Technical Journal, University of Engineering and Technology (UET) Taxila, Pakistan *Vol. 27 No. 3-2022*
ISSN:1813-1786 (Print) 2313-7770 (Online)

Deployment of Security Vulnerabilities in Quantum Cryptographic & QKD using B92 Protocol

M. Pasha[1], R. Zaheer[2], A. Ali[3], M. Asad[4], U. Pasha[5]

[1,3,4]Department of Information Technology, Bahauddin Zakariya University, Multan, Pakistan
[2] Department of Physics, Bahauddin Zakariya University, Multan, Pakistan
[5]Institute of Management Sciences, Bahauddin Zakariya University, Multan, Pakistan

[1]maruf.pasha@bzu.edu.pk

Abstract- Secure communication has always been a key concern while sharing information between two parties. Traditional and lightweight cryptography primitives and protocols are insecure against quantum attacks. The objective of cryptography is to ensure confidentiality, integrity, authentication and non-repudiation between both parties. Quantum key distribution is a safe and sound method for communication between two parties to share their information. However early applications with applied limitations lead to open ambiguities, permitting an eavesdropper to breach the security of quantum cryptographic system. This research proposes a framework for quantum key distribution using B92 protocol. The B92 protocol allows two different users A to share their polarized photons with high security and without any interruption of Eavesdropper. While B92 protocol generates a secrete key, that is known to just sender and receiver. The use of QuVis framework can provide this secure communication and photons are transferred to Bob securely without any Eavesdropper.

I. Introduction

With the revolution of the internet throughout the world, the reputation of cryptography is increasing day by day. We make online transactions through our debit and credit cards every day via internet banking. The main purpose to use online banking is secure communication. For secure communication between two parties' cryptography techniques are utilized. The key purpose of cryptography is to guarantee privacy, verification, and truthfulness among both parties. Although public-key key cryptography contains complex calculations and makes the process slow. Therefore, quantum cryptography is used for secure communication.

According to the latest research, Google has accomplished quantum dominancy [1]. It is the main innovation of quantum computers towards growth. Quantum computers can solve the standard stiff difficulties of discrete logarithms and integer factorization. It also validates a rectangular stimulate to solve the amorphous search problems, that carriages serious security issues to traditional cryptographic algorithms grounded proceeding the difficulty of given complications. Boudot et al. lately declared the factorization of RSA-240 (an RSA number of 795 bits or 240 decimal digits, accompanied by the discrete logarithm of equal size) [2]. While quantum computing contains two types of security mechanisms of information: first is Quantum Cryptography that may contain quantum key distribution (QKD) and second is post-quantum cryptography (PQC), e.g. code-based cryptography and lattice-based cryptography [3]. It cannot be efficiently broken by currently known quantum computing algorithms. The first quantum key distribution protocol was based upon discrete variables (DV), for instance, photon polarization. The QKD protocols are named Discrete Variable Quantum Key Distribution (DVQKD) schemes [4-8], [9-15].

The first DVQKD protocol introduced was BB84 [16], which uses single-photon polarization for converting purposes. In this protocol, classical arbitrary bits are fixed in single-photon polarization (qubits) and contain four random polarization positions belonging to two bases, e.g., rectilinear and diagonal. In the decoding and encoding stage, the selected photons for these bases are used to organize and measure the photons. In quantum computers, single and two-qubit operations implement various circuits [47-48]. After closing a quantum-level transmission, all parties use a reliable classical station to equate these bases. The parties delete all the bits from the key with different bases in the agreement phase. After completing this phase, additional calculations and error-correcting processes are executed on the classical bit string to decrease the likelihood that treasured evidence is trickled to an eavesdropper. It is called the distillation phase. A secure key is obtained from this in-between Alice and Bob. A basic version of the BB84 protocol is the B92 protocol [17], which uses two polarization states as an alternative to four.

Cryptography is the study of encoding and decoding top-secret communications. There are two major cryptography categories: symmetric key (public) cryptography and asymmetric key (private) cryptography [18]. Cryptographers use various methods to make the information more secure and private. Nevertheless, at this point, hackers, code breakers, and eavesdroppers tried their best to crack the systems. In the coding process, the plaintext is converted into cipher text while in decoding, vice versa [43, 44]. in the presence of Eavesdropper, the communication between two users is shown in Figure. 1.

In cryptography, a key is an evidence that controls the process of cryptographic algorithms. Quantum cryptography always uses the random binary key called QKD. It allows the interactive parties to discover the occurrence of eavesdroppers [19]. Quantum systems are always quantum machines and depend continuously on Tron's additional physics. These significant schemes depend on the Heisenberg principle improbability standard as well as the polarization of photons [20, 21]. To desire, a high-level quantum computer needs much computation power and time [49]. So, quantum computers are used to solve security issues efficiently, like finance and traffic flow [50].

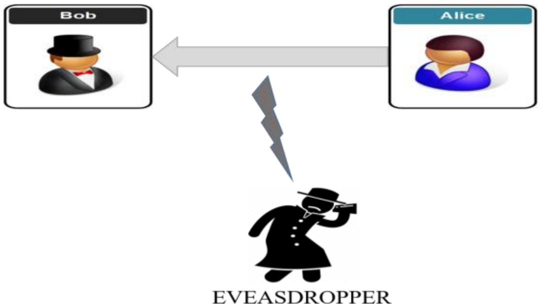


Figure 1. Eve eavesdrops while Alice and Bob communicate

A. Quantum key distribution Protocols

Several quantum key distribution protocols exist and each plays an essential role in the security domain [22].

i. EPR

Artur Ekert presented a quantum protocol in 1991 based on pair particles (pair EPR). In this protocol, a couple of bits exist whose isolation is called EPR pairs. The location of given bits remains constant if the nominated and dignified one bit leads to the route and measurement of the supporting bit. This term is called "action at a distance," as the bits are detached at long-distance [23].

ii. SARG 04

In the BB84 protocol, four states of polarity are recycled. Although given, four positions remain fixed using different archives. It produces a novel decorum named SARG04. It is vigorous against photon-number-splitting attacks while reducing beats of laser are used as an additional particular photon source. In this scenario, Alice sends some single-photon bits to the Bob of length 'a' above the public network. Then Bob chooses some basis while scheming the qubits transferred by Alice. Bob receives identical messages safely. Then he publicizes openly successful transmission. Alice and Bob cancel the procedure if any error occurs during transmission. The chance of communication detachment active to 144 km unrestricted planetary connection is anticipated [24].

iii. COW Protocol

It is single-mode Intelligible, which calculates the photons entrance period going on the indicator information streak. In this protocol, a key is established, and an interferometer is accumulated during a scheduled additional detecting period. So, the primary determinant of this streak is to distinguish the existence of Eve that one intends to stop the reliability via attacks.

iv.S13

Serna presented this protocol, in 2013 to stop the cost of data packets above a broadcast channel. The S13 protocol is scheduled for a kernel state named arbitrary kernel and public-key cryptographic. It is proven to protect after creating equal size secret keys at several connections. Given that this protocol is different from BB84 in the outdated methods [25].

v. SIX-STATE Protocol

SSP protocol is designed by Pasquinucci and Gisin and has two polarization states. This protocol has three polarization state bases, with x, y, and z, respectively. This protocol is parallel to BB84, which has two polarized bases [26]. In 2001 Nicolas Gisin specified that this protocol is harmless and eliminates snooping of the third party. The quantum bit error rate (QBER) of every single photon is 33% as compared to the BB84 protocol having 25% [27].

vi.One Time Pad

It is an unbreakable encryption scheme and contains strictly arbitrary key pairs. This key is lengthy to some extent as plaintext A happens recycled to send the plaintext to B, and both parties know their keys before encryption proceeds. When the key remains assorted with XOR, then this plaintext is converted into ciphertext. At the end encoded communication is assorted through identically of key and plaintext is returned.

A. Encryption Process:

It can be done by taking the XOR of the messages sent by Alice.
Plaintext: 11001101
Secret Key: 01100101
Ciphertext: 10101000
The plaintext is converted into ciphertext by the encryption process, while in decryption this ciphertext is again converted into plaintext.

vii. BB84 Protocol

Bennet and Brassard in 1984 proposed the BB84 protocol, which depends on Heisenberg's Uncertainty principle. It consists of two bases rectilinear (R) and diagonal (D) having four states of polarized photons. The polarization at 0^o contains rectilinear bases or 45^o and is used to represent the binary 0. While the polarization at 90^o on a rectilinear basis or $135^{o\ on}$ a diagonal basis represent the binary 1 [28, 29].

viii. B92 Protocol

A modified version of the BB84 protocol is called the B92 protocol with two states. A polarized photon at 0^o has a rectilinear basis and is used to represent binary 0. While A polarized photon at 45^o has a diagonal basis [30] and is used to represent binary 1 as shown in figure 2.

