Ministry of Education and Science of the Republic of Kazakhstan
Suleyman Demirel University

Selbayev Almas

Development and analysis of the optical communication system with quantum cryptography

THESIS

Presented in Partial Fulfillment for the
Degree of Master of Science in Computing Systems and Software
(degree code: 6M070400)
Department of Computer Sciences
Faculty of Engineering and Natural Sciences

Supervisor: **Aitchanov Bekmurza**

Kaskelen, 2019

Abstract

Cryptography has always been a key distribution problem, which is currently successfully solved using asymmetric encryption algorithms with a private key that does not leave its owner. One of the most common of these today is the RSA algorithm. However, encryption ensured by the lack of computing power in the world at present for the Opportunity of the entire cryptanalysis. In connection with the development of scientific? Therefore, the emergence of such computing power is to look for new methods and technologies for key distribution. One of such technologies, especially for users whose information requires increased protection, in the future may be the technology of quantum key distribution of quantum physics. This work contains the emerging problems of asymmetric algorithms in view of the fundamentals of quantum cryptography, the BB84 protocol, and the possibility of applying technologies for the quantum distribution of keys in passive optical networks and implemented on MatLab.

Аңдатпа

Криптография әркашан кілттерді тарату проблемасы болып табылады, ол енді өз несін қалыпырмайтын жеке кілтпен асимметриялы шифрлау алгоритмі арқылы сәтті шешілді. Бүгінде RSA алгоритмі ең таралған. Дегенмен, шифрлау қазіргі уақытта барлық криптоанализ мүмкіндіктері үшін әлемдегі есептеу қуатының жетіспеушілігінен қамтамасыз етіледі. Ғылым дамуына байланысты? Осылайша, мұндай есептік бірліктің пайда болуы басты тарату үшін жаңа әдістер мен технологияларды іздеуде жатыр. Мұндай технологиялардың бірі, әсіресе ақпаратты қорғауды күшейтетін пайдаланушылар үшін болашақта кванттық физика кванттық кілттерді бөлу технологиясы болуы мүмкін. Бұл мақалада кванттық криптографияның негіздері, BB84 протоколы және пассивті оптикалық желілердегі кванттық кілттерді тарату технологиясының қолданылуы ескеріле отырып, асимметриялық алгоритмдер пайда болған проблемалар бар.

Аннотация

Проблема криптографии является проблемой распространения ключей. На данный момент данная проблема решается через алгоритмы асимметричного шифрования с закрытым ключом, как пример можно взглянуть на наиболее популярный алгоритм RSA. Однако, данная защита обособлена тем, что на данный момент не существуют достаточной вычислительной техники для успешного раскрытия шифра, но с идеей квантовых вычислений, которая может решать данный тип шифрования, за считанные секунды, нам требуется новый метод защиты данных и их шифрования. Одной из таких технологий может стать квантовое распределения ключей, защита которая обусловлена физическими свойствами фотона, которая может стать хорошей заменой для алгоритмов асимметричного шифрования. Эта работа содержит возникающие проблемы асимметричных алгоритмов с учетом основ квантовой криптографии, протокола BB84 и возможности применения технологий для квантового распределения ключей в пассивных оптических сетях и смоделированная на MatLab.

Acknowledgements

Thanks to my thesis supervisors for support and useful discussion. thanks external reviewer for very useful feedback that helped to significantly improve the current work. Thanks to my family and friends.

Contents

1. Introduction

One of the serious problems of cryptography has always been the problem of key distribution. For example, symmetric algorithms that use a common secret key require that both parties already have this key from the beginning. That is, if the poisoner wants to transmit an encrypted message using a symmetric algorithm, then he needs to seriously think about how to safely transmit the key to the recipient. The creation of asymmetric cryptographic algorithms suggested an elegant solution to this problem. A key pair is created: an OPEN and a private key (which causes another name for these algorithms - two key algorithms or public key algorithms). The public key is in free access; the private key is always on each side of the exchange of information and does not leave them. These keys are mathematically related in such a way that they satisfy the following conditions[1]:

- Computationally easy to create a key pair.
- Computationally easy to create an encrypted message with a public key and an unencrypted message.
- Computationally easy to decrypt the message using the private key.
- It is computationally impossible, knowing the public key and the encrypted message, to recover the original Message.

That is, if Alice wants to send the encrypted Message to Bob, then she only needs to take Bob's published public key, encrypt the message and send it to the addressee, and only Bob will be able to decrypt the message with his Private Key. It should be noted that the Secret Key for a symmetric algorithm can be the original message - such a scheme is used very often. An attacker, having freely received both an encrypted message and a public key, cannot do anything with this set.

1.1 Motivation

Quantum cryptography is an extremely powerful part of present day cryptographic science, promising numerous new points of view in customary zones of use - conciliatory correspondences, military, business and different territories that require the exchange of mystery data. Exploratory and hypothetical work on quantum cryptography, completed until today, considered an assortment of different trade plans and expert tools, just as the security of these plans and conventions in connection to different strategies for unapproved get to. Among the effectively thought about methods, there are numerous very intricate ones that are essentially unrealizable in the structure of the innovation of the not so distant.

1.2 Aims and Objectives

The main goal is to develop model on MatLab and show the Eve's probability of eavesdropping, by increasing sending qubits to Bob by Alice.
Objectives:

- Develop models with quantum states for experiments in encrypting and deciphering
- Analysis tools for develop quantum systems
- Analyze algorithms BB84, B82
- Build a model with Quantum Key Distribution based on existing algorithms
- Implementation of quantum encryption methods for token generation

2. Analysis of quantum cryptography system models

Since antiquated times, individuals have looked for methods for correspondence that would beyond any doubt the protection of the transmitted data in mystery from outsiders, which was significant for the requirements of tact, exchange, military Affairs and love correspondence. Different sorts of data coding were utilized for this reason. Every one of them gave the mystery of the transmitted data somehow, yet none of them gave outright assurance. In 1918, Vernam Invented the figure, for which later, toward the finish of the 40-ies,, was held evidence of total mystery. The states of this mystery are, truth be told, the principle downside of this figure: a very irregular key of a similar length as the transmitted message is required, and this key ought to be utilized just once. In this way, before you can send a mystery message, you should initially go through a channel that is exceptionally secure from unapproved get to, a similar length of the message containing the mystery key. Such a framework is bulky, badly arranged to utilize and costly, which is the reason it is occasionally utilized. During the 70s, the supposed open key cryptography framework was created, in which there are two keys: one for scrambling messages, freely unveiled, and the other for unscrambling, stayed discreet. This system currently utilized all over the place, despite the fact that its mystery has not been carefully demonstrated by anybody (as, for sure, the inverse has not been demonstrated). System depends on an exceptional sort of capacities, the computation of which one way is not troublesome, and the other way - troublesome. Specifically, the issue of calculating the mystery key within the sight of an open key is diminished to the issue of factorization of huge numbers, which is viewed as hard to fathom up to this point. Nevertheless, because of the normal appearance of quantum PCs for which quick factorization calcula-

tions have just been created. open key frameworks may lose their adequacy. In this way, there was a requirement for cryptographic frameworks dependent on different standards. The work "Conjugate coding", which composed by Stephen Wiesner from Columbia University, at initial couple of individuals saw and not in any case distributed, denoted the start of another heading in cryptographic science - quantum cryptography. In it, because of the laws of quantum mechanics, it ended up conceivable to disseminate between at least two supporters a mystery key that meets every one of the necessities of the Vernam figure, which means the outright mystery of the transmitted data. In 1984, Bennett and Brassard licensed the primary trade Protocol for a quantum cryptographic framework, known as BB84. From that point forward, enthusiasm for quantum cryptography on the planet started to develop amazingly rapidly, and to date, countless examinations have been led, influencing different parts of it. As indicated by the creators of BB84, quantum cryptography is a strategy that permits two clients who don't at first have any mystery information com-mon to them to concur on an arbitrary key that will be mystery from an outsider who activities unapproved access to their interchanges. In cryptographic science has built up its very own conventional phrasing, explicit sounding at first look, however extremely advantageous by and by. In this manner, lawful clients are generally called "Alice" and "Weave", while the individual who performs unapproved access is classified "eve". We will not go amiss from the groups and will keep this terminology in this paper. The primary quantum mechanical rules that structure the reason for quantum cryptography are: 1. The failure to recognize totally two non-symmetrical quantum States The discretionary condition of any two-level quantum mechanical framework can be spoken to as a direct superposition of its eigenstates and with complex coefficients: . where. The laws of quantum mechanics do not permit to recognize two quantum States completely dependably also, if not met zero, for example the States are symmetrical. 2. The forbiddance of cloning hypothesis Due to the unitarity and linearity of quantum mechanics, it is difficult to make a precise of an obscure quantum state without influencing the underlying state. For instance, assume Alice and Bob utilize two-level quantum frameworks to transmit data, encoding bits of information by the States of these systems. On the off chance that eve catches the transporter of data sent by Alice, measures its state and sends further to Bob, at that point the condition of this bearer will be unique, than at estimation. Hence,

listening stealthily on a quantum channel incites transmission mistakes that can be distinguished by genuine clients. 3. Quantum ensnarement two quantum mechanical frameworks (even isolated spatially) can be in a condition of connection. so the estimation of the chose esteem did on one of the frameworks will decide the aftereffect of the estimation of this incentive on the other. This impact is called quantum ensnarement. None of the caught frameworks is in a specific state. so the snared state cannot be composed as an immediate result of the States of the subsystems. The singlet condition of two particles with turn 1 2 can fill in for instance of an ensnared state: The estimation performed on one of the two subsystems will give with equivalent likelihood or. and the condition of the other subsystem will be inverse (i.e., if the estimation result on the principal framework was. and Vice versa). Causation and superposition Causality. which isn't at first an element of non-relativistic quantum mechanics. can in any case utilized for quantum cryptography in con-intersection with the guideline of superposition: if two frameworks whose States structure a specific superposition are isolated in time. without being associated by causality. it is difficult to decide the superposition state by taking estimation on every one of the frameworks consecutively. The correspondence procedure will be talked about in detail on the case of the BB84 Protocol. as generally the first and most well-known right now. The rest of the conventions will be depicted in all respects quickly. With respect to the particular plans of quantum cryptographic establishments. here will be viewed as just those of them. listening in which is the subject of this investigation utilizing the trade conventions BB84 and B92 on phase states.

