Quantum Information and Computation, Vol. 6, No. 4&5 (2006) 336–350

QUANTUM INFORMATION PROCESSING WITH HYPERENTANGLED PHOTON STATES

S.P. WALBORN, M.P. ALMEIDA, P.H. SOUTO RIBEIRO
Instituto de Física, Universidade Federal do Rio de Janeiro, Caixa Postal 68528
Rio de Janeiro, RJ 21941-972, Brazil

C. H. MONKEN
Universidade Federal de Minas Gerais, Caixa Postal 702,
Belo Horizonte, MG 30123-970, Brazil

Received May 4, 2005
Revised March 15, 2006

We discuss quantum information processing with hyperentangled photon states - states entangled in multiple degrees of freedom. Using an additional entangled degree of freedom as an ancilla space, it has been shown that it is possible to perform efficient Bell-state measurements. We briefly review these results and present a novel deterministic quantum key distribution protocol based on Bell-state measurements of hyperentangled photons. In addition, we propose a scheme for a probabilistic controlled-not gate which operates with a 50 % success probability. We also show that despite its probabilistic nature, the controlled-not gate can be used for an efficient, nonlocal demonstration of the Deutsch algorithm using two separate photons.

Keywords: entanglement, quantum information, key distribution, quantum computation

Communicated by: I Cirac & H Zbinden

1 Introduction

It has been shown that quantum mechanics offers a novel solution to several problems in information processing. Quantum cryptography provides a secure method of sending classical information, while quantum computation may solve some complex computational problems. However, the fragility of the quantum state makes transmission, storage and processing of quantum information difficult.

An interesting aspect of the photon as a carrier of quantum information is that it is possible to create, with currently available techniques, "hyperentangled states" - multi-photon states entangled in multiple degrees of freedom [1]. Using spontaneous parametric down-conversion, it is possible to create entangled mulit-photon states in several degrees of freedom, including linear momentum [2], polarization [3, 4], time-bin [5], orbital angular momentum [6], transverse position and momentum [7, 8] and Hermite-Gaussian modes [9]. In all of these examples it is possible to create and manipulate single qubits and in some cases arbitrary dimensional qudits. The name "hyperentangled states" may be distasteful to some, as it may imply that there is some added resource at hand. In some respects, this is true, since it is possible to construct larger dimensional systems out of smaller systems. Consider the case of

two photons a and b entangled in the following form:

$$\begin{aligned} |\psi\rangle_{ab} &= \left|\psi^+\right\rangle_{12}\left|\psi^-\right\rangle_{34}, \\ &= \frac{1}{2}\left(|01\rangle_{12}+|10\rangle_{12}\right)\left(|01\rangle_{34}-|10\rangle_{34}\right) \\ &= \frac{1}{2}\left(|01\rangle_{12}|01\rangle_{34}-|01\rangle_{12}|10\rangle_{34}+|10\rangle_{12}|01\rangle_{34}-|10\rangle_{12}|10\rangle_{34}\right) \end{aligned} \tag{1}$$

Here qubits 1 and 3 are represented by two degrees of freedom of photon a and qubits 2 and 4 are represented by two degrees of freedom of photon b. The states $|\psi^{\pm}\rangle$ are two of the usual Bell states, which are given by

$$|\psi^{\pm}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle|1\rangle \pm |1\rangle|0\rangle\right) \tag{2}$$

$$|\phi^{\pm}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle|0\rangle \pm |1\rangle|1\rangle\right). \tag{3}$$

The state (1) can of course be rewritten as

$$|\psi\rangle_{ab} = \frac{1}{2}\left(|00\rangle_{13}|11\rangle_{24}-|01\rangle_{13}|10\rangle_{24}+|10\rangle_{13}|01\rangle_{24}-|11\rangle_{13}|00\rangle_{24}\right), \tag{4}$$

and defining $|00\rangle \equiv |0\rangle$, $|01\rangle \equiv |1\rangle$, $|10\rangle \equiv |2\rangle$, $|11\rangle \equiv |3\rangle$, gives

$$|\psi\rangle_{ab} = \frac{1}{2}\left(|03\rangle_{ab}-|12\rangle_{ab}+|21\rangle_{ab}-|30\rangle_{ab}\right), \tag{5}$$