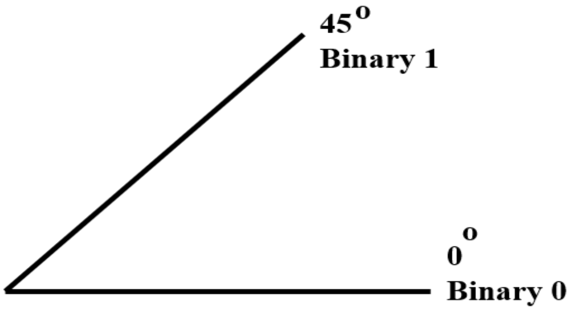


Figure 2. B92 Protocol

B92 protocol is similar to the BB84 protocol having two states instead of four [41]. Several results related to secure communication are discussed in [42]. The absolute B92 protocol security is established for scientific simulations.

The B92 quantum key distribution system of absolute security has been proven only for mathematical models. While security is several errors used to calculate bit error and phase error individually [45, 46].

B. Initiations of Quantum Communication

There are several basics of quantum communication, which we have discoursed in this section.

Heisenberg Uncertainty Principle: In this principle, definite sets of physical belongings are associated with each other. One can easily measure one property without destroying the other. It contains two photons rectilinear (horizontal and vertical) and diagonal (45^o and 135^o).

Assets of Quantum Protocol: Quantum protocols are always
safe, accurate, and vigorous. While in classical protocol security and privacy are the main apprehension.

Accurate: Bob can easily decrypt the unique bases using a decryption key.

Safe: Eve has no access to Alice and Bob's pieces of information.

Forcefulness: Alice and Bob identify the errors if Eve interrupts and at that time an alarming situation will be generated.

Quantum Entanglement: If more than one physical property is connected strongly, it means they are entangled photons. Einstein presented the concept of Quantum entanglement by spooky actions [31]. The chances of Eve are less if two qubits are attached strongly with each other.

The major contribution towards this paper is given as

a. This paper proposed Deployment of security vulnerabilities in Quantum Cryptographic & QKD using the B92 protocol.
b. The basic purpose of the B92 protocol is to enhance the security level against various attacks with and without the presence of Eve.
c. In this paper, the QuVis framework is used for implementation to communicate the secret keys between sender (plaintext) and receiver (ciphertext).
d. Our main contribution towards this paper is that we are using two non-orthogonal states with a single qubit. The B92 protocol performance is better than the BB84 protocol.

The rest of the paper is structured as follows, section II summarizes the literature review, methodology is explained in section III, section IV describes implementation, Section V provides discussion while section VI is the conclusion and future work. The last section is references that we have cited in our whole paper.

II. LITERATURE REVIEW

Quantum cryptography is a major source of secure communication between two parties, according to the values of quantum mechanics. Classical cryptography is less secure due to its liabilities as compared to quantum cryptography. It is important to introduce a strong cryptographic method for secure communication with computational power and speed. In this paper, the authors established a quantum scheme for joint verification and key formation with the assimilation of the IEEE 802.11 network to touch complete security. The basic aim of this paper is to build a high-security scheme with IEEE 802.11 network between validating parties [32]. The security of the proposed model is evaluated by the PRISM tool (model checking approach).

The effect of EVE is investigated in this research along with absolute security. Quantum cryptography is a primary application of quantum physics that uses qubits. The greatest essential of quantum cryptography is QKD. The problems in QKD are often occurred due to a huge number of attacks by EVE. This paper presented a comprehensive design to solve the different security problems using the BB84 and B92 protocols. This proposed architecture guarantees higher security and validity over a quantum channel. The proposed B92 protocol efficiency is high; therefore, it can be seen that the proposed QKD protocol is used to solve many implementation problems [33].

Several attacks may affect the quantum key distribution as well as quantum cryptography as shown in Table 1. These attacks are harmful to both classical and quantum systems. This paper focuses on quantum critical distribution attacks, remarkably, not classical attacks on the quantum protocol. According to this research, it has been observed that quantum systems contain vulnerabilities in the quantum protocol and overall system mechanisms. The attack discussed in this paper does not affect the cryptographic system of receiving side nor the vulnerability of the quantum key distribution protocol. Authors have proposed a method to avoid illegal users. This proposed system uses the sync pulses lessened to the photon with a signal. The experimental results of both theoretical and real parameters of the system are discussed in this paper. The proposed system gives higher accuracy results while obtaining the total length of the channel [34].

The speedy development of quantum computing is growing day by day. Authors are creating different security schemes based on post-quantum algorithms. The effectiveness of quantum algorithms influences the security of post-quantum digital signature patterns. The authors have presented a robust algorithm and applied quantum principles in a post-quantum signature scheme. In this paper, the B92 protocol is used for gaining cipher text. Python framework is used for the implementation and validation of the proposed algorithm. Additionally, B92 is used to distinguish the existence of EVE in case of any attack. So, we conclude that there is a regulation between computation power and security [35].

Security is a key parameter while focusing on quantum key distribution protocols and quantum cryptography. Therefore, device autonomous quantum key distribution presented a

protected key scheme with trusted and untrusted strategies. The basic purpose of this scheme is to ensure higher security after experimental analysis. When a source is producing high entangled photons then chances of EVE or third party becomes low. So, after using this approach Alice and Bob shared their entangled photons strongly which was never known by an EVE. This shows information is shared strongly between Alice and bob without any disturbance of EVE but quantity result is restricted [36].

Quantum key distribution plays an important role to improve security, especially with quantum systems. These quantum systems shared the secret key with quantum-automated assets. Entanglement constructed protocols contain further layers for security. This paper presents the semiconductor-based quantum systems to ensure the loyalty of entangled photons. The proposed system uses a consistently quantum key distribution protocol with two quantum channels. This study shows the semiconductor-based quantum equipment and recovers the best solution for a quantum statement [37]. Quantum cryptography is the best source to ensure security against eavesdropper attacks. QKD protocols, like the BB84 protocol, provides higher security against threats and attacks by the third party. It involves many physical experiments against vulnerabilities. This paper represents a complete overview of quantum key distribution protocol that protects against vulnerabilities. This can be done by merging hypothetical enlargement, error correction, and privacy magnification. This experiment enables higher privacy with two entangled photons on an optical fiber link. The security of our proposed model is based on quantum theory. The results showed secure cryptography with the real-world device and covers the applications established on the device individuality principle [38].

The essential purpose of QKD is to generate the secret key, which is shared between two parties. Various QKD protocols have been proposed for security.

Table 1. Attack on various protocols

	Protocols	**Attack**		
	Source Side Channel [52]	Wavelength-dependent link [53]	Detector control Attack [54]	Trojan-horse attack [55]
QDS				
Identical State sharing	Unforgeability	Unforgeability	Unforgeability	__
Different state sharing	__	__	Unforgeability	Unforgeability
QSS				
Entanglement based	__	__	Confidentiality	__
Single Qubit	__	__	__	Confidentiality
SI QRNG	__	Randomness	Randomness	__
QSDC	__	__	Confidentiality	Confidentiality
BQC	Confidentiality	__	__	Confidentiality

The first protocol was developed for both encoding and decoding purposes. These protocols are classified into a discrete variable (DV-QKD) and a continuous variable (CV-QKD). Authors have proposed a close-fitting and strong method to evaluate the reliability of optical pulse via heterodyne dimensions. A binary phase is conducted using CV-QKD protocol and ensures security against attacks, founded by DV-QKD methods. It is the best method to ensure security using QKD protocols [39].

According to recent trends, quantum computers are growing rapidly. Secure communication depends on quantum cryptography, where several public and private keys are used for security. While some public keys are not secure to some extent. Therefore, quantum computers are the best source of secure communication without any interruption. These QKD protocols are the best source of secure communication between two parties to share their secret key. This paper presents the security of QKD protocols without Eve. So QKD protocols are the best source of authentic and secure communication when two parties are sharing their information
[40].

