Journal of Interdisciplinary Mathematics
ISSN: 0972-0502 (Print), ISSN: 2169-012X (Online)
Vol. 27 (2024), No. 1, pp. 33–55
DOI : 10.47974/JIM-1640

The enhancement of quantum key distribution protocol to increase communication security between two parties

Kritsanapong Somsuk *
Department of Computer and Communication Engineering
Faculty of Technology
Udon Thani Rajabhat University
UDRU
Udon Thani
Thailand

Chalida Sanemueang †
Office of Academic Resources and Information Technology
Udon Thani Rajabhat University
UDRU
Udon Thani
Thailand

Suchart Khummanee §
Department of Computer Science
Faculty of Informatics
Mahasarakham University
Mahasarakham
Thailand

Chanwit Suwannapong ‡
Department of Computer Engineering
Faculty of Engineering
Nakhon Phanom University
Nakhon Phanom
Thailand

* *E-mail:* kritsanapong@udru.ac.th (Corresponding Author)
† *E-mail:* Chalida.sa@udru.ac.th
§ *E-mail:* suchart.k@msu.ac.th
‡ *E-mail:* schanwit@npu.ac.th

Sarutte Atsawaraungsuk [@]
Department of Computer Education
Udon Thani Rajabhat University
Udon Thani 41000
Thailand

Abstract

In this research, a new technique based on quantum key distribution (QKD) is described to lower the likelihood that eavesdroppers can intercept two-party communications without being detected by the sender and the recipient. The central idea is to enhance BB84 by increasing two quantum gates, Pauli-X gate and Pauli-Z gate, on both the sender and receiver sides to change the direction of each quantum state. This signifies that three control parameters must be specified to control three gates on both sides, excluding the control parameter for the quantum gate that generates a random bit on the sender side. In fact, the possibility that eavesdroppers may discreetly capture the information is 0.5 for nearly all methods. However, the probability of information captured by an eavesdropper decreases to 0.25 when all conceivable cases from Tables 1 through 7 are considered. Therefore, the proposed technique for exchanging the secret key is more secure and should be chosen for the implementation.

Subject Classification: *94A60, 68M25, 81P94.*

Keywords: *QKD, BB84, Quantum computer, Cryptography, Secret key.*

1. Introduction

Internet is currently one of the most prevalent information sharing channels. Because it is classified as an insecure channel, sensitive information should be not transmitted directly over the internet. Cryptography is one of the security procedures used to safeguard a secret message by encrypting and decrypting processes. This protocol consists of two distinct groups. The first category is symmetric key cryptography [1], which encrypts and decrypts messages using the secret key. The benefit is about time to complete the task. However, the challenge for all algorithms in this group is exchanging the secret key between two parties. The second category is asymmetric key or public key cryptography [2]. The implementation includes two distinct keys, the public key and the private key, which are mathematically related to one another. In fact, the public key must be made public, but the private key must be kept confidential.

[@] *E-mail:* **sarutte@udru.ac.th**

Although, public key cryptography can solve the problem of key exchange, the time required to complete the procedure is extremely high.

In fact, public key cryptography is always used to exchange the secret key, whereas symmetric key cryptography is used to protect the information. RSA [3] is the most well-known public key cryptography, and it is still used for a variety of tasks today. RSA's security is generally based on the integer factorization issue [4]. Although several factoring methods based on digital computers, such as [5–10], were proposed to break RSA, there is no algorithm that seems to do in polynomial time. P. Shor [11] presented the quantum computer-based factoring technique in 1994. Moreover, he asserted that RSA might be broken quickly if a fully developed quantum computer is created. In addition, it is highly possible that a quantum computer can break all public key cryptography techniques based on digital computer. Therefore, a new technique for exchanging the secret key should be proposed rather than a group of public key cryptography algorithms.

Quantum key distribution (QKD) [12 - 16] which relies on quantum computer is an alternative to public key cryptography for exchanging the secret key. In addition, quantum channel must be utilized for two-party communication. In fact, numerous methods for QKD have been developed. However, the possibility that an eavesdropper may capture the state without the sender or receiver noticing will only be 0.5. Therefore, the length of the key should be quite long to prevent attacks by eavesdroppers.

The purpose of this work is to offer a new quantum computer-based QKD approach to reduce the probability that eavesdroppers can identify the proper state for each state. Consequently, the length of the process's key can be shortened.

2. Related Works

This section examines the concept of quantum computer, some quantum gates, and QKD methods.

2.1 *Quantum Computer*

The quantum computer [17] represents the next generation of the computer. It differs from the digital computer in that the unit of digital computer is referred to as a bit. In fact, a bit's value is either 0 or 1. On the other hand, the quantum state is separated into two types of quantum bits, the unit of quantum computer is called quantum bit (qubit). The first

category is the pure state in which the state is either $|0\rangle$ or $|1\rangle$; it is analogous to a bit. The second state is a superposition state in which it can be both $|0\rangle$ and $|1\rangle$ simultaneously. In addition, quantum computers have unique properties such as superposition, interference, entanglement, etc. In fact, if a quantum computer with a high level of efficiency is created, many public key methods may be broken rapidly.

2.2 *Quantum Gate*

Quantum computing-based algorithms are mostly comprised of quantum circuits. Moreover, a quantum circuit is formed by combining many quantum gates [18]. However, only quantum gates selected for algorithm creation in QKD are assessed.