3. Building model for key generation based on QKD Protocols

3.1 Protocol BB84

Quantum key distribution is the widely used and most studied area of quantum technologies. Firstly introduced in 1984. algorithm of key exchanging based on quantum bits properties. The main feature hidden in physical properties of quantum physics. it says you can not make a identical copy of an unknown quantum. otherwise the state that you are trying to copy will be destroyed. Uncertainty principle of Heisenberg states: when we try to measure one quant, to identify its state. that quant's information is destroyed. The main idea was created by Wiesner. but it was rejected. because everybody decided this idea as fantastic. But then in 1984. C.Bennet and G.Brassard developed this idea more in practical way. They started to send the encrypted key in quants throw optical channel.The secret key can build by simple quantum state. this rule used by BB84 protocol. Alice. sender. sends a big randomly length of photons to the Bob. receiver. Alice chooses one 2 Basises shown on below (Figure 3.1). and the direction of photon. particularly horizontal or vertical or diagonal ones 15 or -15 either [2].

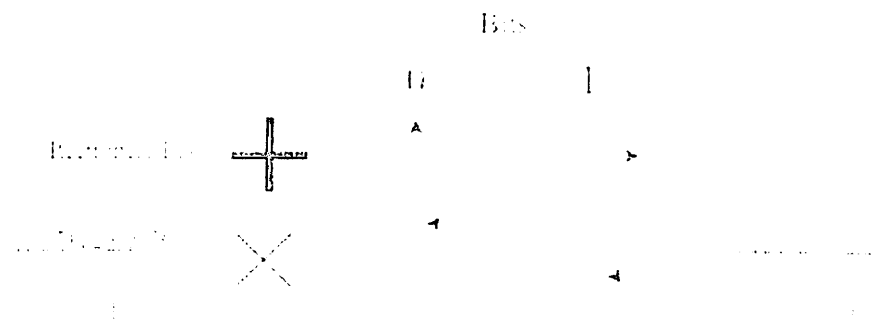

Figure 3.1: Photon Polarization

Each polarization of photon represents bit 1 and the other one represents bit 0 as shown in figure 3.1. Alice sends to Bob a sequence of bits. photons . for each photon there is need to randomly choose the value and in which base it will be. Bob's job is to try identify the polarization . by randomly choosing type of measurement for each photon. The measurement bases are given: horizontal. vertical and diagonal. For example. The beginning of the interaction of the parties begins with the fact that Alice generates and sends photons with the selected polarization to Bob (Figure 3.2). A light emitting diode or a laser can be used as a light source. and a fiber or air can be used as a conductor as shown on table 1.

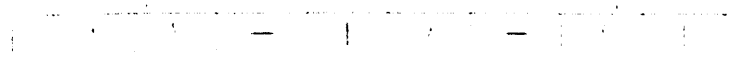

Figure 3.2: Alice sends bits with selected polarization

Then for each photon. Bob randomly chooses the type of polarization measurement: it measures either straight-line polarization (+) or diagonal (x) (Figure 3.3).

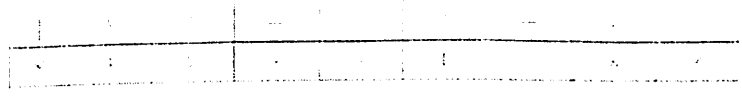

Figure 3.3: Bob's randomly choosen polarizations

Bob records the results of the measurements he just made. which he keeps in secret (Figure 3.1).

Figure 3.4: The Alice and Bob's measurements

Bob openly announces what type of measurements he took, and Alice tells him which measurements were correct. These data are then translated according to a predetermined rule into bits, the sequence of which is the result of the initial quantum transmission (Figure 3.5).

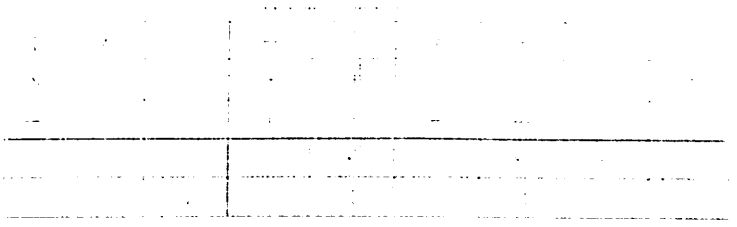

Figure 3.5: The Final Key

Next, the received key is checked for interception by the attacker. If an attacker intercepted information using equipment similar to Bob's equipment, then in about 50% of cases he would choose the wrong analyzer, therefore, he would not be able to determine the state of the photon he received and send the photon to Bob in a random state. In this case, in 50% of cases, he will choose the wrong polarization, which means that in about 25% of cases, the results of Bob's measurements may differ from those of Alice. This number of errors is quite easy to notice. Evaluation of the presence or absence of interception is performed by Alice and Bob over an open channel by comparing and discarding the subsets of the data obtained. If an interception is detected, then Alice and Bob begin the procedure again. If there is no discrepancy, the bits used for the comparison are discarded, the key is accepted.With probability 1- 2- * where K is the number of bits compared) the channel was not tapped. More detailed information about this and other algorithms are discussed in the literature [3].

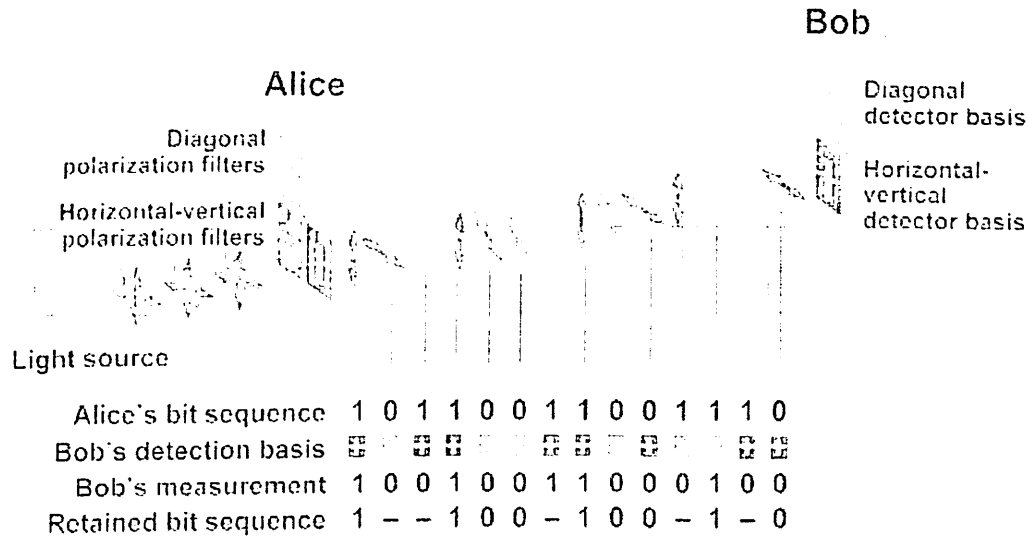

Figure 3.6: Quantum Key Distribution

The bit is the smallest unit of classical information measurement. In the field of quantum cryptography, we use quantum bit-qubit, and a vector of length one in a complicated two-dimensional vector space describes it mathematically. Like in classical systems, there are also several types of gates in quantum systems also. However, unlike classical gates, which can be both reversible (NOT) and irreversible (OR, AND), quantum gates must be reversible as subatomic element interaction must be symmetrical in time. Mathematically expressed as Pauli matrices are three government single qubit gates, which implies 2x2 matrices. For a single quantum bit (a 2x1-column vector), these doors can be practical. The matrices of Pauli are shown below:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad (1.$$

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad (2.$$

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad (3.$$

Figure 3.7: Pauli Matrices

Where i is the representation of complex numbers. Every of the three of these

entryways play out a particular capacity in quantum calculation and data. The entryways are frequently meant as X, Y and Z, individually. Purpose of X gate is same as NOT gate's functionality in classical systems, i.e. returns output 1 for input qubit 0 and vice versa. The Z gate performances on a 1-qubit system by leaving the qubit in the basis state |0 unchanged and performing a sign flip on everything else, as shown in the following mapping: 0 no state alteration 1 sign flip alteration Hadamard Gate The Hadamard gates is a significant quantum entryway regularly utilized in quantum circuits as a result of its capacity to put qubits in a superposition. In quantum data handling, the Hadamard change, all the more frequently called Hadamard door, is a one-qubit task that changes either premise state into an equivalent superposition of both premise states. At the end of the day, there is an equivalent likelihood of estimating either premise state. Numerically, a Hadamard door is communicated as pursues:

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad (4$$

Figure 3.8: Hadamard's matrices

CNOT Gate The controlled NOT door is a reversible entryway frequently composed as CNOT. This door begins with two sources of info and yields two yields. With a CNOT entryway, two sections must be comprehended, the control bit and the objective piece. The control bit (top) is appeared as a strong dab, and the objective piece (base) is spoken to by the image and, known as the selective or administrator (XOR). If the control bit input is a 0 then the target bit will be unchanged. However, if the control bit is a 1 then the target bit will flip. CNOT gate matrix:

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Figure 3.9: CNOT matrices

Toffoli Gate The Toffoli gate is like CNOT gate, like a controlled-controlled NOT gate. The Toffoli gate has two control bits and one target bit. Toffoli gate matrix:

