Quantum cryptography using nonlocal measurements

Helv. Phys. Acta 70 (1997) 710 – 726
0018-0238/97/050710-17 $ 1.50+0.20/0

Helvetica Physica Acta

Quantum Cryptography using Nonlocal Measurements

By O. Cohen

Physics Department, Birkbeck College, University of London,
Malet Street, London WC1E 7HX, England

(21.VIII.1996)

Abstract. We demonstrate that there are a number of ways in which nonlocal measurement techniques can be used to facilitate quantum cryptographic key distribution. We show that cryptography schemes based on nonlocal measurements can possess features which had previously been thought to be impossible in quantum cryptography. We also find that such schemes have interesting implications for the detectability of eavesdroppers, and for the possible ways in which eavesdropping tests can be carried out.

1 Introduction

Quantum cryptography is a new discipline which has its origins in an idea of Wiesner [1] which was subsequently taken up by Bennett and Brassard [2] and others. The objective of this discipline is the transmission of data which can then be used as a secret key for cryptographic purposes, and to guarantee, or at least to ensure with a high level of confidence, that any unauthorized attempt to intercept the transmission will be detected by the two legitimate users ("Alice" and "Bob"). Successful transmission results in Alice and Bob sharing a random and secret sequence of bits which can be used as the key. Quantum cryptography represents a significant development in both physics and cryptography. It encompasses the first practical application of the Bell inequality [3] and one of the first practical applications of Einstein-Podolsky-Rosen-Bohm entangled states [4, 5]. Exploitation of the uncertainty principle and Bell's theorem, which are fundamental quantum principles, enables quantum cryptography to offer a theoretical guarantee of security of key distribution, which is unobtainable in conventional cryptography.

The new cryptography schemes described in this paper involve a novel kind of quantum measurement technique [6, 7, 8] which facilitates the measurement of nonlocal observables. We find that certain conditions previously thought to be necessary for the viability of any quantum cryptography scheme [9] can in fact be bypassed by schemes involving nonlocal measurements. We show that it is possible to formulate a scheme in which the cryptographic key information is generated using eigenstates of two *commuting* operators, which effectively constitute a single "alphabet". We describe another cryptography scheme in which all of Alice and Bob's measurements are carried out on the same two particles. We then examine the opportunities for, and methods for detecting, eavesdroppers. We find that the eavesdropper detection techniques which are made feasible by our new cryptography schemes offer definite advantages when compared to the possible methods for detecting eavesdroppers in previous quantum cryptography schemes. Specifically, we describe a test which is guaranteed to reveal whether an eavesdropper has intercepted any *single* transmission; whereas the eavesdropping tests in previous schemes have been of a statistical nature, and have generally required a large sample of data. We also describe a cryptography scheme where eavesdropper detection takes place automatically during the key generation process itself, so that there is no need for a separate eavesdropping test. In addition we find that the new schemes do not need to sacrifice any of the potential cryptographic key data in order to facilitate eavesdropper detection, whereas previously it had been thought that a "sacrificial protocol" would be unavoidable in any quantum cryptography scheme which uses the minimum number of alphabets [9].

2 Quantum Cryptography

The original quantum cryptography schemes [1, 2] involved the use of a set of four nondegenerate eigenstates, consisting of two nonorthogonal pairs of orthogonal states. There are various ways in which such sets can be realized in practice. One could use photon polarization states (e.g. horizontally and vertically polarized, and left- and right-hand circular polarized) or spin-component eigenstates of spin-$\frac{1}{2}$ particles (e.g. $|\uparrow_x\rangle, |\downarrow_x\rangle$ and $|\uparrow_z\rangle, |\downarrow_z\rangle$). The sender (Alice) attempts to generate a secret shared bit by preparing each transmitted particle in one of the four eigenstates—in doing so she must choose each time between one of two possible measurement bases. The receiver (Bob) measures the polarization (or spin) of the transmitted photon (or spin-$\frac{1}{2}$ particle), choosing randomly between the same two measurement bases as those used by Alice. After a sufficient number of particles have been transmitted, Alice and Bob communicate over a public channel in order to compare the measurement bases they used for each transmission. Each time these bases correspond (i.e. for about 50% of the transmissions), and provided there has been no interception by an eavesdropper, Alice and Bob will have generated a secret shared bit towards their cryptographic key.

The use of such nonorthogonal pairs of states to transmit a random sequence of bits from Alice to Bob means that straightforward passive eavesdropping by an adversary ("Eve") is

impossible. This is because Eve does not know to which of the two pairs of orthogonal states each transmitted state belongs, and so any attempt by her to perform a measurement on the transmitted state will be liable to modify it, with significant probability. (Any measurement procedure chosen by Eve which fails to disturb two nonortogonal pairs of states cannot reveal any information about them [10].) Some of these inadvertant modifications by Eve will almost certainly show up later when Alice and Bob carry out their eavesdropping test. There are various ways in which Alice and Bob can test for the presence of an eavesdropper; the most straightforward method being for them to select a "sacrificial" portion of their transmitted bit sequence and verify, using a public communication channel, that Alice's and Bob's versions of the string are identical. If some or all of the transmitted particles have been intercepted by Eve who has then retransmitted similar particles in an attempt to avoid being discovered, then there will almost certainly be some discrepancies between Alice's and Bob's retained bit strings (i.e. between those results obtained when they chose corresponding measurement bases). The probability of such discrepancies being discovered approaches unity as the size of the dataset used for the eavesdropping test is increased.

Rather than using four nonorthogonal states (i.e. two pairs of orthogonal states), Bennett [11] has shown that quantum cryptography can be carried out using only *two* nonorthogonal states. In Bennett's two-state scheme Alice prepares and transmits one of two nonorthogonal states, $|u\rangle$ and $|v\rangle$, say, which represent respectively 0 and 1, and Bob subsequently chooses to measure one of the two projection operators onto subspaces orthogonal to $|u\rangle$ and $|v\rangle$ (i.e. he measures either $1 - |u\rangle\langle u|$ or $1 - |v\rangle\langle v|$). On some occasions Bob's results will be inconclusive. The remaining instances should consist of occasions when either Alice sent $|u\rangle$ and Bob measured $1 - |v\rangle\langle v|$, or Alice sent $|v\rangle$ and Bob measured $1 - |u\rangle\langle u|$, and should thus give perfectly correlated results which can be used as the basis of the cryptographic key. The security of this two-state scheme against various eavesdropping strategies has been examined in detail by Ekert *et al.* [12]. Recently Huttner *et al.* [13] have proposed a quantum cryptography method which combines features from the four-state and two-state schemes.