III. METHODOLOGY

Secure communication is a prominent feature of quantum cryptography. Various QKD protocols are used for secure communication between two parties. Here we have proposed architecture with the B92 protocol to determine the secure communication between Alice and Bob. Alice and Bob use the single-qubit system to share their information because the B92 protocol is designed for a single non-orthogonal basis (à). In the B92 protocol, Alice (sender) always uses only one non-orthogonal basis. While sharing information with Bob (receiver), two non-orthogonal states are followed. These two non-orthogonal states are shown in table 2.

Table 2 Quantum Bits representation

Symbol	*Bit*
N	0
N	1

In the B92 protocol, several setups must be done via both Quantum and Classical channel

i) First stage (Quantum Channel)

- Alice picks arbitrarily some bits $A \in \{0,1\}^n$, $n > N$, where (N is the size of the ultimate key). If $A_i = 0$ Alice sends the state of $|0\rangle$ to Bob via a quantum channel and if $A_i = 1$, then she shows the state of $|+\rangle$ to Bob, for all $i \in \{0,1,\ldots, n\}$.
- Now, Bob generates some arbitrary bits' n in his turn $B \in \{0,1\}^n$, $n > N$. If $B_i = 0$ then, Bob picks the basis $\oplus$.
- Bob picks the basis $\otimes$ If $B_i = 1$, for all $i \in \{0, 1,\ldots, n\}$.
- So, Bob (sender) measures every quantum state sent by Alice (receiver) ($|0\rangle$ or $|+\rangle$) in the nominated basis ($\otimes$ or $\oplus$).
- Bob forms the vector test $T \in \{0,1\}^n$, $n > N$ by observing the subsequent instruction: if the dimension of Bob produces $|0\rangle$ or $|+\rangle$ then, $T_i = 0$ and if it produces $|1\rangle$ or $|-\rangle$, $T_i = 1$, for all $i \in \{0,1,\ldots , n\} \in$.

Table 3 Mathematical Representation of B92 protocol

Bits selected by Alice	**$A_i = 0$**				**$A_i = 1$**			
States forward by Alice	⎪0⟩				⎪+⟩			
Bob selected bits	B_i=0	B_i = 1			B_i = 0		B_i = 1	
Bob selected basis	⊕	⊗			⊕		⊗	
Bits dignified by Bob	⎪0⟩	⎪1⟩	⎪−⟩	⎪+⟩	⎪0⟩	⎪1⟩	⎪−⟩,	⎪+⟩
Dignified states	1	0	½	½	½	½	1	0
Final bit	0	-	0	1	0	1	0	-

ii) Second Stage (Classical Channel)

Following steps are taken for a classical channel

- Over a classical channel, Bob sends a message T to Alice.
- Alice and Bob reserve only those bits of A and B, where T_i = 1. While during these circumstance with the nonappearance of Eve, it contains: A_i = 1 – B. Hence, shared key is made up with A_i (or 1-B_i).
- Alice picks some bits of the rare key and shares those bits to Bob above the classical channel. If it happens i with $A_i \neq 1 - B_i$. At this time Eve is discovered and the communiqué channel is terminated.
- The mutual secret key K ∈ $\{0,1\}^N$ is made up by the rare key after exclusion.

Table 3 demonstrates the working B92 protocol behind the scene. There are three main arguments that are useful to understand the B92 protocol correctly. Initially, if Bob detects 0 then it does not know which Alice has sent to him.

Consequently, if Bob selects ⊕ and (resp.⊗), then he can get (⎪0⟩ (resp. ⎪+⟩) for any quantum state (⎪0⟩ or ⎪+⟩) sent by Alice. Furthermore, if Bob detects the 1 then he easily knows which basis is sent by Alice. Bob can measure all the bases sent by Alice and choose ⊗ (resp. ⊕). He will also measure the states state ⎪−⟩ (resp. ⎪1⟩) and Alice confidently sent to him ⎪0⟩ (resp. ⎪+⟩)

In the end, Alice and Bob share their secret key in the presence of Eve If there is any disturbance that occurs, one can easily observe the noise in the Quantum channel. In our proposed model both possibilities with and without the presence of Eve are shown in Figure 3. Both quantum and classical channels are used to share the secret key.

iii. Mathematical model for B92 protocol

We can represent the qubits of the B92 protocol in the following manner [43, 44] as shown in equation 1.

$$|\varphi j\ >=\ \beta|0x\ >\ \ +(-1)\ j\alpha|1x\ >$$

n above equation $j = \{0,1\}$ indicate the states of the X basis

$$\beta = \cos\frac{\theta}{2}\ ,\alpha = \sin\frac{\theta}{2} \qquad (2)$$

Two non-orthogonal states exist in B92 protocol; whereas Alice orthogonal states can be written in equation 3 φ_j.

$$|\varphi_j >= \beta|0_x\ >\ -(-1)^j\alpha|1_x\ >$$

The states organized by Alice can be represented by

$$\rho_A\ =\ \frac{|\varphi_0><\varphi_0|+|\varphi_1><\varphi_1|}{2}$$

$$=\ B^2\ |0_x><0_x|\ +\alpha^2\ |1_x><1_x|$$

States that are forwarded by Alice and received by the user bob can be identified from equation 1 and 2. The consequence of this research is to provide a plus point in identifying the Eve instead of the BB84 protocol. The experimental results of B92 exhibit a more secure mechanism to share secret key. The algorithm for the B92 protocol is taken from [51].

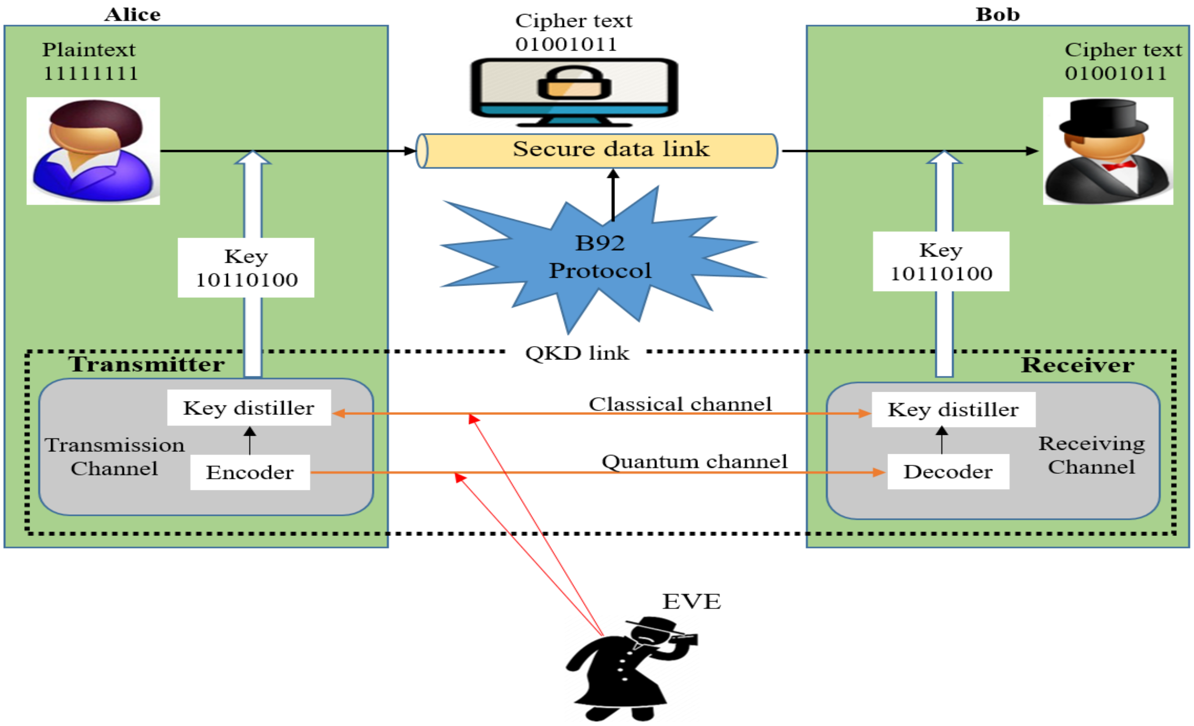


Figure 3. Proposed Model

Algorithm for B92 Protocol:

```
Input n; the size of the key.
b; Alice bit sequence,
Variables
m: counter,
b; (sequence of bits 0 and 1) generated
by Bob.
Begin
Input(n);
m=0;
While (M! n) do;
Alice choose the bit randomly $b_m$ (0, 1),
Bob ($t_m$) choose the basis
If $b_m = 1$ then Alice sends qubit $(0)'$ to
 Bob endif.
If $b_m = 0$ then Alice sends qubit 0 to Bob endif.
Bob measures the incoming qubit in the base
If Bob detects 0 then $b_m$ =? m = m+1 and inform
Alice
Detection Endif,
If Bob detects 1 then
If $t_m$= '+' then $b_m$ =1 endif.
If $t_m$= 'X' then $b_m$ =0 endif.
m= m+1 and inform Alice detection.
Endif
If Bob does not detect anything, so inform Alice
no detection
end while.
End
```

IV. Implementation

QuVis a group of cooperating simulations for knowledge and training of quantum mechanics. The implementation is done by fixed polarization with horizontal and vertical bases. QuVis is the best platform for secure communication. Between Alice and Bob. Through this platform, we choose the B92 protocol for our proposed solution. It has single-photon polarization having two non-orthogonal states and a modified version of BB84 protocol [56].