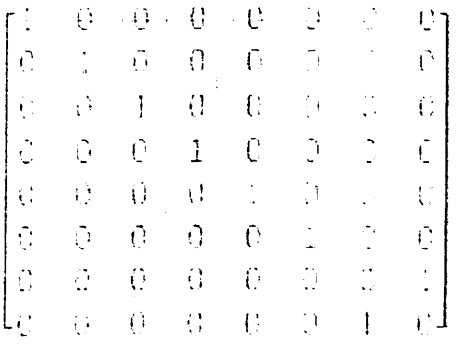

Figure 3.10: Toffoli Gate Matrix

Swap Gate The Swap gate does precisely what it names infers: it swaps two qubits and can be spoken to by the accompanying framework, where the 1s in lines 2 and 3 trigger the 'swapping' scientifically. Swap gate matrix:

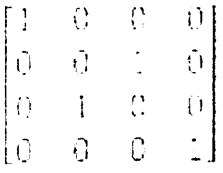

Figure 3.11: Swap Gate Matrix

Fredkin Gate The Fredkin gate is the same as a managed swap with a three-qubit input, with one qubit being a control qubit and the other two qubits being target qubits, which may or may not change depending on the control qubit. The Fredkin gate is the same as a managed swap with an input of three qubits, where one qubit is a control qubit and the other two qubits are target qubits, which may or may not change depending on the control qubit. If the qubit control is "0," no changes will occur and the two target qubits will not swap places. On the other hand, the target qubits change the state if the control qubit is equal to "1". The matrix:

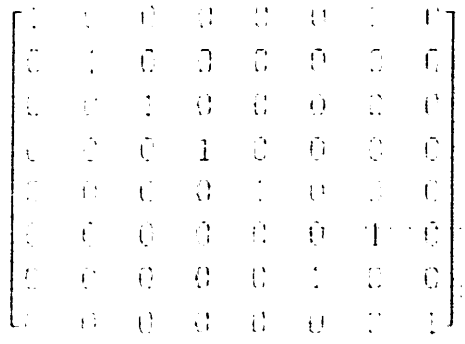

Figure 3.12: The Fredkin Gate Matrix

Quantum entanglement is a property of quantum mechanics where two or more quantum bits, are linked together in a fundamental way: a change in the environment of any of them will directly affect the other particle. Having this knowledge we can start thinking about new ways to create secure system using quantum technologies. Any of these gates can serve as bit transformer and used for encrypting data. As instance, the authors in presented an encryption schema using third part for decrypting and matching messages from both sides and avoided using one time pad techniques explaining it that it was impossible to resist to eavesdropping attack. Pauli-Y gate, Fredkin gate and Hadamard gates have been implemented in order to enhance the security of the encryption algorithm. The primary objective of this scheme is generating a digital signature using quantum technologies. A digital signature is considered an authentication mechanism that allows the sender of the message to add a code that serves as a signature. Quack - quantum MATLAB simulator, have been used for simulation of this work. Authors could encrypt, decrypt, match, and send the Quantum data among all parties of communication. The third party also was able to check and match the messages received from Bob and Alice. Authors compare two protocol BB84 and SARG04, that tolerate using no only single-photon sources, but and two-photon sources. SARG01 protocol tolerates a higher bit error rate than BB84. Explain using the decoy-state method for achieving secure of long distance. For SARG01 protocol made an endeavor to study in different situation, for example provide upper and lower bounds of the bit error rate with two-way classical communications for single-photon source and for two-photon sources. And additional they briefly review an entanglement distillation protocol (EDP) and its relation with the security of QKD, where we especially review the security

proof of BB84 by Shor and Preskill. And yet they explain how SARG04 works and construct an EDP protocol that is equivalent to SARG01 protocol. They furthermore mention the property of the density matrix in the EDP protocol for the later convenience. Thirdly, they explain the key generation rate for BB84 and SARG04, assuming realistic devices and one-way classical communications. Next, they describe the decoy method in BB84 and SARG04. Finally, they review QKD with two-way classical communications. On more paper about scheme based on mesoscopic coherent states often called "Y-00 protocol" has an average photon number of 100-1,000 photons per pulse. Y-00 protocol has robust safety level if it used microscopic coherent states, on really this reason need high performance for implementation and for this reason usual its used mesoscopic ones. They try briefly to show the simplest of cryptography attack to Y-00 protocol. Mesoscopic coherent states of the protocol allow implementation Quantum Key Expansion more than one photon and resist the noise in the channel which uses for realization Quantum Key Distribution. Y-00 protocol uses the secret key for quantum modulation and de-modulation in a quantum channel for expansion of the key. In addition, the level of qualification required to implement the agreement must be consistent with the level of traditional optical systems. If the protocol is almost physically secure, the Y-00 protocol is a fast and easy-to-implement cryptographic encryption system[4]. One research work is based on the way to integrate classical GSM card with quantum technologies such a way, authors described the E91 protocol that is based on the two entangled particles shared from a source to Alice and Bob to distribute a secret key. Authors tried to propose quantum authentication protocols for mobile networks using quantum technologies methods. They proved the possibility of authentication of copied SIM cards that are sometimes provided to eavesdrop on the original SIM cards and prevent them from entering the network. It was researched that whenever the original SIM card and its copy simultaneously request entry to the network then the network can detect the existence of a copy and then can delete both of them. The one more protocol explained is based on the use of quantum memory embedded on the SIM card, and used of a source of two particles entangle state with Bell-state. As a conclusion, these two protocols can be a good way to authenticate the SIM cards that been copied, in the next generation of mobile networks. After learning ways of combining quantum technologies with classical ciphering systems, it was decided

to learn structure of tokens, their ways of generation.

3.2 Protocol B92

One of the first protocols of quantum key distribution, which was proposed in 1992 by Charles Bennett (eng. Charles H. Bennett). Hence the name B92, by which this protocol is known today . The B92 protocol is based on the principle of uncertainty, in contrast to protocols such as E91. Information carriers are 2-level systems, called qubits (quantum bits). An important feature of the protocol is the use of two non-orthogonal quantum states.

The fundamental laws of physics claim that observing a quantum system changes its state. This insurmountable difficulty has a positive effect, allowing you to prevent unwanted receipt of information from a public quantum system and solving the problem of maintaining confidentiality when communicating via an open communication channel.

The B92 protocol is a generalization of the BB84 quantum cryptographic protocol. Unlike its predecessor, this protocol can use non-orthogonal quantum states. Charles Bennett developed this protocol to show the fundamental possibility of such a key separation.

The coding scheme of quantum states [Prim. 1] in the B92 protocol is similar to the BB84 protocol coding scheme, but uses only two non-orthogonal of the four BB84 states, and different polarizations are used as the basis:

Linear (-): - horizontal (): - vertical ():

Circular (): - right circular (): - left circular ():

Since, in accordance with the Heisenberg uncertainty principle during measurement, it is impossible to distinguish two non-orthogonal states from each other, therefore it is impossible to reliably determine the value of a bit. Moreover, any attempt to find out the state of a qubit in an unpredictable way will change it. This is the idea underlying the B92 quantum key-splitting protocol. Since the protocol coding scheme uses only two states, it is sometimes easier to implement than other schemes. However, obtaining sufficient reliability of such a protocol in some experiments is a difficult task, and it often turns out that the protocol is far from secure.

The initial state of the photons depends on the implementation of the protocol

table 5. If the protocol is implemented on the basis of EPR-correlated photons, then Alice generates such pairs of photons and bases in which she measures their state, and sends Bob unperturbed particles. Otherwise, Alice generates photons of random polarization and sends them to Bob. The second stage of the protocol is the identification of the polarizations of the photons received from Alice. The state of the particles is measured in a randomly selected basis. At the next stage, Alice and Bob compare the bases used for the measurement (in the case of non-EPR implementations, Alice uses the polarizations created by the photons) and save the information only when the bases match. Alice and Bob choose a random subset of bits and compare their parity. If at least one bit has changed as a result of Eve's actions, the parties will know about it with a probability of . Then it is necessary to discard one bit, since because of this check one bit of the key is opened. Performing the parity check of an arbitrary subset of bits k times allows you to establish that the communication channel of Alice and Bob is not heard with the probability p (k) = 1 - () k.

As noted earlier, the B92 had no significant advantages over the BB84's predecessor, that is, the same vulnerability to attacks and other disadvantages of BB84 remained in B92. Therefore, scientists took up the creation of new, improved protocols.

In 1991, the Polish physicist proposed a quantum cryptographic protocol based on the Einstein-Podolsky-Rosen "mental experiment" . Unlike the well-known protocols BB84 and B92, this protocol uses the discarded keys to detect the presence of a cryptanalyst (Eve) using Bell's inequality. That is, in the absence of a cryptanalyst, the laws of quantum mechanics will describe the system and, therefore, violate Bell's inequality, and if present, becomes a theory with a hidden parameter that satisfies this inequality.

Then, in 1995, B. Hattner, N. Immoto, N. Gisinom, T. Morom for the first time proposed the BB81 (1 - 2) quantum key distribution protocol[5]. In their work, the scientists described in detail the working principle of the protocol, its implementation and advantages over the BB84 protocol under the threat of PNS attacks. It is believed that this protocol was the first meaningful attempt to resist an attack divided by the number of photons or PNS-attack in the history of the development of cryptography. The protocol uses 1 quantum states to encode "0" and "1" in two bases, which corresponds to the BB84 protocol, and the

states in each basis are selected non-orthogonal, which corresponds to the B92 protocol, the states in different bases are also pairwise non-orthogonal. 4 – 2 uses a peculiar combination of protocols BB84 and B92, hence its name. One of the most important advantages over the other two basic quantum protocols BB84 and B92 is the so-called survivability in terms of the distance or length of the fiber-optic line. The 4 – 2 quantum protocol remains secret to the length of the quantum fiber-optic communication channel, about 150 km, while the critical length for the BB84 protocol is about 50 km, and for B92, about 20 km.

The process of splitting keys can be analyzed in steps. The result of each action corresponds to the row of the table.

Figure 3.13: The process of splitting keys

1. In the case of an EPR implementation, Alice randomly chooses a basis for measuring the state of a single photon from an EPR-correlated pair, either linear or circular.

2. In the second step, Alice's actions depend on the protocol version. During

EPR implementation. selects a random sequence of bases for measuring the polarizations of photons: Alice selects a random sequence of polarized photons and sends them to Bob.