1) Hadamard Gate (H) is a single-qubit gate that produces a superposition state. The result of the Hadamard gate is shown in Equation (1).

$$\begin{aligned} H|0\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ H|1\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{aligned} \tag{1}$$

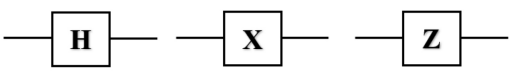
2) The Pauli-X Gate (X) is a single-qubit gate that can flip the state of a single qubit. The consequence of a Pauli-X gate is illustrated by the equation (2).

$$\begin{aligned} X|0\rangle &= |1\rangle \\ X|1\rangle &= |0\rangle \end{aligned} \tag{2}$$

3) Pauli-Z Gate (Z) is a single qubit gate that rotates the state around the z-axis by radians. The result of the Pauli-Z gate is illustrated by the equation (3).

$$\begin{aligned} Z|0\rangle &= |0\rangle \\ Z|1\rangle &= -|1\rangle \end{aligned} \tag{3}$$

In Figure 1 is an illustration of quantum gates: Figure 1.a), 1.b), and 1.c) are, respectively, Hadamard Gate, Pauli-X Gate, and Pauli-Z Gate.



a) Hadamard Gate b) Pauli-X Gate c) Pauli-Z Gate

Figure 1

Example of Quantum Gate

2.3 *QKD Protocols*

Using quantum theory, QKD is the technique for exchanging the secret key between two parties. In this part, some well-known QKD methods are examined.

1) BB84 [19] is recognized as the initial QKD algorithm. It was introduced by C. Bennentt and G. Brassard in 1984. In general, the no-cloning theorem, which states that each qubit cannot be cloned prior to a measurement, and the Heisenberg uncertainty principle are the most important concepts indicating that BB84 is one of the most secure algorithms in QKD. This approach employs two photon polarizations as the basis for encoding the random bit provided by the sender. The linear polarization basis, "+", is the first basis. When a bit "0" is selected and the linear polarization basis is chosen, typically the symbol "↑" is chosen as the sender's polarization for transfer to a receiver. Alternatively, if a sender selects a bit "1" with the linear polarization basis, the symbol "→" will be used to represent the sender's polarization. The second basis is diagonal polarization basis ("×"). Two symbols represent this polarization base. The first symbol that will be chosen when a sender selects a random bit "0" is "↗". Alternatively, if a random bit is "1", the second symbol "↖" will be selected for transmission to a receiver. In fact, the receiver will choose the polarization basis after receiving the sender's polarization. If both the receiver and the sender use the same basis, the photon will be in a pure state, and both parties will use this state as a component of the secret key. However, the photon enters a superposition state whenever the basis of the sender and receiver are different. In addition, the sender will disclose the basis of each qubit with the receiver following the measurement. The selected qubit must be in a pure state after the photon has traveled through the receiver's basis.

In Figure 2, assume that Alice is the sender and Bob is the recipient. If there is an eavesdropper, Eve represents this individual. In this figure, BB84's quantum circuit is depicted. In addition, c_0, c_1, and r are the parameters used to control the quantum gate. If its control parameter is equal to 1, the quantum gate will be triggered. In addition, $|Ø'\rangle$ will be in a pure state when c_1 equals r. Moreover, if $c_1 = 0$ and $r = 0$ then the sender and the receiver pick the linear polarization basis. When $c_1 = 1$ and $r = 1$, however, the diagonal polarization basis is selected.

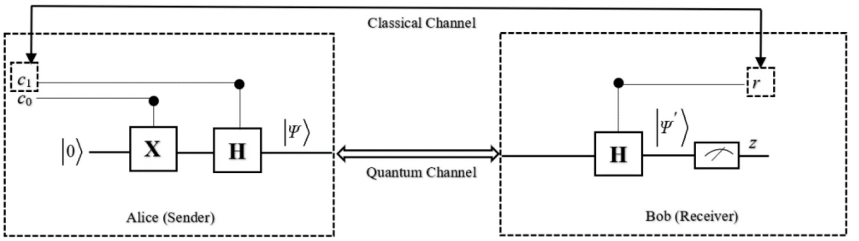


Figure 2

BB84 Quantum Circuit

Assume that eavesdroppers may interfere with the communication between a sender and a receiver, there is only one reason why the photon is trapped and neither the sender nor the receiver is notified of it: eavesdroppers must estimate the correct basis for each qubit chosen by the sender. However, the possibility that eavesdroppers will accurately select the basis of each qubit is only 0.5.

In 2013, A. Chen, W. Peng, and T. Gui [20] reported a variation of the BB84 protocol. This protocol is based on quantum phase with the following four bases: +, ×, +*, ×*. The symbols for the first two bases are equivalent as BB84. Nonetheless, the symbol "↓" represents the down polarization condition in which the basis "+*" and the random bit "0" are chosen. Alternatively, if the basis "+*"and the random bit "1" are chosen, the left polarization state "←" is the representative. Moreover, if the basis "×*"is chosen, there are two polarization states, "↘" and "↙", which represent a random bit "0" and "1" respectively. However, the quantum circuit for this method has not yet been presented.

Moreover, the BB84 attack strategy [21] was proposed in 2009. The plan is for Eve to intercept photons and store them in quantum memory. After then, each photon with a Breidbart basis will be sent to Bob at random. In fact, Eve will be informed of the basis of each photon when Alice and Bob trade bases. Accordingly, Eve can also be notified of all bases, as they are transmitted over the classical channel. Consequently, Eve will measure each photon stored in quantum memory using each of the disclosed bases. Because devices to process or manage quantum states are still in development, some information stored in quantum memory may be lost or corrupted by noise when it is held in the memory for an extended period. Alice and Bob may therefore agree to withhold their information until the appropriate time to avoid an attack utilizing this method.

