Execution Based Comparison of Quantum Cryptography Protocols [3]

Ajanta Das[1[0000-0002-3368-5144]] and **Shalbani Das**[2]
[1] Amity Institute of Information Technology, Amity University Kolkata, India.
ajanta.desarkar@gmail.com
[2] Amity Institute of Information Technology, Amity University Kolkata, India.
beingshalbanidas@gmail.com

ABSTRACT

With the advancement of science and technology, cyber cryptography is classified into classical and quantum cryptography. Unlike classical cryptography, the public key is not shared between sender and receiver before communication, in case of quantum cryptography. In quantum cryp- tography, secret key is shared using quantum key distribution methodology. Quantum key distri- bution is based on qubits and fundamental theory of quantum mechanics. In this paper two quan- tum cryptography protocols, BB84 and E91 are presented with the basic theory, algorithm and implemented circuit in qiskit. The objective of this paper is to compare and analyze the quantum cryptography protection protocols, BB84 and E91 varying number of qubits.

Keywords**: Quantum Cryptography, Quantum Key Distribution, BB84 protocol, E91 Pro- tocol.**

1. INTRODUCTION

In twenty first century, there's a first-rate wide variety of economic transac- tions, such as shopping, exchanging information related to monitory transac- tion and promoting of goods and services, or the delivery of touchy facts, etc. In the era of information, cryptography affords simple mechanisms to make certain pri- vateness, integrity, authentication, and non-rejection. Given the quick develop- ment in technology, hacking or breaking protection and privacy is also easily possible. With the latest advancement society is moving toward improvement of basic online transactions and interactions of various tasks, at the same point of time hackers are also improved their skills to steal online data to break the privacy and trust between the sender and receiver during online communication.

Quantum cryptography plays a major role to provide the solution of above-men- tioned problems. In quantum communication, there is very less chances to hack the data while it's traversing through network to reach the destination. Quantum communication is based on quantum bits (qubit), two different channels, classical and quantum, and the corresponding bases of qubits. Qubits are not vulnerable in quantum channel. However, since the encryption is based on basis of qubits and the sender and receiver need to chances of occurrence of eavesdropping.

This paper presents the study of an evaluation and security analysis of the protocols, BB84 and E91. The purpose of these protocols is to enhance safety in community ver- bal exchange, where security is a critical concern. With the motive of compar- ing both protocols, a python-based simulator, qiskit, proposed by IBM [9], is used to simulate behavior and execution patterns of the protocols and to execute a chain of tests to ensure security through quantum key distribution; acquiring rec- ords that introduced the theoretical aspect and imparting a foundation for this evalua- tion. The principal purpose of this research is the assessment and evaluation of Quan- tum Cryptography protocols, such as, BB84 and E91, using simulation in qiskit envi- ronment.

The paper is organized as follows. Fundamentals of quantum computing is presented in section 2 and quantum cryptography protocols are elaborated with concepts and al- gorithms in section 3. Section 4 presents all the experimental results and the compara- tive discussion of the qiskit implementation of two quantum key distribution (QKD) protocols varying qubits. The paper is concluded in section 5 with future directives of this research work.

2. CONCEPTS OF QUANTUM COMPUTING

This section briefs the basic concepts of quantum computing with qubits, superposi- tion of qubits, entanglement and Einstein–Podolsky–Rosen (EPR).

a. Qubit: A qubit is the abbreviated version of quantum bit. In analogy, it is the classical bit in quantum mechanics. As we know, the classical convention en- codes the information in bits where each bit is either of value 0 or 1, the qubit
has two states written as $|0\rangle$ and $|1\rangle$. Two states, $|0\rangle$, $|1\rangle$ or sometimes even a
combination of both states are possible values
for a qubit.

b. Superposition: As discussed above, a qubit may exist as a combination of
both states i.e., $|0\rangle$ and $|1\rangle$. This ability of a quantum system to exist in multi-
ple states at the same point of time is termed as superposition.

c. Entanglement: Entanglement is a property of the quantum system that en- sures that both the members of a pair exist in the same state. Changing the state of any one qubit will automatically change the state of the other member in a predictable way.

d. EPR: The Einstein–Podolsky–Rosen (EPR) or the bell

state is the pair of qubits that significantly plays an important role in many quantum protocol applications. They represent the simplest and the maximal examples of the quantum entanglement.