3. Bob measures the polarization of his photons using a sequence of random bases.

4. The measurement results of Bob (imperfections of the source. communication channel and detector lead to the loss of photons).

5. Bob tells Alice the basis for measuring the polarization of each photon received.

6. Alice tells Bob which bases are right.

7. Alice and Bob retain data on photons measured in the correct polarizations. and all others are discarded.

8. The remaining data is interpreted in accordance with the code table.

9. Alice and Bob check their keys for the parity of the selected subset of bits. If at least one bit is different. then such a check shows the existence of Eve listening to the channel.

10. The sides discard one of the bits of the selected subset.

3.3 Protocol BB84 (4+2)

Quantum Protocol 4 + 2 (BB84 (4 + 2)) for information coding. the protocol uses four quantum states of a two-level system that form two conjugate bases. the states in each of which are not orthogonal. and the state in different bases are also not orthogonal in pairs.Information carriers are two-tier systems - quantum bits. The basic idea of the 4 + 2 quantum protocol is that once the BB84 protocol's PNS vulnerability is caused by the fact that after the bases are negotiated. the interceptor can get accurate information about the transmitted state. you can make the states inside each base non-orthogonal. thereby making it impossible for the interceptor to accurately determine transmitted state even with a known basis. Thus. the protocol uses 4 quantum states to encode "0" and "1" in two

bases, which corresponds to the BB84 protocol, and the states in each basis are selected non-orthogonal, which corresponds to the B92 protocol, and the states in different bases are also pairwise non-orthogonal. 4 + 2 uses a peculiar combination of protocols BB84 and B92, hence its name.

1. In First Basis:

$$|0\rangle = \cos\left(\frac{\pi}{8}\right)|0\rangle + \sin\left(\frac{\pi}{8}\right)|1\rangle$$
$$|1\rangle = \cos\left(\frac{\pi}{8}\right)|0\rangle - \sin\left(\frac{\pi}{8}\right)|1\rangle$$

2. In Second Basis:

$$|+\rangle = \cos\left(\frac{3\pi}{8}\right)|+\rangle + \sin\left(\frac{3\pi}{8}\right)|-\rangle$$
$$|-\rangle = \cos\left(\frac{3\pi}{8}\right)|+\rangle - \sin\left(\frac{3\pi}{8}\right)|-\rangle$$

As in the BB84 protocol, we have 4 states that form 2 bases.As an example of such a configuration of states, it is convenient to take a set of four states that lie in two perpendicular planes on the Puankare sphere (fig. 4), but are not orthogonal, for example:

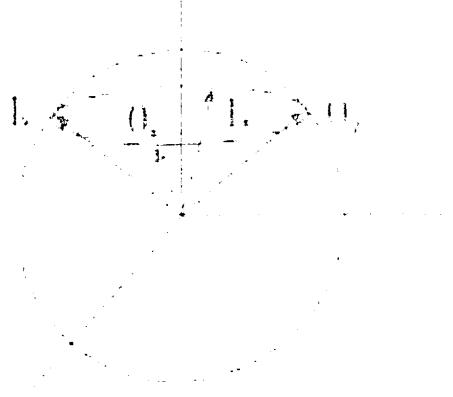

Figure 3.14: Quantum states of the 4 + 2 protocol on the Puankare's sphere

Attack on BB84 protocol As already mentioned, the BB84 protocol with 2 bases, the states within each of which are orthogonal, and the states from different bases are pairwise non-orthogonal. The photon separation operation can

be applied to BB84 hacking. Eve can easily find out the number of photons in each of the pulses. The attack itself is built like this: if a pulse contains only one photon, Eve blocks it, otherwise it leaves in its quantum memory (to realize it, it is enough to have a regular delay line) one of the photons, sending the rest to Bob through its ideal channel without loss. After the operation of matching the bases, which is produced through an open channel, Eve receives all the necessary information to reliably distinguish the photons that she has. Accordingly, Eva is able to recognize the whole key without being detected. Thus, BB84 is completely vulnerable to PNS attacks. According to history, the 4 + 2 quantum protocol was the first attempt to resist a PNS attack. As its creators believed, Eve would face a double challenge. First, once the BB84 protocol's vulnerability to a PNS attack is that after aligning the bases, Eva can get accurate information about the transmitted state, then the states inside each base can be made non-orthogonal, which makes it impossible for Eva to accurately determine the transmitted state even with a known basis . Secondly, if Eve conducts the same measurements that Bob makes, then this will lead to a situation similar to explicit listening, that is, Eve will introduce an error into the channel, taking measurements at random in the chosen basis, and her intervention will be detected. Thus, at first glance, we see a significant advantage over BB84, and it seems that 4 + 2 is not vulnerable to PNS attacks, however A. Acin, N. Gisin and V. Scarani in one of his works showed that Eva can take a measurement that they called filtering:

$$A_{ok} = \frac{1}{\sqrt{1+\cos\eta}}(|x\rangle\langle 1_x| + |x\rangle\langle 0_x|) \cdot A_? = \sqrt{1 - A_{ok}A_{ok}^{\dagger}}$$

Figure 3.15: Eve measurement's filter

3.4 Protocol SARG04

SARG01 - quantum key distribution protocol, obtained by improving the BB84 protocol. Known for its resistance to attack divided by the number of photons. After testing BB84 (4 + 2) protocol for PNS attacks group of scientists showed the weaknesses of this protocol. Also, they suggested new way of solution of this problem, namely, the configuration of vectors was invented, which did not allow a measurement that would orthogonalize the states in each pair of bases (with a

nonzero probability)[6]. The protocol is vulnerable to PNS attacks if an attacker is able to block all the packages with one and two photons, and in the packages with three photons can measure two of them on different bases, blocking the impulse when receiving at least one incompatible outcome. With the angle 45 the probability to get an incompatible outcome at least in one dimension is greater 1/2, therefore, for effective interception, Eve should be able to block the parcels with three photons. We obtain that for a successful protocol attack, it is necessary to be able to block all the packages with one, two, and three photons, which means SARG04 is noticeably better protected from PNS attacks than BB84. In their work, the authors of SARG04 also described an important special case of the protocol, which uses similar signaling states as BB84, but has a different encoding technique, which allows increasing the resistance to PNS attacks, sacrificing data transfer speed.

4. Analysis of quantum properties and their conditions for hacking.

Classical quantum systems methods are quite distinctive. And the outcome of the method is regarded as the randomly produced key x that was acquired using quantum states. All a third party can do is intercept the produced important x state. And you can use the density matrix to define it

$$\rho_{XE} = \sum P_X(x)|x\rangle\langle x| \otimes \rho_E^x$$

Quantum Key Distribution seeks to minimize the likelihood of anticipating the produced important status if an unauthorized access is obtained by a third party. And this can only be accomplished if the key generation is totally random. Which will lead to a discrepancy in the results of errors. and the proof is the density matrix ρ_{XE}. Recall that in addition to its impeccable protection. the system is able to implement on the threshold of ideality of the environment and the device parameters are at the level of the minimum allowable threshold. which means non-correlated density matrix $\rho_{\Gamma} \otimes \rho_E$

The distance between the circumstances is the distance between the traces:

$$\|\rho_{XE} - \rho_{\Gamma} \otimes \rho_E\|_1 < \varepsilon_1$$

By definition. it is connected by a trace metric:

$$\rho_{XE} = \sum_{x \in X} P_X(x)|x\rangle\langle x| \otimes \rho_E^x.$$

ρ_{Γ} a density matrix (in terms of homogeneity and ideality)

All third-party actions are just attempts to acquire the $y \in Y = \{0,1\}^n$ key states, and not the sender's x key itself, which consists of a bit string. y is the value of the connection of the third party system and the key x, which is a bit string and which depends on the analysis of the third party system ρ_E to the system of authenticated process users[7]. The analysis from the third-party can be written down by the decomposition of the unit: $I_E = \sum_{y \in Y} M_y$, $y \in Y = \{0,1\}^n$. M_y- a positive operator-valued measure in the third-party states.

$P_{XY}(x,y)$ - joint probability distribution x, y.
$P_X(x)$ and $P_Y(y)$ - marginal probability distribution.
$P_{x \setminus y}(X = x \vee y)$ - probability of occurrence of y, if x occurred.
$P_{X \setminus y}(x \vee Y = y)$ - probability of x occurring if y occurred.

Formula Bayes:

$$P_{XY}(x,y) = P_X(x) P_{X \setminus Y}(X = x \vee y)$$

$$P_{XY}(x,y) = P_{X \vee Y}(x \vee Y = y) P_Y(y)$$

$$\sum_{x \in X} P_{X \setminus Y}(x \vee Y = y) = \sum_{y \in Y} P_{X \setminus Y}(X = x \vee y) = 1$$

$$\sum_{x \in X} P_{XY}(x,y) = P_Y(y).$$

$$\sum_{y \in Y} P_{XY}(x,y) = P_X(x).$$

The situation in which it is conditionally probable that the authenticated users have the key x generated among themselves, at the same time its copy is in the third party after the unauthorized analysis by the third party is equal to y:

$$P_{X \vee Y}(X = x|y) = \{M_y \rho_E^x\}.$$

According to which we reproduce the summation:

$$\sum_{y \in Y} P_{X \setminus Y}(X = x|y) = 1$$

Probability of a positive result for a third party:

$$P_{X \setminus Y}(X = x|y) = \{M_x \rho_E^x\}, \; x = y.$$

According to the laws of probability theories, we can safely say that the probability of a positive outcome for a third party in quantum cryptography does not exceed

$$P_{Guess}(X|Y) = \max_M \sum_{x \in X} P_X(x) Tr\{\rho_E^x M_x\} = \sum_{x \in X} P_X(x) P_{XY}(X = x|x) = \sum_{x \in X} P_{XY}(x, x).$$

$P_{XY}(x, y)$ - joint probability distribution of authenticated users (x) and third parties (y), which does not exceed:

$$P_{Guess}(X|E) = \sum_{x \in X} P_{XY}(x, x) \leq \frac{1}{N} + \|\rho_{XE} - \rho_U \otimes \rho_E\|_1 < \frac{1}{N} + \varepsilon, \ N = 2^n.$$

ε - is the privacy setting of authenticated users, which is obtained by clearing the generated state.