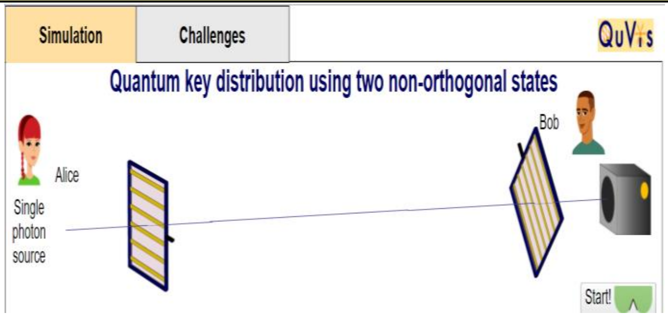
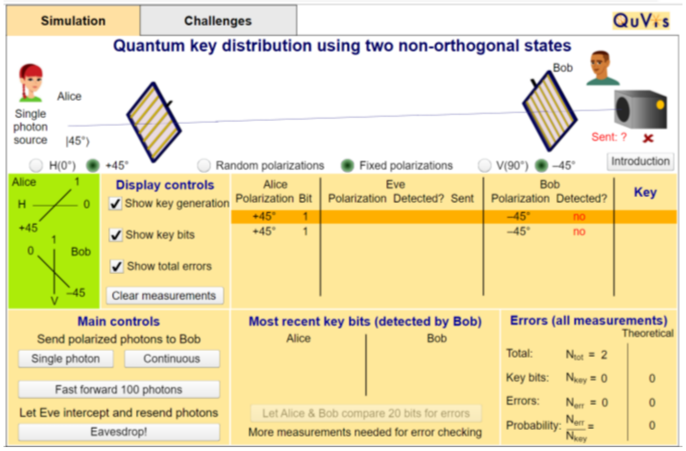
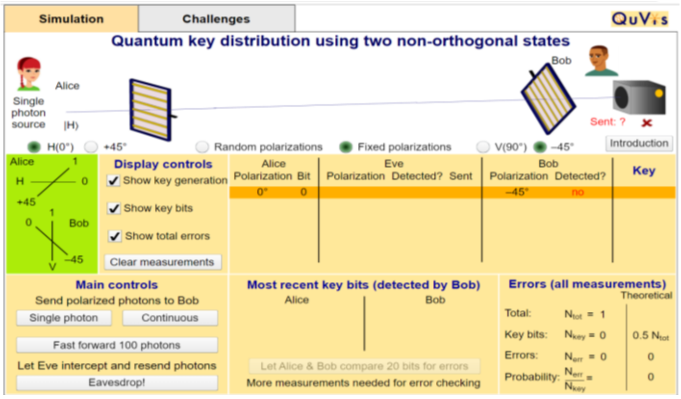
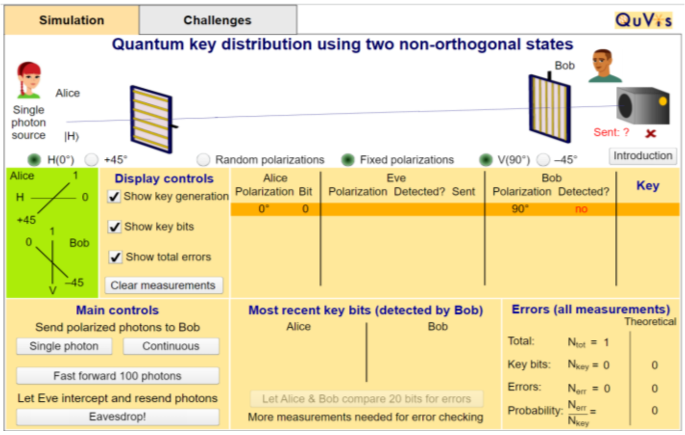
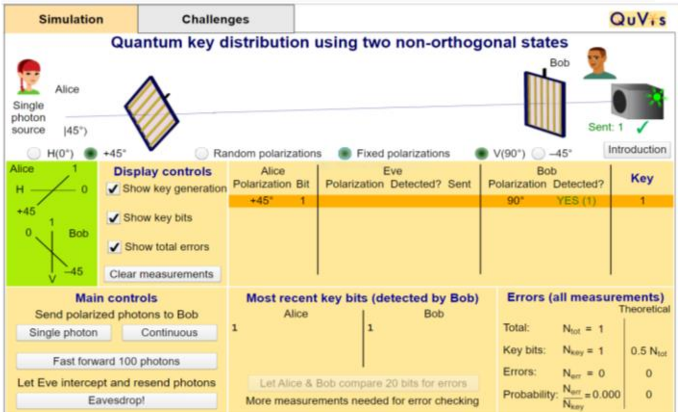
Explanations	**Simulation Results**
Figure 4: Alice wants to start conservation with Bob using two non-orthogonal states. Alice has only one single photon because in B92 protocol is based on a single photon.	 Simulation Challenges QuVis Quantum key distribution using two non-orthogonal states Alice Single photon source Bob Start! *Figure 4. Connection Establishment*
Figure 5: In this scenario, Alice propagates a Photon to another user Bob using (+45^0 and -45^0) polarization bits without any Eve. Here we can observe that no more recent keys are matched by Alice and Bob.	 Simulation Challenges QuVis Quantum key distribution using two non-orthogonal states Alice Single photon source |45°) Bob Sent: ? ✗ Introduction Alice 1 H 0 +45 1 0 Bob V −45 Clear measurements Main controls Send polarized photons to Bob Single photon Continuous Fast forward 100 photons Let Eve intercept and resend photons Eavesdrop! Let Alice & Bob compare 20 bits for errors ○ H(0°) ● +45° ○ Random polarizations ● Fixed polarizations ○ V(90°) ● −45° Display controls: ☑ Show key generation ☑ Show key bits ☑ Show total errors Alice Polarization Bit | Eve Polarization Detected? Sent | Bob Polarization Detected? | Key +45° 1 | | −45° no | +45° 1 | | −45° no | Most recent key bits (detected by Bob): Alice | Bob More measurements needed for error checking Errors (all measurements) Theoretical Total: N_{tot} = 2 Key bits: N_{key} = 0 | 0 Errors: N_{err} = 0 | 0 Probability: $\frac{N_{err}}{N_{key}}$ = | 0 *Figure 5*
Figure 6:In this case Alice sent a single Photon to Bob using (0^0 and -45^0) polarization bits without any Eve. Here we can observe that no more recent keys are matched by Alice and Bob.	 Simulation Challenges QuVis Quantum key distribution using two non-orthogonal states Alice Single photon source |H) Bob Sent: ? ✗ Introduction Alice 1 H 0 +45 1 0 Bob V −45 Clear measurements Main controls Send polarized photons to Bob Single photon Continuous Fast forward 100 photons Let Eve intercept and resend photons Eavesdrop! Let Alice & Bob compare 20 bits for errors ● H(0°) ○ +45° ○ Random polarizations ● Fixed polarizations ○ V(90°) ● −45° Display controls: ☑ Show key generation ☑ Show key bits ☑ Show total errors Alice Polarization Bit | Eve Polarization Detected? Sent | Bob Polarization Detected? | Key 0° 0 | | −45° no | Most recent key bits (detected by Bob): Alice | Bob More measurements needed for error checking Errors (all measurements) Theoretical Total: N_{tot} = 1 Key bits: N_{key} = 0 | 0.5 N_{tot} Errors: N_{err} = 0 | 0 Probability: $\frac{N_{err}}{N_{key}}$ = | 0 *Figure 6*
Figure 7:In this case Alice sent a single Photon to Bob using (0^0 and 90^0) polarization bits without any Eve. Here we can observe that no more recent keys are matched by Alice and Bob.	 Simulation Challenges QuVis Quantum key distribution using two non-orthogonal states Alice Single photon source |H) Bob Sent: ? ✗ Introduction Alice 1 H 0 +45 1 0 Bob V −45 Clear measurements Main controls Send polarized photons to Bob Single photon Continuous Fast forward 100 photons Let Eve intercept and resend photons Eavesdrop! Let Alice & Bob compare 20 bits for errors ● H(0°) ○ +45° ○ Random polarizations ● Fixed polarizations ● V(90°) ○ −45° Display controls: ☑ Show key generation ☑ Show key bits ☑ Show total errors Alice Polarization Bit | Eve Polarization Detected? Sent | Bob Polarization Detected? | Key 0° 0 | | 90° no | Most recent key bits (detected by Bob): Alice | Bob More measurements needed for error checking Errors (all measurements) Theoretical Total: N_{tot} = 1 Key bits: N_{key} = 0 | 0 Errors: N_{err} = 0 | 0 Probability: $\frac{N_{err}}{N_{key}}$ = | 0 *Figure 7*