2

Next section elaborates quantum cryptography protocols.

share their chosen bases through classical channel. So, in classical channel, there is 25%

3. QUANTUM CRYPTOGRAPHY PROTOCOLS

Goal of any QKD protocol is to create a shared secret key that is transmit- ted across a public communication channel between two remote parties. The cru-cial point in this situation is that the key generation process is probably se-cure against any practical attack that an eavesdropper may launch in between during communication classical channel. The safety of the protocol is guaran- teed by the laws of physics, or more specifically, quantum mechanics. Typically, there are two parts to a quantum key distribution protocol: the quantum transmission segment, where Alice and Bob transmit and/or measure quantum states. The second step is the classical post-processing segment, where a pair of secure keys are created by converting the bit strings produced in the quantum part into this pair. This paper briefly presents BB84 and E91 protocols.

A. BB84 Protocol

Besides classical cryptography, QKD along with other quantum cryptography proto- col uses the ideologies of quantum mechanics in order to provide a public-key cryptosys- tem that is secured. BB84 is the first quantum cryptography protocol that was devel- oped by Charles Bennett and Gilles Brassard in 1984 [1]. In the BB84 protocol, Alice can send a random secret key to Bob where the secret key is encoded in their polariza- tion. The no-cloning theorem guarantees that Eve is unable to measure these photons and transfer them to Bob without significantly altering their state.
Given that there is no mistake on the quantum channel, the aforementioned statement is accurate. Alice and Bob won't be able to consistently identify Eve's existence if the channel is prone to errors.

Methodology of the protocol:
At first, Alice and Bob start speaking via a quantum channel. Alice chooses a set of bases (rectilinear or diagonal) and a set of bits that are both the same length. She then uses an optical fiber to transmit a photon for each bit corresponding to the polarization. Bob now selects a basis at random for every photon in order to determine its polarization. For a particular photon, if Bob selects the same basis as Alice, he will find the correct bit Alice communicated. He will receive a random bit if his guess is incorrect. The next action is for Alice and Bob to choose a traditional public channel for communication. Bob discusses the bases he used to measure each photon with Alice. The bases Bob accurately predicted to measure the encoded bits are then revealed to Bob by Alice. Alice and Bob then make the decision to discard the bits that were encoded and measured using various bases. Now, Alice and Bob have an identical bit-string, namely, the *shifted key*. The above-mentioned methodology is represented in Table 1.

Alice's Random Bits	1	1	1	0	0	0	1	1	1	1
Alice Basis	X	Z	Z	X	Z	X	X	Z	Z	X
What Alice sends Bob	↗	→	→	↖	↑	↖	↗	→	→	↗
Bob's Basis	X	Z	X	X	Z	Z	X	Z	Z	X
Shared Classical Bit	1	1	-	0	0	-	1	1	1	1

Table I: Communication details in BB84 protocol

In case of communication over classical channel, eavesdropping may happen. Alice and Bob might share a few of the alleged identical bits from the altered key in order to iden- tify Eve. Any discrepancy in the compared bits will summon Eve's presence. Alice and Bob will easily be aware of the eavesdropping if the probability values are abrupt.

Algorithm:
Step 1: Over a quantum channel, Alice and Bob attempt to speak. According to her preference, Alice chooses a string of bits and a string of bases (rectilinear or diagonal) that are both the same length. Then, she sends a photon to Bob using an optical fiber (or any channel that permits transferring photons) for each bit with the corresponding polar- ization.

Step 2: Bob then chooses a basis for each photon to measure its polarization. If Bob's chosen bases are same as Alice, he will receive the message correctly, which is sent by Alice. Otherwise, a random bit which will not match with Alice.

Step 3: A conventional public channel is used by Alice and Bob to converse. The bases Bob used to measure each photon are disclosed to Alice. Bob is informed by Alice of the bases he properly predicted. The measured and decoded bits are then removed by Alice and Bob using distinct bases. The shifted key is now a bit-string that both Alice and Bob own.

Step 4: Alice and Bob might share a few bits from the shifted key that are intended to be the same in order to verify Eve's existence. Any discrepancy in the compared bits will reveal Eve's existence.