2) B92 [22] is one of the QKD protocols. It was introduced in 1992 by C. Bennett. B92, which utilizes a non-orthogonal state to transmit information across a quantum channel, requires just two states, $|0\rangle$ and $\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$, for each qubit on the sender side, which is fewer than BB84, that typically requires four states for implementation. A sender will select a string of qubits (A) where $A \in \{0,1\}^n$ and n is the length of the qubits. When $A_i = 0$, the state $|0\rangle$ will be transmitted to a receiver, while when $A_i = 1$, the state $\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$ will be transmitted. After each qubit reaches a receiver, the basis will be chosen to determine the final state. In fact, if both the sender and the receiver select the same state, the final state is always 0. In contrast, if the basis chosen by the sender differs from the basis chosen by the recipient, the probability that the outcome is 0 or 1 is 0.5. Nonetheless, only the result equal to 1 will be chosen for implementation. Additionally, it implies that the sender's basis differs from the receiver's when the result equals 1. Although the probability that eavesdroppers will correctly select the basis of each qubit is comparable to that of BB84, B92 has a more resilient approach with optical imperfection and detector noise.

3) Artur K. Ekert [23] proposed the E91 protocol for exchanging the secret key through quantum channel in 1991. This technique uses EPR pairs (or Bell States) which was discovered by Einstein, Podolsky and Rosen in 1935 for the communication between two parties. In fact, Bell states are the relationship between two entangled qubits; this phenomenon is known as quantum entanglement. The equation (4) illustrates the Bell state examples.

$$\begin{aligned} |\Psi_1\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ |\Psi_2\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\ |\Psi_3\rangle &= \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) \\ |\Psi_4\rangle &= \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle) \end{aligned} \tag{4}$$

The initial step of E91 is for the sender to generate a sequence of EPR pairs. One photon must be stored in quantum memory, while the other qubit is delivered to a receiver. Both the sender and the receiver will then select their measurement basis for the particle. In general, only results that the sender and the receiver select the same basis will be implemented. Assume that eavesdroppers wish to interfere without being detected

between a sender and a receiver, they must accurately guess all basses. Consequently, the probability that eavesdroppers will properly select the basis of each qubit remains at 0.5.

4) In 2004, V. Scarani, A. Acin, G. Ribordy, and N. Gisin introduced the SARG04 Protocol [24 - 25], which is the algorithm for QKD. This algorithm's core notion is quite close to BB84. In fact, SARG04 employs two bases, the linear polarization basis and the diagonal polarization basis, as well as four states; all bases and states are identical to those of BB84. However, the advantage of SARG04 is that it is resistant to the Photon-Number Splitting attack (PNS attack), which is one of the quantum computing-based strategies used to disrupt communication between two parties.

5) Coherent One-Way protocol (COW Protocol) [26 – 27] was proposed by N. Gisin et al. This approach is based on decoding the information into time slots. Therefore, the COW protocol does not depend on the polarization of optical signals, but rather on the arrival time of the signal. In addition, COW provides protection against both reduced interference visibility and PNS attack.

3. The Proposed Method

The purpose of this study is to present the improvement of BB84 that will limit the probability of information interfered by eavesdroppers. For nearly all QKD methods, the probability that eavesdroppers will predict the basis to obtain the same state as the sender is 0.5. However, it is reduced to 0.25 when the proposed method is chosen for the implementation. In addition, the probability that a receiver will guess the basis in order to determine the correct state remains constant at 0.5. Furthermore, the quantum circuit for the suggested technique is described.

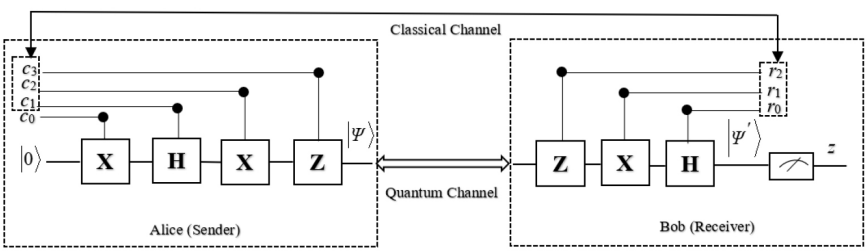


Figure 3

Quantum Circuit of the Proposed Method

The quantum circuit of the proposed method is shown in Figure 3. There are four quantum gates for the implementation on the sender side, from left to right. Each gate has a control parameter. If the value of the control parameter is 1, the gate is executed. On the other hand, when the control parameter is equal to 0, the gate will do nothing. The first gate is a Pauli-X gate that assigns each qubit's state. The parameter to control the first gate is c_0. The second gate is Hadamard gate with the control parameter c_1. This gate is used for basis selection. Pauli-X gate and Pauli-Z gate with respective control parameters c_2 and c_3 are the final two gates. In fact, these gates are chosen to assign each photon's direction. Therefore, each photon has four directions in each basis. For instance, assuming a sender selects the linear polarization basis, the four directions of a photon are $|0\rangle$, $-|0\rangle$, $|1\rangle$ and $-|1\rangle$. Under contrast, in the diagonal polarization basis, the directions of a photon are $\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$, $\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$, $\frac{1}{\sqrt{2}}(|1\rangle-|0\rangle)$, and $\frac{1}{\sqrt{2}}(-|0\rangle-|1\rangle)$.

There are three quantum gates from left to right on the receiver side. Pauli-Z gate and Pauli-X gate with respective control parameters r_2 and r_1 are the first two gates. These gates are utilized to choose the direction of each qubit. The final gate is the Hadamard gate, which is employed by a receiver to select the basis. The parameter r_0 controls the operation of this gate.

