Journal of Modern Optics

ISSN: 0950-0340 (Print) 1362-3044 (Online) Journal homepage: http://www.tandfonline.com/loi/tmop20

Three-state quantum cryptography

Simon J. D. Phoenix , Stephen M. Barnett & Anthony Chefles

To cite this article: Simon J. D. Phoenix , Stephen M. Barnett & Anthony Chefles (2000) Three-state quantum cryptography, Journal of Modern Optics, 47:2-3, 507-516

To link to this article: http://dx.doi.org/10.1080/09500340008244056

Published online: 03 Jul 2009.

JOURNAL OF MODERN OPTICS, 2000, VOL. 47, NO. 2/3, 507–516

Three-state quantum cryptography

SIMON J. D. PHOENIX†, STEPHEN M. BARNETT‡ and ANTHONY CHEFLES‡

† BT Laboratories Martlesham Heath, Ipswich IP5 3RE, UK
‡ Department of Physics and Applied Physics, University of Strathclyde, Glasgow, G4 0NG, UK

(*Received 26 April 1999; revision received 8 July 1999*)

Abstract. We introduce a protocol for quantum key distribution using three mutually non-orthogonal states. The protocol generates key bits most efficiently for three symmetric states. The generalized measurements which minimize the error probability and maximize the mutual information for such a system are known and can be implemented optically. We analyse eavesdropping strategies based on these optimal measurements.

1. Introduction

One of the more exciting techniques to have emerged from quantum physics in recent years is quantum cryptography. More properly called quantum key distribution (QKD) this technique uses the laws of quantum mechanics to allow two users in remote locations to establish a key such that any attempt to intercept the key reveals the attempt at eavesdropping. Current optical fibre based systems can operate at distances up to 50 km over an installed fibre network [1].

The original protocol, known as the BB84 protocol, was invented in 1984 [2] and uses a total of 4 states; 2 states forming the eigenbasis of one observable and the other two being the eigenbasis of the complementary observable. It is not, however, necessary to use a complete eigenbasis to achieve security and secure key distribution can be achieved using just two quantum states, each of the states being an eigenstate of one of two complementary observables [3]. Using more observables allows a greater range of possibilities for eavesdropper detection [4]. In particular, a minimum of 3 observables is required to detect an eavesdropper using those bits that would normally be rejected in any protocol. Previous 'rejected-data' protocols have used 3 sets of eigenbases giving a total of 6 states to achieve security [5–7] although the minimum number of states required is 3 [4].

Three state systems are particularly interesting for quantum cryptography because of the existence of two powerful theorems concerning the optimal measurement strategies on three mutually non-orthogonal symmetric states [8, 9]. These theorems describe the measurement strategies required to achieve a minimum error probability and maximum mutual information and allow us to place rigorous bounds on the capabilities of any eavesdropper.

In this paper we introduce a protocol using 3 mutually non-orthogonal states. The optimum measurement strategies are then discussed and the security of the

Journal of Modern Optics ISSN 0950–0340 print/ISSN 1362–3044 online
http://www.tandf.co.uk/JNLS/mop.htm
http://www.taylorandfrancis.com/JNLS/mop.htm

protocol demonstrated. We describe an optical implementation of these optimum measurement strategies.

2. Protocol

As is customary, our two protagonists wishing to establish a secret key are Alice and Bob. The eavesdropper, Eve, wishes to obtain this key material without detection. The purpose of using quantum states in any QKD protocol is so that measurements performed by Eve can be reliably detected no matter how sophisticated a measurement strategy she adopts. The 3-state quantum cryptography protocol proceeds as follows.

Alice randomly and with equal *a priori* probabilities prepares each qubit in one of three mutually non-orthogonal states $|A\rangle$, $|B\rangle$ and $|C\rangle$. We write the projector onto a state $|k\rangle$ as $\hat{P}_k$ and the complementary projection as $\hat{P}_{\bar{k}}$ such that $\hat{P}_k + \hat{P}_{\bar{k}} = 1$. We shall initially consider communication in the absence of an eavesdropper.