An alternative quantum crytography method using Einstein-Podolsky-Rosen-Bohm (EPRB) [5] pairs was put forward by Ekert [14]. In Ekert's scheme a central source sends EPRB particle pairs to Alice and Bob, one particle of each pair going to Alice and one to Bob. Alice and Bob each choose between three possible spin-measurement directions, two of which they share. On those occasions when they choose the same direction for their spin measurements, Alice and Bob can exploit the perfect EPRB correlations to generate a secret shared bit. The eavesdropping test is carried out by using the rejected data (i.e. results obtained when Alice and Bob choose different measurement bases) to check for an expected violation of the Bell inequality. Subsequently, Bennett, Brassard and Mermin [10] showed that EPRB states can be used for quantum cryptography without recourse to Bell's theorem, by using just two measurement bases, shared by Alice and Bob, and carrying out an eavesdropping test similar to that used in Bennett and Brassard's single particle scheme [2]. Bennett, Brassard and Mermin went on to show that their simplified EPRB-based scheme is equivalent to Bennett and Brassard's scheme.

In cryptography schemes involving EPRB pairs, a more sophisticated eavesdropper might attempt to replace the particle source with a device producing three-particle entangled states. She would arrange that two particles from each triplet are transmitted to Alice and Bob, with the intention of remaining undetected while obtaining information about Alice and Bob's key data through correlations between the results of Alice's and Bob's measurements and the results of her own measurements on the third particle. However, Bennett, Brassard and Mermin have shown that, for their EPRB-based scheme, any such eavesdropping strategy cannot succeed; any such fake source certain of passing the subsequent eavesdropping test would fail to yield any information whatsoever.

As well as security considerations relating to the possibility of eavesdropping occurring during the particle transmissions, we must also take into account the security of the key data once it is in the hands of both legitimate parties. From this point of view, the particles used in EPRB-pair cryptography schemes could in principle be stored by Alice and Bob until the key is needed, and any attempt by an intruder to obtain the key prior to Alice and Bob's measurements would be detectable in the subsequent eavesdropping test. On the other hand, in single particle quantum cryptography schemes the information stored by Alice, after each particle transmission, is classical and could in theory be copied without detection.

All the cryptography schemes described so far in this section involve binary "alphabets"; that is, each measurement performed by Bob can, at best, distinguish between only two states and hence can generate at most one bit towards the key. However, Bennett and Wiesner [15] have described a two-bit cryptography scheme which uses an alphabet of size four, arising from the use of the "Bell operator" basis [16] which has dimension four. Phoenix [17] has pointed out that quantum cryptography can in theory be carried out with alphabets of arbitrary size, by using operators with the appropriate number of nondegenerate eigenstates.

3 Measurement of Nonlocal Observables

In this paper we examine methods of implementing quantum cryptography which involve the application of *nonlocal* measurement procedures. Although, to the best of our knowledge, nonlocal measurements have not been involved in any previous quantum cryptography scheme, it has recently been shown [18] that nonlocal measurements can be used to carry out another kind of quantum communication, namely "teleportation" in the sense originally described by Bennett *et al.* [19]. The sort of nonlocal observables we will use in this paper were first described by Aharonov and Albert [6, 7], and the concept was developed by Aharonov, Albert and Vaidman [8]. The basic objective of a nonlocal measurement is to measure a *combined* property of two (or more) spacelike-separated regions in such a way that the corresponding *separate* properties of these regions may remain undetermined and not well-defined. A nonlocal measurement is carried out by preparing a number of apparatuses in an entangled state, and then arranging that impulsive interactions take place between the different apparatuses and the separated components of the measured system, and that these

interactions take place simultaneously (or in spacelike separated regions).

This technique is best demonstrated by means of a simple example. Although Aharonov and Albert's analyses of the technique are carried out using the Heisenberg picture, it can be described straightforwardly in the Schrödinger representation. We choose for our example a system consisting of two spin-$\frac{1}{2}$ particles, intially in an arbitrary state which is not necessarily entangled. Our nonlocal observable is the total z-component of spin for the two particles, given by $\sigma_{1z} + \sigma_{2z}$. We want to measure this observable at time t_0. In order to demonstrate that this is possible, we first consider an apparatus that carries out an impulsive measurement of the local observable σ_{1z} through the Hamiltonian

$$H_{int}^{(1)} = g(t) P \sigma_{1z}, \tag{3.1}$$

where P refers to the momentum of an internal "pointer" in the apparatus and $g(t)$ is zero everywhere except in the interval $[t_0 - \epsilon, t_0 + \epsilon]$ and satisfies

$$\int_{t_0-\epsilon}^{t_0+\epsilon} g(t)dt = \Delta. \tag{3.2}$$

Before the interaction between apparatus and particle takes place, the position Q of the apparatus's internal pointer is measured and found to be q_i. The initial spin-state of the particle is unknown and assumed to be $\alpha|\uparrow_z\rangle + \beta|\downarrow_z\rangle$. Hence the initial state of apparatus plus particle can be written

$$|\Psi(t_i)\rangle = |q_i\rangle \otimes (\alpha|\uparrow_z\rangle + \beta|\downarrow_z\rangle) \tag{3.3}$$

where

$$\langle q|q_i\rangle = \delta(q - q_i). \tag{3.4}$$

The Hamiltonian $H_{int}^{(1)}$ leads to the time evolution

$$|\Psi(t)\rangle = e^{-\frac{i}{\hbar}\int_{t_-}^{t} g(t')dt' P\sigma_{1z}} |\Psi(t_i)\rangle \tag{3.5}$$

where

$$\int g(t')dt'\Big|_{t'=t_-} = 0. \tag{3.6}$$

Hence

$$|\Psi(t)\rangle = \left\{1 - \frac{i}{\hbar}\int_{t_-}^{t} g(t')dt' P\sigma_{1z} - \frac{1}{2!\hbar^2}\left(\int_{t_-}^{t} g(t')dt'\right)^2 P^2(\sigma_{1z})^2 - \cdots\right\} |q_i\rangle\otimes(\alpha|\uparrow_z\rangle + \beta|\downarrow_z\rangle) \tag{3.7}$$

and

$$\begin{aligned}\langle q|\Psi(t)\rangle \;=\; & \alpha\left\{1 - \int_{t_-}^{t} g(t')dt'\frac{\partial}{\partial q} + \frac{1}{2!}\left(\int_{t_-}^{t} g(t')dt'\right)^2 \frac{\partial^2}{\partial q^2} - \cdots\right\}\langle q|q_i\rangle \otimes |\uparrow_z\rangle \\ & + \beta\left\{1 + \int_{t_-}^{t} g(t')dt'\frac{\partial}{\partial q} + \frac{1}{2!}\left(\int_{t_-}^{t} g(t')dt'\right)^2 \frac{\partial^2}{\partial q^2} + \cdots\right\}\langle q|q_i\rangle \otimes |\downarrow_z\rangle.\end{aligned} \tag{3.8}$$