Figure 8: In this case, Alice send a photon to Bob without the presence of Eve using (+45 and 90º). We can observe that bit is successfully shared with Bob without the presence of Eve. The most recent key bit (1) is matched and sent to Bob.



○ H(0°) ● +45° ○ Random polarizations ● Fixed polarizations ● V(90°) ○ –45°

Display controls
☑ Show key generation
☑ Show key bits
☑ Show total errors

Alice Polarization	Alice Bit	Eve Polarization	Eve Detected?	Eve Sent	Bob Polarization	Bob Detected?	Key
+45°	1				90°	YES (1)	1

Main controls
Send polarized photons to Bob
Let Eve intercept and resend photons

Most recent key bits (detected by Bob)

Alice	Bob
1	1

More measurements needed for error checking

Errors (all measurements)

		Theoretical
Total:	N_{tot} = 1	
Key bits:	N_{key} = 1	0.5 N_{tot}
Errors:	N_{err} = 0	0
Probability:	$\frac{N_{err}}{N_{key}}$ = 0.000	0

Figure 8

Figure 9: Eve is placed between Alice and Bob to share the single photon. We can analyze the interruption rate by adding the Eve and validate how Eve attacks during photon transmission. All the results are shown below figures.

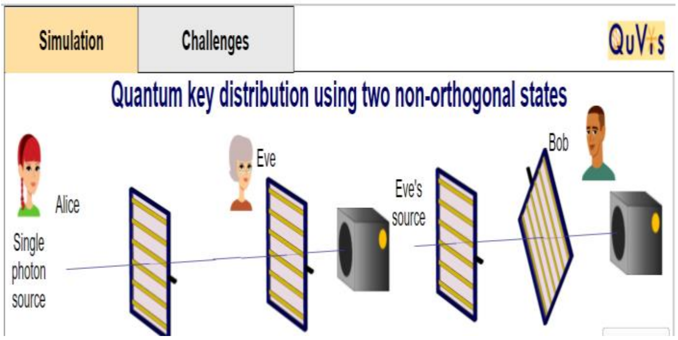
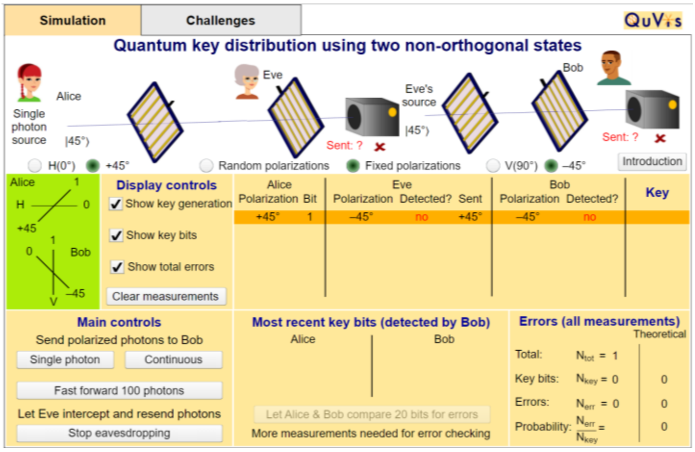


Figure 9

Figure 10: When we involve Eve between Alice and Bob during transmission of single Photon using (+45º and -45º) polarization states. We can observe that no most recent key is matched by Alice and Bob. So, Bob has not detected any key.



○ H(0°) ● +45° ○ Random polarizations ● Fixed polarizations ○ V(90°) ● –45°

Display controls
☑ Show key generation
☑ Show key bits
☑ Show total errors

Alice Polarization	Alice Bit	Eve Polarization	Eve Detected?	Eve Sent	Bob Polarization	Bob Detected?	Key
+45°	1	–45°	no	+45°	–45°	no	

Main controls
Send polarized photons to Bob
Let Eve intercept and resend photons

Most recent key bits (detected by Bob)

Alice	Bob

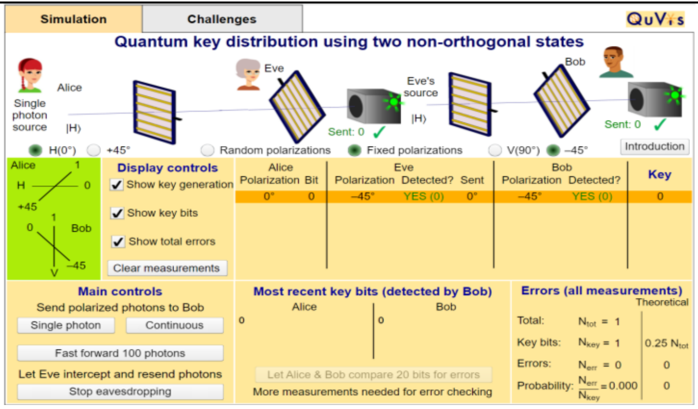
More measurements needed for error checking

Errors (all measurements)

		Theoretical
Total:	N_{tot} = 1	
Key bits:	N_{key} = 0	0
Errors:	N_{err} = 0	0
Probability:	$\frac{N_{err}}{N_{key}}$ =	0

Figure 10

Figure 11: In this case, Alice is forwards a photon to Bob in the presence of Eve using two polarization states (0° and -45°). The transmissions of a photon using a quantum channel are absolutely successful with two non-orthogonal states. Here most recent key matched by Alice and Bob is 0.



● H(0°) ○ +45° ○ Random polarizations ● Fixed polarizations ○ V(90°) ● −45°

Display controls
☑ Show key generation
☑ Show key bits
☑ Show total errors
Clear measurements

Alice Polarization	Alice Bit	Eve Polarization	Eve Detected?	Eve Sent	Bob Polarization	Bob Detected?	Key
0°	0	−45°	YES (0)	0°	−45°	YES (0)	0

Main controls
Send polarized photons to Bob
Single photon | Continuous
Fast forward 100 photons
Let Eve intercept and resend photons
Stop eavesdropping

Most recent key bits (detected by Bob)

Alice	Bob
0	0

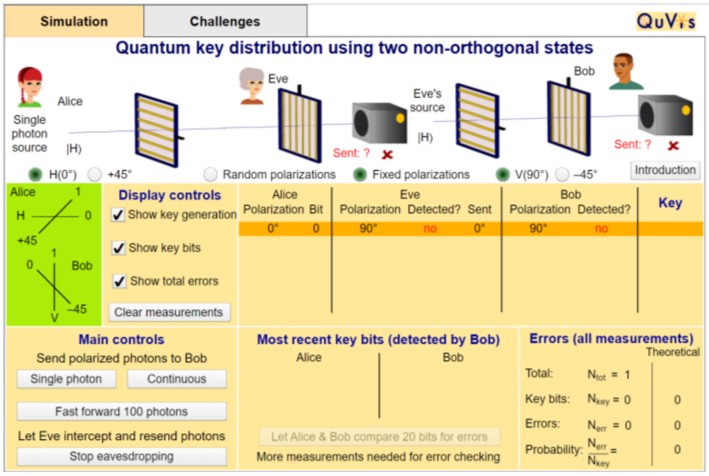
Let Alice & Bob compare 20 bits for errors
More measurements needed for error checking

Errors (all measurements)

		Theoretical
Total:	N_{tot} = 1	
Key bits:	N_{key} = 1	0.25 N_{tot}
Errors:	N_{err} = 0	0
Probability:	$\frac{N_{err}}{N_{key}}$ = 0.000	0

Figure 11

Figure 12: In this case, Alice is sending a single photon to Bob in the presence of Eve using two polarization states (0° and 90°). No more recent keys are matched here and the message is not sent to Bob, due to the interruption of Eve.