Because there are four control parameters to assign the state in sender side, the basis, and the direction of each qubit, it is subdivided into the following 16 cases:

Case 1: Alice sends a qubit '0' in rectilinear basis with the following control parameters: $c_0 = 0$, $c_1 = 0$, $c_2 = 0$ and $c_3 = 0$, then $|\Psi\rangle = |0\rangle$. Therefore, each instance of $|\Psi'\rangle$ is shown in Table 1.

Case 2: Alice sends a qubit '1' in rectilinear basis with the following control parameters: $c_0 = 1$, $c_1 = 0$, $c_2 = 0$ and $c_3 = 0$, then $|\Psi\rangle = |1\rangle$. Therefore, each instance of $|\Psi'\rangle$ is shown in Table 2.

Case 3: Alice sends a qubit '0' in diagonal basis with the following control parameters: $c_0 = 0$, $c_1 = 1$, $c_2 = 0$ and $c_3 = 0$, then $|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$. Therefore, **e**ach instance of $|\Psi'\rangle$ is shown in Table 3.

Case 4: Alice sends a qubit '1' in diagonal basis with the following control parameters: $c_0 = 1$, $c_1 = 1$, $c_2 = 0$ and $c_3 = 0$, then $|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Therefore, **e**ach instance of $|\Psi'\rangle$ is shown in Table 4.

Case 5: Alice sends a qubit '0' in rectilinear basis with the following control parameters: $c_0 = 0$, $c_1 = 0$, $c_2 = 1$ and $c_3 = 0$, then $|\Psi\rangle = |1\rangle$. Therefore, **e**ach instance of $|\Psi'\rangle$ is like the information in Table 2.

Case 6: Alice sends a qubit '1' in rectilinear basis with the following control parameters: $c_0 = 1$, $c_1 = 0$, $c_2 = 1$ and $c_3 = 0$, then $|\Psi\rangle = |0\rangle$. Therefore, **e**ach instance of $|\Psi'\rangle$ is like the information in Table 1.

Case 7: Alice sends a qubit '0' in diagonal basis with the following control parameters: $c_0 = 0$, $c_1 = 1$, $c_2 = 1$ and $c_3 = 0$, then $|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Therefore, **e**ach instance of $|\Psi'\rangle$ is like the information in Table 3.

Case 8: Alice sends a qubit '1' in diagonal basis with the following control parameters: $c_0 = 1$, $c_1 = 1$, $c_2 = 1$ and $c_3 = 0$, then $|\Psi\rangle = \frac{1}{\sqrt{2}}(|1\rangle - |0\rangle)$. Therefore, **e**ach instance of $|\Psi'\rangle$ is shown in Table 5.

Case 9: Alice sends a qubit '0' in rectilinear basis with the following control parameters: $c_0 = 0$, $c_1 = 0$, $c_2 = 0$ and $c_3 = 1$, then $|\Psi\rangle = |0\rangle$. Therefore, **e**ach instance of $|\Psi'\rangle$ is like the information in Table 1.

Case 10: Alice sends a qubit '1' in rectilinear basis with the following control parameters: $c_0 = 1$, $c_1 = 0$, $c_2 = 0$ and $c_3 = 1$, then $|\Psi\rangle = -|1\rangle$. Therefore, **e**ach instance of $|\Psi'\rangle$ is shown in Table 6.

Case 11: Alice sends a qubit '0' in diagonal basis with the following control parameters: $c_0 = 0$, $c_1 = 1$, $c_2 = 0$ and $c_3 = 1$, then $|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Therefore, **e**ach instance of $|\Psi'\rangle$ is like the information in Table 4.

Case 12: Alice sends a qubit '1' in diagonal basis with the following control parameters: $c_0 = 1$, $c_1 = 1$, $c_2 = 0$ and $c_3 = 1$, then $|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Therefore, **e**ach instance of $|\Psi'\rangle$ is like the information in Table 3.

Case 13: Alice sends a qubit '0' in rectilinear basis with the following control parameters: $c_0 = 0$, $c_1 = 0$, $c_2 = 1$ and $c_3 = 1$, then $|\Psi\rangle = -|1\rangle$. Therefore, **e**ach instance of $|\Psi'\rangle$ is like the information in Table 6.

Case 14: Alice sends a qubit '1' in rectilinear basis with the following control parameters: $c_0 = 1$, $c_1 = 0$, $c_2 = 1$ and $c_3 = 1$, then $|\Psi\rangle = |0\rangle$. Therefore, **e**ach instance of $|\Psi'\rangle$ is like the information in Table 1.

Case 15: Alice sends a qubit '0' in diagonal basis with the following control parameters: $c_0 = 0$, $c_1 = 1$, $c_2 = 1$ and $c_3 = 1$, then $|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Therefore, **e**ach instance of $|\Psi'\rangle$ is like the information in Table 4.

Case 16: Alice sends a qubit '1' in diagonal basis with the following control parameters: $c_0 = 1$, $c_1 = 1$, $c_2 = 1$ and $c_3 = 1$, then $|\Psi\rangle = \frac{1}{\sqrt{2}}(-|0\rangle - |1\rangle)$. Therefore, **e**ach instance of $|\Psi'\rangle$ is shown in Table 7.