B. E91 Protocol

The second protocol is E91, based on entangled photons, is proposed by Arthur Ekert in 1991 [3, 5, 7]. These can be prepared by Alice, Bob or any third character, such that everytime Alice and Bob have one photon of each pair. It is based on the con- cept of quantum entanglement. Beginning with the fact that entangled photons are cre- ated, Alice and Bob may always get the opposite results if they measure the orientation of the photon (whether it is vertical or horizontal), just as they would if they measured the diagonal bases. The individual results are random, meaning that it cannot are ex- pecting what Alice will obtain on her degree, for instance, a vertical or horizontal ori- entation. Alternatively, trying to pay attention made via the undercover agent (Eve) will henceforth damage the correlation, that Alice and Bob may be capable of coming across the intrusion. Table II presents E91 protocol example with *(a) Bases. (b) 8 En- tangled qubits.*

Table II: E91 with (a) Bases and (b) 8 Entangled qubits

	(a)		(b)	
Received photon	$\|1\rangle \|-\rangle$	$\|1\rangle \|-\rangle$	$\|0\rangle \|-\rangle$	$\|1\rangle \|+\rangle$
Alice's scheme	B_0	B_1	B_0	B_1
Alice's values	1	0	0	1
Received photon	$\|1\rangle \|+\rangle$	$\|0\rangle \|-\rangle$	$\|0\rangle \|+\rangle$	$\|0\rangle \|+\rangle$
Bob' scheme	B_1	B_1	B_1	B_1
Bob's values	1	0	1	1
Coincidences		yes		yes
Key		0		1

Methodology of the protocol: This protocol is primarily based on the following set of rules:

1. Random generation of n pairs of entangled states are used; n is the key's initial duration.
2. One copy of the entangled state is sent to Alice and Bob received another pair.

Bob and Alice choose a degree base at random and independently witness each photon.

3. Alice and Bob find their schemes, which can be the bases' lists used in each measurement, after the measurements. (preserving secretly they received con- sequences).
4. Everytime Alice and Bob checks their information and bases through qubits.

If it matches, the qubits are considered for secret or shifted key. Otherwise, mismatches are not considered for shifted key. Mismatching may occurs through eavesdropping or noise in quantum channel.

5. To accept or reject the key, Alice and Bob exchange the key hashes.

Step 1*:* Eckert uses a single photon source in this protocol that produces entangled photons. One of the photons from each entangled pair goes to Alice and the other goes to Bob.

Step 2: Alice and Bob randomly select their bases to measure the photons. They will get correlated results for each measurement, where they chose the same basis. After removing the photons measured on different bases, they will have a bit-string binary related, Alice and Bob can convert their key to the shifted key.

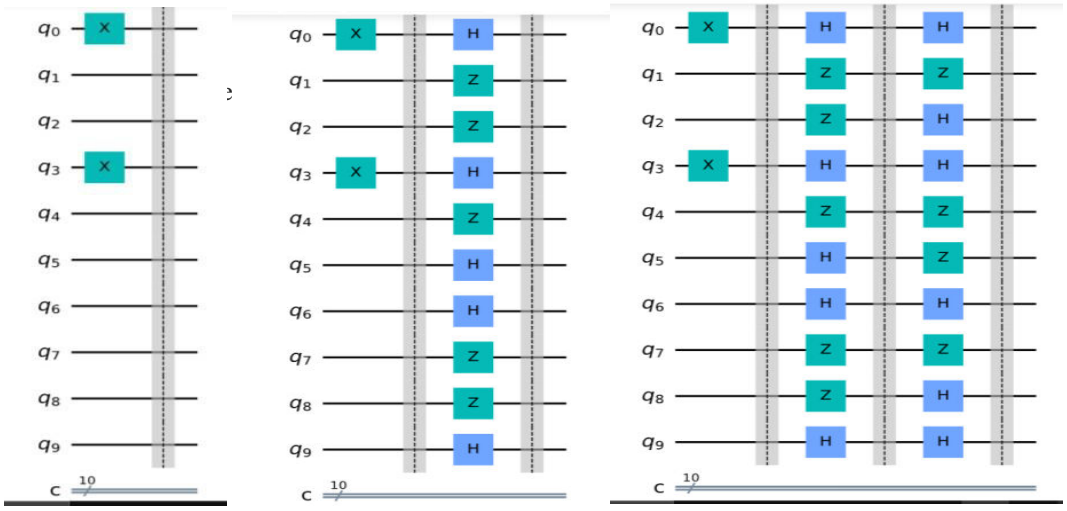
Step 3: With the results of their measurement of a photon on a third basis, they may test Bell's Inequality to determine whether Eve is present. Even sometimes mismatch of information or qubits through eavesdropping, it must be identified in quantum channel.