● H(0°) ○ +45° ○ Random polarizations ● Fixed polarizations ● V(90°) ○ −45°

Display controls
☑ Show key generation
☑ Show key bits
☑ Show total errors
Clear measurements

Alice Polarization	Alice Bit	Eve Polarization	Eve Detected?	Eve Sent	Bob Polarization	Bob Detected?	Key
0°	0	90°	no	0°	90°	no	

Main controls
Send polarized photons to Bob
Single photon | Continuous
Fast forward 100 photons
Let Eve intercept and resend photons
Stop eavesdropping

Most recent key bits (detected by Bob)

Alice	Bob

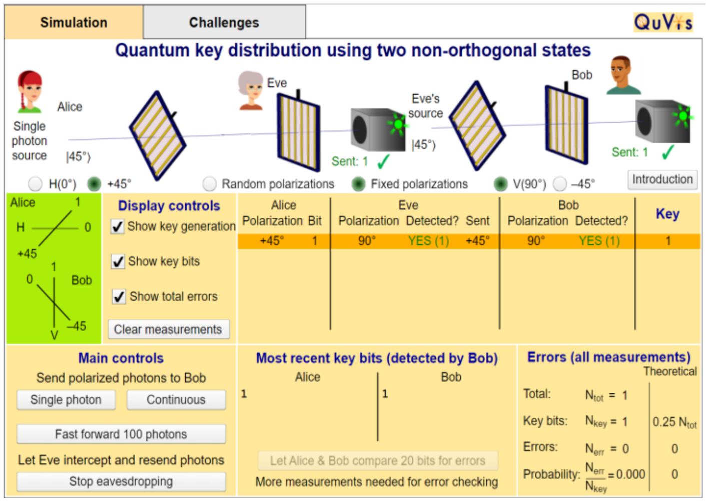
Let Alice & Bob compare 20 bits for errors
More measurements needed for error checking

Errors (all measurements)

		Theoretical
Total:	N_{tot} = 1	
Key bits:	N_{key} = 0	0
Errors:	N_{err} = 0	0
Probability:	$\frac{N_{err}}{N_{key}}$ =	0

Figure 12

Figure 13: In this scenario, Alice is sending a single photon to Bob in the presence of Eve using two polarization states (+45° and 90°). The transmission of a photon using a quantum channel is absolutely successful with two non-orthogonal states. Here most recent key matched by Alice and Bob is 1.



○ H(0°) ● +45° ○ Random polarizations ● Fixed polarizations ● V(90°) ○ −45°

Display controls
☑ Show key generation
☑ Show key bits
☑ Show total errors
Clear measurements

Alice Polarization	Alice Bit	Eve Polarization	Eve Detected?	Eve Sent	Bob Polarization	Bob Detected?	Key
+45°	1	90°	YES (1)	+45°	90°	YES (1)	1

Main controls
Send polarized photons to Bob
Single photon | Continuous
Fast forward 100 photons
Let Eve intercept and resend photons
Stop eavesdropping

Most recent key bits (detected by Bob)

Alice	Bob
1	1

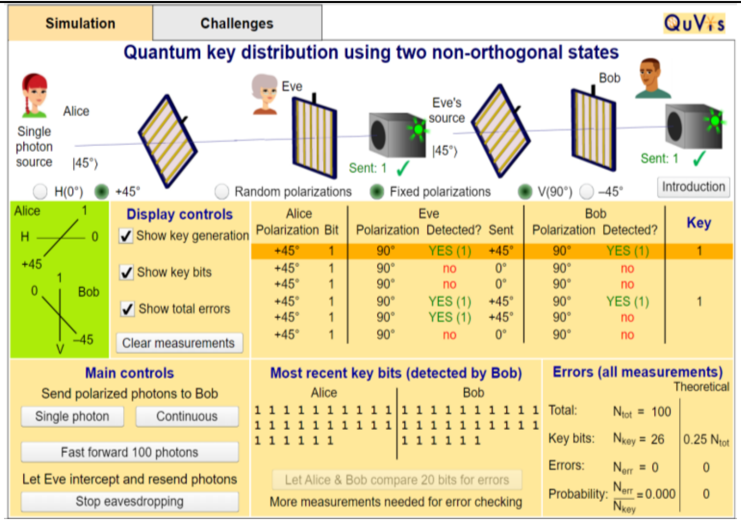
Let Alice & Bob compare 20 bits for errors
More measurements needed for error checking

Errors (all measurements)

		Theoretical
Total:	N_{tot} = 1	
Key bits:	N_{key} = 1	0.25 N_{tot}
Errors:	N_{err} = 0	0
Probability:	$\frac{N_{err}}{N_{key}}$ = 0.000	0

Figure 13

Figure 14: In this scenario, Alice propagates multiple photon bits with Bob using two non-orthogonal states as shown in figure 14. We can observe that there are only two cases in which Alice and Bob successfully shared their bits without any interruption of Eve.



Quantum key distribution using two non-orthogonal states

○ H(0°) ● +45° ○ Random polarizations ● Fixed polarizations ● V(90°) ○ –45°

Display controls

☑ Show key generation

☑ Show key bits

☑ Show total errors

Alice Polarization	Alice Bit	Eve Polarization	Eve Detected?	Eve Sent	Bob Polarization	Bob Detected?	Key
+45°	1	90°	YES (1)	+45°	90°	YES (1)	1
+45°	1	90°	no	0°	90°	no	
+45°	1	90°	no	0°	90°	no	
+45°	1	90°	YES (1)	+45°	90°	YES (1)	1
+45°	1	90°	YES (1)	+45°	90°	no	
+45°	1	90°	no	0°	90°	no	

Main controls

Send polarized photons to Bob

Let Eve intercept and resend photons

Most recent key bits (detected by Bob)

Alice	Bob
1 1 1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1 1 1
1 1 1 1 1 1	1 1 1 1 1 1

More measurements needed for error checking

Errors (all measurements)

		Theoretical
Total:	$N_{tot} = 100$	
Key bits:	$N_{key} = 26$	$0.25\ N_{tot}$
Errors:	$N_{err} = 0$	0
Probability:	$\frac{N_{err}}{N_{key}} = 0.000$	0

Figure 14

V. Discussion

QuVis platform is the best source of Quantum mechanics implementation. There are various Quantum cryptographic protocols that are used for secure communication between two users. We have used the B92 protocol for our proposed Model. As it is a modification of BB84 and provides more security than earlier OKD protocols B92 protocols consist of two non-orthogonal states having single-polarization photons. There are two non-orthogonal states e.g. horizontal and vertical with bit values 0 & 1 respectively as shown in Figure 14. In our proposed Model there are dual collaborative festivities Alice and Bob. Our basic purpose is to establish a secure communication link via B92 protocol through and deprived of third party or Eve. We have two possibilities

Without the presence of Eve

With the presence of Eve

While generating a secure communication between Alice and bob following steps are performed as shown in figure 15;

- First of all, Alice & Bob intend to initiate a secure communication link to share their secret key without the presence of an eavesdropper.
- For secure communication, both users share their secret key on a Quantum channel via B92 protocol. Because classically it is not possible, quantum is the best source of secure communication.
- Alice organizes every photon at 0° (horizontal) or +45° polarization. Here, horizontal polarization is assigned a bit value (0), and 45° is assigned a bit value (1).
- Alice sends the orthogonal states (90° or -45°) to Bob, and she informs Bob after sharing the secret key.