For each received qubit Bob measures at random and with equal *a priori* probability one of the three operators $\hat{P}_{\bar{A}}$, $\hat{P}_{\bar{B}}$ and $\hat{P}_{\bar{C}}$. When the transmission has been completed Alice and Bob publicly confer to establish a key.

Bob informs Alice of those timeslots corresponding to received qubits for which his measurement result was zero. These timeslots are then discarded. For each of the remaining timeslots Alice announces one of the states, chosen at random with equal *a priori* probability, that she *did not* send. For example, if we suppose that she sent $|A\rangle$ for a particular timeslot she would announce either $|B\rangle$ or $|C\rangle$ each with probability 1/2.

Let us further suppose that for this particular timeslot Bob measured $\hat{P}_{\bar{B}}$. As this timeslot has not been discarded Bob would know that either $|A\rangle$ or $|C\rangle$ had been sent by Alice. If Alice announced that she did not send $|C\rangle$, Bob would immediately know that Alice had, in fact sent the state $|A\rangle$. If, however, Alice had announced that she did not send the state $|B\rangle$ Bob would obtain no further useful information. Under these circumstances Bob replies by telling Alice to discard this timeslot. Similar reasoning applies to the other possible combinations of transmitted qubits and measurements.

From the remaining timeslots it is now possible for Alice and Bob to establish a binary string using the following convention. Consider the cyclic arrangement depicted in figure 1 where each state is joined by an arrow pointing in the clockwise direction. We begin with the state transmitted by Alice, which at this stage of the protocol is known to both Alice and Bob. If the state announced as 'not sent' by Alice is only one hop away in a clockwise direction Alice and Bob take this bit value to be '0'. If this state is two hops in a clockwise direction Alice and Bob take the bit value for this timeslot to be '1'. Table 1 shows an example transmission between Alice and Bob. The resulting sequence of bits is Alice and Bob's shared, secret key.

This protocol is symmetric in the sense that either Alice or Bob, but not both, can declare which observable 'was not used'. In Bob's case he simply declares one of the observables, chosen randomly with equal *a priori* probability, that he did not measure. The coding and protocol follows in a similar fashion to that outlined above.

We will consider a more sophisticated eavesdropper strategy shortly but meanwhile let us consider an eavesdropper performing the same kinds of meas-

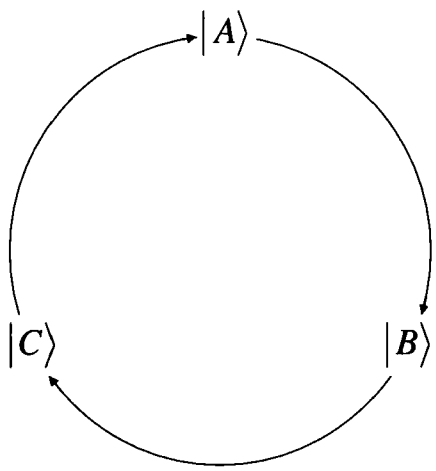

Figure 1. Cyclic convention used to assign values to key bits. For signals that have not been eliminated Alice and Bob know which state Alice sent and which state she announces that she did not send. Beginning with the state Alice sent a '1' is read if the state announced as 'not sent' by Alice is two hops away in a clockwise direction and '0' if this state is only one hop away.

Table 1. An example transmission of qubits between Alice and Bob showing some of the various possibilities and the resulting inferred bits.