4.1 Heisenberg's uncertainty principle and no-cloning theorem

As Heisenberg's uncertainty principle says: It is not possible to make a precise measurement of quant, and do not change it phase. It means you can not make a perfect copy an unknown quantum state. In this chapter we describe an elementary proof of this fact that captures the essential reason this is not possible.

Let's have a quantum machine with two slots labeled as A and B. Slot A, the data slot, starts out in an unknown but pure quantum state, $|\psi\rangle$. This is the state which is to be copied into slot B, the target slot[5]. We assume that the *target slot* starts out in some standard pure state, $|s\rangle$. Thus the initial state of the copying machine is

$$|\psi\rangle \otimes |s\rangle$$

Some unitary evolution U now effects the copying procedure, ideally,

$$|\psi\rangle \otimes |s\rangle \rightarrow U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle$$

Suppose this copying procedure works for two particular pure states, $|\psi\rangle$ and $|\phi\rangle$. Then we have

$$U(|v\rangle \otimes |s\rangle) = |v\rangle \otimes |v\rangle$$

$$U(|o\rangle \otimes |s\rangle) = |o\rangle \otimes |o\rangle$$

Taking the inner product of these two equations gives

$$\langle v|o\rangle = (\langle v|o\rangle)^2$$

But $x = x^2$ has only two solutions, x = 0 and x = 1, so either $|o\rangle = |v\rangle$ or $|v\rangle$ and $|o\rangle$ are orthogonal. Thus a cloning device can only clone states which are orthogonal to one another, and therefore a general quantum cloning device is impossible. A potential quantum cloner cannot, for example, clone the qubit states $|v\rangle = |0\rangle$ and $|o\rangle = (|0\rangle + |1\rangle)\sqrt{2}$, since these states are not orthogonal.

What we have demonstrated is that using unitary evolution it is impossible to completely clone an unknown quantum state. The brief overview of this work is that the cloning of non-orthogonal pure states remains impossible even if one enables non-unitary cloning equipment unless one is prepared to tolerate a finite loss of fidelity in the copied states. Similar conclusions hold also for mixed states, although a somewhat more sophisticated approach is necessary to even define what is meant by the notion of cloning a mixed state.

4.2 Threat to key with transfer from one mode to another

This threat consists of stages in which a third party re-sends the state of the sender (intercepted in the quantum channel). In this case, the third party after analyzing in a random basis and increases the intensity so as to transfer the detector to the classic mode. This thin line between the modes is retained by the method of insufficient intensity, which is used so as not to lose the blinding mode.) There are moments: 1. With the coincidence of third party bases and authenticated participants. This leads to a complete constructive interference, the reason for this is to capture the detector full intensity, and that leads to the count in time. 2. If there is no coincidence of the bases of the third party and the authenticated participants. In this case, the detector is transferred to the blinding mode, the cause of which is not enough intensity in time. The intensity

with which the detector exits the blinding mode registers the signal as a linear device, and is equal to I_{th}, and the intensity with which the detector is blinded (lies in the âno clickâ zone) is equal to I_{bl}. ($I_{bl} < I_{th}$).

The intensity of the falsified state is equal to I_{facked}. The intensity in the side time windows (see Fig. 2) does not depend on the choice of third party bases and authenticated participants and is equal to $I_{facked}8$ (see Fig.?? and formulas (3) - (7)). In this case, two situations are possible: a) The intensity of I_{facked} is such that in the side time windows, where the intensity does not depend on constructive or destructive interference, it is equal to $.I_{facked}8$. At the same time, $.I_{facked}8$ is obviously less than the threshold intensity I_{th}, at which the detector works as linear, but more than the intensity , which causes the blinding effect: $I_{th} < I_{facked} =< I_{th}$. There will be no counts in the side time windows (Fig. ??).

b) The intensity I_{facked} in the side time windows is equal to $I_{facked}8$, less than the threshold intensity I_{th}, and the intensity I_{bl} causing the blinding effect: $I_{facked}8 < I_{bl}.I_{th}4$. In this case, counts in side time windows (Fig. ??) will take place. The detector is not blinded and works as a single-photon counting mode. The whole point of the threat from the third party comes down to what she is trying to guess, but at the same time minimizes the ratio of permissible and received errors as a result of the distribution process, if attempts to guess will be in vain, and she will reveal herself about her presence.

4.3 The Threat for Quantum Key Distribution with a transfer of a modified condition

From the standpoint of the laws of ordinary mechanics, the quantum world is complex as these laws are limited in the expanses of quantum physics. Quantum countries unmeasurability is one of these legislation's main limitations. The statutes limitations, rendering quantum cryptography one of the safest systems, is the main fundamental link. There are many ways to take advantage of quantum physics in systems. One of the most realized uses of quantum technologies is the creation of a randomly generated secret key for encryption. There is a vulnerability of the system, due to the imperfection of the devices used[8]. For example, one of the fundamental conditions for the application of quantum technologies in cryptography is the creation of a pure single-photon source. This difficulty

will have to be solved in the future when more advanced devices appear. Today, multi-photon devices are used, which, as the study shows, leave unauthorized access.

The quantum key distribution protocol usually means authentication, preprocess preparation, transfer, examination of states, handling errors (eliminating or enhancing secrecy using the compression method), analyzing and verifying the obtained keys. The data transmitted by the system must be absolutely protected from third parties and, if necessary, disclose the audition. When unauthorized access to the transmitted data occurs, the system should detect this attempt using the ratios of valid and resulting error. In other situations, the system is considered unprotected when unauthorized access by a third party goes unnoticed and the key is known to it. For several years, research has been conducted in which the capabilities of quantum cryptography have been demonstrated. Currently, in quantum systems, attenuated laser radiation is used as a source of a single-photon state (which is not purely single-photon), single-photon avalanche photo detectors (which has dark noise), efficiency (whose properties are not rare), communication channels (fiber optic and open space), which are subject to loss and noise. This in turn leads to the emergence of the possibility of a photon-splitting system attack (PNS, Photon Number Splitter attack) and an attack with measurements with a certain outcome (Unambiguous Measurements). We included these factors in the analysis of the security of protocols. Unauthorized access to a key using photo-detector blinding is one of the new threats to quantum key distribution. In this threat, a third party uses the possibility of affecting a communication channel in which it sends a modified (falsified) state. This allows a third party to control the counts or their absence at the receiving side, and impose their own counting, which does not lead to an error at the recipient (receiving side). As a result, the third party remains unnoticed and informed about the key. This new method of threat significantly reduces the secrecy of the system. Most of the protocols, with no additional parameters, were potentially not resistant to this threat (BB84, SARG04, Six-State QKD , DPS (Differential Phase Shift) , COW (Coherent One Way), E91 , Decoy State QKD . One way to solve this problem is to create a strictly single-photon source, which at the present time has proved difficult to implement. Until this difficulty is resolved, the threat will always exist. To date, the search for solutions to these problems. From the basic solutions, it

is proposed to complicate and add additional parameters to existing protocols. The proposed solution does not solve the problem, but only complicates access by a third party. The methods of the third party in turn become cleverer. The best way to create an over-secure system is to create a protocol in which security is achieved through internally-structured methods, rather than an improvement and addition in technical terms.

4.4 Threat with photon modification

Below we provide information about this new threat on the host device, while not trying to look at all this in terms of technical vision, since all this is in the articles. The more devices are not perfect, the some ways to use these imperfections. One of these ways to influence the receiving side: 1. On avalanche photo-detectors, there is a difference in the sensitivity of temporal dependencies. This allows a third party to modify (falsify) the state and blind the devices of the receiving party. 2. Using the state of the lower threshold of intensity, in order to include only one device, in situations where the bases of the third party and the recipient will be the same. Otherwise, everything happens without counting. Basically, the possibility of third-party unauthorized access arises from the work of semiconductors (the so-called avalanche photo-detectors InGaAs:P). A blocking voltage is applied to the avalanche photo-diode. At the moment of arrival of the photon, a gate voltage pulse (typical duration of the order of several nanoseconds and an amplitude of several volts) is applied, which opens the photo-diode[9]. The absorption of a photon leads to the formation of an avalanche of carriers and a voltage pulse, which is recorded. 1. The first blinding attack is based on the following property. If the radiation intensity is increased slightly above the quasi-single-photon mode, this will lead to an increase in the current flowing through the photo-diode at the time of registration. Due to the fact that a photo-diode without illumination is not active (locked), the dynamic increase in current above a certain value will lead to an effective decrease in the bias voltage during the action of the strobe and to lock the diode and, accordingly, decrease, up to its absence, the avalanche current (à no click â). Thus, the photo-diode is effectively blinded. 2. The second attack is connected with the transfer of the photo-diode from the counting mode to the linear classical photo-detection mode, when the current is a function of the

radiation intensity (usually proportional to it). If we further increase the radiation intensity, then after blinding the photo-diode (see paragraph 1 above) and the absence of the registration current, starting with a certain threshold intensity value, a signal will appear again on the photo-diode through the photodiode a current proportional to the radiation intensity will flow.

The correct state transforms the count after the D_0 sensitivity of the detector falls into the curve, but this does not happen because the modified state is shifted in time. And this leads to the fact that on D_0, produces a count and errors in D_1. All this is caused by the interference of the state, which constructively extends over the different arms of the interferometer for D_0, and is extinguished on the D_1 state, along the upper and lower arms. And this whole process not only allows the third party to remain unnoticed in relation to the recipient (reducing the error to a valid one), but also in the end to intercept real information about the registered keys, which the recipient will not suspect[10]. In the real world, of course, it is difficult to carry out this threat, but it is quite provable and feasible. When it comes to analyzing the strength limit of any cryptographic system, it is taken into account that the third party will have the most advanced equipment and will have an ideal condition for implementing unauthorized interception and access to an encrypted and secure channel.

