Journal of Quantum Information Science, 2015, 5, 33-40
Published Online June 2015 in SciRes. http://www.scirp.org/journal/jqis
http://dx.doi.org/10.4236/jqis.2015.52005

Six-State Symmetric Quantum Key Distribution Protocol

Makhamisa Senekane[1], Mhlambululi Mafu[1,2], Francesco Petruccione[1,3]

[1]Centre for Quantum Technology, School of Chemistry and Physics, University of KwaZulu-Natal, Durban, South Africa
[2]Department of Physics and Astronomy, Botswana International University of Science and Technology, Palapye, Botswana
[3]National Institute for Theoretical Physics (NITheP), University of KwaZulu-Natal, Durban, South Africa
Email: makhamisa12@gmail.com, mhlambululi.mafu@gmail.com, petruccione@ukzn.ac.za

Received 15 March 2015; accepted 20 May 2015; published 28 May 2015

Abstract

We propose and demonstrate an optical implementation of a quantum key distribution protocol, which uses three-non-orthogonal states and six states in total. The proposed scheme improves the protocol that is proposed by Phoenix, Barnett and Chefles [J. Mod. Opt. 47, 507 (2000)]. An additional feature, which we introduce in our scheme, is that we add another detection set; where each detection set has three non-orthogonal states. The inclusion of an additional detection set leads to improved symmetry, increased eavesdropper detection and higher security margin for our protocol.

Keywords

Quantum Key Distribution, QKD, Symmetric, Protocol, Six-State, Quantum, PBC00, Optical Implementation

1. Introduction

Quantum key distribution (QKD) is a cryptographic protocol which allows two communicating parties, conventionally called Alice and Bob, to distribute a secret key in such a way that the presence of an eavesdropper, Eve could be revealed [1]. QKD makes use of quantum mechanical concepts such as the Heisenberg uncertainty principle and the no-cloning theorem in order to ensure that Eve cannot gain non-negligible amount of information without being detected, even if her computational power is unlimited [2]. Since the proposal of the BB84

How to cite this paper: Senekane, M., Mafu, M. and Petruccione, F. (2015) Six-State Symmetric Quantum Key Distribution Protocol. *Journal of Quantum Information Science*, **5**, 33-40. http://dx.doi.org/10.4236/jqis.2015.52005

protocol by Bennett and Brassard in 1984, both theorists and experimentalist have invented various protocols due to various security needs and applications. For example, in 1991, Ekert [3] extended the idea of the BB84 protocol by introducing quantum entanglement and the violation of Bell's theorem [1]. Several variations of these protocols include: Bennett 1992 (B92) [4], six states [5], the Scarani Acn Ribordy Gisin 2004 (SARG04) [6], the differential-phase shift (DPS) [7], the coherent-one-way (COW) [8] and the Phoenix Barnett and Chefles 2000 (PBC00) protocol [9]. The PBC00 protocol is based on the B92 protocol, with the main difference between the two beings that the latter uses two states whilst the former uses three states. Consequently, the PBC00 protocol is more symmetrical (in the sense that either Alice or Bob, but not both, can declare unused observables) and shows lower qubit losses than the B92 protocol. Our proposed scheme improves the PBC00 protocol by making use of additional detection set which has three non-orthogonal states. Moreover, the additional detection states allow increased possibility for eavesdropper detection. As a result, this greatly improves the security of our protocol.

2. Operation of Our Protocol

In our scheme, Alice uses one of the three mutually non-orthogonal states in one set to encode her bit of information, and on the receiving side, Bob uses one of the three mutually non-orthogonal states of the other set to make measurements. The protocol is realized through the following steps, as shown in **Table 1**:

1) Alice randomly and with equal probability prepares and sends quantum signals using any of the two detection sets. Detection set0 is made up of the following mutually non-orthogonal states: $|A\rangle = |0\rangle$, $|B\rangle = \frac{1}{2}|0\rangle - \frac{\sqrt{3}}{2}|1\rangle$ and $|C\rangle = -\frac{1}{2}|0\rangle - \frac{\sqrt{3}}{2}|1\rangle$, while detection set$_1$ is made up of these states: $|A'\rangle = |1\rangle$, $|B'\rangle = \frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle$ and $|C'\rangle = \frac{\sqrt{3}}{2}|0\rangle - \frac{1}{2}|1\rangle$.