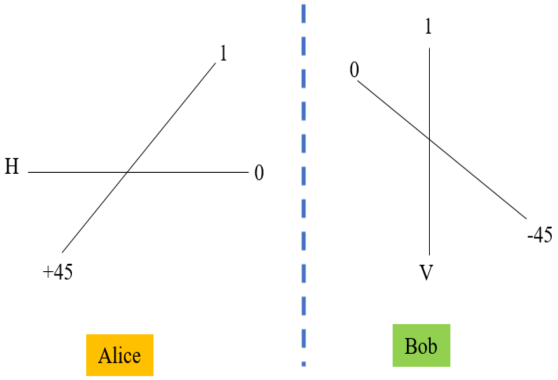


Figure 15. Horizontal and Vertical Basis

- Now Alice sends one polarization photon to Bob without the interference of Eve and uses two non-orthogonal states.
- Different possibilities are made for secure communication. There is only one possible communication link, where the bit is successfully shared with Bob without the presence of Eve. The most recent key bit (1) is matched and sent to Bob using a (+45 and 90°) basis.
- On the other hand in the presence of Eve, one can have two possibilities where Alice and Bob shared their bits successfully.
- If Bob detects the photon with two possible bits (0, 1) sent by Alice, then the bit is shared successfully to Bob without any Eve. Only one-bit value is assigned to Bob 0 or 1.

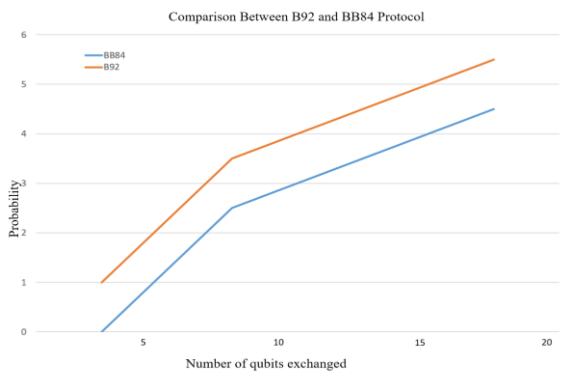


Figure 16. Comparison between B92 and BB84

This comparison graph in both protocols is done with the presence of eavesdroppers because without the presence of Eve, Alice & Bob can exchange their secret keys easily. From the above results, we can presume that Quantum cryptography is the best answer for secure communication between two entities. Alice and Bob share their keys using this orthogonal basis via B92 protocol. Graphically representation of B92 and BB84 protocols shows that B92 protocol is performing better than BB84 protocol. So one can say that B92 is more secure as compare to BB84 protocol. The graph is drawn between probability and the number of qubits exchanged in both protocols. In this graph rate of exchanged qubits is extremely large instead of probability. The exchange Qubits rate of the B92 is higher than BB84 protocol as shown in figure 16. Therefore, we have chosen the B92 protocol to share the random keys between sender and receiver.

VI. Conclusion and Future Work

Secure Communication is an important factor to share information between two parties. Cryptography guarantees privacy, verification, and truthfulness between both parties. Corresponding cryptography, QKD is a safe and sound method for communication between two parties to share their photos. This research presents a framework for quantum key distribution using the protocol B92. The B92 protocol helps two users to exchange their polarized photons with high security and without any interruption of Eavesdropper. While B92 protocol generates a secrete key, that is known to just sender and receiver. QuVis framework is used for this purpose and photons are transferred to Bob securely with and without any Eavesdropper. Photon transmission is done on both classical and quantum channels. In the quantum channel, we can conclude that there is only one possibility (0^{o} and -45^{o}) without any presence of Eve, where Bob detects a key shared by Alice. While in the presence of the key, there are only two cases (+45^{o} and 90^{o}) and (0^{o} and -45^{o}) where Bob detects a secret key shared by Alice. Peter Chapson, CEO of quantum startup IonQ, said that "quantum computers develop the information uniquely. Therefore, one can be able to discourse humanity's largest challenges. In the future, post-quantum computers can be used to understand biology, cure the diseases like cancer, and even be helpful to inverse climate changes.

References

[1] Wendin, G. (2022). Quantum information processing with superconducting circuits: a perspective. arXiv preprint arXiv:2302.04558.

[2] Li, B. H., Xie, Y. M., Cao, X. Y., Li, C. L., Fu, Y., Yin, H. L., & Chen, Z. B. (2022). One-Time Universal Hashing Quantum Digital Signatures without Perfect Keys. arXiv preprint arXiv:2301.01132..

[3] Portmann, C., & Renner, R. (2022). Security in quantum cryptography. Reviews of Modern Physics, 94(2), 025008.

[4] Marudhai, V., Prince, S., & Kumari, S. (2022). Design and Simulation of Physical Layer Security for Next Generation Intelligent Optical Networks. Wireless Personal Communications, 1-20.

[5] Sun, S., & Huang, A. (2022). A review of security evaluation of practical quantum key distribution system. Entropy, 24(2), 260.

[6] Liu, R., Rozenman, G. G., Kundu, N. K., Chandra, D., & De, D. (2022). Towards the industrialisation of quantum key distribution in communication networks: A short survey. IET Quantum Communication, 3(3), 151-163.

[7] Sharma, P., Bhatia, V., & Prakash, S. (2022). Efficient ordering policy for secret key assignment in quantum key distribution-secured optical networks. Optical Fiber Technology, 68, 102755.

[8] Geng, J. Q., Fan-Yuan, G. J., Li, K. J., Tang, M., Wang, S., He, D. Y., ... & Han, Z. F. (2022). Integration in the C-band between quantum key distribution and the classical channel of 25 dBm launch power over multicore fiber media. Optics Letters, 47(12), 3111-3114.

[9] Yu, X., Liu, Y., Zou, X., Cao, Y., Zhao, Y., Nag, A., & Zhang, J. (2022). Secret-Key Provisioning with Collaborative Routing in Partially-Trusted-Relay-based Quantum-Key-Distribution-Secured Optical Networks. Journal of Lightwave Technology, 40(12), 3530-3545.

[10] Zhang, X. X., Jiang, M. S., Wang, Y., Lu, Y. F., Li, H. W., Zhou, C., ... & Bao, W. S. (2022). Analysis of an injection-locking-loophole attack from an external source for quantum key distribution. Physical Review A, 106(6), 062412.

[11] Yu, X., Liu, Y., Zou, X., Cao, Y., Zhao, Y., Nag, A., & Zhang, J. (2022). Secret-Key Provisioning with Collaborative Routing in Partially-Trusted-Relay-based Quantum-Key-Distribution-Secured Optical Networks. Journal of Lightwave Technology, 40(12), 3530-3545.

[12] Yu, X., Liu, Y., Zou, X., Cao, Y., Zhao, Y., Nag, A., & Zhang, J. (2022). Secret-Key Provisioning with Collaborative Routing in Partially-Trusted-Relay-based Quantum-Key-Distribution-Secured Optical Networks. Journal of Lightwave Technology, 40(12), 3530-3545.

[13] Yu, X., Liu, Y., Zou, X., Cao, Y., Zhao, Y., Nag, A., & Zhang, J. (2022). Secret-Key Provisioning with Collaborative Routing in Partially-Trusted-Relay-based Quantum-Key-Distribution-Secured Optical Networks. Journal of Lightwave Technology, 40(12), 3530-3545.

[14] Xu, S., Li, P., Guo, S.Y. and Qiu, X., 2018. Fiber-wireless network virtual resource embedding method based on load balancing and priority. *IEEE Access*, *6*, pp.33201-33215.

[15] Lucamarini, M., Yuan, Z.L., Dynes, J.F. and Shields, A.J., 2018. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature*, *557*(7705), pp.400-403.

[16] Bennett, C.H. and Brassard, G., 2020. Quantum cryptography: Public key distribution and coin tossing. *arXiv preprint arXiv:2003.06557*.

[17] Sixto, X., Zapatero, V., & Curty, M. (2022). Security of decoy-state quantum key distribution with correlated intensity fluctuations. Physical Review Applied, 18(4), 044069.

[18] Pathare, A., & Deshmukh, B. (2022). Review on Cryptography Using Quantum Computing.

[19] Ahn, J., Kwon, H. Y., Ahn, B., Park, K., Kim, T., Lee, M. K., ... & Chung, J. (2022). Toward quantum secured distributed energy resources: Adoption of post-quantum cryptography (pqc) and quantum key distribution (qkd). Energies, 15(3), 714.

[20] Vartanian, T. P. (2022). The Unhackable Internet: How Rebuilding Cyberspace Can Create Real Security and Prevent Financial Collapse. Rowman & Littlefield.