5. Implementation of quantum mechanics for key generation

5.1 Building source code using MatLab

To build a new key. let us turn into BB84 protocol that uses quantum key distribution. In spite of this. the key must consent to a few laws of cryptographic dependability: 1) It must be very arbitrary. 2) It must not be connected twice. 3) And the key length must not be shorter than the message itself. For traditional calculations. there is an issue that is halfway understood - this is the age of a completely arbitrary number. How might not confuse the scientific procedure. in specialized terms. it remained not flawless. Just with the utilization of quantum advances. this wound up conceivable [2]. This is one of the fundamental favorable circumstances of the quantum world. We endeavored to join quantum techniques with old style ones. One of the looked for after great territories that needs a symmetric key creation is the creation and trade of tokens for authentications. The utilization of the token has as of late achieved another dimension with the approach of cryptographic money. The significance and security of tokens is the principal heading of the improvement of cryptosystems. Quantum strategies given another chance to utilize symmetric encryption calculations. Of course. the length of our key ought not be under 256 bits to conform to the third law of Shannon. Along these lines. we will create the key with in any event 576 qubits. We presently can't seem to dissect later on what time interim is ideal and most extreme utilization of the key. after which we should restart the age.

Basis:

$$B^{+} = \{\epsilon_0^{+} = \binom{1}{0}, \epsilon_1^{-} = \binom{0}{1}\}$$

$$B^{\times} = \{\epsilon_0^{\times} = \frac{e_0 - e_1}{\sqrt{2}}, \epsilon_1^{\times} = \frac{e_0 - e_1}{\sqrt{2}}\}$$

Alice implementing operation $T : \{0,1\}^2 \to H$

$$T(x,y) = \begin{cases} \epsilon_0^{+} & \text{if}(x,y) = (0,0), \\ \epsilon_1^{+} & \text{if}(x,y) = (1,0), \\ \epsilon_0^{\times} & \text{if}(x,y) = (0,1), \\ \epsilon_1^{\times} & \text{if}(x,y) = (1,1). \end{cases}$$

$$\|T(x,y)\| = 1$$

Alice generated bits and basis randomly for use this in key generation

Require: Random Generator (0,1), T, n

Ensure: Strings $a, b \in \{0,1\} and sequence (\{\ \})_{i=1,\ldots,n}$

We randomly generate bits of information $a_1, \ldots, a_n$

$a \leftarrow (a_1, \ldots, a_n) \in \{0,1\}_n$

Then randomly generate basis for encode bits $b_1, \ldots, b_n$

$b \leftarrow (b_1, \ldots, b_n)$

locally store our bits a and list of basis b

repeat

$|v_i\rangle \leftarrow T(a_i, b_i)$

transmit $|v_i\rangle$ to Bob via quantum channel

$i \leftarrow i + 1$

until $i = n$

Here: n - number of qubits a - bits of information b - basis that Alice using for encode bits $|v_i\rangle$ - encoded state of qubits

Bob received encoded state of qubits and try decode with help basis, which he choose randomly

In Bob side we require random generator ($\{\ 0,1\ \}$) for $M = |\epsilon_1\rangle\langle\epsilon_1|$, for $\in \{+, \times, \}$, n, $sequence\ |v_i\rangle$, for $i, \ldots, n$

After process Bob will have two strings of n bits a', $b' \in \{0,1\}_n$

Randomly generate list of basis $b'_1, \ldots, b'_n$

$b' \leftarrow (b'_1, \ldots, b'_n) \in \{0,1\}_n$

$n \leftarrow 1$

Repeat

if $b'_i = 0$ then

Ask whether M_+ takes value 1 in state $|e_i\rangle$

else

Ask whether $M_\times$ takes value 1 in state $|e_i\rangle$

end if

if counter triggered then

$a'_i \leftarrow 1$

else

$a'_i \leftarrow 0$

end if

$i \leftarrow i + 1$

until $i = n$

$a' \leftarrow (a'_1, \ldots, a'_n) \in \{0,1\}_n$

Bob transmit string $b' \in \{0,1\}_n$ to Alice via public classical channel All information and result Bob store locally $a'.b'$ M - list of basis, with the help of measure Alice's qubits b' - one basis of Bob a' - result of Bob, which he obtain after measure

After measure Bob sent list of basis to Alice and she compares bases, and discards all the mismatched

Alice have $b.b' \in \{0,1\}$

In this situation we ensure that sequence $(k_1, \ldots, k_L)$ (with $L \leq n$) $of positions of c$

$c \leftarrow b \oplus b_l$

$i \leftarrow 1$

$k \leftarrow 1$

Repeat

$k \leftarrow min\{j : k \leq j \leq n$ such that with $j = 0\}$

if $k \leq n$ then

$k_i \leftarrow k$

$i \leftarrow i + 1$

end if

until $k = n$

$L \leftarrow i - 1$

Alice transmit $(k_1, \ldots, k_L)$ to Bob via public classical channel

If no eavesdropping on quantum channel

$P(a'_{k_1}, \ldots, a'_{k_L}) = (a_{k_1}, \ldots, a_{k_L}) = 1$

a_i	b_i	c_i	b'_i	$\langle c_i \vert M_+ c_i \rangle$	a'_i	b'_i	$\langle c_i \vert M_\times c_i \rangle$	a'_i
0	0	ϵ_0^+	0	0	0	1	1/2	0 or 1
1	0	ϵ_1^-	0	1	1	1	1/2	0 or 1
0	1	$\epsilon_0^\times$	0	1/2	0 or 1	1	0	0
1	1	$\epsilon_1^\times$	0	1/2	0 or 1	1	1	1

if $b'_i = b_i$ then $P(a'_i = a_i) = 1$ Certainty on coincidences although a's never exchanged

If no intrusion. Alice and Bob will use a — sampled at places of coincidence — as key because

$$(a'_{k_1}, \ldots, a'_{k_L}) = (a_{k_1}, \ldots, a_{k_L})$$

Code in Appendix A.B

5.2 Token generation using quantum technologies

Token generation using quantum technologies can be performed in several ways. Classically token-based authentication works by ensuring that each request to a server is accompanied by a signed token, which the server verifies for authenticity and only then responds to the request. In this way as explained in previous chapter, encryption algorithms of classic cryptography have been used. As said before, using Shor's algorithm they can be easily broken. Analyzing and summing up it all, we consider the way of integrating quantum cryptography methods to generate token for authentication[11]. A - Kx - Zt - Bt - Hn (5) K - Server Z - Login B - Password H - ID of device Using 4 qubit states will let the system have a high security level, since each qubit has 4 different states, and let the token be valid 256 times against using sessions for reaching some web server.

Currently we have to develop system. which will be able to generate token based on quantum methods. First of all it was decided to implement a simple QKD system. i.e. system consisting Alice. Bob and Eve – 3rd part as a. Alice generates variable sized qubits randomly. and sends it via quantum channel to Bob. Alice (table 5.1)

X	·	·	X	X	–
1	0	0	1	1	0

Table 5.1:

Bob also generates set of bases randomly. and receives data from Alice (table 5.2).

X	X	·	·	X	–
1	-	0	-	1	0

Table 5.2:

Since some of bases are. different Bob will lose some amount of data (table 5.3)

1	-	0	-	1	0

Table 5.3:

Bob will send his bases to Alice to be show which elements he could read. Knowing his bases Alice will be able to know information on which indices have been read correctly. and sends list of indices. which are same. Then both sides will only reset different bases. In this case. Eve is only in role of observer. She will also create random set of bases and catch the set of qubits (We are taking situation when Eve has some equipment (table 5.1). which is able to read qubit. without changing qubit. since currents systems cannot have all properties of pure quantum system).

·	X	·	X	X	·

Table 5.4:

Now she will be able to read this information (table 5.5).

-	-	0	1	1	0

Table 5.5:

In addition, when she will know set of indices where Alice and Bob have same base, she will remove unnecessary ones. So, her last key will be '10', since key agreed between Alice and Bob is '1010'. We did 100 experiments for 3 different lengths 20, 30 and 40 qubits: calculate the percentage of key found by Eve. The results are in Table 2. We also considered one more case: situation where Eve cannot copy information, change it because of property of qubit. Alice generates set of qubits on random base (table 5.6).

X	-	-	X	X	-
1	0	0	1	1	0

Table 5.6:

Bob also creates his set of bases and waits for message from Alice (table 5.7).

X	X	-	-	X	-

Table 5.7:

Eve intercepts qubits with her randomly generated basis (table 5.8).

-	X	-	X	X	-

Table 5.8:

Because of property of qubits, only information on those indices, where Eve and Alice have same basis will be read, and other will be lost immediately(table 5.9).

-	-	0	1	1	0

Table 5.9:

Now she has to fabricate set of qubits to Bob, since he waits message from Alice (table 5.10).

-	X	-	X	X	-
0	1	1	0	1	1

Table 5.10:

Bob receives fake message from Eve thinking that it is from Alice, puts on his basis, reads this (table 5.11):

-	1	1	-	1	1

Table 5.11:

Since here Bob have received incorrect information, the key generated in this process is incorrect. Later they will be unable to read messages from each other, what will give them knowledge about existence of Eve. Here we calculated the percentage of mismatch of keys between Alice and Bob. If this value is not bigger than 10%, it can be accepted as noise[12].

As a result, we can list steps such as statistics of quantum technologies development, analysis of each field separately, defining protocols and methods for forming qubits and quantum systems. Experiments were set on possibility of being compromised by Eve and on mismatch percentage of Alice and Bob's keys (table 5.12).