Timeslot	1	2	3	4	5	6	7	8	9	10
Alice prepares	$\|A\rangle$	$\|B\rangle$	$\|C\rangle$	$\|C\rangle$	$\|C\rangle$	$\|B\rangle$	$\|A\rangle$	$\|A\rangle$	$\|B\rangle$	$\|A\rangle$
Bob measures	$\hat{P}_{\bar{A}}$	$\hat{P}_{\bar{A}}$	$\hat{P}_{\bar{B}}$	$\hat{P}_{\bar{A}}$	$\hat{P}_{\bar{C}}$	$\hat{P}_{\bar{C}}$	$\hat{P}_{\bar{C}}$	$\hat{P}_{\bar{B}}$	$\hat{P}_{\bar{C}}$	$\hat{P}_{\bar{B}}$
Result	0	1	1	0	0	1	1	0	1	1
Alice says not		$\|C\rangle$	$\|B\rangle$			$\|A\rangle$	$\|B\rangle$		$\|C\rangle$	$\|C\rangle$
Bob says		✓	×			✓	✓		×	✓
Sequence		BC				BA	AB			AC
Inferred bit		0				1	0			1

urements as Bob. Let us suppose again that Alice transmits the state A. It is clear that on the basis of a single measurement of this kind Eve cannot distinguish which state has been sent by Alice. It is therefore inevitable that Eve will introduce errors in her re-transmission. These errors can be detected by Alice and Bob thus revealing the presence of Eve. It is possible, although not described here, to use only the rejected data to detect Eve.

3. Optimum measurements

Two optimum measurement strategies are known for the system of the three symmetric states described above. One minimizes the probability that the state is assigned incorrectly [8, 10] and the other maximizes the mutual information between Alice and the party (Eve) performing the measurement [9]. These measurements are of interest because they have been proven to be optimal, but

also because they are not simple von Neumann measurements but rather fall into the more general class usually described in terms of effects [11] or probability operator measures (POMs) [8]. We will describe a possible optical implementation of the required measurements in section 5 [9, 12].

The measurement strategy which will be most profitable to Eve depends upon the kind of information she wishes to obtain. If she is interested in obtaining as much information as possible from single measurements the quantity she will aim to maximize is the probability P_D of correctly discriminating between the states

$$P_D = \sum_j \chi_j P(j,j), \tag{1}$$

where χ_j is the *a priori* probability of the state $|j\rangle$ and $P(j,j)$ is the probability that the state $|j\rangle$ is sent and that Eve's measurement reveals the result j. If, on the other hand, Eve is interested in extracting as much classical information as possible from long strings of bits she will be more interested in maximizing the Shannon mutual information (2) than minimizing the error probability

$$I(X:Y) = \sum_{i,j} \chi_i P(j|i) \log_2 \frac{P(j|i)}{P_Y(j)}, \tag{2}$$

where $P_Y(j) = \sum_k \chi_k P(j|k)$ is the absolute probability of obtaining the result j and $P(j|k)$ is the probability for obtaining the result j given that the state $|k\rangle$ was prepared. It should be noted that the results j in the mutual information can be more general than assigning the identity of the state and can include statements such as 'the state was not $|A\rangle$'.

The strategy maximizing the discrimination probability P_D (or equivalently the minimization of the error probability $1 - P_D$) has been known for many years [8, 10]. For the three *a priori* equally likely symmetric states, this probability is

$$P_D^{\max} = \tfrac{2}{3}. \tag{3}$$

The probabilities that the state is incorrectly identified as a given one of the other two states is 1/6. The optimum measurement POM has the three elements

$$\hat{E}_j = \tfrac{2}{3}|j\rangle\langle j| \quad (j = A,B,C). \tag{4}$$

That these elements form a POM is a consequence of the facts that they are positive semi-definite operators and form a resolution of the identity:

$$\sum_j \hat{E}_j = \hat{I}. \tag{5}$$

This measurement strategy is a special case of the 'square-root' [13] or 'pretty good' measurement [14].