which is a two qudit (dimension $D = 4$) antisymmetric singlet state [10]. It has been shown that these larger dimensional two-photon systems can be used for "all-or-nothing" violation of local realism [11] as well as efficient quantum cryptography [12]. Moreover, it has been shown that these hyperentangled states may be advantageous in certain quantum information tasks. There are several methods of using the additional degree of freedom provided by hyperentangled photon states to perform a complete Bell-state measurement [13, 14], a task that is at best 50% efficient with linear optics and single photon detectors [15, 16, 17]. In section 2 we briefly describe the experimental generation of hyperentangled photon states and in section 3 we describe the implementation of quantum logic gates on qubits encoded in the same photon. Using these basic ingredients, we then review a recent Bell-state measurement proposal in section 4 and discuss its utility for dense coding. In section 4.2 we show that this type of Bell-state measurement can be used to implement a novel "dense" quantum key distribution (QKD) scheme, which offers increased bit transmission rate as well as increased sensitivity to eavesdropping. Hyperentangled states of this form have also been used to realize quantum teleportation [18] and a destructive controlled-not (CNOT) gate between two photons has been implemented by teleportation [19, 20]. In section 5 we present a similar scheme for a hyperentangled CNOT gate which operates with a success rate of 1/2. We discuss the pros and cons of our scheme and show that our hyperentangled CNOT gate can be used to implement the two-qubit Deutsch algorithm on two separate photons. An interesting feature of this scheme is that the algorithm can then be implemented non-locally.

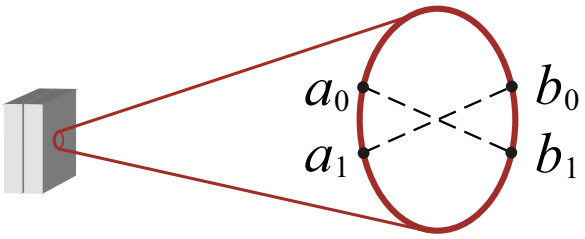

Fig. 1. A source of hyperentangled states using parametric down-conversion.

2 Hyperentangled states

Through parametric down-conversion, it is possible to create two or more hyperentangled photons [1]. Hyperentangled states of the form (1) have been experimentally created and characterized [21, 22]. A simple scheme based on the two type-I crystal source [4] is shown in Fig. 1. Polarization-entangled photons of the same wavelength can be collected around the rim of a cone (Fig. 1). In this source, the first crystal emits pairs of horizontally-polarized photons and crystal 2 emits pairs of vertically-polarized photons in superimposed emission cones. Phase-matching conditions guarantee that photon pairs are emitted on opposite sides of the cone, such as positions a_0 and b_1 or a_1 and b_0, for example. Let qubits 1 and 2 represent the polarization degree of freedom and qubits 3 and 4 correspond to momentum degree of freedom. The two-photon state corresponding to coincident photon pairs at positions a_0 and b_1 is $(|0\rangle_1 |0\rangle_2 + e^{i\varphi} |1\rangle_1 |1\rangle_2) |0\rangle_3 |1\rangle_4$, where horizontal (vertical) polarization represents the 0 (1) logical state. Similarly, the two-photon state corresponding to coincidences at a_1 and b_0 is $(|0\rangle_1 |0\rangle_2 + e^{i\varphi} |1\rangle_1 |1\rangle_2) |1\rangle_3 |0\rangle_4$. If the interaction region of both crystals lies entirely within a coherence volume of the pump laser beam, one can control the relative phase so that a polarization- and momentum-entangled state of the form $|\psi\rangle_{ab} = |\phi^+\rangle_{12} |\psi^-\rangle_{34}$ is created by selecting the photon pairs at the two sets of regions $a_0 b_1$ and $a_1 b_0$. One can adjust the phase so that the momentum state is $|\psi^+\rangle$. Half- and quarter-wave plates can be used to switch between the four polarization Bell-states [3]. It should be noted that because there are also vacuum and higher-order terms present with this source, a hyperentangled state is achieved only by post-selection: considering only those events which give two-photon coincidence detections.

3 Single photon quantum computing

There has been considerable work in quantum computation using optical qubits defined in multiple degrees of freedom of the same field [23, 24]. These implementations are physically unary realizations of quantum computation which are not scalable [25]. However, small-scale implementations may offer some advantages. For one, it is a simple matter to realize controlled logic operations deterministically. For example, if polarization and spatial mode of a photon are used to represent two qubits, a polarizing beam splitter can be used to perform a CNOT as illustrated in Fig. 2 a). Nesting the PBS among Hadamard gates (beam splitters and half-wave plates) switches the control and target qubits (Fig. 2 b) [26]. A much simpler implementation of the CNOT operation in b) can be implemented using a HWP in one optical

path (Fig. 2 c). The HWP should be oriented at 22.5° so as to swap horizontal and vertical polarization. A similar CNOT gate was performed using polarization and transverse spatial degrees of freedom [27].