So

$$|\Psi\,(t > t_0 + \epsilon)\rangle = \alpha|q_i + \Delta\rangle \otimes |\uparrow_z\rangle + \beta|q_i - \Delta\rangle \otimes |\downarrow_z\rangle. \tag{3.9}$$

It follows that if we measure the apparatus pointer position Q after the interaction has taken place, and obtain the result q_f, then the z-component of spin of the measured particle will be given (in units of $\hbar/2$) by

$$s_z = \frac{1}{\Delta}\,(q_f - q_i)\,. \tag{3.10}$$

Now suppose we have two such apparatuses that interact with two spatially separated spin-$\frac{1}{2}$ particles through the Hamiltonian

$$H_{int}^{(12)} = g(t)\,(P_1\sigma_{1z} + P_2\sigma_{2z}) \tag{3.11}$$

where once again $g(t)$ is zero everywhere except in the interval $[t_o - \epsilon, t_0 + \epsilon]$ and satisfies

$$\int_{t_0-\epsilon}^{t_0+\epsilon} g(t)dt = \Delta. \tag{3.12}$$

We prepare the internal pointers of the two apparatuses in an entangled state $|\Phi_{12}\rangle$ which satisfies

$$\left.\begin{array}{l}(Q_1 + Q_2)\,|\Phi_{12}\rangle = 0|\Phi_{12}\rangle \\ (P_1 - P_2)\,|\Phi_{12}\rangle = 0|\Phi_{12}\rangle\end{array}\right\} \tag{3.13}$$

and then separate the two apparatuses and allow them to interact with the two spin-$\frac{1}{2}$ particles at time t_0.

$(Q_1 + Q_2)$ and $(P_1 - P_2)$ together constitute a complete commuting set of observables for the two-pointer system and so $|\Phi_{12}\rangle$ is uniquely determined by (3.13), and can be written

$$|\Phi_{12}\rangle = \int_{-\infty}^{\infty} dq_i|q_i\rangle_1|-q_i\rangle_2. \tag{3.14}$$

The initial spin state of the two spin-$\frac{1}{2}$ particles is completely arbitrary, and so the initial combined state of apparatuses plus particles can be written

$$|\Psi^{12}(0)\rangle = \int_{-\infty}^{\infty} dq_i|q_i\rangle_1|-q_i\rangle_2 \otimes (a|\uparrow_{1z}\uparrow_{2z}\rangle + b|\uparrow_{1z}\downarrow_{2z}\rangle + c|\downarrow_{1z}\uparrow_{2z}\rangle + d|\downarrow_{1z}\downarrow_{2z}\rangle)\,. \tag{3.15}$$

After the interactions between apparatuses and spin-$\frac{1}{2}$ particles have taken place the combined state will be

$$\begin{aligned}|\Psi^{(12)}\,(t > t_0 + \epsilon)\rangle = \\ \int_{-\infty}^{\infty} dq_i\,\{&a|q_i + \Delta\rangle_1|-q_i + \Delta\rangle_2 \otimes |\uparrow_{1z}\uparrow_{2z}\rangle + b|q_i + \Delta\rangle_1|-q_i - \Delta\rangle_2 \otimes |\uparrow_{1z}\downarrow_{2z}\rangle \\ &+c|q_i - \Delta\rangle_1|-q_i + \Delta\rangle_2 \otimes |\downarrow_{1z}\uparrow_{2z}\rangle + d|q_i - \Delta\rangle_1|-q_i - \Delta\rangle_2 \otimes |\downarrow_{1z}\downarrow_{2z}\rangle\}\,.\end{aligned} \tag{3.16}$$

Hence the total z-component of spin $\sigma_{1z} + \sigma_{2z}$ for the two particles will have the value S_z given (in units of $\hbar/2$) by

$$S_z = \frac{1}{\Delta}\,(q_{f1} + q_{f2}) \tag{3.17}$$

where q_{f1} and q_{f2} are the final pointer positions of the two apparatuses, which can be determined by carrying out measurements of Q_1 and Q_2. This means that, if Q_1 and Q_2 are measured *locally*, a *nonlocal* measurement of $\sigma_{1z} + \sigma_{2z}$ will have been completed. It is not necessary to bring the apparatuses to the same place in order to measure Q_1 and Q_2. The actual final pointer position readings q_{f1} and q_{f2} could be recorded automatically at each apparatus, or the readings could be taken by two experimenters observing the apparatuses and exchanged through a communication channel. Both experimenters would then be aware of the result of the measurement of $\sigma_{1z} + \sigma_{2z}$, but the local observables σ_{1z} and σ_{2z} will not have been measured.

The reader will no doubt have realized that the state $|\Phi_{12}\rangle$ in which the apparatuses are prepared is an idealized state with no limits on the possible positions of the internal pointers. A more realistic state would be $|\tilde{\Phi}_{12}\rangle$ given by

$$|\tilde{\Phi}_{12}\rangle = \int_{-E}^{E} dq_i |q_i\rangle_1 |-q_i\rangle_2. \tag{3.18}$$

In this state the possible positions of the pointers are restricted to the range $[-E, E]$. This restriction necessarily precludes the possibility of the momentum representation of $|\tilde{\Phi}_{12}\rangle$ giving an absolute correlation between the initial momenta of the two apparatuses. The momentum representation of $|\tilde{\Phi}_{12}\rangle$ is given by

$${}_1\langle p_1|\,{}_2\langle p_2|\tilde{\Phi}_{12}\rangle = \frac{1}{\pi\,(p_1 - p_2)} \sin\left[\frac{E}{\hbar}\,(p_1 - p_2)\right]. \tag{3.19}$$

This function is sharply peaked about $p_1 - p_2 = 0$, but it has a non-negligible value over a range of width $\sim h/E$, as we would expect from the uncertainty principle because of the restriction on the range of q_{i1} and q_{i2}. However, our derivation of the nonlocal measurement formula $S_z = (q_{f1} + q_{f2})/\Delta$ will go through in exactly the same way if we take the initial state of the apparatuses to be $|\tilde{\Phi}_{12}\rangle$ rather than $|\Phi_{12}\rangle$.