4. RESULTS AND DISCUSSIONS

This section presents experimental results of two above mentioned protocols in qiskit environment. Qiskit is an open source software development kit pro- vided by *IBM Quantum Lab* [9]. Circuits for various QKD protocols can be presented in qiskit environment.

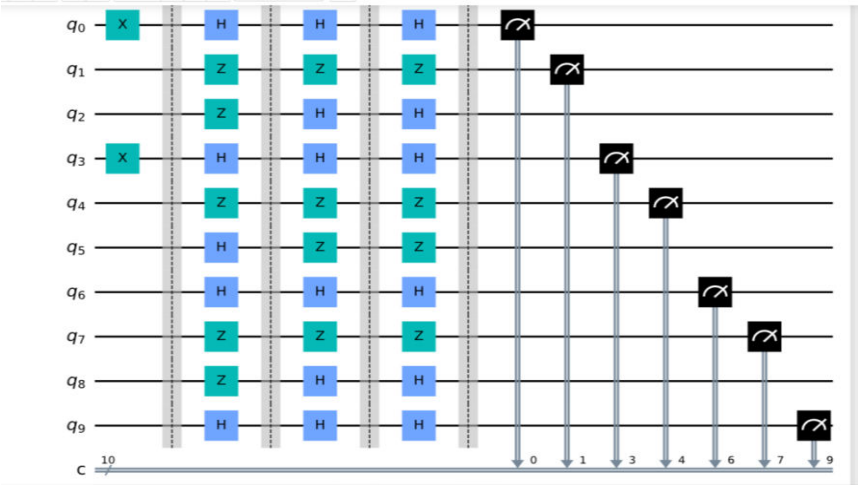
a. *BB84 Protocol*: The protocol is implemented for two cases, with 5 qubits and 10 qubits. The algorithm and the methodology of this protocol is ex- plained in details for 10 qubits with the figures Fig. 1(a), (b) and (c).

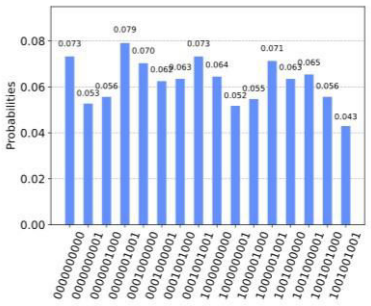
Fig. 1: (a) Alice sends random qubits, (b) Alice's chosen bases, (c) Bob's chosen bases



The above method is explained for ideal case. Eve may interfere after the phase Alice's chosen bases. The eavesdropping situation is considered as real case and is presented in Fig. 2. In Fig. 2, as it is mentioned first column represents Alice's random qubits, second column represents Alice's chosen bases. Now, third column represents Eve's chosen bases while fourth column represents Bob's chosen bases. At last, it is measured to identify whether Bob has received the exact message or not.

Fig. 2: Real Case Measurement of BB84 protocol





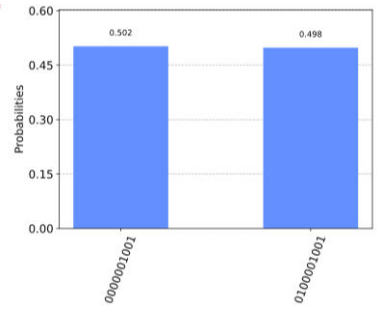


Fig. 3: Probability Graph for (a) Ideal Case and (b) Real Case of BB84 protocol

It is evident that in real case chances of receiving correct message is 50%. However, if Eve interferes, the probability drops. Eve is unable to learn the fundamentals. Before Alice shared her coding bases in the conventional channel, Alice used to encode the bits. To measure the photons, Eve actually guess and estimates to the bases. Information that is encoded on the other bases will be lost if she measures using the incorrect basis. Once more, Eve is unable to duplicate the states of the photons that are intercepted before they are delivered to Bob. According to likelihood, Eve will go unnoticed $(3/4)^n$ times if she listens in on n bits. Eve will have a 0.0563 escape probability in our example of 10 bits, which is extremely low.

b. E91 Protocol: E91 is also implemented and tested in qiskit simulation frame- work. The generated output is represented in Fig. 4. The chances of eavesdropping is very less in case of E91 protocol, as EPR based implementation uses teleportation tech- nology. In case of, teleportation at the same instant receiver and sender receives the mes- sage and it is highly authenticated and distance does not matter.