Another consideration is that two-qubit gates involving more than one photon operate probabilistically, as will be discussed in further detail in section 5. To date the best gate operates with a theoretical efficiency of 1/4 [53, 56]. In some cases, the probabilistic nature of these gates does not present a problem. However, consider the simplest case of the Deutsch algorithm involving two qubits, which provides a speedup of 1/2 and requires a two-qubit controlled logic operation. Any speedup provided by quantum mechanics is lost due to inefficiency of the two-qubit gate. Using multiple degrees of freedom of the same photon, however, the two-qubit Deutsch algorithm can be implemented efficiently and deterministically [28].

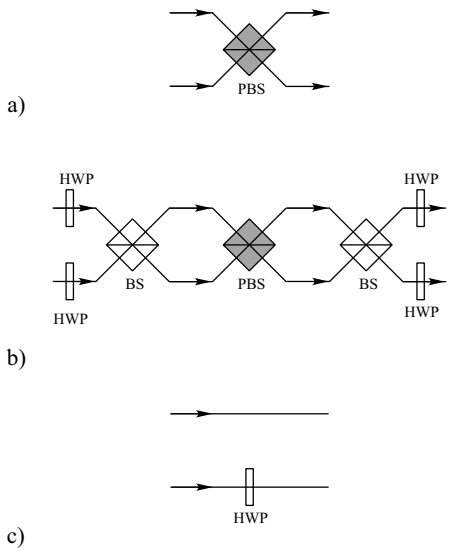

Fig. 2. Controlled operations between qubits defined by different degrees of freedom of the same photon can be implemented with simple linear optical elements. a) A polarizing beam splitter (PBS) implements a CNOT operation where the polarization controls the spatial mode (target) of the photon. b) Nesting the PBS among Hadamard rotations in both degrees of freedom implemented by half-wave plates (HWP) and 50-50 beam splitters (BS) switches the role of the control and target qubits. c) The CNOT operation in b) can also be implemented in a much simpler arrangement using only a HWP in one optical path.

4 Bell State Measurements

A Bell-state measurement (BSM) is a necessary step in many quantum information schemes, including quantum dense coding [29, 30], quantum teleportation [18, 31, 32] and entanglement swapping [31, 33, 34]. However, it has been proven that a complete BSM (distinguishing between the four states with 100% efficiency) is impossible using only linear operations and classical communication [15, 16, 17, 35]. In fact, Ghosh *et. al.* [35] have proven that, if only a single copy is provided, the best one can do is to discriminate between two Bell states. Likewise, Calsamiglia and Lütkenhaus [17] have shown that the maximum efficiency for a

linear Bell-state analyzer is 50%. It is possible to discriminate the four Bell states using nonlinear processes [36, 37, 38] or two-photon absorption [39, 40]. However, these methods suffer from low efficiency. It is also possible to implement a CNOT gate and consequently a Bell-state measurement using the teleportation-based quantum computation model proposed by Gottesman and Chuang [19] and further advanced by Knill, Laflamme and Milburn [50], which requires linear optics, photo-detectors and N ancillary photons. The success probability increases as $N^2/(N+1)^2$; approaching unity for large N. The difficulty with this method arises from the need for ancillary photons on demand. Currently, this is not possible for more than a few photons.

Recently, it has been shown that one can increase the efficiency of a Bell-state measurement by using hyperentangled states [13, 14, 42]. Utilizing the entanglement present in an additional auxiliary degrees of freedom, it is possible to perform a complete BSM. Due to the enlarged Hilbert space, this type of complete BSM is not restricted to the efficiency limits presented in [15, 16, 17, 35]. We will first briefly review the BSM scheme presented in Ref. [14] and then discuss application of this technique to dense coding and secure key distribution.

Consider hyperentangled product states of the form

$$|\psi\rangle_{ab} = |\mathsf{B}\rangle_{12} \otimes |\psi^+\rangle_{34}, \tag{6}$$

where again 1 and 3 refer to photon a and 2 and 4 refer to photon b. Here $|\mathsf{B}\rangle$ represents any one of the four Bell states given in Eqs. (2) and (3). Applying CNOT gates to qubits 1 and 3 and 2 and 4 respectively, where 1 and 2 are the control qubits and 3 and 4 are the target qubits, the state given in Eq. (6) transforms as

$$|\psi^\pm\rangle_{12} |\psi^+\rangle_{34} \longrightarrow |\psi^\pm\rangle_{12} |\phi^+\rangle_{34} \tag{7}$$

$$|\phi^\pm\rangle_{12} |\psi^+\rangle_{34} \longrightarrow |\phi^\pm\rangle_{12} |\psi^+\rangle_{34}. \tag{8}$$