Based on the data presented in Tables 1 through 7, it appears that:

1) A qubit output ($|\Psi'\rangle$) has four pure states and four superposition states before the measurement. Therefore, the probability that a qubit will be selected as a part of the secret key is 0.5. In addition, there is a 50 percent chance that a qubit in the same location will be dropped.
2) Assume Alice selects a diagonal basis with a control parameter of 1 for the Hadamard gate. The state of $|\Psi\rangle$ is always a superposition state. On the other hand, it becomes a pure state. In addition, the information in Tables 1 through 7 indicates that if $|\Psi\rangle$ is a pure state, the result of $|\Psi'\rangle$, which is also a pure state, appears in 1st row, 3rd row, 5th row and 7th row. However, the superposition state is visible in 2nd row, 4th row, 6th row and 8th row. On the other hand, $|\Psi'\rangle$ becomes an opposite state whenever $|\Psi'\rangle$ is a superposition state.

Table 1

Finding the State $|\Psi'\rangle$ and Output z from the measurement when $|\varnothing\rangle = |0\rangle$

Row	Input			$\|\Psi'\rangle$	Measurement (z)
	r_2	r_1	r_0		
1	0	0	0	$\|0\rangle$	$\|0\rangle$
2	0	0	1	$\frac{1}{\sqrt{2}}(\|0\rangle+\|1\rangle)$	Random
3	0	1	0	$\|1\rangle$	$\|1\rangle$
4	0	1	1	$\frac{1}{\sqrt{2}}(\|0\rangle-\|1\rangle)$	Random
5	1	0	0	$\|0\rangle$	$\|0\rangle$
6	1	0	1	$\frac{1}{\sqrt{2}}(\|0\rangle+\|1\rangle)$	Random
7	1	1	0	$\|1\rangle$	$\|1\rangle$
8	1	1	1	$\frac{1}{\sqrt{2}}(\|0\rangle-\|1\rangle)$	Random

Table 2

Finding the State $|\Psi'\rangle$ and Output z from the measurement when $|\varnothing\rangle = |1\rangle$

Row	Input			$\|\Psi'\rangle$	Measurement (z)
	r_2	r_1	r_0		
1	0	0	0	$\|1\rangle$	$\|1\rangle$
2	0	0	1	$\frac{1}{\sqrt{2}}(\|0\rangle-\|1\rangle)$	Random
3	0	1	0	$\|0\rangle$	$\|0\rangle$
4	0	1	1	$\frac{1}{\sqrt{2}}(\|0\rangle+\|1\rangle)$	Random
5	1	0	0	$-\|1\rangle$	$\|1\rangle$
6	1	0	1	$\frac{1}{\sqrt{2}}(\|1\rangle-\|0\rangle)$	Random
7	1	1	0	$-\|0\rangle$	$\|0\rangle$
8	1	1	1	$\frac{1}{\sqrt{2}}(-\|0\rangle-\|1\rangle)$	Random

Table 3

Finding the State $|\Psi'\rangle$ and Output z from the measurement when $|\varnothing\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

Row	Input			$\|\Psi'\rangle$	Measurement (z)
	r_2	r_1	r_0		
1	0	0	0	$\frac{1}{\sqrt{2}}(\|0\rangle+\|1\rangle)$	Random
2	0	0	1	$\|0\rangle$	$\|0\rangle$
3	0	1	0	$\frac{1}{\sqrt{2}}(\|0\rangle+\|1\rangle)$	Random
4	0	1	1	$\|0\rangle$	$\|0\rangle$
5	1	0	0	$\frac{1}{\sqrt{2}}(\|0\rangle-\|1\rangle)$	Random
6	1	0	1	$\|1\rangle$	$\|1\rangle$
7	1	1	0	$\frac{1}{\sqrt{2}}(\|1\rangle-\|0\rangle)$	Random
8	1	1	1	$-\|1\rangle$	$\|1\rangle$

Table 4

Finding the State $|\Psi'\rangle$ and Output z from the measurement when

$$|\varnothing\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Row	Input			$\|\Psi'\rangle$	Measurement (z)
	r_2	r_1	r_0		
1	0	0	0	$\frac{1}{\sqrt{2}}(\|0\rangle-\|1\rangle)$	Random
2	0	0	1	$\|1\rangle$	$\|1\rangle$
3	0	1	0	$\frac{1}{\sqrt{2}}(\|1\rangle-\|0\rangle)$	Random
4	0	1	1	$-\|1\rangle$	$\|1\rangle$
5	1	0	0	$\frac{1}{\sqrt{2}}(\|0\rangle+\|1\rangle)$	Random
6	1	0	1	$\|0\rangle$	$\|0\rangle$
7	1	1	0	$\frac{1}{\sqrt{2}}(\|0\rangle+\|1\rangle)$	Random
8	1	1	1	$\|0\rangle$	$\|0\rangle$

Table 5

Finding the State $|\Psi'\rangle$ and Output z from the measurement when

$$|\varnothing\rangle = \frac{1}{\sqrt{2}}(|1\rangle - |0\rangle)$$

Row	Input			$\|\Psi'\rangle$	Measurement (z)
	r_2	r_1	r_0		
1	0	0	0	$\frac{1}{\sqrt{2}}(\|1\rangle - \|0\rangle)$	Random
2	0	0	1	$-\|1\rangle$	$\|1\rangle$
3	0	1	0	$\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$	Random
4	0	1	1	$\|1\rangle$	$\|1\rangle$
5	1	0	0	$\frac{1}{\sqrt{2}}(-\|0\rangle - \|1\rangle)$	Random
6	1	0	1	$-\|0\rangle$	$\|0\rangle$
7	1	1	0	$\frac{1}{\sqrt{2}}(-\|0\rangle - \|1\rangle)$	Random
8	1	1	1	$-\|0\rangle$	$\|0\rangle$

Table 6

Finding the State $|\Psi'\rangle$ and Output z from the measurement when $|\Psi\rangle = -|1\rangle$