[21] Gill, S. S., Kumar, A., Singh, H., Singh, M., Kaur, K., Usman, M., & Buyya, R. (2022). Quantum computing: A taxonomy, systematic review and future directions. Software: Practice and Experience, 52(1), 66-114.

[22] Moizuddin, M., Winston, J. and Qayyum, M., 2017, March. A comprehensive survey: quantum cryptography. In *2017 2nd International Conference on Anti-Cyber Crimes (ICACC)* (pp. 98-102). IEEE.

[23] Subramani, S., & Svn, S. K. (2022). Review of Security Methods Based on Classical Cryptography and Quantum Cryptography. Cybernetics and Systems, 1-19.

[24] Hasan, S. R., Chowdhury, M. Z., Saiam, M., & Jang, Y. M. (2022). Quantum Communication Systems: Vision, Protocols, Applications, and Challenges. arXiv preprint arXiv:2212.13333.

[25] Hasan, S. R., Chowdhury, M. Z., Saiam, M., & Jang, Y. M. (2022). Quantum Communication Systems: Vision, Protocols, Applications, and Challenges. arXiv preprint arXiv:2212.13333.

[26] Frigyik, A. (2022). Quantum Cryptography: Quantum Key Distribution, a Non-technical Approach. arXiv preprint arXiv:2211.17089.

[27] Huang, Z., Joshi, S. K., Aktas, D., Lupo, C., Quintavalle, A. O., Venkatachalam, N., ... & Rarity, J. G. (2022). Experimental implementation of secure anonymous protocols on an eight-user quantum key distribution network. npj Quantum Information, 8(1), 25..

[28] Bennett, C.H. and Brassard, G., 2020. Quantum cryptography: Public key distribution and coin tossing. *arXiv preprint arXiv:2003.06557*.

[29] Bennett, C.H. and Brassard, G., 2020. Quantum cryptography: Public key distribution and coin tossing. *arXiv preprint arXiv:2003.06557*.

[30] Lin, J., Tsai, C. W., & Yang, C. W. (2022). Cryptanalysis and improvement of the measurement-device-independent quantum key distribution with hyper-encoding. Modern Physics Letters A, 2250212.

[31] Einstein, A., Podolsky, B. and Rosen, N., 1935. Can quantum-mechanical description of physical reality be considered complete?. *Physical review*, *47*(10), p.777.

[32] Kumari, S. (2022). Enhancing the quantum communication channel using a novel quantum binary salt blowfish strategy. Wireless Personal Communications, 1-18.

[33] Miljkovic, N.N. and Stojanovic, A.D., 2018. Multiparameter QKD authentication protocol design over optical quantum channel. *Optical and Quantum Electronics*, *50*(8), pp.1-11.

[34] Pljonkin, A., Petrov, D., Sabantina, L. and Dakhkilgova, K., 2021. Nonclassical Attack on a Quantum Key Distribution System. *Entropy*, *23*(5), p.509.

[35] Ghosh, S., Zaman, M., Sakauye, G. and Sampalli, S., 2021. An Intrusion Resistant SCADA Framework Based on Quantum and Post-Quantum Scheme. *Applied Sciences*, *11*(5), p.2082.

[36] Sekatski, P., Bancal, J.D., Valcarce, X., Tan, E.Y.Z., Renner, R. and Sangouard, N., 2021. Device-independent quantum key distribution from generalized CHSH inequalities. *Quantum*, *5*, p.444.

[37] Basset, F.B., Valeri, M., Roccia, E., Muredda, V., Poderini, D., Neuwirth, J., Spagnolo, N., Rota, M.B., Carvacho, G., Sciarrino, F. and Trotta, R., 2021. Quantum key distribution with entangled photons generated on demand by a quantum dot. *Science Advances*, *7*(12), p.eabe6379.

[38] Nadlinger, D.P., Drmota, P., Nichol, B.C., Araneda, G., Main, D., Srinivas, R., Lucas, D.M., Ballance, C.J., Ivanov, K., Tan, E. and Sekatski, P., 2021. Device-Independent Quantum Key Distribution. *arXiv preprint arXiv:2109.14600*.

[39] Matsuura, T., Maeda, K., Sasaki, T. and Koashi, M., 2021. Finite-size security of continuous-variable quantum key distribution with digital signal processing. *Nature communications*, *12*(1), pp.1-13.

[40] Amer, O., Garg, V. and Krawec, W.O., 2021. An Introduction to Practical Quantum Key Distribution. *IEEE Aerospace and Electronic Systems Magazine*, *36*(3), pp.30-55.

[41] Rao, D., Jayaraman, R., & Pozueco, L. (2022). Effective Machine Communication Using Quantum Techniques Provides Improvement in Performance and Privacy through IoT Application. In Human-Machine Interaction and IoT Applications for a Smarter World (pp. 271-294). CRC Press.

[42] Tan, Y., Zhang, L., Sun, T., Song, Z., Wu, J., & He, Z. (2022). Polarization compensation method based on the wave plate group in phase mismatch for free-space quantum key distribution. EPJ Quantum Technology, 10(1), 1-12.

[43] Dušek, M., Lütkenhaus, N. and Hendrych, M., 2006. Quantum cryptography. *Progress in Optics*, *49*, pp.381-454.

[44] Lin, J., Tsai, C. W., & Yang, C. W. (2022). Cryptanalysis and improvement of the measurement-device-independent quantum key distribution with hyper-encoding. Modern Physics Letters A, 2250212.

[45] Kanitschar, F., George, I., Lin, J., Upadhyaya, T., & Lütkenhaus, N. (2022). Finite-Size Security for Discrete-Modulated Continuous-Variable Quantum Key Distribution Protocols. arXiv preprint arXiv:2301.08686.

[46] Tamaki, K., Koashi, M. and Imoto, N., 2003. Unconditionally secure key distribution based on two nonorthogonal states. *Physical review letters*, *90*(16), p.167904.

[47] Park, G., Zhang, K., Yu, K., & Korepin, V. (2022). Quantum multi-programming for Grover's search. Quantum Information Processing, 22(1), 54.

[48] Krantz, P., Kjaergaard, M., Yan, F., Orlando, T.P., Gustavsson, S. and Oliver, W.D., 2019. A quantum engineer's guide to superconducting qubits. *Applied Physics Reviews*, *6*(2), p.021318.

[49] Ding, Y., Wu, X.C., Holmes, A., Wiseth, A., Franklin, D., Martonosi, M. and Chong, F.T., 2020, May. SQUARE: strategic quantum ancilla reuse for modular quantum programs via cost-effective uncomputation. In *2020 ACM/IEEE 47th Annual International Symposium on Computer Architecture (ISCA)* (pp. 570-583). IEEE.

[50] Phalak, K., Ash-Saki, A., Alam, M., Topaloglu, R.O. and Ghosh, S., 2021. Quantum PUF for Security and Trust in Quantum Computing. *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, *11*(2), pp.333-342.

[51] Ouchao, B. and Jakimi, A., Performance Evaluation of Secure Key Distribution Based on the B92 Protocol. *International Journal of Advanced Engineering, Management and Science*, *4*(6), p.264297.

[52] Genêt, A., Guertechin, N.L.D. and Kaluđerović, N., 2021, October. Full key recovery side-channel attack against ephemeral SIKE on the Cortex-M4. In *International Workshop on Constructive Side-Channel Analysis and Secure Design* (pp. 228-254). Springer, Cham.

[53] Shakhovoy, R., Puplauskis, M., Sharoglazova, V., Maksimova, E., Hydyrova, S., Kurochkin, V., & Duplinskiy, A. (2022). Wavelength-and time-division multiplexing via pump current variation of a pulsed semiconductor laser-a method of synchronization for quantum key

distribution. IEEE Journal of Quantum Electronics.

[54] Lin, Y. Q., Wang, M., Yang, X. Q., & Liu, H. W. (2022). Counterfactual quantum key distribution with untrusted detectors. Heliyon, e13719.

[55] Alghenaim, M. F., Bakar, N. A. A., & Rahim, F. A. (2022, February). Awareness of Phishing Attacks in the Public Sector: Review Types and Technical Approaches. In Proceedings of the 2nd International Conference on Emerging Technologies and Intelligent Systems: ICETIS 2022 Volume 1 (pp. 616-629). Cham: Springer International Publishing.

[56] A. Ali et al., "Practically implementation of information loss: sensitivity, risk by different feature selection techniques," in IEEE Access, doi: 10.1109/ACCESS.2022