The nonlocal measurement of $\sigma_{1z} + \sigma_{2z}$ can leave the system of two spin-$\frac{1}{2}$ particles, which may never have interacted with *each other*, in an entangled state. If the measurement of $\sigma_{1z} + \sigma_{2z}$ yields $S_z = 0$ then after the measurement the two-particle spin state will be a superposition of the form $\gamma|\uparrow_{1z}\downarrow_{2z}\rangle + \delta|\downarrow_{1z}\uparrow_{2z}\rangle$.

By carrying out alternate nonlocal measurements of $\sigma_{1z} + \sigma_{2z}$ and $\sigma_{1x} + \sigma_{2x}$ it is possible to prepare any system of two spin-$\frac{1}{2}$ particles in the Einstein-Podolsky-Rosen-Bohm (EPRB) [5] state $1/\sqrt{2}\,(|\uparrow_1\downarrow_2\rangle - |\downarrow_1\uparrow_2\rangle)$; this preparation will be achieved whenever we get two successive null results [18]. In other words, if we measure $\sigma_{1z} + \sigma_{2z}$ and obtain $S_z = 0$, and then measure $\sigma_{1x} + \sigma_{2x}$ immediately afterwards and obtain $S_x = 0$, then after these measurements the particles' spin-state will be the EPRB state; the particles can have arbitrary spatial separation and need never have interacted with each other. If we subject a large number of pairs of spin-$\frac{1}{2}$ particles, initially in arbitrary spin-states, to successive measurements of $\sigma_{1z} + \sigma_{2z}$ and $\sigma_{1x} + \sigma_{2x}$, we would expect about one quarter of these pairs to give null outcomes for both measurements and hence to be in the EPRB state immediately following these measurements.

It is possible to measure nonlocal observables with continuous spectra by applying a similar procedure to that outlined in this section [6]. However, for the purposes of cryptographic applications, we restrict the nonlocal observables used in this paper to combinations of spin-components such as $\sigma_{1z} + \sigma_{2z}$.

It should also be mentioned that a detailed analysis of causality constraints on nonlocal measurements has recently been carried out by Popescu and Vaidman [20], but their conclusions do not affect the validity of the results presented here.

4 Using Nonlocal Measurements for Quantum Cryptography

In this section we describe three new cryptography schemes, all of which incorporate nonlocal measurements.

4.1 Scheme A

As we have just seen, nonlocal measurements can be used to prepare any spatially separated pair of spin-$\frac{1}{2}$ particles in the EPRB state. Hence an obvious way in which nonlocal measurements could be incorporated into a quantum cryptography scheme would be for Alice and Bob to prepare a series of pairs of spin-$\frac{1}{2}$ particles in the EPRB state by such a method. For each pair of particles, they can monitor, over a public communication channel, whether they have successfully prepared the EPRB state, by measuring and comparing the internal pointer variables of their respective apparatuses for each pair of successive nonlocal measurements of $\sigma_{1z} + \sigma_{2z}$ and $\sigma_{1x} + \sigma_{2x}$, and checking that they sum to zero in each case. Each time they succeed in preparing a pair of particles in the EPRB state they can then generate a secret shared bit towards their cryptographic key by carrying out local spin-component measurements on their spin-$\frac{1}{2}$ particles along an agreed direction. The results of these measurements will, with probability 1, be anticorrelated and known only to Alice and Bob. Previous EPRB-based cryptography schemes [10, 14] have required Alice and Bob to choose between two [10] or three [14] directions for their spin-component measurements. The use of more than one direction for spin-component measurements in these schemes is necessary in order that the subsequent tests for the presence of eavesdroppers can be carried out effectively. In our EPRB-based scheme only one direction for the spin-component measurements is needed, because the eavesdropping test can be carried out on the transmitted *apparatuses*, rather than on the spin-$\frac{1}{2}$ particles which never leave Alice and Bob's possession. We will consider the eavesdropping possibilities for nonlocal measurement based quantum cryptography in Section 5.

4.2 Scheme B

The method just described (Scheme A) is an unnecessarily complicated and inefficient way of exploiting nonlocal measurements for quantum cryptography. Alice and Bob do not need to prepare each pair of spin-$\frac{1}{2}$ particles in the EPRB state in order to be able to use that pair to generate a secret shared bit. Rather, they simply need to prepare each pair of particles in a state which will guarantee that the results of their subsequent spin-component measurements will have a definite correlation (or anticorrelation) and will be known only to them. They can achieve this by measuring just *one* nonlocal observable, for example $\sigma_{1z} + \sigma_{2z}$. If this measurement yields the result $S_z = 0$, which can be confirmed by Alice and Bob through a public communication channel, they will know that the spin-state of their pair of particles must be some arbitrary superposition $\alpha|\uparrow_{1z}\downarrow_{2z}\rangle + \beta|\downarrow_{1z}\uparrow_{2z}\rangle$. Subsequent local measurements of σ_{1z} and σ_{2z} by Alice and Bob will then, with certainty, give anticorrelated results and can thus be used to generate a secret shared bit towards the cryptographic key.

Blow and Phoenix [9] have argued that any secure quantum cryptography scheme requires the use of at least two "alphabets", consisting of eigenststates of noncommuting operators, and that any such scheme that uses the minimum number of alphabets must sacrifice some of the potential cryptographic key data in the test for eavesdropping. (An alphabet is defined as a set of given symbols, which are used for the assignment of numbers for the cryptographic key.) However, Scheme B uses as alphabets the eigenstates of σ_{1z} and σ_{2z}, which operators commute; and since the results of measuring σ_{1z} and σ_{2z} will always be anticorrelated we can reasonably argue that essentially only *one* alphabet is involved. Furthermore, *none* of the potential key data need be sacrificed in the eavesdropping test which, as we will see, can be carried out on the apparatuses prior to the generation of key data from each pair of spin-$\frac{1}{2}$ particles.