The strategy which attains the maximum value of the mutual information is described by a POM with the three elements [9]

$$\hat{E}_{\bar{j}} = \tfrac{2}{3}|\bar{j}\rangle\langle\bar{j}| \quad (j = A,B,C) \tag{6}$$

corresponding to the results that the system is *not* in one of the signal states. If, for example, this measurement strategy is applied to a signal state $|A\rangle$ then the probability that the measurement will give the result $\bar{A}$ is zero, but the two remaining possible outcomes will occur with equal probability. This measurement

strategy tells us for certain one of the two states that was not sent, but reveals no further information. The amount of mutual information obtained using this measurement strategy is

$$I_{\max}(X : Y) = (\log_2 3 - 1)\,\text{bits}, \tag{7}$$

which compares with the $(2/3)\log_2(9/8)$ bits obtained using the strategy associated with the maximum state-discrimination probability.

4. Eavesdropper detection

The activity of the eavesdropper is revealed in a public discussion between Alice and Bob following the transmission and measurement of the qubits. During this discussion information about a random selection of the data can be exchanged. The only pertinent things that are unknown to both Alice and Bob is the strategy employed by Eve and the results of her measurements. Eve will carry out a chosen measurement on each qubit and, depending on the outcome of her measurement, transmit a new state to Bob. We begin by considering the simplest case in which Eve does not further modify the state she receives. That is, if she performs a measurement aimed at minimizing her error probability and finds the result B then she retransmits to Bob the state $|B\rangle$. If, however, she performs a measurement aimed at maximizing the mutual information between her and Alice and finds the result $\bar{A}$ she retransmits the state $|\bar{A}\rangle$ to Bob.

Consider the case in which Alice sends the state $|A\rangle$. If Eve performs the optimal state-discrimination measurement then she will get the results A, B and C with probabilities 2/3, 1/6 and 1/6, respectively. It follows that the average state received by Bob will, if Alice sent the signal state $|A\rangle$, have the density matrix

$$\rho_A = \tfrac{2}{3}|A\rangle\langle A| + \tfrac{1}{6}|B\rangle\langle B| + \tfrac{1}{6}|C\rangle\langle C| = \tfrac{1}{2}|A\rangle\langle A| + \tfrac{1}{4}, \tag{8}$$

where we have used the fact that

$$|A\rangle\langle A| + |B\rangle\langle B| + |C\rangle\langle C| = \tfrac{3}{2}\hat{I}. \tag{9}$$

If Eve performs the optimal mutual information measurement then she will get the results $\bar{B}$ and $\bar{C}$, each with probability 1/2. It follows that the average state received by Bob will have the density matrix

$$\tilde{\rho}_A = \tfrac{1}{2}|\bar{B}\rangle\langle\bar{B}| + \tfrac{1}{2}|\bar{C}\rangle\langle\bar{C}| = \tfrac{3}{4}\hat{I} - \tfrac{1}{2}|\bar{A}\rangle\langle\bar{A}| = \tfrac{1}{2}|A\rangle\langle A| + \tfrac{1}{4} = \rho_A, \tag{10}$$

that is, the same state as for the maximum state-discrimination measurement.

We can use ρ_A to calculate the probabilities that any given qubit will lead to a correct (that is matching) key bit (P_C) or an incorrect (that is mismatching key bit) (P_M). Bob chooses to measure $P_{\bar{A}}$, $P_{\bar{B}}$ or $P_{\bar{C}}$ with equal probability of 1/3. The protocol will give a correct key bit if Bob measures $P_{\bar{B}}$ or $P_{\bar{C}}$ and gets the result 1 and if Alice reveals that she did not send C or B, respectively. The probability for this to happen is

$$P_C = \tfrac{1}{3}\tfrac{1}{2}\,\text{Tr}\,(P_{\bar{B}}\rho_A + P_{\bar{C}}\rho_A) = \tfrac{1}{3}(\tfrac{1}{4} + \tfrac{1}{2}|\langle\bar{B}|A\rangle|^2 + \tfrac{1}{2}|\langle\bar{C}|A\rangle|^2) = \tfrac{5}{24}, \tag{11}$$

where the factor of 1/3 is that for Bob to have chosen the given measurement and the factor of 1/2 arises from Alice's random choice of announcing which state she

did not send. 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 gets the answer 1:

$$P_{\mathrm{M}} = \tfrac{1}{3}\mathrm{Tr}\,(P_{\bar{A}}\rho_A) = \tfrac{1}{3}\tfrac{1}{4} = \tfrac{1}{12}. \tag{12}$$

It follows that if Eve adopts an intercept–resend strategy based on either the minimum error probability or maximum mutual information strategies she will induce errors in Alice and Bob's shared key with probability $(1/12)/(1/12 + 5/24) = 2/7$. This figure holds irrespective of whether Eve chooses to maximize her mutual information with Alice or minimize her error probability.