2) Bob performs a positive operator valued measurement (POVM) on each received signal, using any of the two detector sets. He then announces to Alice which detection set he used. They discard signals corresponding to time slots where they used similar detection sets for both preparation and measurement, and keep the rest. This is shown as the first result in the table.

3) On the remaining measured signals, Bob announces the time slots where he received no detections at all. Again, they discard the signals corresponding to these time slots and keep the rest.

4) Alice then announces one of the states she did not send. After this, Bob would then know what state Alice sent, and the signals corresponding to such time slots would be used to construct the secret key.

Table 1. An illustration of exchange of qubits between Alice and Bob showing some various possibilities and the result of the inferred bits.

Time slot	1	2	3	4	5	6	7	8	9	10
Alice prepares	$\|A'\rangle$	$\|A\rangle$	$\|B'\rangle$	$\|C\rangle$	$\|A'\rangle$	$\|C'\rangle$	$\|B\rangle$	$\|A\rangle$	$\|A\rangle$	$\|C'\rangle$
Bob detection set choice	0	1	1	1	0	1	1	0	1	0
Result	1	1	0	1	1	0	1	0	1	1
Bob measures	M_B	M_B		$M_{C'}$	M_B		$M_{A'}$		$M_{B'}$	M_A
Result	1	1		0	1		1		1	1
Alice says not in	$\|C'\rangle$	$\|C\rangle$			$\|B'\rangle$		$\|C\rangle$		$\|C\rangle$	$\|B'\rangle$
Bob says	√	√			×		√		√	√
Sequence	$A'C'$	AC					BC		AC	$C'B'$
Inferred bit	1	1					0		1	1

Consider the states of detection set$_0$ to be $|A\rangle = |0\rangle$, $|B\rangle = \frac{1}{2}|0\rangle - \frac{\sqrt{3}}{2}|1\rangle$ and $|C\rangle = \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$, while detection set$_1$, which has a set of states orthogonal to those in detection set$_0$, has the states: $|A'\rangle = |1\rangle$, $|B'\rangle = \frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle$ and $|C'\rangle = \frac{\sqrt{3}}{2}|0\rangle - \frac{1}{2}|1\rangle$.

In order to assign bit values shown in **Table 1**, the following procedure is followed. The signals that have not been eliminated are used for this protocol, and this is shown by the first result in the table. From this, Alice and Bob will know which state was sent and which state she announces that she did not send. Detection set$_0$ is assigned the basis "0" and detection set$_1$ is assigned basis state "1". The major additional feature, which happens in our protocol, occurs when Alice sends signals in a particular detection set and Bob uses the same detection set to make measurements. During this time slot, they discard their results. This happens in time slots 3, 6 and 8. In time slot 1, Alice prepares the state $|A'\rangle$ which in fact corresponds to basis in the detection set$_1$, Bob uses detection set$_0$ to make the measurements, since they use different detection sets, they use signals from this time slot and they record "1" (yes). Bob then performs some measurements on the signals, which he received. Since Alice has announced the result as not a $|C'\rangle$ (this is two hops clockwise from $|A'\rangle$), so they record a "1". The sequence becomes $A'C'$ and then the inferred bit is "1". If the state that Alice announces is one hop away in a clockwise direction they record a "0" as in time slot 3. Moreover, the bit inferred will also be "0".

