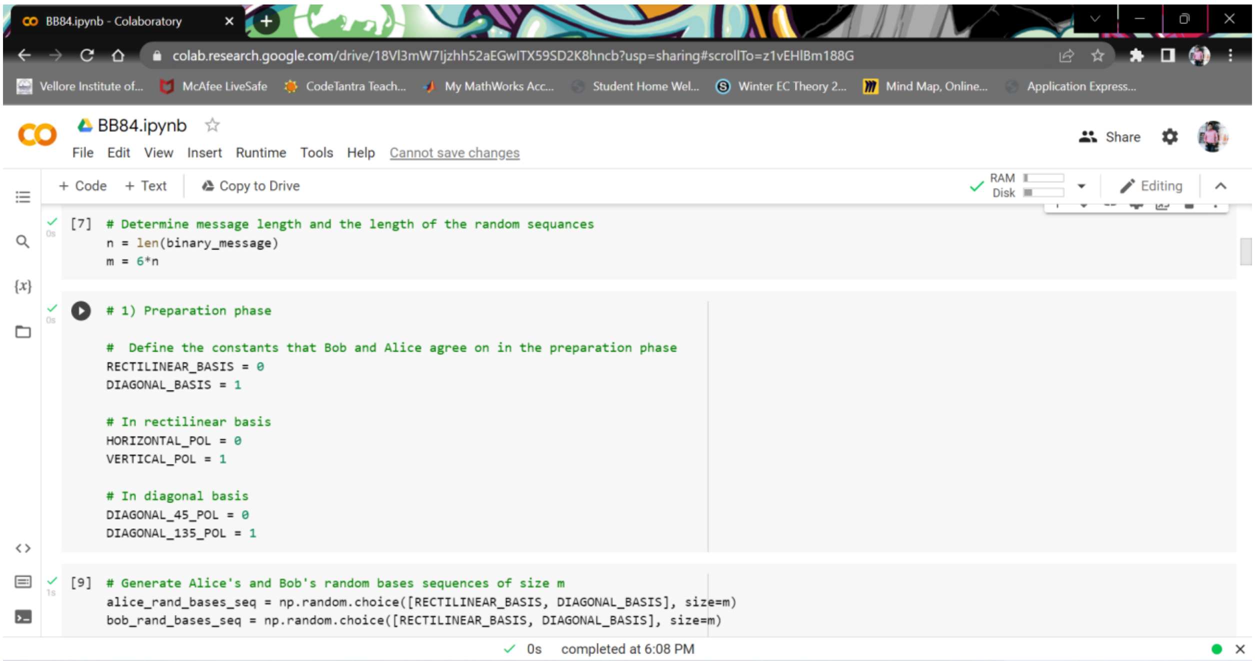
1. Importing qutip and numpy libraries in python.



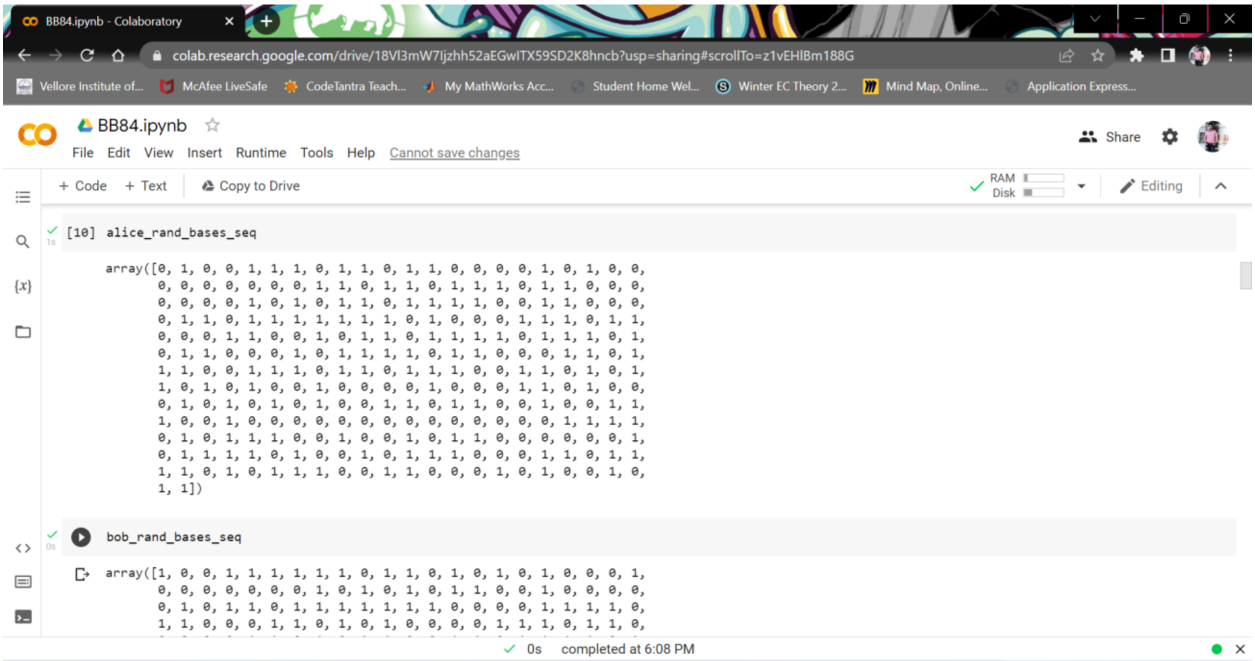
2. Here, we can see that we are giving our message as amrith after defining our converting function.