Length	20	30	40
Percentage of being compromised	49.10	47.68	49.66
Alice and Bob's key mismatch	47.68	49.19	49.67

Table 5.12:

The average results have been obtained from 100 experiments for each case. The 19 experiments excerpt shown below for 1st case to visualize the general situation.(Fig 5.1.5.2.5.3)

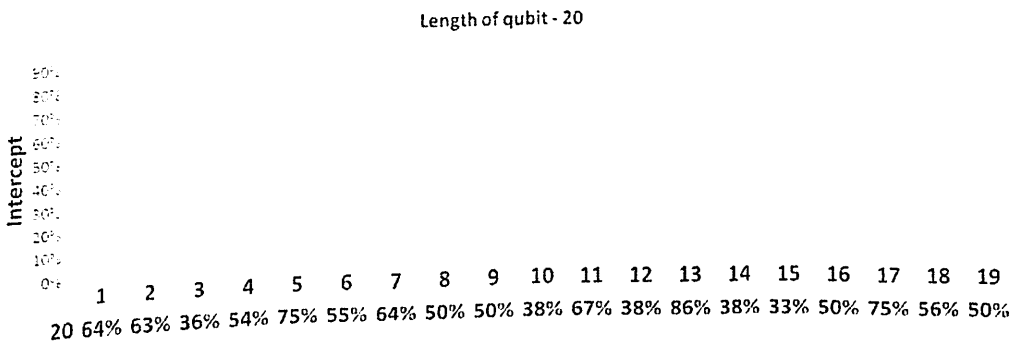

Figure 5.1: Qubit of 20 length

In figure 5.2 below, shown the Eve's percentage of eavesdrop, for each iteration of sequence of 30 length qubits, as we see the average eavesdropping is about 44%-46%.

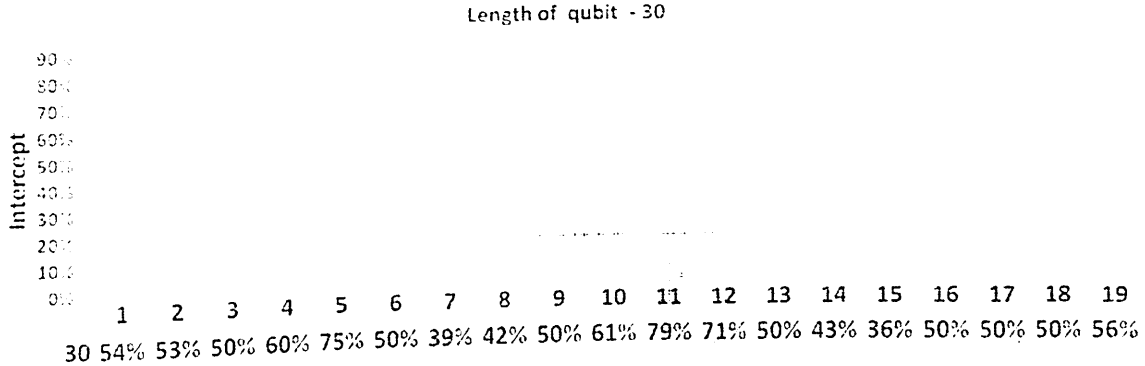

Figure 5.2: Qubit of 30 length

In figure 5.2 below. shown the Eve's percentage of eavesdrop. for each iteration of sequence of 40 length qubits. as we see the average eavesdropping is about 44%-16%.

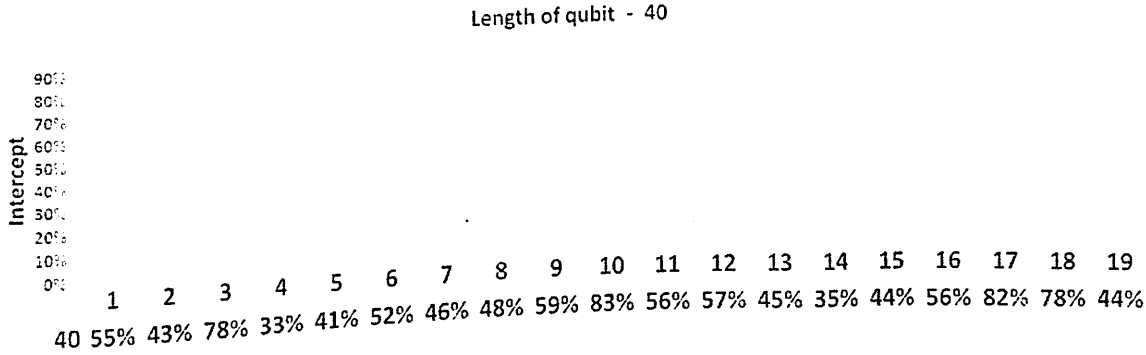

Figure 5.3: Qubit of 30 length

The summary of all three conditions of 20.30 and 40 length qubit sequence is that in any case there is about 45% of copying of sequnces. with out any information of basis's that Alice had chosen before. At any case Alice and Bob can identify the eavesdropping by formula shown previous, they can check out first 10 or 15 bits. to be confident that key they are using is build secretly and unknown for Eve.

6. Conclusion

Further development of quantum key distribution systems will lead to the creation of communication networks with a higher level of information protection. These networks will be used both in the civilian sector of the economy and in those organizations whose activities are related to ensuring state security. Based on this, domestic developments in this area will increase the level of the country's defense. Quantum key distribution systems are complex software and hardware systems that may contain undocumented features, which is unacceptable for defense systems. This explains the interest of developers to this topic and the relevance of work on creating their own systems for generating and distributing a quantum key.

The analysis shows, that asymmetric cryptographic algorithms can be broken by enough computational machine and secured information is about to be revealed. The main problem of using quantum key distribution is distance. While other cyphering cryptography algorithms have not such kind of problems, this is the main issue, need to be solved. As experimental, there was reached for about 50-100 km, although we need for thousands and thousands km [13].

In thesis, there are simulation of quantum properties behavior, written in code, that proves secured connection between Alice and Bob, by means of quantum technologies. The realized algorithm BB84 protocol shows good result in case of eavesdropping. Eve cannot broke and define the basis of each qubit, and thus she cannot identify the secure sequence of bits between Alice and Bob.

References

[1] Birin D.A. "Quantum key distribution in passive optical network". In: *T-Comm* 7 (2012). pp. 27–31.

[2] C.Bennett B.Brassard. "Experimental quantum cryptography". In: *Journal of Cryptology* 5 (1992). pp. 3–28.

[3] Khaled E. Zakariya Q. "A New Hardware Quantum-based Encryption Algorithm". In: *IEEE Long Island Systems, Applications and Technology (LISAT) Conference 2014* 377.2 (2014). pp. 1–5. DOI: http://sci-hub.tw/10.1109/LISAT.2014.6845201.

[4] Vivekanand M. Arun G. "A REVIEW ON QUANTUM COMPUTING AND COMMUNICATION". In: *Cryptol* 5 (1996). pp. 7–29.

[5] Cajlinger A. Baumester D. Jekert A. *Physics of quantum information*. Postmaster. 2003.

[6] B. Lari. "Quantum Authentication Protocols for GSM". In: *Arxiv* 377.2 (2018). pp. 1–19. DOI: https://arxiv.org/abs/1812.02081.

[7] Hoi-Kwong Lo Chi-Hang Fred Fung Kiyoshi T. "On the performance of two protocols: SARG04 and BB84". In: *Arxiv* 377.2 (2005). pp. 9–28. DOI: https://arxiv.org/abs/quant-ph/0510025.

[8] G. Brassard H. Bennett. "Quantum cryptography: Public key distribution and coin tossing". In: *Theoretical Computer Science* (1984). pp. 175–179. DOI: http://sci-hub.tw/10.1016/j.tcs.2011.08.039.

[9] H. Ives J. D. Franson. "Quantum cryptography using optical fibers". In: *Appl. Opt* 33 (1994). pp. 2949–2954. DOI: http://sci-hub.tw/10.1364/AO.33.002949.

[10] Guihua Zeng Nanrun Zhou. "A novel quantum block encryption algorithm based on quantum computation". In: *Physica A: Statistical Mechanics and its Applications* 362.2 (2006), pp. 305–313. DOI: https://doi.org/10.1016/j.physa.2005.08.053.

[11] Colin P.Williams. *Explorations in Quantum Computing*. Springer, 2011.

[12] Jeremy M. Weathers. "METHODS FOR QUANTUM CIRCUIT DESIGN AND SIMULATION". In: *Naval* 377.2 (2010), pp. 255–272.

[13] Schaffner C. Broadbent A. "Quantum cryptography beyond quantum key distribution". In: *Physica A: Statistical Mechanics and its Applications* 362.2 (2016), pp. 351–382. DOI: https://doi.org/10.1007/s10623-015-0157-4.

A. Appendix A

```
% plot Bloch Sphere

[Xs, Yx, Zx] = sphere(25);
mySphere = surf(Xs, Yx, Zx);
axis equal
shading interp
mySphere.FaceAlpha = 0.25

line([-1 1], [0 0], [0 0],'LineStyle',':', ...
            'LineWidth', 1, 'Color', [0 0 0])
line([0 0], [-1 1], [0 0],'LineStyle',':', ...
            'LineWidth', 1, 'Color', [0 0 0])
line([0 0], [0 0], [-1 1],'LineStyle',':', ...
            'LineWidth', 1, 'Color', [0 0 0])

text(0, 0, 1.1, '$\left|␣0␣\right>$', 'Interpreter', 'latex', ...
    'FontSize', 20, 'HorizontalAlignment', 'Center')
text(1.1, 0, 0, '$\left|␣+␣\right>$', 'Interpreter', 'latex', ...
    'FontSize', 20, 'HorizontalAlignment', 'Center')
text(-1.1, 0, 0, '$\left|␣-␣\right>$', 'Interpreter', 'latex', ...
    'FontSize', 20, 'HorizontalAlignment', 'Center')
text(0, 0, -1.1, '$\left|␣1␣\right>$', 'Interpreter', 'latex', ...
    'FontSize', 20, 'HorizontalAlignment', 'Center')

% ------------------------------------------------------

% Visualize Bloch Vector

X = [0 1; 1 0];
Z = [1 0; 0 -1];
Y = 1i * X * Z;

H = (1/sqrt(2)) * (X + Z);
```

```
E0_plus = bin2vec('0');
E1_plus = bin2vec('1');

E0_X = (E0_plus + E1_plus)/sqrt(2);
E1_X = (E0_plus - E1_plus)/sqrt(2);

plotBlochSphere

rho = ket2dm(ket0);
lambda0 = ket2bv(E0_plus);
lambda1 = ket2bv(E1_plus);
lambdaX0 = ket2bv(E0_X);
lambdaX1 = ket2bv(E1_X);

plotBlochVect(E0_plus,[1 0 0]);
plotBlochVect(E1_plus,[1 0 0]);
plotBlochVect(E0_X,[0 0 1]);
plotBlochVect(E1_X,[0 0 1]);

function rho = ket2dm(ket)
% Convert ket tp a density matrix rho

rho = ket * ket';
end

function lambda = ket2bv(ket)
    rho = ket2dm(ket);
    X = [0 1; 1 0];
    Z = [1 0; 0 -1];
    Y = 1i * X * Z;

    lambda = [trace(X*rho); trace(Y*rho); trace(Z*rho)];
end

function plotBlochVect(ket,color)
    lambda = ket2bv(ket);

    someBV = line([0 lambda(1)], [0 lambda(2)], [0 lambda(3)], ...
        'LineWidth', 2, 'Marker','0','Color',color)
end
```