4.3 Scheme C

It is possible in principle for Alice and Bob to carry out cryptographic key distribution by performing a series of measurements of $\sigma_{1z} + \sigma_{2z}$ and $\sigma_{1x} + \sigma_{2x}$ alternately, on the *same* pair of particles. Each time one of these measurements yields a null result a secret shared bit can be generated by carrying out local spin-component measurements, as in Scheme B. Alice and Bob's two-particle system will then be in a suitable state for their *next* nonlocal measurement, the result of which will be completely unpredictable. Suppose for example Alice and Bob measure $\sigma_{1z} + \sigma_{2z}$ and obtain the result $S_z = 0$; the state of their two-particle system will then be a superposition of the form $a|\uparrow_{1z}\downarrow_{2z}\rangle + b|\downarrow_{1z}\uparrow_{2z}\rangle$. They then carry out local measurements of σ_{1z} and σ_{2z}. Suppose these measurements yield $s_{1z} = 1$ and $s_{2z} = -1$. These results will contribute one bit towards the cryptographic key, and the two-particle system will be left in the state $|\uparrow_{1z}\downarrow_{2z}\rangle$. Alice and Bob then measure $\sigma_{1x} + \sigma_{2x}$; the outcome of this measurement will be unpredictable since

$$|\uparrow_{1z}\downarrow_{2z}\rangle \equiv \tfrac{1}{2}\{|\uparrow_{1x}\uparrow_{2x}\rangle - |\downarrow_{1x}\downarrow_{2x}\rangle - |\uparrow_{1x}\downarrow_{2x}\rangle + |\downarrow_{1x}\uparrow_{2x}\rangle\}$$

$$= \frac{1}{2}\left\{|S_x = 2\rangle - |S_x = -2\rangle - \sqrt{2}|S_x = 0\rangle\right\}.$$

If Alice and Bob obtain $S_x = 0$, they can generate another secret shared bit towards their key, and they then proceed with the next measurement of $\sigma_{1z} + \sigma_{2z}$. If they obtain $S_x = \pm 2$ they cannot generate a secret bit from the $\sigma_{1x} + \sigma_{2x}$ measurement, but just proceed with the next measurement of $\sigma_{1z} + \sigma_{2z}$. In both cases the outcome of the next measurement of $\sigma_{1z} + \sigma_{2z}$ will be completely unpredictable. This method shows that, in principle, nonlocal measurement based quantum cryptography can be just as efficient in its use of resources as other quantum cryptography schemes. Whereas previous schemes have used a small number of apparatuses but a large number of transmitted particles to generate the key data, the scheme we have just described requires a large number of apparatuses but only two particles to generate the key data. There is no reason why the apparatuses themselves should not be microscopic, with the internal pointers consisting of single particles.

5 Detecting Eavesdroppers

In the cryptography schemes described in the last section, the spin-$\frac{1}{2}$ particles on which the key data generating measurements are performed never leave Alice's and Bob's possession. Hence any risk of eavesdropping must arise from the possibility of a third party ("Eve") intercepting the transmitted apparatuses prior to their interactions with the spin-$\frac{1}{2}$ particles. The two apparatuses used for each nonlocal measurement could be prepared in an entangled state by Alice, and one of the apparatuses transmitted to Bob; or the two apparatuses could be prepared at a central source, and one apparatus transmitted to Alice and one to Bob. In the first case there is a risk of Eve intercepting one, and in the second case both, of the apparatuses.

We will consider two different kinds of eavesdropping which we label "type 1" and "type 2". Type 1 eavesdropping involves interception of the transmitted apparatuses, straightforward measurement of one of the variables P and Q for each apparatus, and then retransmission of the apparatuses. This sort of eavesdropping is analogous to the more straightforward cases of eavesdropping considered by Bennett and Brassard [2] and by Ekert [14]. Type 2 eavesdropping is more sophisticated; in this case, after intercepting one or both of a pair of entangled apparatuses, Eve does not measure P or Q directly but attempts to prepare the intercepted apparatus(es), together with a similar apparatus already in her possession, in a suitable entangled state. She then retransmits the intercepted apparatus(es) to their intended destination(s) and allows her own apparatus to interact with a spin-$\frac{1}{2}$ particle in her possession. (Alternatively, if the apparatuses originate from a central source, Eve could attempt to replace this source with a new source producing three-apparatus entangled states; she would retain one apparatus of each triplet, which would later interact with her spin-$\frac{1}{2}$ particle.) By doing this Eve hopes that a nonlocal measurement will be carried out involving her own particle and one or both members of Alice and Bob's pair of particles. If this objective is achieved, Eve may be able to infer the results of Alice's and Bob's subsequent

local spin-component measurements from the result of a spin-component measurement on her own particle; thus she could gain access to Alice and Bob's key data. A similar type of eavesdropping, but where Eve attempts to replace the legitimate two-*particle* source with a source producing suitable three-particle entangled states, was considered by Bennett, Brassard and Mermin [10] for their EPRB-based cryptography scheme; they showed that any such attempt would be incapable of yielding any useful information relating to the key.

We consider first type 1 eavesdropping. Suppose that the two apparatuses, labelled "1" and "2", with interaction Hamiltonian given by (3.11), are prepared by Alice in the state $|\Phi_{12}\rangle$ given by (3.13), and that apparatus 2 is then transmitted to Bob. Eve manages to intercept this apparatus and measures Q_2, obtaining the result q_{i2}. Once Eve has carried out this measurement the position of the pointer of apparatus 1 will also be well-defined and equal to q_{i1}, say; and if Eve knows how the apparatuses were prepared she will be able to determine the value of q_{i1}, since

$$q_{i1} + q_{i2} = 0. \tag{5.1}$$

Eve then retransmits apparatus 2 to Bob. Once Bob receives this apparatus Alice and Bob allow their apparatuses to interact with a pair of spin-$\frac{1}{2}$ particles as usual. They then measure Q_1 and Q_2. If the results q_{f1} and q_{f2} of these measurements satisfy $q_{f1} + q_{f2} = 0$, Alice and Bob will erroneously infer that the spin-state of their two-particle system must be some superposition $\alpha|\uparrow_{1z}\downarrow_{2z}\rangle + \beta|\downarrow_{1z}\uparrow_{2z}\rangle$. In fact, as a consequence of Eve's intervention Alice and Bob will not have carried out a nonlocal measurement; without realizing it, they will have performed two *local* measurements, of σ_{1z} and σ_{2z}, and immediately after these measurements the spin-state of their two-particle system will be *either* $|\uparrow_{1z}\downarrow_{2z}\rangle$ *or* $|\downarrow_{1z}\uparrow_{2z}\rangle$. This is because Eve's measurement will have disentangled the apparatuses' two-pointer wavefunction, thus precluding the possibility of the apparatuses being used for a nonlocal measurement. After interacting with the apparatuses, the values of the z-components of spin of the two particles will be given by