3. We will fix the length of random sequence here. We will also define constants before sending message.



4. We will determine random base sequence of size m for both the sender and receiver.



Random bit sequence for sender

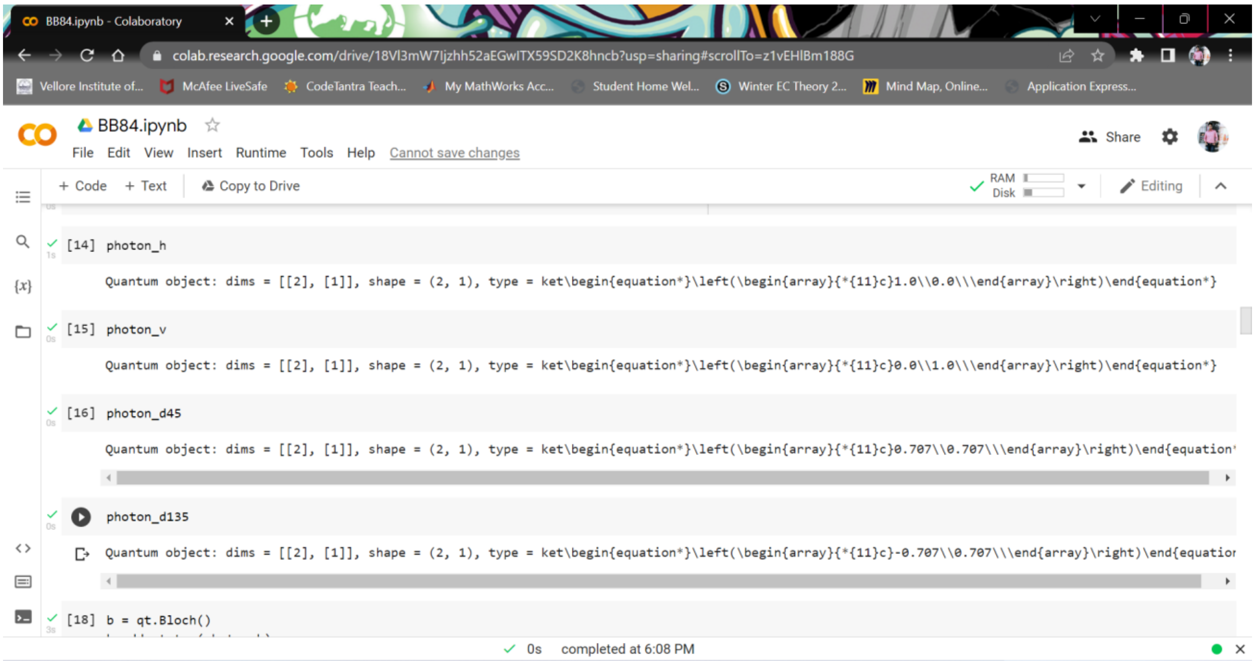
Random bit sequence for receiver.

```
[11] bob_rand_bases_seq

array([1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1,
       0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0,
       0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0,
       1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0,
       0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1,
       1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1,
       1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0,
       0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1,
       1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1,
       1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1,
       0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1,
       0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1,
       1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1,
       0, 1])
```

5. We will define polarization state for different vector space(horizontal,vertical,etc).

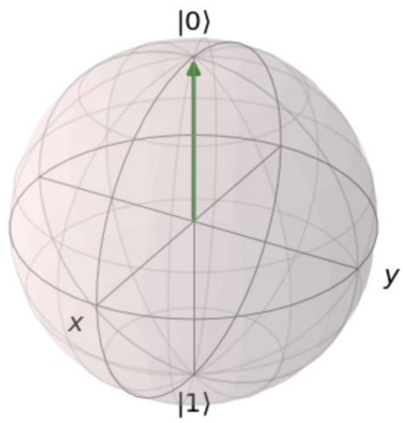
```
[13] # Describe bases of Hilbert vector space
     basis_0 = qt.basis(2,0)
     basis_1 = qt.basis(2,1)

     # Describe polarization states in Hilbert vector space
     photon_h = basis_0                            # horizontally polarized photon
     photon_v = basis_1                            # vertically polarized photon
     photon_d45 = (basis_0 + basis_1).unit()       # diagonally polarized photon (45 deg)
     photon_d135 = ((-1)*basis_0 + basis_1).unit() # diagonally polarized photon (135 deg)
```