Row	**Input**			$\|\Psi'\rangle$	**Measurement (z)**
	r_2	r_1	r_0		
1	0	0	0	$-\|1\rangle$	$\|1\rangle$
2	0	0	1	$\frac{1}{\sqrt{2}}(\|1\rangle - \|0\rangle)$	Random
3	0	1	0	$-\|0\rangle$	$\|0\rangle$
4	0	1	1	$\frac{1}{\sqrt{2}}(-\|0\rangle - \|1\rangle)$	Random
5	1	0	0	$\|1\rangle$	$\|1\rangle$
6	1	0	1	$\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$	Random
7	1	1	0	$\|0\rangle$	$\|0\rangle$
8	1	1	1	$\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$	Random

Table 7

Finding the State $|\Psi'\rangle$ and Output z from the measurement when

$$|\varnothing\rangle = \frac{1}{\sqrt{2}}(-|1\rangle - |0\rangle)$$

Row	Input			$\|\Psi'\rangle$	Measurement (z)
	r_2	r_1	r_0		
1	0	0	0	$\frac{1}{\sqrt{2}}(-\|0\rangle - \|1\rangle)$	Random
2	0	0	1	$-\|0\rangle$	$\|0\rangle$
3	0	1	0	$\frac{1}{\sqrt{2}}(-\|0\rangle - \|1\rangle)$	Random
4	0	1	1	$-\|0\rangle$	$\|0\rangle$
5	1	0	0	$\frac{1}{\sqrt{2}}(\|1\rangle - \|0\rangle)$	Random
6	1	0	1	$-\|1\rangle$	$\|1\rangle$
7	1	1	0	$\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$	Random
8	1	1	1	$\|1\rangle$	$\|1\rangle$

3) Although the result from the measurement differs from the random bit supplied by the sender in certain rows of each case, a receiver will identify this event by comparing their control parameters with the case chosen by the sender whenever $|\Psi'\rangle$ is a pure state.

4) Due to four superposition states and two pure states that are distinct from a random bit, the probability that eavesdroppers will choose the incorrect basis is 0.75, which is more than BB-84. In fact, this is the method's primary contribution.

Table 8

The Example of Process to exchange the secret key by using the Proposed Method

6 / 5			Qubit						
			4	**3**	**2**	**1**	**0**		
Alice	**Sending bit**		1	1	1	0	1	1	0
	Random basis (Control parameters)	$\mathbf{c}_1$	0	1	0	1	1	0	0
		$\mathbf{c}_2$	0	0	0	1	1	0	1
		$\mathbf{c}_3$	0	0	1	0	1	0	0
	Qubit from Sender ($\|\emptyset\rangle$)		$\|1\rangle$	$\frac{1}{\sqrt{2}}(\|0\rangle-\|1\rangle)$	$-\|1\rangle$	$\frac{1}{\sqrt{2}}(\|0\rangle+\|1\rangle)$	$\frac{1}{\sqrt{2}}(-\|0\rangle-\|1\rangle)$	$\|1\rangle$	$\|1\rangle$
Bob	**Random measuring basis** (Control parameters)	$\mathbf{r}_0$	0	1	1	0	1	0	0
		$\mathbf{r}_1$	0	0	1	1	0	1	1
		$\mathbf{r}_2$	0	1	0	0	0	0	0
	Qubit output ($\|\emptyset'\rangle$)		$\|1\rangle$	$\|0\rangle$	$\frac{1}{\sqrt{2}}(-\|0\rangle-\|1\rangle)$	$\frac{1}{\sqrt{2}}(\|0\rangle+\|1\rangle)$	$-\|0\rangle$	$\|0\rangle$	$\|0\rangle$
	Measurement		1	0	Random	Random	0	0	0
The Secret Key			1	1	-	-	1	1	0

Example Exchanging the secret key by using the proposed method

Sol: From Table 8, the following reason may be said about the outcome of each qubit:

Qubit 0 (Bob receives a bit '0' from the measurement): after exchanging the control parameters, Bob will determine that Alice has chosen either case 5 or case 6 ($c_3 = 0$, $c_2 = 1$, $c_1 = 0$). However, Bob can verify with high confidence that Alice chose case 5 in which the random bit is '0' based on the result of the measurement. Bob will therefore recognize that a bit '0' is selected in this position.

Qubit 1 (Bob receives a bit '0' from the measurement): after exchanging the control parameters, Bob will determine that Alice has chosen either case 1 or case 2 ($c_3 = 0$, $c_2 = 0$, $c_1 = 0$). However, Bob can establish with high confidence that Alice chooses case 2 in which the random bit is '1' due to the measurement result.

Qubit 2 (Bob receives a bit '0' from the measurement): after exchanging the control parameters, Bob will know that Alice has selected either case 15 or case 16 ($c_3 = 1$, $c_2 = 1$, $c_1 = 1$). Due to the result of the measurement, Bob can confirm with high confidence that Alice chose case 16 and that the random bit is '1'. Therefore, Bob will recognize that a bit '1' is selected for this place.

Qubit 3: After exchanging the control parameters, Bob will recognize that Alice has chosen either case 7 or case 8 ($c_3 = 0$, $c_2 = 1$, $c_1 = 1$). In this position, however, Bob picks the control parameters $r_2 = 0$, $r_1 = 1$, and $r_0 = 0$ so that $|\Psi'\rangle$ is always a superposition state. Therefore, a bit is eliminated from this position.

Qubit 4: Following the exchange of control parameters, Bob will know that Alice has selected either case 9 or case 10 ($c_3 = 1$, $c_2 = 0$, $c_1 = 0$). In this position, however, Bob picks the control parameters $r_2 = 0$, $r_1 = 1$, and $r_0 = 1$ such that $|\Psi'\rangle$ is always in a superposition state. Therefore, a bit is erased from this position.