It is easy to show that an Eve who establishes that a given signal state $|A\rangle$ was either not B or not C, does significantly worse if she then chooses randomly to send one of $|A\rangle$ and $|C\rangle$ or $|A\rangle$ and $|B\rangle$, respectively. In this case, the average state received by Bob will be

$$\rho'_A = \tfrac{1}{2}|A\rangle\langle A| + \tfrac{1}{4}|B\rangle\langle B| + \tfrac{1}{4}|C\rangle\langle C| = \tfrac{3}{8}\hat{I} + \tfrac{1}{4}|A\rangle\langle A|. \tag{13}$$

In this case the probabilities that correct and incorrect key bits will be generated in Bob's string are

$$\begin{aligned} P_{\mathrm{C}} &= \tfrac{1}{3}\tfrac{1}{2}\mathrm{Tr}\,(P_{\bar{B}}\rho'_A + P_{\bar{C}}\rho'_A) = \tfrac{3}{16}, \\ P_{\mathrm{M}} &= \tfrac{1}{3}\mathrm{Tr}\,(P_{\bar{A}}\rho'_A) = \tfrac{1}{8}, \end{aligned} \tag{14}$$

so that 2 in 5 of Bob's key bits will now be incorrect.

5. Optical implementation

An optical implementation of the trine measurement which works on polarization-encoded qubits has been devised by Sasaki and co-workers [9, 12]. A similar device has been proposed by Busch for the simultaneous measurement of two incompatible components of spin [15]. Here we present a slightly simplified version of Sasaki and co-worker's proposal. We represent our three polarization states as column vectors in which the first and second entries represent respectively the states of horizontal and vertical polarization:

$$|A\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |B\rangle = \begin{pmatrix} 1/2 \\ -\sqrt{3}/2 \end{pmatrix}, \quad |C\rangle = \begin{pmatrix} -1/2 \\ -\sqrt{3}/2 \end{pmatrix} \tag{15}$$

These states are normalized and clearly have the desired property that the squared moduli of their overlaps is 1/4. The measuring device, which is depicted in figure 2, consists of three polarizing beam-splitters, two half-wave plates and three photodetectors. The polarizing beam-splitters are aligned so as to transmit horizontally polarized light and reflect vertically polarized light. The two half-wave plates act to rotate the state of linear polarization†.

† The need for the second half-wave plate is removed if the following polarizing beam-splitter is rotated through 45° so that it transmits and reflects light with polarizations at 45° to the horizontal. We feel, however, that the it is easier to follow the operation of the device if all three polarizing beam-splitters are aligned in the same way.