Performing Hadamard transformations on qubits 1 and 2, we have

$$\begin{aligned}
|\psi^+\rangle_{12} |\phi^+\rangle_{34} &\longrightarrow |\phi^-\rangle_{12} |\phi^+\rangle_{34} \\
|\psi^-\rangle_{12} |\phi^+\rangle_{34} &\longrightarrow |\psi^-\rangle_{12} |\phi^+\rangle_{34} \\
|\phi^+\rangle_{12} |\psi^+\rangle_{34} &\longrightarrow |\phi^+\rangle_{12} |\psi^+\rangle_{34} \\
|\phi^-\rangle_{12} |\psi^+\rangle_{34} &\longrightarrow |\psi^+\rangle_{12} |\psi^+\rangle_{34}
\end{aligned} \tag{9}$$

It is easy to see that it is possible to discriminate between the four states Eq. (9) by simply measuring qubits 1-4 in the computational basis. Table 1 shows the appropriate measurement results for each Bell state. A quantum circuit diagram for this scheme is shown in Fig. 3. It is interesting to note that this BSM scheme can be implemented non-locally, provided the two parties can communicate classically.

4.1 Dense Coding

In quantum dense coding [29], Alice and Bob are able to transmit two bits of information in one quantum bit. To do so they each possess one photon of an entangled Bell-state ($|\psi^+\rangle$, for example). Since the reduced density matrix for each photon is $\mathsf{I}/2$, where I is the 2×2 identity matrix, there is no information present in either Alice or Bob's photons alone. Suppose that

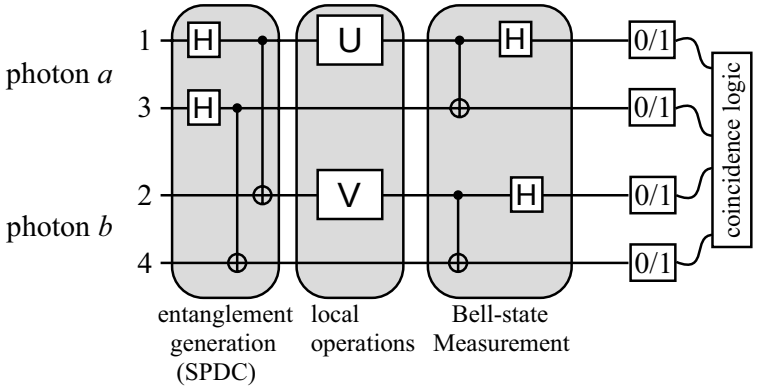

Fig. 3. Quantum circuit for hyperentangled Bell-state analysis. SPDC can be used to create hyperentangled photons. Single qubit operators U and V implement arbitrary local operations on qubits 1 and 2. Single photon logic operations are then used to distinguish between the four Bell states encoded into qubits 1 and 3, while qubits 2 and 4 form an ancilla space. The boxes "0/1" are detectors in the computational basis.

some time later, Alice wishes to send 2 bits of information to Bob. She first switches among the four Bell-states using local operations on her photon, and then sends it to Bob, who performs a Bell-state measurement on the photon pair, and retrieves Alice's message. Since there was no information present in Bob's photon, then the 2 bits of information was sent in Alice's photon. However, there is no information present in Alice's photon alone: all information is retrieved through correlations.

Using only linear optics, complete dense coding is impossible, since it is not possible to distinguish between the four Bell states using only linear optics [15, 16, 17]. In fact, the first experimental demonstration of dense coding [30] transmitted approximately 1.58 bits of information in Alice's photon and used symmetry of the two-photon state as an added resource. Using hyperentangled states and the BSM technique described above, it is possible to implement a "dense" coding protocol which transmits 2 bits per photon. However, each photon must carry two qubits. The fact that neither Alice's nor Bob's photons alone contain any information can be exploited to implement secure quantum key distribution protocols [44, 45, 46, 47, 48]. Here we provide a key distribution protocol using hyperentangled states.

4.2 Key Distribution

In section 4 we showed that an additional entangled state ($|\psi^+\rangle$ for example) in an auxilary degree of freedom can be used as an ancilla space to discriminate between the four Bell-

Table 1. Detection signature of Bell states.

initial state	measurement results
$\|\psi^+\rangle_{12}$	0000 or 0011 or 1100 or 1111
$\|\psi^-\rangle_{12}$	0100 or 0111 or 1000 or 1011
$\|\phi^+\rangle_{12}$	0010 or 0001 or 1110 or 1101
$\|\phi^-\rangle_{12}$	0110 or 0101 or 1010 or 1001

states. Here we show that states of the form (6) can be used for quantum key distribution. Two main goals in fundamental research in quantum cryptography are increasing the security and transmission rate of a cryptographic protocol. Below, we show that hyper-entangled photons can be used to achieve both of these objectives.