3. Optimum Measurements

In this section we begin by describing some of the most important aspects of information, *i.e.*, measurement of information. Information can be measured according to its degree of uncertainty, *i.e.*, if an event is likely then one gains little information in learning that it finally occurred and the converse is true. This brings us to the concept of entropy [10], specifically the Shannon entropy. The Shannon entropy is used to quantify the expected value of information contained in a message. It is defined as

$$H(X) = -\sum_i P_X(i) \log P_X(i) \tag{1}$$

where X is a discrete random variable. One can also describe the Shannon mutual information of two events X and Y. The Shannon mutual information gives the amount of information that one can obtain from the bitstring shared between Alice (X) and Bob (Y). It is defined in terms of conditional probability $P(j|i)$ as:

$$I(X:Y) = \sum_{ij} P_{XY}(i,j) \log \frac{P_{XY}(i,j)}{P_X(i) P_Y(j)} \tag{2}$$

where $P_{XY}(i,j)$ is the joint probability, and $P_X(i)$ and $P_Y(j)$ are the marginal probabilities of the input and output letters x_i and y_j, respectively. In the context of QKD, this can be interpreted as the amount of information that one (Eve) additionally obtains when considering both Alice and Bob's source, and not only Alice's source *X*. The eavesdropper can use any strategy in order to obtain any information shared between Alice and Bob. For example, Eve can obtain as much information as possible from the long strings by maximizing the Shannon mutual information. On the other hand, if Eve wants to obtain as much information as possible from single measurements then she has to maximize the discrimination probability. The probability of correctly discriminating between states is given as

$$P_d = \sum_j \chi_j P(j,j) \tag{3}$$

where χ_j is the apriori probability of the state $|j\rangle$ and $P(i,j)$ refers to the probability that the state $|j\rangle$ is sent and that the measurement performed by Eve shows the outcome j. In the case of six apriori equal likely symmetric states, the discrimination probability is expressed as

$$P_d^{\max} = \frac{5}{6}. \tag{4}$$

By introducing an extra detection set, we obtain a discrimination probability which is higher than that of the original scheme (where $P_d^{\max} = 2/3$). This means that the proposed protocol makes it difficult for Eve to discriminate between the states sent by Alice to Bob. The probability that the state is incorrectly detected as one of

the other five states is 1/30. The optimum measurement has six elements, which are defined as

$$\hat{E}_j = \frac{5}{6}|j\rangle\langle j|, \quad (j = A, B, C, A', B', C') \tag{5}$$

Since these elements are positive semi-definite and form an identity, they are positive operator-valued measures (POVMs). The maximum value of the mutual information can be achieved by a POVM with six elements described by

$$\hat{E}_j = \frac{5}{6}|\bar{j}\rangle\langle\bar{j}|, \quad (j = A, B, C, A', B', C') \tag{6}$$

which implies that the system is not in one of the signal states. The signal states are the ones that carry the necessary information from which the secret key would be extracted.

4. Eavesdropper Detection

Alice and Bob can detect the presence of an eavesdropper during the classical communication. This is achieved when they realize that the bits sent by Alice and measured by Bob are different. Let's consider the case where Alice sends the state $|A\rangle$. When Eve performs optimal state discrimination measurement, she will obtain the measurement results A, B, C, A', B', C' with probabilities 5/6, 1/30, 1/30, 1/30, 1/30 and 1/30, respectively.

If Alice sends the signal state $|A\rangle$, the average state which Bob receives is then defined as

$$\begin{aligned}\rho_A &= \frac{5}{6}|A\rangle\langle A| + \frac{1}{30}|B\rangle\langle B| + \frac{1}{30}|C\rangle\langle C| + \frac{1}{30}|A'\rangle\langle A'| + \frac{1}{30}|B'\rangle\langle B'| + \frac{1}{30}|C'\rangle\langle C'| \\ &= \frac{4}{5}|A\rangle\langle A| + \frac{1}{25}.\end{aligned} \tag{7}$$