$$\left.\begin{aligned} s_{1z} &= \frac{1}{\Delta}(q_{f1} - q_{i1}) \\ s_{2z} &= \frac{1}{\Delta}(q_{f2} - q_{i2}) \end{aligned}\right\} \tag{5.2}$$

and so it will still be the case that

$$s_{1z} + s_{2z} = \frac{1}{\Delta}(q_{f1} + q_{f2}) = 0 \tag{5.3}$$

as it would be if a nonlocal measurement of $\sigma_{1z} + \sigma_{2z}$ yielding $S_z = 0$ had been carried out. However, immediately after Eve's intervention, q_{i1} and q_{i2} will have well-defined values known only to her, and since she can also obtain the values of q_{f1} and q_{f2} by listening in on the public communication channel through which Alice and Bob exchange the results of their pointer measurements, she will be able to calculate the values of s_{1z} and s_{2z} from (5.2). In this way Eve can gain access to the spin-component measurement results on which Alice and Bob base their cryptographic key.

It is essential, then, that Alice and Bob devise a reliable test that will detect the presence of a type 1 eavesdropper. A suitable such test can be carried out as follows. Alice and

Bob arrange that they are in contact through a public communication channel just *before* they carry out their apparatus pointer measurements. Every so often they agree to measure P_1 and P_2 instead of Q_1 and Q_2. (The occasions when they do this can be determined by a random number generator held by one of the two parties.) If there has been no type 1 eavesdropping, (i.e. if Eve has *not* intercepted one or both of the apparatuses and measured Q_1 and/or Q_2) then Alice and Bob will certainly find that the results p_{f1} and p_{f2} of their P measurements are equal, because of the pointer momentum correlation in the initial preparation of the apparatuses, given by (3.13). However, if Eve has intercepted one (or both) of the apparatuses and measured Q_1, Q_2, or indeed any linear combination of Q_1 and Q_2 (apart from $Q_1 + Q_2$ which would yield no useful information whatsoever), then any such measurements will definitely have disturbed the pointer momentum of the intercepted apparatus(es). Since neither Q_1 nor Q_2 commutes with $P_1 - P_2$, any measurement by Eve of Q_1, Q_2, or any linear combination of Q_1 and Q_2 apart from $Q_1 + Q_2$, will mean that Alice and Bob will almost certainly *not* obtain $p_{f1} = p_{f2}$ when they measure P_1 and P_2. Hence, by measuring P_1 and P_2, Alice and Bob should be able to detect Eve's presence immediately. The P measurements can be carried out before or after the apparatuses have interacted with Alice and Bob's spin-$\frac{1}{2}$ particles, since the Hamiltonian given by (3.11) will not change the apparatuses' momenta.

For this test to be effective, it is necessary that Alice and Bob are able to measure their pointer momenta to an accuracy of $\sim h/\Delta$, where Δ, the change in pointer position resulting from a measurement of spin $\hbar/2$, is the accuracy with which Eve needs to measure the pointer position, and is given by (3.12). If the initial state of the apparatuses is $|\tilde{\Phi}_{12}\rangle$, given by (3.18), rather than $|\Phi_{12}\rangle$, then it is also necessary that the disturbance of pointer momentum resulting from Eve's intervention be much greater than the "intrinsic" momentum uncertainty which in this case is $\sim h/E$. This condition will be satisfied provided $\Delta << E$, i.e. provided that the pointer deflection for spin $\hbar/2$ is only a very small fraction of the full range of the pointer.

The test just described is in some ways similar to the eavesdropping test in Bennett and Brassard's scheme [2], where a random subset of the data for which Alice and Bob choose corresponding measurement directions is compared using a public commmunication channel and checked for agreement. However, the probability, in our scheme, of Eve being detected after a single transmission if she has measured Q_1 and/or Q_2 and Alice and Bob subsequently carry out the eavesdropping test as described by measuring P_1 and P_2, is effectively unity; whereas in Bennett and Brassard's scheme the equivalent probability that Eve is detected for a single transmission is only 0.25. (In Ekert's EPRB-based scheme [14] the possible presence of an eavesdropper is monitored using a statistical test based on the Bell inequality; such a test necessarily involves a large dataset and rules out the possibility of detecting an eavesdropper from data relating to a single particle-pair transmission.) Eve's greater vulnerability to immediate detection in our scheme arises because P_1, P_2, and hence $P_1 - P_2$, have continuous spectra, so that if the initial state of the apparatuses is an eigenstate of $P_1 - P_2$ with eigenvalue zero, then any uncontrollable disturbance of the pointer momenta (such as would be caused by Eve measuring Q_1 and/or Q_2) will mean that subsequent

measurements of P_1 and P_2 will have a negligible probability of yielding equal results, whereas in the absence of such a disturbance these measurements would be certain to yield equal results. Previous quantum cryptography schemes [1, 2, 10, 14] have used polarization or spin-component measurements, for both the key-generation processes and the eavesdropping tests. The operators corresponding to these measurements have spectra of just two eigenvalues. It follows that in these schemes, if Bob measures the polarization or spin of a transmitted particle using the same basis as that chosen by Alice for the initial preparation, then there is at least a 50% chance that Alice and Bob's results will agree even if the particle has been intercepted and subjected to an intermediate measurement using an alternative basis so that the initial state is disturbed.

If the observables used for generating the cryptographic key data in a quantum cryptography scheme did not have discrete spectra, it would be impossible to form an alphabet from the eigenstates. In this sense the use of discrete spectra for the key generation process is unavoidable. This is why previous quantum cryptography schemes, in which the eavesdropping tests are carried out on the *same* quantum systems, and using the *same* observables, as those used for key generation, *cannot* exploit the much enhanced detectability of eavesdroppers which arises from the use of observables with continuous spectra. Our cryptography schemes using nonlocal measurements *can*, however, take advantage of this enhanced detectability, since the eavesdropping test is carried out on the apparatus pointers, which are not involved in the generation of the key data itself. This key data can still be generated using a practical binary alphabet, as in previous schemes. Furthermore, as we have already pointed out, none of the potential key data is sacrificed in our eavesdropping test.