6. Different vector spaces configured for photon.



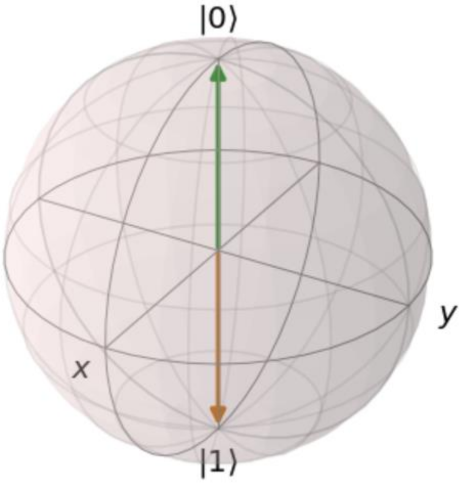
Horizontal photon

```
b = qt.Bloch()
b.add_states(photon_h)
b.show()
```



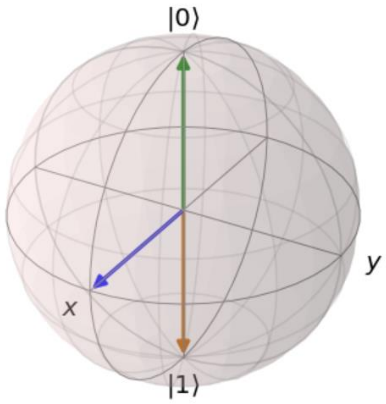
Vertical photon

```
b.add_states(photon_v)
b.show()
```



Diagonal_45_degree Photon

```
b.add_states(photon_d45)
b.show()
```



7. Define the measurement operators simulating receiver's choice of polarization filters. Receiver uses vertically oriented filter for measurement in rectilinear basis and diagonally oriented filter (45 deg) for measurement in diagonal basis.
   Here, we are going to transmit our message to receiver on his random sequences. We have defined the various signs for various basis of vector of photon transmitted by polarizer.

```python
# 2) Transmission phase

def pick_photon_polarization(basis, bit_value):
    # Polarization of the photon Alice sends depends on her random sequances
    if basis == RECTILINEAR_BASIS:
        if bit_value == HORIZONTAL_POL:
            photon = photon_h
            sign = "H"
        else:  # bit_value == VERTICAL_POL:
            photon = photon_v
            sign = "V"

    else:  # basis == DIAGONAL_BASIS
        if bit_value == DIAGONAL_45_POL:
            photon = photon_d45
            sign = "D45"
        else:  # bit_value == DIAGONAL_135_POL
            photon = photon_d135
            sign = "D135"

    return photon, sign
```

Transmission getting performed.

```python
# Perform transmission

bob_measured_values = []
photons_sent = [] # keep track of the photons Alice sent (for demonstration purposes)

for basis_a, bit_value, basis_b, i in zip(alice_rand_bases_seq, alice_rand_bit_seq, bob_rand_bases_seq, range(m)):

    # Alice picks a polarized foton source according to her random sequances
    photon, sign = pick_photon_polarization(basis_a, bit_value)
    photons_sent.append(sign)

    # Alice sends the picked photon to Bob
    if eavesdropper_present:
        _, photon = measure_polarization(photon, eve_rand_bases_seq[i])

    #Bob measures the photon
    value, _ = measure_polarization(photon, basis_b)
    bob_measured_values.append(int(value))  # append value to the end of Bob's measurements sequence
```

New array or stack created after transmission.

```
np.vstack([
          np.array(photons_sent),
          bob_rand_bases_seq,
          np.array(bob_measured_values)
          ]).T[:11, :]
```

```
array([['V', '1', '1'],
       ['D45', '0', '1'],
       ['H', '0', '0'],
       ['H', '1', '0'],
       ['D45', '1', '0'],
       ['D45', '1', '0'],
       ['D135', '1', '1'],
       ['H', '1', '1'],
       ['D45', '1', '0'],
       ['D45', '0', '1'],
       ['H', '1', '1']], dtype='<U21')
```

8. We will check here whether eavesdropping is happening by comparing the keys of both parties.

```
[40] # Compare chosen subsets
     sequences_identical = bob_measured_values == alice_rand_bit_seq
```

```
[41] sequences_identical
```

```
True
```

```
if sequences_identical:
    secret_key = alice_rand_bit_seq[:n]  # use first n bits of final sequance as key
    print("Key was safely established.")

else:
    raise SystemExit("Eavesdropper was detected! Key couldn't be safely established.")
    # The bellow code is not executed, communication has to be repeated until a safe key is established.
```

```
Key was safely established.
```

9. Our new binary and encrypted message.

Our binary message-

```
[43] binary_message
```

```
'0110000101101101011100100110100101110100011010000'
```

```
[44] np.array(secret_key)
```

```
array([0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1,
       0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1,
       1, 1, 1, 1])
```

10. Applying Verman cipher to encrypt message before quantized transmission.

```python
def encrypt_message(message, key_seq):
    """ Encrypt message by Vernam cipher
    """
    key = ''.join(map(str, key_seq))
    bin_message = message_to_binary_str(message)

    # Perform binary XOR on the message and the key bitwise
    encrypted_bin_seq = [str(int(m) ^ int(k)) for m, k in zip(bin_message, key)]

    encrypted_bin_str = ''.join(encrypted_bin_seq)
    encrypted_message = binary_str_to_message(encrypted_bin_str)

    return encrypted_message


def decrypt_message(message, key_seq):
    """ Decrypt message encrypted by Vernam cipher
    """
    return encrypt_message(message, key_seq)  # messages are encrypted en decrypted the same way in Vernam binary cipher
```

Our encrypted message.

```python
# Encrypted messages can be send over classical chanel with unconditional security
encrypted_message = encrypt_message(message, secret_key)

print("The encrypted message is: " + encrypted_message)
```

```
The encrypted message is: A
?b;W
```

Our decrypted message which we sent.