We have simplified the above equation by applying the fact that

$$|A\rangle\langle A| + |B\rangle\langle B| + |C\rangle\langle C| + |A'\rangle\langle A'| + |B'\rangle\langle B'| + |C'\rangle\langle C'| = \frac{6}{5}\hat{\mathcal{I}} \tag{8}$$

By performing optimal mutual information measurement, it follows that Eve will obtain the results of $\frac{1}{5}|\bar{B}\rangle\langle\bar{B}|$, $\frac{1}{5}|\bar{C}\rangle\langle\bar{C}|$, $\frac{1}{5}|\bar{A}'\rangle\langle\bar{A}'|$, $\frac{1}{5}|\bar{B}'\rangle\langle\bar{B}'|$, $\frac{1}{5}|\bar{C}'\rangle\langle\bar{C}'|$, each with probability 1/5. Then a density matrix that describes the average state received by Bob is written as

$$\begin{aligned}\bar{\rho}_A &= \frac{1}{5}|\bar{B}\rangle\langle\bar{B}| + \frac{1}{5}|\bar{C}\rangle\langle\bar{C}| + \frac{1}{5}|\bar{A}'\rangle\langle\bar{A}'| + \frac{1}{5}|\bar{B}'\rangle\langle\bar{B}'| + \frac{1}{5}|\bar{C}'\rangle\langle\bar{C}'| \\ &= \frac{6}{25}\mathcal{I} - \frac{1}{5}|\bar{A}\rangle\langle\bar{A}| \\ &= \frac{4}{5}|A\rangle\langle A| + \frac{19}{25},\end{aligned} \tag{9}$$

that is the state with a similar form as that obtained for the maximum state-discrimination measurement.

For detection set$_0$, the protocol will give a correct key bit if Bob measures $P_{\bar{B}}$, and $P_{\bar{C}}$ and gets the result 1 and if Alice reveals that she didn't send C or B respectively. Conversely, for detection set$_1$, the protocol will give a correct key bit if Bob measures $P_{\bar{B}'}$, and $P_{\bar{C}'}$ and gets the result 1 and if Alice reveals that she didn't send C' or B' respectively. The probability for this to happen is

$$\begin{aligned}P_C &= \frac{1}{6}\frac{1}{5}\mathrm{Tr}\left(P_{\bar{B}}\rho_A + P_{\bar{C}}\rho_A + P_{\bar{A}'}\rho_A + P_{\bar{B}'}\rho_A + P_{\bar{C}'}\rho_A\right) \\ &= \frac{1}{6}\left(\frac{1}{25} + \frac{1}{5}\left|\langle\bar{B}|A\rangle\right|^2 + \frac{1}{5}\left|\langle\bar{C}|A\rangle\right|^2 + \frac{1}{5}\left|\langle\bar{A}'|A\rangle\right|^2 + \frac{1}{5}\left|\langle\bar{B}'|A\rangle\right|^2 + \frac{1}{5}\left|\langle\bar{C}'|A\rangle\right|^2\right) \\ &= \frac{11}{150},\end{aligned} \tag{10}$$

where 1/6 is the probability for Bob to have chosen the given measurement and 1/5 is the probability that arises from Alice's random choice of announcing which state she did not send. This probability is less than the one proposed in [9]. However, our scheme makes it easier for the presence of Eve to be detected. In detection set_0, if Alice prepares state $|A\rangle$, the probability that Eve's activity will produce an incorrect key bit is simply the probability that Bob chooses to measure $P_{\bar{A}}$ and obtains a non-zero number. The opposite also holds for detection set_1.

$$P_M = \frac{1}{6}\mathrm{Tr}\left(P_{\bar{A}}\rho_A\right) = \frac{1}{6}\frac{1}{25} = \frac{1}{150} \tag{11}$$

As compared to the previous scheme, we realize that in our protocol, there is a higher chance that Eve will be detected. If Eve performs an intercept and resend attack, she will introduce errors in Alice's and Bob's shared key with the probability $\left((1/6)+(1/6)+11/150\right) = 61/150$.