We now describe a second method which can be used to test for the presence of a type 1 eavesdropper in nonlocal measurement based cryptography. In order to carry out this test, Alice and Bob must use two different kinds of apparatus pair. The first kind of apparatus pair interacts with Alice and Bob's spin-$\frac{1}{2}$ particles through the Hamiltonian

$$H_{int}^{(\Phi)} = g(t)\,(P_1\sigma_{1z} + P_2\sigma_{2z}) \tag{5.4}$$

and is prepared in the state $|\Phi_{12}\rangle$, given by

$$\left.\begin{aligned}(Q_1 + Q_2)\,|\Phi_{12}\rangle &= 0|\Phi_{12}\rangle \\ (P_1 - P_2)\,|\Phi_{12}\rangle &= 0|\Phi_{12}\rangle\end{aligned}\right\} \tag{5.5}$$

as previously. The second kind of apparatus pair interacts with the particles through the Hamiltonian

$$H_{int}^{(\Psi)} = g(t)\,(Q_1\sigma_{1z} + Q_2\sigma_{2z}) \tag{5.6}$$

and is prepared in the state $|\Psi_{12}\rangle$, given by

$$\left.\begin{aligned}(Q_1 - Q_2)\,|\Psi_{12}\rangle &= 0|\Psi_{12}\rangle \\ (P_1 + P_2)\,|\Psi_{12}\rangle &= 0|\Psi_{12}\rangle.\end{aligned}\right\} \tag{5.7}$$

In both cases $g(t)$ is zero everywhere except in the interval $[t_0 - \epsilon, t_0 + \epsilon]$ and satisfies

$$\int_{t_0-\epsilon}^{t_0+\epsilon} g(t)dt = \Delta. \tag{5.8}$$

The two kinds of apparatuses are externally identical. It is arranged that the apparatus preparer (i.e. either Alice or a central source) tosses a coin just before each transmission, and depending on the outcome, distributes a pair of apparatuses of either the first or second kind. Alice and Bob make contact with each other (or with a central source if such a source is used) through a public communication channel, immediately after each interaction between a pair of apparatuses and a pair of spin-$\frac{1}{2}$ particles, but before they carry out their apparatus pointer measurements. Alice informs Bob (or the central source informs Alice and Bob) which kind of apparatus pair was sent. If a pair of apparatuses of the first kind was sent, then Alice and Bob measure Q_1 and Q_2, thus carrying out a nonlocal measurement of $\sigma_{1z} + \sigma_{2z}$, the outcome of which will be given by

$$S_z = \frac{1}{\Delta}(q_{f1} + q_{f2}) \tag{5.9}$$

as previously. If a pair of apparatuses of the second kind was sent, then Alice and Bob measure P_1 and P_2; once again they will have carried out a nonlocal measurement of $\sigma_{1z}+\sigma_{2z}$, but this time the outcome will be given by

$$S_z = -\frac{1}{\Delta}(p_{f1} + p_{f2})\,. \tag{5.10}$$

Now, if Eve intercepts one (or both) of the apparatuses before they reach their destination(s), she will not know which kind of apparatus she has intercepted; hence she will not know whether to measure P or Q. If she has intercepted an apparatus (or a pair of apparatuses) of the first kind, and she then measures P_2 (and/or P_1) then such a measurement will disturb the apparatus pointer *positions*, and Alice and Bob will almost certainly *not* subsequently find that, after the apparatuses have interacted with their particles, $q_{f1} + q_{f2} = 0$, 2Δ, or -2Δ; whereas they will definitely obtain one of these results if neither P_1 nor P_2 has been measured. Similarly, if Eve has intercepted an apparatus (or a pair of apparatuses) of the second kind, and she then measures Q_2 (and/or Q_1), then Alice and Bob will almost certainly *not* find that $p_{f1} + p_{f2} = 0$, 2Δ, or -2Δ, whereas they will be certain to obtain one of these outcomes if neither Q_1 nor Q_2 has been measured. Hence there will be a probability of 0.5 that Eve is detected each time she attempts to gain access to one cryptographic bit; and Eve's presence will become manifest during the cryptographic key generation process itself, so that Alice and Bob do not need to carry out a separate eavesdropping test.

We now address the question of whether our nonlocal measurement based cryptography schemes are vulnerable to "type 2" eavesdropping. This time Eve's strategy is not to measure P or Q for the intercepted apparatus(es), but to attempt to prepare the intercepted apparatus(es), together with a similar apparatus of her own, so that the three-apparatus system is left in a suitable entangled state. Suppose for example, that Alice and Bob use just one kind of apparatus pair, with interaction Hamiltonian given by (5.4), and prepared in the state $|\Phi_{12}\rangle$ given by (5.5). Eve manages to intercept one or both of the apparatuses before they reach their destination(s). Her aim then is to prepare the intercepted apparatus(es) and her own apparatus so that the three-apparatus system is left in the state $|\Phi_{123}\rangle$ which satisfies

$$\left.\begin{aligned}(Q_2 + Q_3)\,|\Phi_{123}\rangle &= 0|\Phi_{123}\rangle \\ (P_2 - P_3)\,|\Phi_{123}\rangle &= 0|\Phi_{123}\rangle.\end{aligned}\right\} \tag{5.11}$$

If she can achieve this undetected, and if she then retransmits the intercepted apparatus(es) and allows her own apparatus to interact with a spin-$\frac{1}{2}$ particle in her possession, Eve will be able to arrange that a nonlocal measurement of $\sigma_{2z} + \sigma_{3z}$ is carried out, the outcome of which will be given by

$$S_z^{(23)} \equiv s_{2z} + s_{3z} = \frac{1}{\Delta}\,(q_{f2} + q_{f3})\,. \tag{5.12}$$

She can determine the result of this nonlocal measurement after measuring her apparatus pointer position Q_3 (which will yield the result q_{f3}), since Alice and Bob exchange the results q_{f1} and q_{f2} of their pointer position measurements through a public communication channel. In those instances where $q_{f1} + q_{f2} = 0$, Eve proceeds to measure σ_{3z}, and the result s_{3z} of this measurement will enable her to determine s_{2z} from (5.12), and hence she will also be able to determine s_{1z} since $s_{1z} = -s_{2z}$ in these cases. In this way Eve would be able to gain access to Alice and Bob's cryptographic key data.