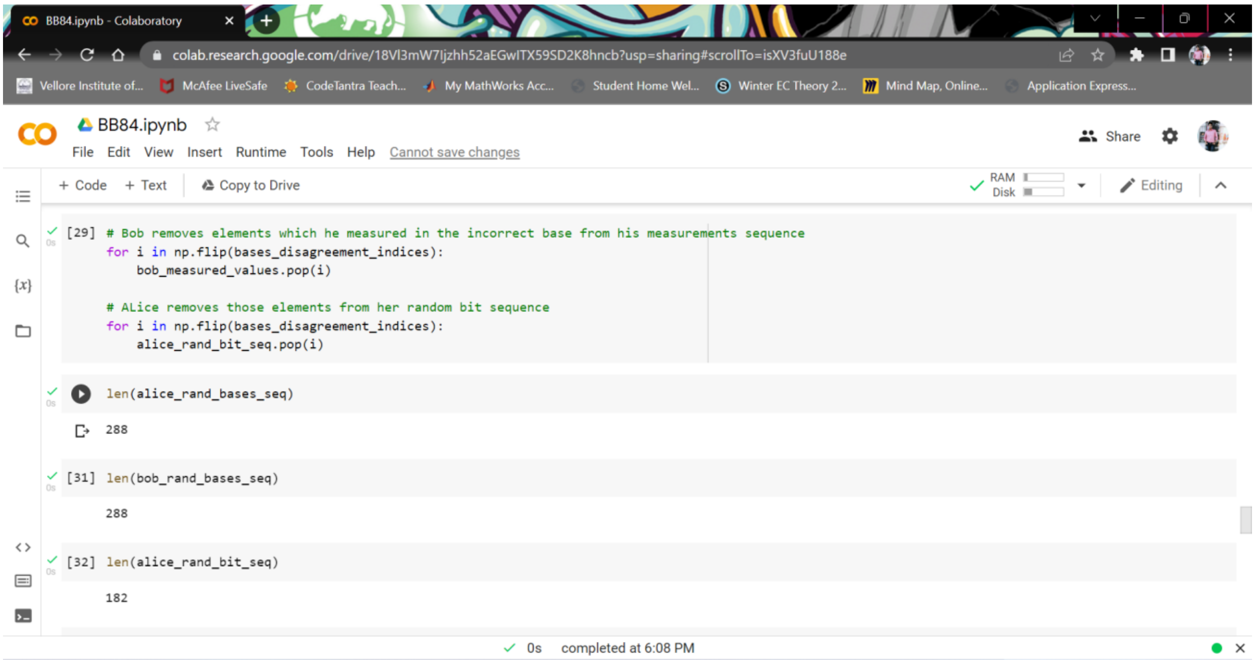
```python
# Bob can decrypt the messages with his copy of the secret key
decrypted_message = decrypt_message(encrypted_message, bob_measured_values[:n])

print("The decrypted message is: " + decrypted_message)
```

```
The decrypted message is: amrith
```