Ultimately the average state received by Bob will be

$$\begin{aligned}\rho'_A &= \frac{4}{5}|A\rangle\langle A| + \frac{1}{25}|B\rangle\langle B| + \frac{1}{25}|C\rangle\langle C| + \frac{1}{25}|A'\rangle\langle A'| + \frac{1}{25}|B'\rangle\langle B'| + \frac{1}{25}|C'\rangle\langle C'| \\ &= \frac{6}{125}\mathcal{I} + \frac{4}{25}|A\rangle\langle A|.\end{aligned} \tag{12}$$

For Bob, the probabilities of correct detection P_C and incorrect detection P_M are given by

$$\begin{aligned}P_C &= \frac{1}{6}\frac{4}{5}\mathrm{Tr}\left(P_{\bar{B}}\rho'_A + P_{\bar{C}}\rho'_A + P_{\bar{A}'}\rho'_A + P_{\bar{B}'}\rho'_A + P_{\bar{C}'}\rho'_A\right) \\ &= \frac{24}{625},\end{aligned} \tag{13}$$

and $P_M = \frac{1}{6}\mathrm{Tr}\left(P_{\bar{A}}\rho'_A\right) = 1/125$, respectively. This shows another improvement of our scheme since the probability that Bob will generate an incorrect key bit is lower than in the original scheme. This means that most of the time Bob will be able to correctly generate the correct bit.

5. Optical Implementation

We provide an optical implementation of this scheme in **Figure 1**. Different trine and anti-trine measurement values for the proposed protocol are depicted in **Table 2**. In each arm three polarising beamsplitters and two half-wave plates are used. On the right had side, the polarising beamsplitters transmit horizontally polarised light and reflect the vertically polarised light. In the left arm, the opposite happens, the vertically polarised light is transmitted and the horizontally polarised one is reflected. In **Table 2**, we show the signal states at different locations. For each set, the input state after the non-polarising beamsplitter at position 2 goes through the polarising beamsplitter. On the right arm, between positions 3 and 4, we have a half-wave plate, which is given by the following unitary operator:

$$U_1^0 = \begin{pmatrix} 1/\sqrt{3} & -\sqrt{2/3} \\ \sqrt{2/3} & 1/\sqrt{3} \end{pmatrix}. \tag{14}$$

In a like manner, on the left arm, between positions 3 and 4, we have a half-wave plate, which is given by the following unitary operator:

$$U_1^1 = \begin{pmatrix} 1/\sqrt{3} & \sqrt{2/3} \\ -\sqrt{2/3} & 1/\sqrt{3} \end{pmatrix}. \tag{15}$$

In both arms, these unitary operators are responsible for producing the states at position 4. On the right arm, the vertically polarised light at position 7, will be detected by D4, while on the left arm at the same position, the horizontally polarised light will be detected by D1. Between positions 8 and 9 of the right arm, the following unitary operator describes the half-wave plate:

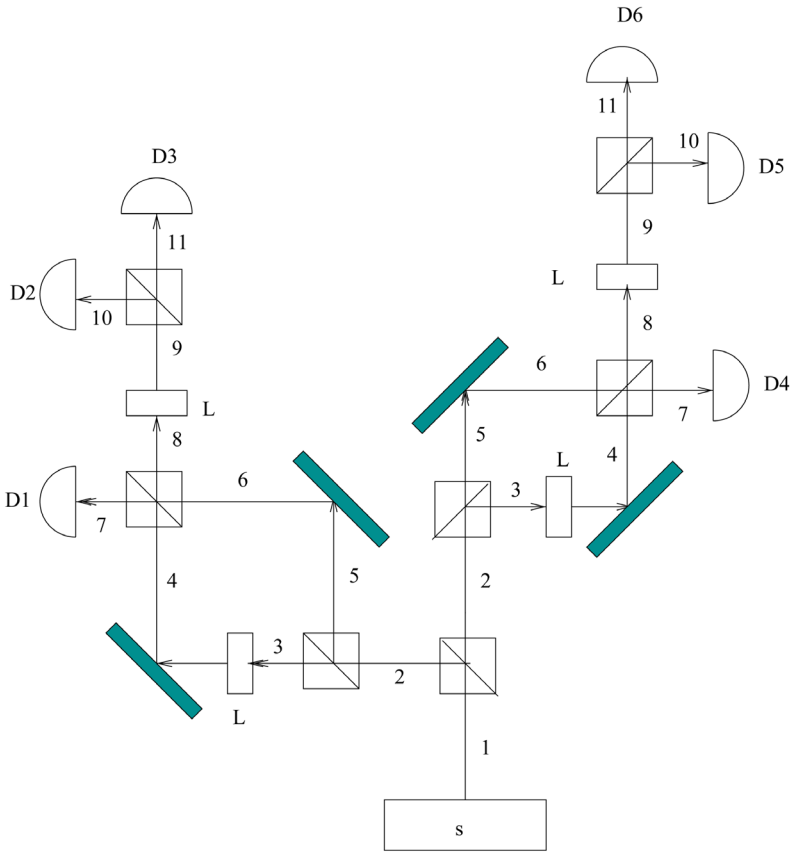

Figure 1. An optical implementation of the proposed six-state QKD protocol. The part S is the signal from Alice, and this signal goes a non-polarising beamsplitter and either goes to the left arm or right arm. We assume the interferometers used in each arm are balanced. The left arm represents the set_0 measurements and the right arm represents the set_1 measurements. From position 2, the polarising beamsplitters are used together with half-wave plates. The signals states for the positions marked are shown in **Table 2** and the single photon detectors are marked D1 - D6.

Table 2. States at each location, as depicted in **Figure 1**.