Qubit 5 (Bob receives a bit '0' from the measurement): after exchanging the control parameters, Bob will determine that Alice has chosen either case 3 or case 4 ($c_3 = 0$, $c_2 = 0$, $c_1 = 1$). Due to the result of the measurement, Bob can validate with high confidence that Alice chose case 4 and that the

random bit is '1'. Therefore, Bob will recognize that a bit '1' is selected for this place.

Qubit 6 (Bob receives a bit '1' from the measurement): after exchanging the control parameters, Bob will determine that Alice has chosen either case 1 or case 2 ($c_3 = 0$, $c_2 = 0$, $c_1 = 0$). However, Bob can determine with high confidence that Alice chooses case 2 in which the random bit is '1' due to the measurement result. Therefore, Bob will recognize that a bit '1' is selected for this position.

Therefore, the secret key is "11110".

Listed below is the algorithm for the Proposed method:

Algorithm: The Proposed Method (Consider 1 qubit)
Output: a part of secret key (1 qubit)
Sender Side:

1. Selecting a random bit, c_0, and the basis, c_1, c_2 and c_3
2. Generating the state $|\Psi\rangle$
3. Transferring the state $|\Psi\rangle$ to a receiver

Receiver Side:

1. Getting the state $|\Psi\rangle$ from a sender
2. Selecting the basis, r_0, r_1 and r_2
3. Finding the state $|\Psi'\rangle$
4. Measuring the state $|\Psi'\rangle$ to get the pure state (z)

Exchanging the information via classical channel:

1. IF a sender chooses $c_1 = 0$ then
2. IF a receiver chooses the parameters in one of odd rows in Table 1 to Table 7
3. This state is selected as a part of a secret key
4. Else
5. This state is eliminated
6. EndIF
7. Else
8. IF a receiver chooses the parameters in one of even rows in Table 1 to Table 7
9. This state is selected as a part of a secret key
10. Else

11. This state is eliminated
12. EndIF
13. EndIF

4. Security Analysis

This section will assess the security of the proposed method. For nearly all QKD methods, the probability that eavesdroppers can estimate the basis creating the state that is similar to the input state generated by the sender and is not a superposition state is 0.5. However, this section demonstrates that the risk that Eve will guess the incorrect basis when the proposed method is chosen for implementation is increased. There are three ways to examine the event.

Case 1 (Eve guesses the basis yielding the correct state): based on the information in Tables 1 through Table 7, the probability that Eve will guess the basis that generates a state identical to the one given by Alice and that is not a superposition is 0.25. In fact, this probability is less than the analyzed result from the algorithms in the related works section.

Case 2: (Eve guesses the wrong basis for the incorrect state, which is a pure state): assume Alice wishes to transmit the state $|0\rangle$ with the basis generated from the following parameters: $c_1 = 0$, $c_2 = 0$ and $c_3 = 0$, to Bob, then $|\varnothing\rangle = |0\rangle$. However, Eve can capture $|\Psi\rangle$ in the middle before Bob receives this state. She guesses the basis with the following parameters: $r_0 = 0$, $r_1 = 1$ and $r_2 = 0$, then she will get the state $|1\rangle$ which is wrong, see in Table 1. Therefore, Eve will send Bob this state. After Bob receives the state from Eve, he chooses the following parameters: $r_0 = 0$, $r_1 = 0$ and $r_2 = 0$. In fact, Bob will get the state $|1\rangle$ from the measurement. Therefore, it implies that Alice and Bob may verify that Eve has interfered with this qubit by exchanging their bases and comparing the random bit at this position. In addition, this event's probability is 0.25.

Case 3 (Eve guesses the basis, resulting in a superposition state): this event is comparable to BB84, in which the likelihood of obtaining the incorrect state following the measurement is at its maximum (0.5). Then, the probability of getting the erroneous state from the measurement is 0.75. Therefore, it means that it is extremely difficult to capture the state in the middle of a conversation compared to other QKD protocol techniques.

In fact, if there is no eavesdropper to trap the information, Bob has to guess the basis that generates the correct state before the measurement. There are three distinct cases as follows:

Case 1 (Bob guesses the basis creating the correct state): based on the information in Tables 1 through Table 7, the probability that Bob will anticipate the basis that generates a state identical to that obtained by Alice and it is not a superposition is 0.25.

Case 2 (Bob predicts the basis causing the incorrect state): based on the data presented in Tables 1 through Table 7, the probability that Bob will anticipate the basis that the state is similar to the state generated by Alice and it is not a superposition is 0.25. However, by flipping the state, Bob can forecast the correct state.

Case 3 (Bob guesses the basis, resulting in a superposition state): this event is analogous to BB84, in which the probability of obtaining the incorrect state following the measurement is at its highest (0.5).

Therefore, it implies that the probability to find the correct state is 0.5.

Table 9

Comparison of the probability of obtaining the correct state versus the incorrect state

Algorithm (QKD)	Probability to Find the same state with Sender for each qubit (Before Measurement)		The maximum Probability for Eavesdropper to get the error State
	Receiver	Eavesdropper	
BB84	0.5	0.5	0.5
B92	0.5	0.5	0.5
E91	0.5	0.5	0.5
SARG04	0.5	0.5	0.5
The Proposed Method	0.5	**0.25**	**0.75**

The information in Table 9 compares the probability of obtaining the correct state vs the incorrect state. The probability for eavesdroppers to determine the correct state using the proposed method is the lowest; the

probability is only 0.25. Therefore, the benefit of the suggested method is the ease with which eavesdroppers may be verified.