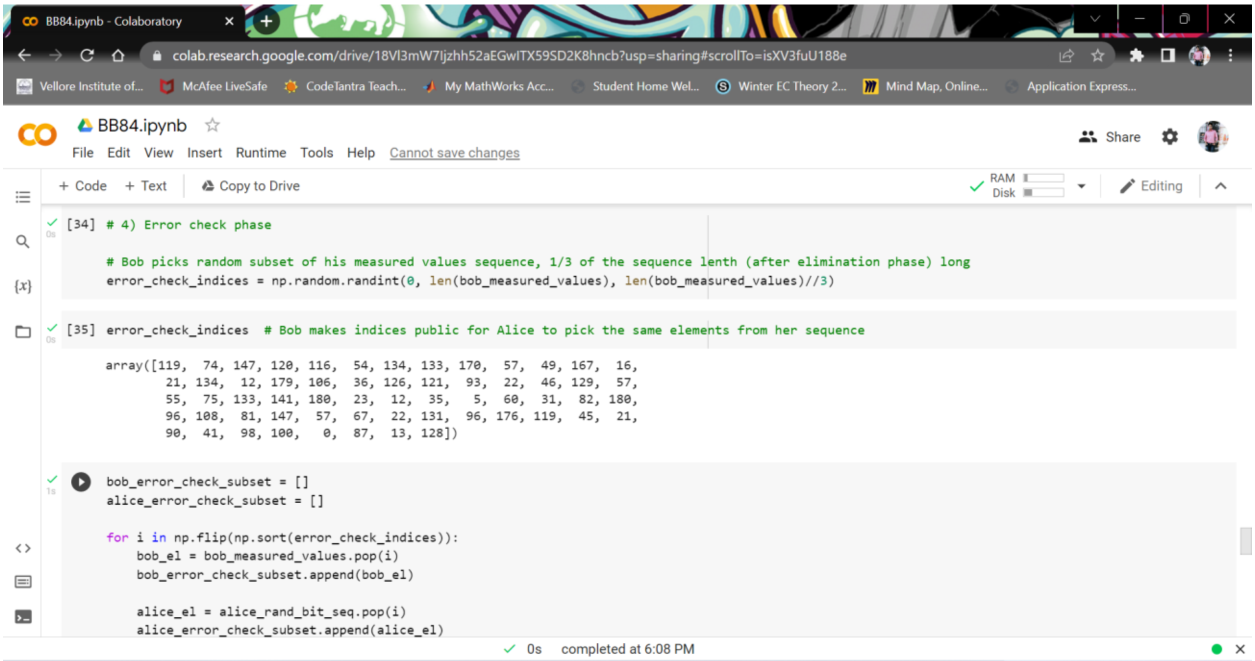
Analysis

<u>Error handling-</u>

Removing incorrect bases of vector from measurement. Checking length as well.



Error checking part. We will be comparing length of both values.



Length of sender & receiver message are same. So, no error.

```
[37] m

288

[38] len(bob_measured_values)  # see that a big part of bits from the original sequence had to be sacrificed,
                               # that's why m was chosen 6 times bigger that n in the begining

122

len(alice_rand_bit_seq)

122
```

Total time taken for the process: 7.919414043426514 Seconds

Analyzing the efficiency

Simulation of quantum cryptography.

In this simulation we can see the different polarities (bases of vector) of photons being transmitted from person1 to person2. Here we will keep changing the key length to check efficiency of various transmission.

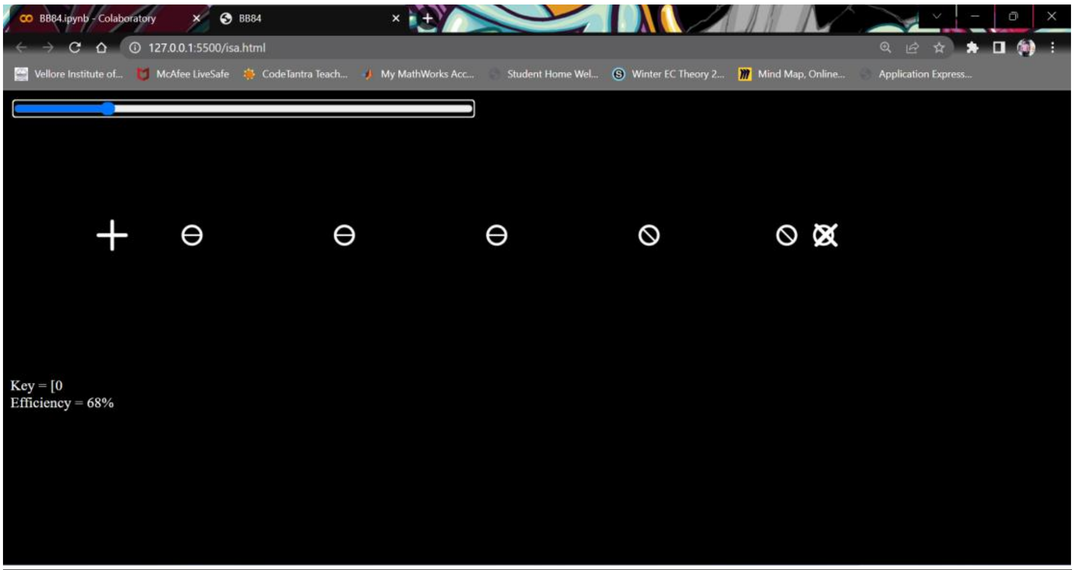
*Parameter used for calculation of efficiency is floor value of (100*keysize/countqubits).*

Basic algo being used here is

```
var q = [];
var a = new detector_emitter(w/9,h/2);
var b = new detector_emitter(8*w/9,h/2);//20BCE2005
var key=" ";

function setup() {
  createCanvas(w, h);
  background(0);
  noFill();
  stroke(255,0,0);
  strokeWeight(5);

  frameRate(70);
  keyDisp = createDiv('');
  eff = createDiv('');
  q.push(new qubit(a.x,a.y,a.basis));

  keyDisp.html("Key =  "+key);
  eff.html("Efficiency = 0%");

  time = createSlider(25, 750, 40);
  time.position(10,10);
  time.style('width', '500px');
}
function draw() {
  if(frameCount%Math.floor(time.value())==0){
    a.updateBasis();
    q.push(new qubit(a.x,a.y,a.basis));
  }
  background(0);
```