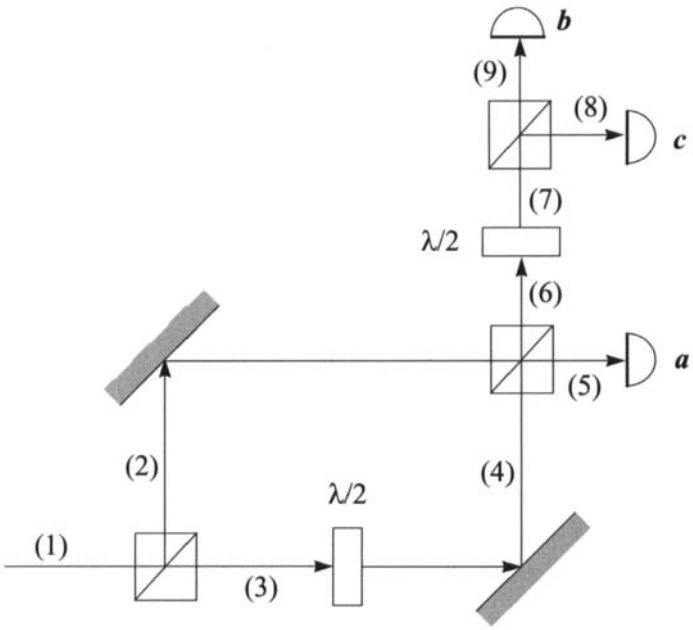

Figure 2. Optical implementation of the trine measurement. Polarizing beamsplitters are used along with half-wave plates. The positions marked are discussed in the text and table 2. Single-photon detectors are placed at *a*, *b* and *c*.

The operation of the trine measurement device is most readily appreciated by considering the state of polarization at nine different positions along the optical paths. These polarization states are presented in table 2 for both the trine and anti-trine measurements. We will assume for simplicity that the optical path lengths in the two arms of the interferometer are equal and will ignore phase factors due to propagation. The input state prepared by Alice and to be measured by Eve is passed into the device at position (1). The first polarizing beam-splitter transmits the horizontally polarized component and reflects the vertically polarized component of the state. In the lower arm, a half-wave plate rotates the polarization of the light through the angle $\cos^{-1}\left(1/\sqrt{3}\right)$. This is equivalent to implementing the action of the unitary operator

$$U_1 = \begin{pmatrix} \frac{1}{\sqrt{3}} & -\sqrt{\frac{2}{3}} \\ \sqrt{\frac{2}{3}} & \frac{1}{\sqrt{3}} \end{pmatrix} \tag{16}$$

on the polarization state at position (3) to produce the state at position (4). The polarizing beam-splitter at the output of the interferometer again transmits horizontally polarized light and reflects vertically polarized light. The light at position (5) is vertically polarized. A detection registered in detector *a* corresponds to the assignment of the input state as $|A\rangle$. The probabilities for this event to occur for each of the three possible input states can be read off as the squared moduli of

Table 2. The amplitudes for the various states at each of the locations labelled (1)–(9) in figure 2. The upper table relates to anti-trine measurements and the lower table to trine measurements.

Anti-trine measurement

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
$\|A\rangle$	$\begin{pmatrix} 0 \\ 1 \end{pmatrix}$	$\begin{pmatrix} 0 \\ 1 \end{pmatrix}$	$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 0 \\ 1 \end{pmatrix}$	$\begin{pmatrix} \frac{-1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$	$\begin{pmatrix} 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix}$	$\begin{pmatrix} \frac{-1}{\sqrt{2}} \\ 0 \end{pmatrix}$
$\|B\rangle$	$\begin{pmatrix} \frac{\sqrt{3}}{2} \\ \frac{1}{2} \end{pmatrix}$	$\begin{pmatrix} 0 \\ \frac{1}{2} \end{pmatrix}$	$\begin{pmatrix} \frac{\sqrt{3}}{2} \\ 0 \end{pmatrix}$	$\begin{pmatrix} \frac{1}{2} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$	$\begin{pmatrix} 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix}$	$\begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \end{pmatrix}$	$\begin{pmatrix} 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix}$	$\begin{pmatrix} 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix}$	$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$
$\|C\rangle$	$\begin{pmatrix} \frac{\sqrt{3}}{2} \\ \frac{-1}{2} \end{pmatrix}$	$\begin{pmatrix} 0 \\ \frac{-1}{2} \end{pmatrix}$	$\begin{pmatrix} \frac{\sqrt{3}}{2} \\ 0 \end{pmatrix}$	$\begin{pmatrix} \frac{1}{2} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$	$\begin{pmatrix} 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix}$	$\begin{pmatrix} \frac{1}{2} \\ \frac{-1}{2} \end{pmatrix}$	$\begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \end{pmatrix}$	$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$	$\begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \end{pmatrix}$