B. Appendix B

```
function [a,b,e] = bb84(n)

fprintf('\n\n===␣BB84␣protocol␣===\n\n');

list_qubits = cell(1,n);

H = hadamard(1);

%  ---------- Alice generates bits and basis -------
bits = rand(1,n) > 0.5;
basis_A = rand(1,n) > 0.5;

result_A = 1:n;

for a=1:n
    if bits(a)==0
        result_A(a)=0;
    else
        result_A(a)=1;
    end
end

E0_plus = bin2vec('0');
E1_plus = bin2vec('1');

E0_X = (E0_plus + E1_plus)/sqrt(2);
E1_X = (E0_plus - E1_plus)/sqrt(2);

% ------------- Alice encode qubits ------------------

for k = 1:n
    if basis_A(k)==0
        if bits(k)==0
            phi = E0_plus;
```

```
            list_qubits{k} = (H*phi);
        else
            phi = E1_plus;
            list_qubits{k} = (H*phi);
        end
    else
        if bits(k)==0
            phi = E0_X;
            list_qubits{k} = (H*phi);
        else
            phi = E1_X;
            list_qubits{k} = (H*phi);
        end
    end
end

% --------- Alice sent list qubits to Bob --------------

% --------- Eve eavesdrop qubits -----------------------

n_E = length(list_qubits);
basis_E = rand(1,n_E) > 0.5;

result_E = 1:n_E;

for i = 1:n_E
    if basis_E(i) == 0
        ppp = pretty(measure(H*list_qubits{i}));

        if ppp == pretty(measure(bin2vec('1')))
            result_E(i) = 1;
        elseif ppp == pretty(measure(bin2vec('0')))
            result_E(i) = 0;
        else
            disp('Else1 :');
            disp(pretty(measure(list_qubits{i})));
        end
    elseif basis_E(i) == 1
        ppp = pretty(measure(list_qubits{i}));
        if ppp == pretty(measure(bin2vec('1')))
            result_E(i) = 1;
        elseif ppp == pretty(measure(bin2vec('0')))
            result_E(i) = 0;
        else
            disp('Else2 :');
```

```
            disp(pretty(measure(list_qubits{i})));
        end
    end
end

% ------------ Eve encode and sent list qubits ------------

list_qubits_E = cell(1,n_E);

for e = 1:n_E
    if basis_E(e)==0
        if bits(e)==0
            phi = E0_plus;
            list_qubits_E{e} = (H*phi);
        else
            phi = E1_plus;
            list_qubits_E{e} = (H*phi);
        end
    else
        if bits(e)==0
            phi = E0_X;
            list_qubits_E{e} = (H*phi);
        else
            phi = E1_X;
            list_qubits_E{e} = (H*phi);
        end
    end
end


% --------- Bob received list qubits ----------

% ----------- Bob generated basis ------------

n_B = length(list_qubits);

basis_B = rand(1,n_B) > 0.5;

result_B = 1:n_B;

for i = 1:n_B
    if basis_B(i) == 0
        ppp = pretty(measure(H*list_qubits{i}));

        if ppp == pretty(measure(bin2vec('1')))
```

```
            result_B(i) = 1;
        elseif ppp == pretty(measure(bin2vec('0')))
            result_B(i) = 0;
        else
            disp('Else1 :');
            disp(pretty(measure(list_qubits{i})));
        end
    elseif basis_B(i) == 1
        ppp = pretty(measure(list_qubits{i}));
        if ppp == pretty(measure(bin2vec('1')))
            result_B(i) = 1;
        elseif ppp == pretty(measure(bin2vec('0')))
            result_B(i) = 0;
        else
            disp('Else2 :');
            disp(pretty(measure(list_qubits{i})));
        end
    end
end

% ---------- Create keys -------------

keys = [];
count = 1;

for c=1:n
    if basis_A(c)==basis_B(c)
        keys(count) = result_B(c);
        count = count + 1;
    end
end

keys_E = [];
count_E = 1;
for c=1:n
    if basis_A(c)==basis_E(c)
        keys_E(count_E) = result_B(c);
        count_E = count_E + 1;
    end
end
a = result_A;
b = result_B;
e = result_E;
end
```

C. Appendix C

```
% ------------------------------------------------
% --- Alice generated bits and sent list qubits ------
% ------------------------------------------------

function y = bb92(n)


H = hadamard(1);
bits_A = rand(1,n) > 0.5;

list_qubits = cell(1,n);

E0_plus = bin2vec('0');
E1_plus = bin2vec('1');
E0_X = (E0_plus + E1_plus)/sqrt(2);

for i=1:n
    if bits_A(i) == 0
        list_qubits{i}= (H*E0_plus);
    elseif bits_A(i) == 1
        list_qubits{i} = (H*E0_X);
    end
end

% ------------------------------------------------
% -------- Eve received list qubits ----------------
% ------------------------------------------------


n_E = length(list_qubits);

basis_E = rand(1,n_E) > 0.5;
```

```
bits_E = [];

for e = 1:n_E
    if basis_E(e) == 0
        ppp = pretty(measure(H*list_qubits{e}));
        %disp(ppp);

        if ppp == pretty(measure(bin2vec('1')))
            bits_E(e) = 1;
        elseif ppp == pretty(measure(bin2vec('0')))
            bits_E(e) = 0;
        else
            disp('Else1 :');
            disp(pretty(measure(list_qubits{e})));
        end
    elseif basis_E(e) == 1
        ppp = pretty(measure(list_qubits{e}));
        %disp(ppp)

        if ppp == pretty(measure(bin2vec('1')))
            bits_E(e) = 1;
        elseif ppp == pretty(measure(bin2vec('0')))
            bits_E(e) = 0;
        else
            disp('Else1 :');
            disp(pretty(measure(list_qubits{e})));
        end
    end
end

result_E = [];
ccc_E = 1;

for e = 1:length(bits_E)
    if bits_E(e) == 1
        result_E(ccc_E) = basis_E(e);
        ccc_E = ccc_E + 1;
    end
end

% ------------------------------------------------------
% ---------- Bob received list qubits ------------------
%-------------------------------------------------------

n_B = length(list_qubits);
```

```
basis_B = rand(1,n_B) > 0.5;

bits_B = [];

for b = 1:n_B
    if basis_B(b) == 0
        ppp = pretty(measure(H*list_qubits{b}));
        %disp(ppp);

        if ppp == pretty(measure(bin2vec('1')))
            bits_B(b) = 1;
        elseif ppp == pretty(measure(bin2vec('0')))
            bits_B(b) = 0;
        else
            disp('Else1␣:');
            disp(pretty(measure(list_qubits{b})));
        end
    elseif basis_B(b) == 1
        ppp = pretty(measure(list_qubits{b}));
        %disp(ppp)

        if ppp == pretty(measure(bin2vec('1')))
            bits_B(b) = 1;
        elseif ppp == pretty(measure(bin2vec('0')))
            bits_B(b) = 0;
        else
            disp('Else1␣:');
            disp(pretty(measure(list_qubits{b})));
        end
    end
end

result_B = [];
ccc_B = 1;

for b = 1:length(bits_B)
    if bits_B(b) == 1
        result_B(ccc_B) = basis_B(b);
        ccc_B = ccc_B + 1;
    end
end

% ------------------------------------------------
% -------- Bob sent bits to Alice ----------------
```

```
% ------------------------------------------------

result_A = [];
ccc = 1;

for a = 1:length(bits_A)
    if bits_B(a) == 1
        result_A(ccc) = bits_A(a);
        ccc = ccc + 1;
    end
end

% ------------------------------------------------
% ------------- Results ------------------------
% ------------------------------------------------

% ----------- Alice --------------------

rev_result_A = [];
for a = 1:length(result_A)
    if result_A(a) == 1
        rev_result_A(a) = 0;
    elseif result_A(a) == 0
        rev_result_A(a) = 1;
    end
end

%disp('Binary to Hexadecimal: ');
disp(binaryVectorToHex(result_A));
disp(binaryVectorToHex(rev_result_A));
disp('------------------------------------------------------------------');

% ------------------------------ Bob ---------------------------------

rev_result_B = [];
for b = 1:length(result_B)
    if result_B(b) == 1
        rev_result_B(b) = 0;
    elseif result_B(b) == 0
        rev_result_B(b) = 1;
    end
end

%disp('Binary to Hexadecimal: ');
disp(binaryVectorToHex(result_B));
```

```
disp(binaryVectorToHex(rev_result_B));
% ------------ Eve --------------------

rev_result_E = [];
for e = 1:length(result_E)
    if result_E(e) == 1
        rev_result_E(e) = 0;
    elseif result_E(e) == 0
        rev_result_E(e) = 1;
    end
end

%disp('Binary to Hexadecimal: ');
disp(binaryVectorToHex(result_E));
disp(binaryVectorToHex(rev_result_E));
```