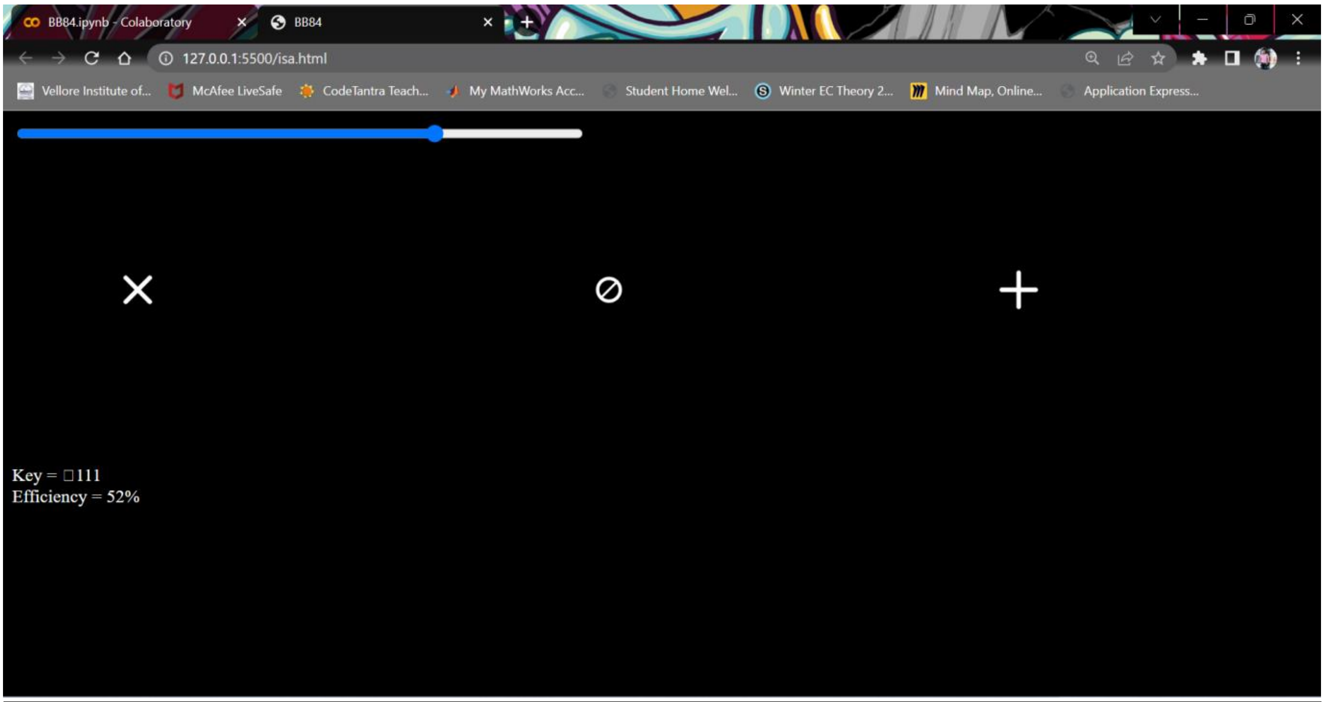
```
a.renderBasis();
b.renderBasis();
for(i=0;i<q.length;i++){
  q[i].renderQubit();
  q[i].renderSpin(q[i].basis);
  q[i].updatePos(1,0);
}
if((q[0].x-b.x)*(q[0].x-b.x)+(q[0].y-b.y)*(q[0].y-b.y)<=2){
  countqubits++;
  if(q[0].basis==b.basis){
    key=key+q[0].state
    keyDisp.html("Key =  "+key);
    keysize++;
  }
  eff.html("Efficiency = "+Math.floor(100*keysize/countqubits)+"%");
  b.updateBasis();
  q.shift()
}
```

Different efficiency for different key. For ex let’s say our key is [0, the efficiency comes out to be 68%. Here length of our key 8 bits.