Trine measurement

$\|A\rangle$	$\begin{pmatrix} 1 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 1 \\ 0 \end{pmatrix}$	$\begin{pmatrix} \frac{1}{\sqrt{3}} \\ \sqrt{\frac{2}{3}} \end{pmatrix}$	$\begin{pmatrix} 0 \\ \sqrt{\frac{2}{3}} \end{pmatrix}$	$\begin{pmatrix} \frac{1}{\sqrt{3}} \\ 0 \end{pmatrix}$	$\begin{pmatrix} \frac{1}{\sqrt{6}} \\ \frac{1}{\sqrt{6}} \end{pmatrix}$	$\begin{pmatrix} 0 \\ \frac{1}{\sqrt{6}} \end{pmatrix}$	$\begin{pmatrix} \frac{1}{\sqrt{6}} \\ 0 \end{pmatrix}$
$\|B\rangle$	$\begin{pmatrix} \frac{1}{2} \\ \frac{-\sqrt{3}}{2} \end{pmatrix}$	$\begin{pmatrix} 0 \\ \frac{-\sqrt{3}}{2} \end{pmatrix}$	$\begin{pmatrix} \frac{1}{2} \\ 0 \end{pmatrix}$	$\begin{pmatrix} \frac{1}{2\sqrt{3}} \\ \frac{1}{\sqrt{6}} \end{pmatrix}$	$\begin{pmatrix} 0 \\ \frac{1}{\sqrt{6}} \end{pmatrix}$	$\begin{pmatrix} \frac{1}{2\sqrt{3}} \\ \frac{-\sqrt{3}}{2} \end{pmatrix}$	$\begin{pmatrix} \frac{\sqrt{2}}{3} \\ \frac{-1}{\sqrt{6}} \end{pmatrix}$	$\begin{pmatrix} 0 \\ \frac{-1}{\sqrt{6}} \end{pmatrix}$	$\begin{pmatrix} \frac{\sqrt{2}}{3} \\ 0 \end{pmatrix}$
$\|C\rangle$	$\begin{pmatrix} \frac{-1}{2} \\ \frac{-\sqrt{3}}{2} \end{pmatrix}$	$\begin{pmatrix} 0 \\ \frac{-\sqrt{3}}{2} \end{pmatrix}$	$\begin{pmatrix} \frac{-1}{2} \\ 0 \end{pmatrix}$	$\begin{pmatrix} \frac{-1}{2\sqrt{3}} \\ \frac{1}{\sqrt{6}} \end{pmatrix}$	$\begin{pmatrix} 0 \\ \frac{-1}{\sqrt{6}} \end{pmatrix}$	$\begin{pmatrix} \frac{-1}{2\sqrt{3}} \\ \frac{-\sqrt{3}}{2} \end{pmatrix}$	$\begin{pmatrix} \frac{1}{\sqrt{6}} \\ \frac{-\sqrt{2}}{3} \end{pmatrix}$	$\begin{pmatrix} 0 \\ \frac{-\sqrt{2}}{3} \end{pmatrix}$	$\begin{pmatrix} \frac{1}{\sqrt{6}} \\ 0 \end{pmatrix}$

the amplitudes at position (5) and clearly realize the optimal probability of 2/3 for correct assignment of the state and 1/6 for each of the two incorrect possibilities.

The light at position (6) has linear polarization, the horizontal component of which comes from the upper interferometer path and the vertical component from the lower path. The second half-wave plate rotates the polarization through 45° which is equivalent to implementing the action of the unitary operator

$$U_2 = \begin{pmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix}, \tag{17}$$

on the polarization state at position (6). The final polarizing beam-splitter separates the horizontally and vertically polarized components so that the light at positions (8) and (9) is vertically and horizontally polarized respectively. A detection registered in detector *b* corresponds to the assignment of the input state as $|B\rangle$. The probabilities for this event to occur for each of the three possible input states can be read off as the squared moduli of the amplitudes at position (8) and again clearly realize the optimal probability of 2/3 for correct assignment of the state and 1/6 for each of the two incorrect possibilities. Similarly, a detection registered in detector *c* corresponds to the assignment of the input state as $|C\rangle$ with the probability that this is correct again being 2/3.