However, Eve must ensure that, after her interception, the state $|\Phi_{123}\rangle$ in which she leaves the three-apparatus system is an eigenstate of $(Q_1 + Q_2)$; otherwise Alice and Bob will almost certainly find that $q_{f1} + q_{f2} \neq 0$, 2Δ, or -2Δ, which will immediately alert them to the presence of an eavesdropper. But since, from (5.11), $|\Phi_{123}\rangle$ is an eigenstate of $(P_2 - P_3)$, it cannot also be an eigenstate of $(Q_1 + Q_2)$ because $(Q_1 + Q_2)$ does not commute with $(P_2 - P_3)$. Hence, by preparing the apparatuses in the state $|\Phi_{123}\rangle$ Eve risks immediate discovery. Eve may instead attempt to prepare the apparatuses in a different state $|\Phi'_{123}\rangle$ which is an eigenstate of $(Q_2 + Q_3)$ but not an eigenstate of $(P_2 - P_3)$, and so could still be an eigenstate of $(Q_1 + Q_2)$. By doing this she would again hope to establish a correlation between q_{f2} and q_{f3}, and hence between s_{2z} and s_{3z}. However, $|\Phi'_{123}\rangle$ cannot be an eigenstate of $(P_1 - P_2)$ because $(Q_2 + Q_3)$ does not commute with $(P_1 - P_2)$. This means that, if she prepares the apparatuses in the state $|\Phi'_{123}\rangle$, Eve risks immediate detection if Alice and Bob carry out the first of the type 1 eavesdropping tests described earlier, i.e. if they decide to measure P_1 and P_2 instead of Q_1 and Q_2. On the other hand, if Alice and Bob use the second type 1 eavesdropper detection method and use two different kinds of apparatuses, Eve will not know the state of any apparatuses she intercepts, and so will risk destroying the initial entanglement of the legitimate apparatuses if she attempts to prepare the three-apparatus systems in suitable entangled states. This will once again show up in Alice and Bob's pointer measurements and so Eve risks immediate detection in this case also. We conclude that a type 2 eavesdropper is just as vulnerable to detection as a type 1 eavesdropper for the nonlocal measurement based quantum cryptography schemes we have described.

We end this section by briefly assessing how secure Alice and Bob's stored information is during the key-generation process, for the schemes we have described. For those schemes where Alice and Bob use a new pair of spin-$\frac{1}{2}$ particles for each nonlocal measurement (i.e. Schemes A and B in Section 4), they will in principle be able to store the entangled pairs created by successful nonlocal measurements, until the key is needed. Any raiding of Alice's and Bob's particle stores prior to the key-generation process will not, in these cases, yield any useful information. This feature is similar to the storage advantage of Ekert's scheme [14], in which Alice and Bob's particle pairs can in principle be maintained in the EPRB

tate until needed for the key. However, in the last of our cryptography schemes in Section 4 (Scheme C), where Alice and Bob's nonlocal measurements are all carried out on the same pair of particles, it will be necessary for them to perform their key-generating local spin measurements immediately after each successful nonlocal measurement. In this case their stored information will be classical and hence vulnerable to theft and/or duplication. In Bennett and Brassard's scheme [2] Alice's information is also classical and so is vulnerable in a similar way.

5 Conclusion

We have examined a number of quantum cryptography schemes which incorporate nonlocal measurements. These schemes contain a number of interesting features. All of the key data can be generated using a single alphabet; alternatively, all of the key data can be generated from a single pair of particles held by Alice and Bob.

The use of entangled apparatus states for which the correlated observables have continuous spectra leads to enhanced detectability of both straightforward ("type 1") and more sophisticated ("type 2") eavesdroppers. In both of these cases we have formulated a test where the eavesdropper will be revealed immediately after a single intercepted transmission. We have also described an alternative method for detecting eavesdroppers which is built into the key distribution process itself and obviates the requirement for a separate test. None of the potential cryptographic key data need be sacrificed in order to facilitate eavesdropper detection by either of these methods.

The cryptography schemes described in this paper are not the first applications of nonlocal measurements for quantum communication; previously a method using nonlocal measurements for teleportation of quantum states has been formulated [18]. So far, however, there have been few practical suggestions as to how applications such as these might be implemented in the laboratory. It is hoped that the work presented here will help to motivate further research in this field.

References

[1] S. Wiesner, SIGACT News **15**, 78 (1983).

[2] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175.

[3] J. S. Bell, *Physics* **1**, 195 (1964).

[4] A. Einstein, B. Podolsky and N. Rosen, *Phys. Rev.* **47**, 777 (1935).

[5] D. Bohm, *Quantum Theory* (Prentice Hall, Englewood Cliffs, NJ, 1951) pp. 611–623.

[6] Y. Aharonov and D. Z. Albert, *Phys. Rev.* **D 21**, 3316 (1980).

[7] Y. Aharonov and D. Z. Albert, *Phys. Rev.* **D 24**, 359 (1981).

[8] Y. Aharonov, D. Z. Albert and L. Vaidman, *Phys. Rev.* **D 34**, 1805 (1986).

[9] K. J. Blow and S. J. D. Phoenix, *J. Mod. Opt.* **40**, 33 (1993).

[10] C. H. Bennett, G. Brassard, and N. D. Mermin, *Phys. Rev. Lett.* **68**, 557 (1992).

[11] C. H. Bennett, *Phys. Rev. Lett.* **68**, 3121 (1992).

[12] A. K. Ekert *et al.*, *Phys. Rev.* **A 50**, 1047 (1994).

[13] B. Huttner *et al.*, *Phys. Rev.* **A 51**, 1863 (1995).

[14] A. K. Ekert, *Phys. Rev. Lett.* **67**, 661 (1991).

[15] C. H. Bennett and S. J. Wiesner, *Phys. Rev. Lett.* **69**, 2981 (1992).

[16] S. L. Braunstein, A. Mann, and M. Revzen, *Phys. Rev. Lett.* **68**, 3259 (1992).

[17] S. J. D. Phoenix, *Phys. Rev.* **A 48**, 96 (1993).

[18] L. Vaidman, *Phys. Rev.* **A 49**, 1473 (1994).

[19] C. H. Bennett *et al.*, *Phys. Rev. Lett.* **70**, 1895 (1993).

[20] S. Popescu and L. Vaidman, *Phys. Rev.* **A 49**, 4331 (1994).