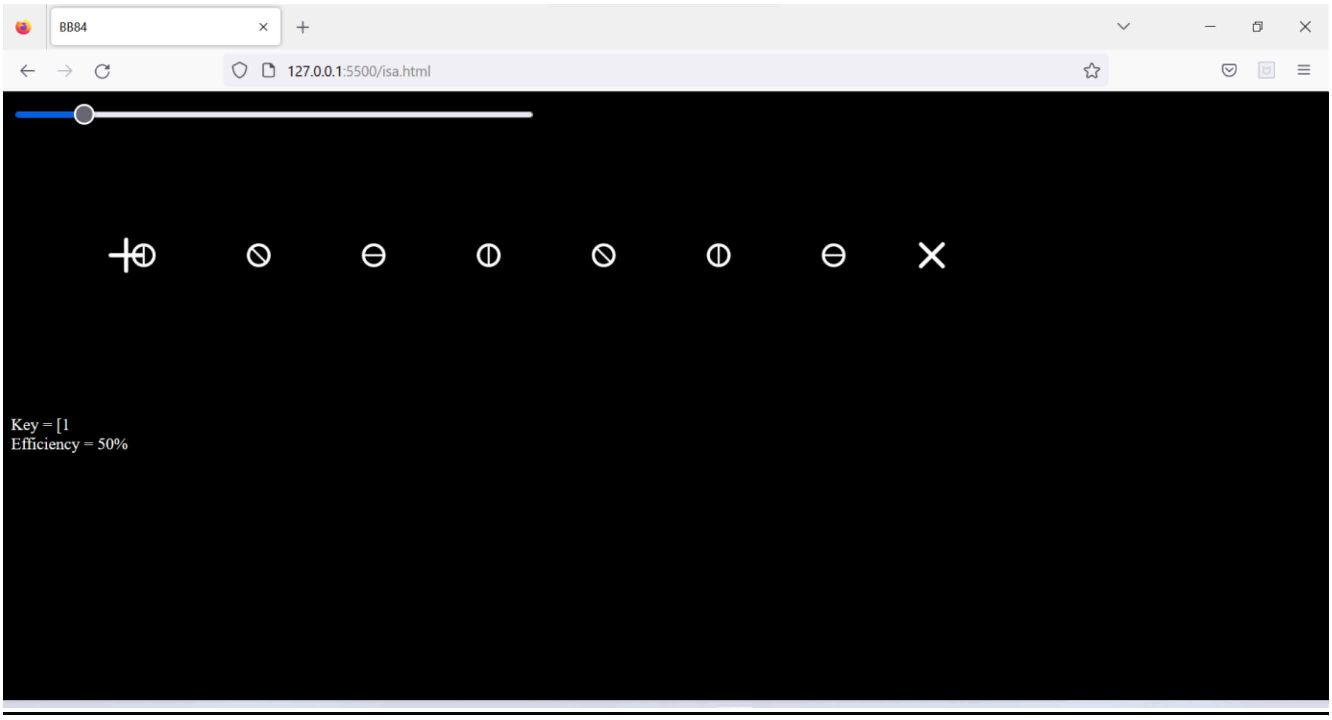


Now let’s decrease length of our key to 2. Efficiency comes out to be 55%

We are increasing our key length to 16 bits with key as []11. Here efficiency decrease to 52%



Now again we are decreasing our key length to 4 bits with key as 11, efficiency as 50%

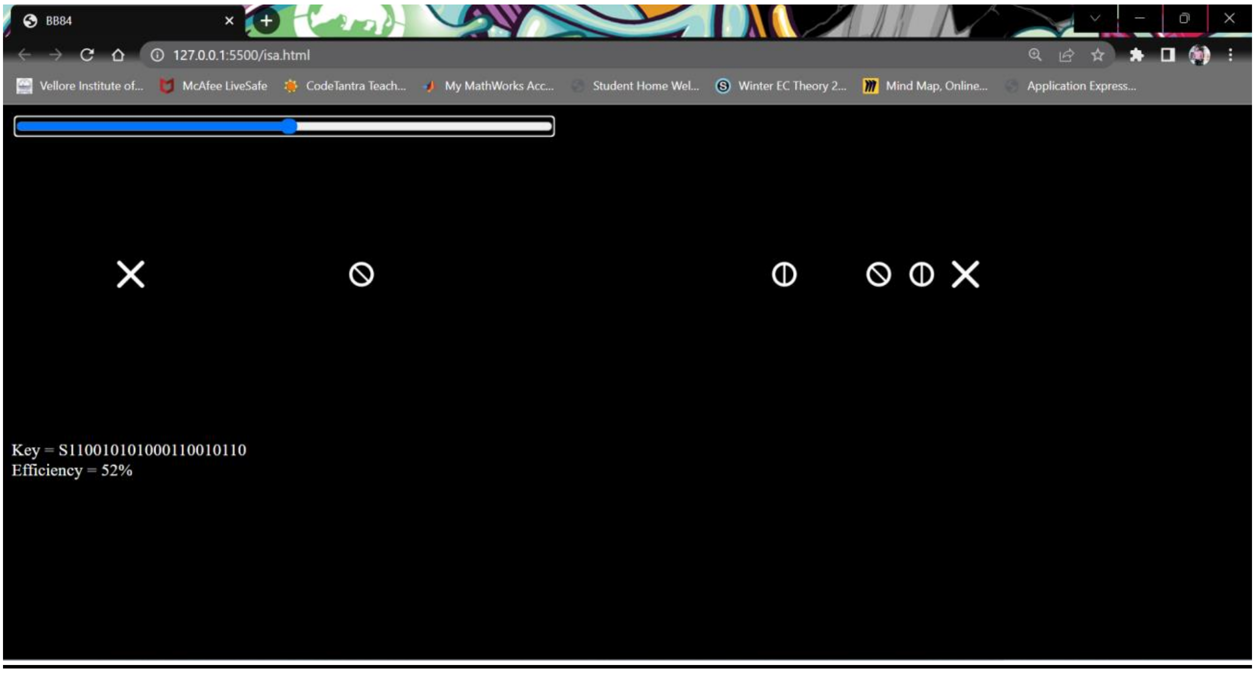


With key as []0100, efficiency of transmission comes out to be 54%

If we change key to 0011, efficiency decreases to 52%

Here, we are waiting for transmission to almost complete and efficiency comes out to be 48% at the end.

At the end of transmission, with a key of length of 28 bits, efficiency is 52%.