1	2	3	4	7	8	9	10	11
$\begin{pmatrix}1\\0\end{pmatrix}$	$\begin{pmatrix}1\\0\end{pmatrix}$	$\begin{pmatrix}1\\0\end{pmatrix}$	$\begin{pmatrix}1/\sqrt{3}\\\sqrt{2/3}\end{pmatrix}$	$\begin{pmatrix}0\\\sqrt{2/3}\end{pmatrix}$	$\begin{pmatrix}\sqrt{1/3}\\0\end{pmatrix}$	$\begin{pmatrix}1/\sqrt{6}\\1/\sqrt{6}\end{pmatrix}$	$\begin{pmatrix}0\\1/\sqrt{6}\end{pmatrix}$	$\begin{pmatrix}1/\sqrt{6}\\0\end{pmatrix}$
$\begin{pmatrix}1/2\\-\sqrt{3}/2\end{pmatrix}$	$\begin{pmatrix}1/2\\-\sqrt{3}/2\end{pmatrix}$	$\begin{pmatrix}1/2\\0\end{pmatrix}$	$\begin{pmatrix}1/2\sqrt{3}\\1/\sqrt{6}\end{pmatrix}$	$\begin{pmatrix}0\\1/\sqrt{6}\end{pmatrix}$	$\begin{pmatrix}1/2\sqrt{3}\\-\sqrt{3}/2\end{pmatrix}$	$\begin{pmatrix}\sqrt{2/3}\\-1/\sqrt{6}\end{pmatrix}$	$\begin{pmatrix}0\\-1/\sqrt{6}\end{pmatrix}$	$\begin{pmatrix}\sqrt{2/3}\\0\end{pmatrix}$
$\begin{pmatrix}-1/2\\-\sqrt{3}/2\end{pmatrix}$	$\begin{pmatrix}-1/2\\-\sqrt{3}/2\end{pmatrix}$	$\begin{pmatrix}-1/2\\0\end{pmatrix}$	$\begin{pmatrix}-1/2\sqrt{3}\\-1/\sqrt{6}\end{pmatrix}$	$\begin{pmatrix}0\\-1/\sqrt{6}\end{pmatrix}$	$\begin{pmatrix}-1/2\sqrt{3}\\-\sqrt{3}/2\end{pmatrix}$	$\begin{pmatrix}1/\sqrt{6}\\-\sqrt{2}/3\end{pmatrix}$	$\begin{pmatrix}0\\-\sqrt{2}/3\end{pmatrix}$	$\begin{pmatrix}1/\sqrt{6}\\0\end{pmatrix}$
$\begin{pmatrix}0\\1\end{pmatrix}$	$\begin{pmatrix}0\\1\end{pmatrix}$	$\begin{pmatrix}0\\1\end{pmatrix}$	$\begin{pmatrix}\sqrt{2/3}\\1/\sqrt{3}\end{pmatrix}$	$\begin{pmatrix}\sqrt{2/3}\\0\end{pmatrix}$	$\begin{pmatrix}0\\1/\sqrt{3}\end{pmatrix}$	$\begin{pmatrix}1/\sqrt{6}\\1/\sqrt{6}\end{pmatrix}$	$\begin{pmatrix}1/\sqrt{6}\\0\end{pmatrix}$	$\begin{pmatrix}0\\1/\sqrt{6}\end{pmatrix}$
$\begin{pmatrix}\sqrt{3}/2\\1/2\end{pmatrix}$	$\begin{pmatrix}\sqrt{3}/2\\1/2\end{pmatrix}$	$\begin{pmatrix}0\\1/2\end{pmatrix}$	$\begin{pmatrix}1/\sqrt{6}\\1/2\sqrt{3}\end{pmatrix}$	$\begin{pmatrix}1/\sqrt{6}\\0\end{pmatrix}$	$\begin{pmatrix}\sqrt{3}/2\\1/2\sqrt{3}\end{pmatrix}$	$\begin{pmatrix}2/\sqrt{6}\\-1/\sqrt{6}\end{pmatrix}$	$\begin{pmatrix}2/\sqrt{6}\\0\end{pmatrix}$	$\begin{pmatrix}0\\-1/\sqrt{6}\end{pmatrix}$
$\begin{pmatrix}\sqrt{3}/2\\-1/2\end{pmatrix}$	$\begin{pmatrix}\sqrt{3}/2\\-1/2\end{pmatrix}$	$\begin{pmatrix}0\\-1/2\end{pmatrix}$	$\begin{pmatrix}-1/\sqrt{6}\\-1/2\sqrt{3}\end{pmatrix}$	$\begin{pmatrix}-1/\sqrt{6}\\0\end{pmatrix}$	$\begin{pmatrix}\sqrt{3}/2\\-1/2\sqrt{3}\end{pmatrix}$	$\begin{pmatrix}-\sqrt{2}\\-2/\sqrt{6}\end{pmatrix}$	$\begin{pmatrix}-\sqrt{2}\\0\end{pmatrix}$	$\begin{pmatrix}0\\-2/\sqrt{6}\end{pmatrix}$

$$U_2^0 = \begin{pmatrix} 1/\sqrt{2} & -1/\sqrt{2} \\ 1/\sqrt{2} & 1/\sqrt{2} \end{pmatrix}, \tag{16}$$

while on the left arm the unitary operator is given as

$$U_2^1 = \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ -1/\sqrt{2} & 1/\sqrt{2} \end{pmatrix}. \tag{17}$$

On the right arm, the vertically polarised light at position 10, will be detected by D5, while on the left arm at the same position, the horizontally polarised light will be detected by D2. The horizontally polarised light at position 11 for the right arm will be detected by D6 while the vertically polarised light on the left arm at position 11 will be detected by D3.