5. Conclusion

In this paper, the improvement method based on QKD is proposed to increase the security to avoid attacking by eavesdroppers. This method is modified from BB84. The key idea is to increase the number of quantum gates on both the sender and receiver sides to enhance the photon's direction. With more directions, it is more difficult for eavesdroppers to guess the basis to generate the correct state. After considering all potential scenarios, it is determined that the probability of an eavesdropper obtaining an incorrect quantum state is 0.75.

References

[1] D. Coppersmith, "Cryptography", *IBM Journal of Research and Development*, vol. 31, pp. 244-248 (1987).

[2] W. Diffie and M.E. Hellman, "New directions in cryptography", *IEEE Trans. Inf. Theory*, vol. 22, pp. 644 – 654 (1976).

[3] R.L. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems", *Commun. ACM*, vol. 21, pp. 120 – 126 (1978).

[4] R. Imam, Q. M. Areeb, A. Alturki and F. Anwer, "Systematic and Critical Review of RSA Based Public Key Cryptographic Schemes: Past and Present Status", *IEEE Access*, vol. 9, pp. 155949-155976 (2021).

[5] K. Omar and S. László, "Sufficient conditions for factoring a class of large integers", *Journal of Interdisciplinary Mathematics*, vol. 13, pp. 95 – 103 (2010).

[6] K. Omar, "Algorithm for factoring some RSA and Rabin moduli", *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 11, pp. 537 – 543 (2008).

[7] J.M. Pollard, "Monte Carlo methods for index computation (mod p)", *J. Math. Comput*, vol. 32, pp. 918 – 924 (1974).

[8] K. Somsuk, "The improvement of initial value closer to the target for Fermat's factorization algorithm", *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 21(7 – 8), pp. 1573 – 1580 (2018).

[9] K. Somsuk, "The Improvement of Elliptic Curve Factorization Method to Recover RSA's Prime Factors", *Symmetry*, vol. 13, pp. 1 – 15 (2021).

[10] K. Somsuk, "Efficient Variant of Pollard's p – 1 for the Case That All Prime Factors of the p – 1 in B-Smooth", *Symmetry*, vol. 14, pp. 1 – 17 (2022).

[11] P.W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring", In Proceedings of Annual Symposium on Foundations of Computer Science, Santa Fe, NM, USA, 20–22 November 1994; pp. 124–134.

[12] A.A. Abushgra, "Variations of QKD Protocols Based on Conventional System Measurements: A Literature Review", *Cryptography,* vol. 12, pp. 1 – 25 (2022).

[13] E. Mohamed, A. Mostafa and A. Abdelmalek, "Quantum Key Distribution Protocols: A Survey", *International Journal of Universal Computer Sciences*, vol. 1-2010, pp. 59 – 67 (2010).

[14] M. Kalra and R.C. Poonia, "Design a new protocol for quantum key distribution", *Journal of Information and Optimization Sciences*, vol. 38-6, pp. 1047-1054 (2017).

[15] A. Kumar, P. Dadheech, V. Singh, R.C. Poonia and L. Raja, "An improved quantum key distribution protocol for verification", *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 22(4), pp. 491-498 (2019).

[16] A. Kumar, P. Dadheech, V. Singh, L. Raja and R.C. Poonia, "An enhanced quantum key distribution protocol for security authentication", *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 22(4), pp. 499-507 (2019).

[17] P. F. Richard, "Simulating Physics with Computers", *International Journal of Theoretical Physics*, vol. 21, pp. 467 – 488 (1982).

[18] D. Copsey, M. Oskin, F. Impens, T. Metodiev, A. Cross, F.T. Chong, L.L. Chuang and J. Kubiatowicz, "Toward a scalable, silicon-based quantum computing architecture", *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 9, pp. 1552-1569 (2003).

[19] C.H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing", In Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, pp. 175-179 (10-12 December 1984).

[20] A. Cheng, W. Peng and T. Gui, "A variant of BB84 Protocol based on quantum phase", in Proceedings of 2013 International Conference on Information and Network Security (ICINS 2013), 2013, Beijing, pp. 1-5 (22-24 November 2013).

[21] L. Dan, P. Chang-xing, Q. Dong-xiao, H. Bao-bin, and Z. Nan, "A new attack strategy for BB84 protocol based on, Breidbart basis", In Proceedings of 2009 Fourth International Conference on Communications and Networking in China, China, pp. 1-3 (26-28 August 2009).

[22] C.H. Bennett, "Quantum cryptography using any two nonorthogonal states", *Phys. Rev. Lett*., vol. 68, pp. 3121-3124 (1992).

[23] A.K. Ekert, "Quantum cryptography based on Bell's theorem", *Phys. Rev. Lett*. vol. 67, pp. 661 - 663 (1991).

[24] V. Scarani, A. Acin, G. Ribordy and N. Gisin, "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations", *Phys. Rev. Lett*., vol. 92, pp. 057901 (2004).

[25] F.F. Chi-Hang, T. Kiyoshi and L. Hoi-Kwong, "Performance of two quantum-key-distribution protocols", *Physical Review A*, vol. 73, pp. 1 - 9 (2006).

[26] N. Gisin, G. Ribordy, H. Zbinden, D. Stucki, N. Brunner and V. Scarani, "Towards practical and fast quantum cryptography", arXiv2004, pp. 1-7.

[27] D. Stucki, N. Brunner, N. Gisin, V. Scarani and H. Zbinden, "Fast and simple one-way quantum key distribution", *Appl. Phys. Lett*., vol. 87, pp. 194108 (2005).

Received August, 2022
Revised November, 2022