By the various scenarios presented above, we concluded that efficiency remains to be around 52% for 28 bits key. But it decreases as we decrease the size of our key and goes around 48%. So, our code is working efficiently for larger key value. The average efficiency of transmissions of different sizes of key remains to be around 50%.

Conclusion and Future Work

A significant and special trait of quantum cryptography is the capacity to identify the presence of any outsider between two conveying clients. The security of quantum cryptography relies upon the establishment of quantum mechanics, and that can change the organization security. QKD methods can be hitched to standard web innovation so as to give profoundly tie down correspondences to handy use. While there have been significant headways in the field of quantum cryptography in the most recent decade, there are still difficulties ahead before quantum cryptography can turn into a broadly conveyed key dispersion framework for governments, organizations, and academics.

Basically, these difficulties incorporate growing further developed equipment to empower higher caliber and longer transmission separations for quantum key trade. The advances in PC preparing power and the danger of impediment for the present cryptography frameworks will stay a main thrust in the proceeded with innovative work of quantum cryptography. The innovation can possibly make an important commitment to the organization security among government, organizations, and scholastic climate.

Setting the topology that allows for multiple users to access the network is challenging. The popular star topology is suitable for relatively short distance transfers (up to 400km); as a result, more networks and devices are required to cover a greater distance. An effective solution for increasing the range of communication would be introducing an intermediate node between any two users. This could allow for secure quantum communication among all users without requiring a trusted relay. Thus, reducing the cost per user since only one set of measurement devices is necessary for a large shared network.
There are several challenges facing quantum cryptography that range from infrastructure development to public adoption and global-scale networks. Addressing these challenges is complex, and many of the world's brightest individuals are working hard to come up with the necessary solutions.

References:

[1] L. Strate, “The varieties of cyberspace: Problems in definition and delimitation,” Western Journal of Communication, vol. 63, no. 3, pp. 382–412, 1999.

[2] J. Shen, J. Shen, X. Chen, X. Huang, and W. Susilo, “An efficient public auditing protocol with novel dynamic structure for cloud data,” IEEE Transactions on Information Forensics and Security, vol. 12, pp. 2402–2415, 2017.

[3] J. Li, Y. Zhang, X. Chen, and Y. Xiang, “Secure attribute-based data sharing for resource limited users in cloud computing,” Computers & Security, 2017.

[4] 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 Inter- national Conference on Embedded and Ubiquitous Computing (EUC), pp. 46–50, Guangzhou, China, July 2017.

[5] 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.

[6] 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.

[7] 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.

[8] Y.-M. Tseng, “An efficient two-party identity-based key exchange protocol,” Informatica, vol. 18, no. 1, pp. 125–136, 2007.

[9] 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 Publish- ing, Cham, 2017.

[10] 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.

[11] J. Shen, T. Zhou, F. Wei, X. Sun, and Y. Xiang, “Privacy- Preserving and Lightweight Key Agreement Protocol for V2G in the Social Internet of Things,” IEEE Internet of Things Journal, pp

[12] A. Peres, Quantum Theory: Concepts And Methods, Springer Science & Business Media, 2006.

[13] S. Wiesner, “Conjugate coding,” ACM SIGACT News, vol. 15, no. 1, pp. 78–88, 1983.

[14] C. H. Bennett and G. Brassard, “WITHDRAWN: Quantum cryptography: Public key distribution and coin tossing,” Theoretical Computer Science, 2011.

[15] A. K. Ekert, “Quantum cryptography based on Bellaˆs theorem,” Physical Review Letters, vol. 67, no. 6, pp. 661–663, 1991.

[16] C. H. Bennett, “Quantum cryptography using any two nonorthogonal states,” Physical Review Letters, vol. 68, no. 21, pp. 3121–3124, 1992.

[17] B. Huttner, N. Imoto, N. Gisin, and T. Mor, “Quantum cryp- tography with coherent states,” Physical Review A: Atomic, Molecular and Optical Physics, vol. 51, no. 3, pp. 1863–1869, 1995.

[18] D. Bruß, “Optimal eavesdropping in quantum cryptography with six states,” Physical Review Letters, vol. 81, no. 14, pp. 3018– 3021, 1998.

[19] P. Li, J. Li, Z. Huang, C.-Z. Gao, W.-B. Chen, and K. Chen, “Privacy-preserving outsourced classification in cloud comput- ing,” Cluster Computing, pp. 1–10, 2017.

[20] C. Crépeau, “Quantum oblivious transfer,” Journal of Modern Optics, vol. 41, no. 12, pp. 2445–2454, 1994.

Appendix:

Link for code-
https://colab.research.google.com/drive/18Vl3mW7Ijzhh52aEGwITX59SD2K8hncb?usp=sharing#scrollTo=0vKis5p9188v

Work carried out

S.NO	**NAME**	**WORK**
1.	Amirth Raj	• Establishing Method flow (Overall Architecture and Methodology) • Code implementation
2.	Snehil Sinha	• Creating Report (Results, Analyzing Efficiency) • Code implementation
3.	Anshuman Gupta	• Research (Abstract, Introduction, Literature Survey and Conclusion) • Code collection