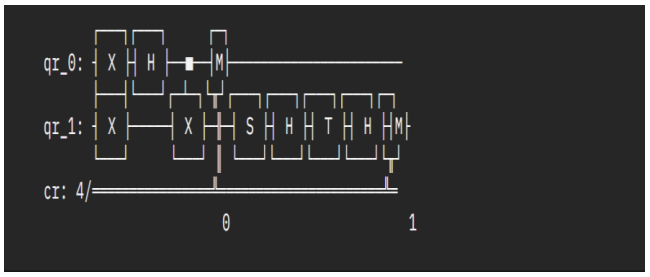


Fig. 4: Circuit of E91 protocol

Discussion: In E91, an EPR pair is used for the duration of the conversation. The EPR pair is divided, and one qubit is sent to sender and receiver individually. As we are aware, keeping EPR entangled is a difficult problem. In other words, the E91 protocol is more difficult to implement than the BB84 protocol. however there's a center source that sends one of the EPR debris to Alice and Bob, respectively, with the E91 protocol. that is just like the classical cryptographic protocol shape. Since its launch, the E91 has drawn enormous attention.

5. CONCLUSION

The laws of quantum mechanics must be fully understood in order to adhere to the standards of quantum computing and quantum cryptography. Quantum cryptography re- lies on novel rules that have no analogues in more traditional systems. Two quantum cryptography protocols, BB84 and E91, are simulated in this study, and the findings are reported with thorough justification. The BB84 protocol uses the four quantum bits. It does not use quantum entangled states and storing quantum debris thus making it easy to perform. Later in 1991, Ekert17 is proposed using of the quantum entangled states and experimented by the famous scientist Einstein Podolsky Rosen and hence it is referred as E91 protocol. The E91 protocol is more trustworthy and significantly im- proves security when compared to the BB84 protocol, which allows Alice to communi- cate quantum photons to Bob. In this study, a three-qubit entanglement pair is generated or an E91 simulation is shown. This team is still working on simulation using different qubits to attain 100% security in the case of extensive real-world data.

6. REFERENCES

1. C. H. Bennet and G. Brassard, “Quantum cryptography: public key distribution and coin tossing,” in International Conference on Computers, Systems & Signal Processing, Bangalore, India, 1984.
2. Caceres Alvarez, L, Fritis Palacios, R, Collao Caiconte, P. Development of a simulator for the quantum
3. Chin J Quantum Ling, A, Peloso, M, Marcikic, I. Experimental E91 quantum key distribution. In: Pro- ceedings of the international society for optical engineering, San Jose, CA, 19 February 2008, vol. 69030U. Society of Photo-optical Instrumentation Engineers (SPIE).
4. Chong, SK, Hwang, T. Quantum key agreement protocol based on BB84. Opt Com- mun 2010; 283(6): 1192–1195.
5. cryptography protocol E91 in a distributed environment. Ingeniare 2015; 23(2): 245–258
6. Díaz Caro and J. Samborski Forlese, “Brevísima Introducción a la Computación Cuántica,” Departamento de Ciencias de la Computación [Online], Universidad Nacional de Rosario, 2006. Available: http://www.fceia.unr.edu.ar/ diazcaro/QC/Brevisima.Introduccion.pdf [August 12, 2013].
7. K. Ekert, “Quantum cryptography based on Bell’s theorem,” in Phys. Rev. Lett. [Online], vol. 67, no. 6, pp. 661–663, 1991. Available: http:dx.doi.org/10.1103/PhysRevLett.67.661
8. M. Baig, “Criptografía Cuántica,” Grup de Física TeòÃ²rica - IFAE [Online], Facultad de Ciencias, Universidad Autónoma de Barcelona, 08193 Bellaterra, 2001. Available: http://giq.ifae.es/EducationalMaterial/Cripto.pdf [August 13, 2013].
9. Qiskit: IBM Quantum Lab”,” https://qiskit.org/
10. Wan, L, Huang, Y, Huang, C. Quantum noise theory for phonon transport through nanostructures. Physica B 2017; 510: 22–28. Zhiyong, Z, Yanbo, W, Min, H. Intercept-resent eavesdropping in polarization-drift