For an anti-trine measurement, Eve need only place an additional half-wave plate in the input of her device to rotate each state into its complement; $|A\rangle \rightarrow |\bar{A}\rangle$ (and similarly for states $|B\rangle$ and $|C\rangle$). This corresponds to implementing the action of the unitary operator

$$U_3 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

on the states prepared by Eve. The rest of the device operates as described above and the polarization states at our nine positions are listed in table 2. The probabilities for detections to occur in any of the three detectors can again be read from the table as the squares of the amplitudes at the relevant positions. We see that detections registered in detectors *a*, *b* and *c* now correspond to the correct conclusions that the state prepared was *not* $|A\rangle$, $|B\rangle$ and $|C\rangle$, respectively, although no indication is given as to which of the two remaining states was sent, in accord with the requirements for an anti-trine measurement.

6. Conclusion

We have presented a new protocol for quantum key distribution using 3 mutually non-orthogonal states. This protocol is of interest both because of the existence of powerful general theorems concerning measurements on such systems and because of the existence of an optical implementation of these measurements.

The original motivation for this protocol was to find a way of overcoming the 'suppression' attack in the B92 protocol [3]. If we consider that Alice occasionally and randomly injects a third mutually non-orthogonal state during the operation of the standard B92 protocol, this extra qubit can be used to aid eavesdropper detection. Indeed, 3 states is the minimum requirement necessary for the successful operation of a rejected-data protocol in which the presence of the eavesdropper is revealed using only those bits that would be thrown away. The extension of the protocol we have described to both augment the B92 protocol and as a rejected-data protocol is straightforward.

Acknowledgments

A. Chefles would like to thank EPSRC for support. We are also grateful to Masahide Sasaki and Richard Jozsa for illuminating discussions on the problem of measuring three mutually non-orthogonal states.

References

[1] TOWNSEND, P. D., 1998, *Opt. Fiber Technol.*, **4,** 345.
[2] BENNETT, C. H., and BRASSARD, G., 1984, *Proceedings of the IEEE Conference on Computers, Signals and Signal Processing*, Bangalore, p. 175.
[3] BENNETT, C. H., 1992, *Phys. Rev. Lett.*, **68,** 3121.
[4] BLOW, K. J., and PHOENIX, S. J. D., 1993, *J. mod. Optics*, **40,** 33.
[5] BARNETT, S. M., and PHOENIX, S. J. D., 1993, *Phys. Rev.* A, **48,** R5.
[6] EKERT, A. K., 1991, *Phys. Rev. Lett.*, **67,** 661.
[7] BARNETT, S. M., and PHOENIX, S. J. D., 1993, *J. mod. Optics*, **40,** 1443.
[8] HELSTROM, C. W., 1976, *Quantum Detection and Estimation Theory* (New York: Academic Press).
[9] SASAKI, M., BARNETT, S. M., JOZSA, R., OSAKI, O., and HIROTA, O., 1999, *Phys. Rev.* A, **59,** 3325.
[10] HOLEVO, A. S., 1973, *J. multivar. Anal.*, **3,** 337.
[11] KRAUS, K., 1983, *States, Effects and Operations* (Berlin: Springer-Verlag).
[12] SASAKI, M., private communication, 1998.
[13] SASAKI, M., KATO, K., IZUTSU, M., and HIROTA, O., 1998, *Phys. Rev.* A, **58,** 146.
[14] HAUSLADEN, P., and WOOTERS, W. K., 1994, *J. mod. Optics*, **41,** 2385.
[15] BUSCH, P., 1987, *Found. Phys.*, **17,** 905.