It is worth noting that in order to switch from set_0 to set_1, the following unitary is used:

$$U_{0\text{ to }1} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \tag{18}$$

Conversely, the unitary used for switching from set_1 to set_0 is given as:

$$U_{1\text{ to }0} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{19}$$

Apart from our proposed protocol being more secure, the additional symmetry that exists in our protocol also allows the various security proofs methods to be applied for instance the post-selection technique which was proposed by Renner and Christandl [11] and has recently been applied in [12].

6. Conclusion

In this work, we have demonstrated an optical implementation of a six-state symmetric QKD protocol. Since our protocol uses additional detection set, this improves its symmetry, increases the discrimination probability and thereby improves the detection of Eve. In our proposed scheme, we have also demonstrated that the Bob's probability of generating error-free bitstring is lower than that of the original scheme. This shows that our proposed six-state symmetric QKD protocol is more secure.

Acknowledgements

This work is based on research supported by the South African Research Chair Initiative of the Department of Science and Technology and National Research Foundation.

References

[1] Scarani, V., Bechmann-Pasquinucci, H., Cerf, N., Dušek, M., Lütkenhaus, N. and Peev, M. (2009) The Security of Practical Quantum Key Distribution. *Reviews of Modern Physics*, **81**, 1301-1350. http://dx.doi.org/10.1103/RevModPhys.81.1301

[2] Gisin, N., Ribordy, G., Tittel, W. and Zbinden, H. (2002) Quantum Cryptography. *Reviews of Modern Physics*, **74**, 145. http://dx.doi.org/10.1103/RevModPhys.74.145

[3] Ekert, A. (1991) PRL Milestone. *Physical Review Letters*, **67**, 661-663. http://dx.doi.org/10.1103/PhysRevLett.67.661

[4] Bennett, C.H. (1992) Quantum Cryptography Using Any Two Nonorthogonal States. *Physical Review Letters*, **68**, 3121-3124. http://dx.doi.org/10.1103/PhysRevLett.68.3121

[5] Bru*β*, D. (1998) Optimal Eavesdropping in Quantum Cryptography with Six States. *Physical Review Letters*, **81**, 3018-3021. http://dx.doi.org/10.1103/PhysRevLett.81.3018

[6] Scarani, V., Acn, A., Ribordy, G. and Gisin, N. (2004) Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations. *Physical Review Letters*, **92**, Article ID: 057901. http://dx.doi.org/10.1103/PhysRevLett.92.057901

[7] Inoue, K., Waks, E. and Yamamoto, Y. (2002) Differential Phase Shift Quantum Key Distribution. *Physical Review Letters*, **89**, Article ID: 037902. http://dx.doi.org/10.1103/PhysRevLett.89.037902

[8] Stucki, D., Fasel, S., Gisin, N., Thoma, Y. and Zbinden, H. (2007) Coherent One-Way Quantum Key Distribution. *So-*

ciety of Photo-Optical Instrumentation Engineers (*SPIE*) *Conference Series*, **6583**, 18.

[9] Phoenix, S.J., Barnett, S.M. and Chefles, A. (2000) Three-State Quantum Cryptography. *Journal of Modern Optics*, **47**, 507-516. http://dx.doi.org/10.1080/09500340008244056

[10] Cover, T.M. and Thomas, J. A. (1991) Elements of Information Theory. John Willey, New York. http://dx.doi.org/10.1002/0471200611

[11] Christandl, M., König, R. and Renner, R. (2009) Postselection Technique for Quantum Channels with Applications to Quantum Cryptography. *Physical Review Letters*, **102**, Article ID: 020504. http://dx.doi.org/10.1103/PhysRevLett.102.020504

[12] Mafu, M., Garapo, K. and Petruccione, F. (2014) Finite-Key-Size Security of the Phoenix-Barnett-Chefles 2000 Quantum-Key-Distribution Protocol. *Physical Review A*, **90**, Article ID: 032308. http://dx.doi.org/10.1103/PhysRevA.90.032308