A schemtic of the key distribution protocol is illustrated in figure 4. Let $|\mathsf{B}_{ij}\rangle$ represent one of the four Bell states such that $|\mathsf{B}_{00}\rangle = |\psi^-\rangle$, $|\mathsf{B}_{01}\rangle = |\psi^+\rangle$, $|\mathsf{B}_{10}\rangle = |\phi^-\rangle$ and $|\mathsf{B}_{11}\rangle = |\phi^+\rangle$. Suppose that Alice and Bob share a pair of hyperentangled photons in the state $|\mathsf{B}_{00}\rangle_{12}\,|\psi^+\rangle_{34}$. Alice can perform local operations on one of her photons to transform $|\mathsf{B}_{00}\rangle$ to one of the four states $|\mathsf{B}_{ij}\rangle$. Thus, she can encode 2 bits of classical information into the shared hyperentangled pair. The key distribution protocol goes as follows:

1. Alice generates two random bits i and j and uses them to encode $|\mathsf{B}_{ij}\rangle_{12}\,|\psi^+\rangle_{34}$. She records each pair of random bits and keeps them secret.

2. Alice sends one photon of the hyperentangled pair to Bob.

3. Alice and Bob perform their respective parts of the BSM on the pair of hyperentangled photons as discussed in section 4. Alice (Bob) records the measurement results of qubits 1 and 3 (2 and 4).

4. Alice and Bob repeat the above steps N times.

5. Bob randomly chooses a fraction of his results and announces them publicly to Alice. Call this set of results $\{R_{\mathrm{check}}\}$.

6. Since Alice knows which state B_{ij} was sent in each case, she checks each of Bob's measurement results in $\{R_{\mathrm{check}}\}$ with her's to confirm that the correct set of measurements was obtained, and calculate the maximum amount of information available to an eavesdropper (see below).

7. Confident that an eavesdropper on the quantum channel does not have access to an excess of information, Alice publicly announces her set of results for all those measurements not publicly announced by Bob in $\{R_{\mathrm{check}}\}$. These results can then be used to construct the secret key.

8. Knowing both his and Alice's results, Bob knows which state B_{ij} was sent, and thus knows the secret key.

We note that the use of the ancilla space does not reduce the security of the key distribution protocol, since it is straightforward to check that in all cases the reduced density matrix of both Alice and Bob's photons is $\mathsf{I}_4/4$, where I_4 is the 4×4 identity matrix. Thus, no information can be obtained by *either* Alice or Bob revealing their measurement results.

Let us look briefly at the effects of an eavesdropper Eve. For simplicity, let us suppose that Eve measures every hyperentangled photon sent from Alice to Bob, and furthermore that she employs the same BSM detection system employed by Alice and Bob. Since in every case each of Bob's measurement results have an equal probability ($= 1/4$), Eve can essentially extract no information. Moreover, her presence will be detected during Alice and Bob's check procedure (step 6 above). As an example, suppose that Alice sends the state

$|\psi^+\rangle_{12}|\psi^+\rangle_{34}$ to Bob, and that Eve obtains measurement result 0_20_4. Furthermore, suppose that she employs a simple intercept-resend strategy: she sends a new photon in state $|0\rangle_2|0\rangle_4$ on to Bob. Bob and Alice's joint state is then $|1\rangle_1|0\rangle_2|1\rangle_3|0\rangle_4$. After the CNOT gates and Hadamard transformations, their joint state is $|0000\rangle + |0100\rangle - |1000\rangle - |1111\rangle$, where the qubit order 1-2-3-4 has been maintained. Comparing with the correct measurement results in Table 4 shows that 50% of the time Eve's eavesdropping will go unnoticed while the other 50% of the time Alice and Bob will detect the wrong state. The bit error rate (in the absence of noise) induced by the presence of Eve is 50%, which can be detected by Alice and Bob. We note that this is twice the error rate of the usual BB84 protocol, and equal to the upper limit of the error rate for any two-basis protocol using a d-dimensional alphabet [43].

In addition to increased security, there is an increased transmission rate, since each photon sent from Alice to Bob can be used to establish two bits of information. Furthermore, we stress that this protocol is deterministic, in the sense that every photon sent from Alice to Bob is used in either $\{R_{\text{check}}\}$ or as part of the secret random key. In other words, there is no basis reconciliation or sifting procedure, which would decrease the efficiency of the protocol.

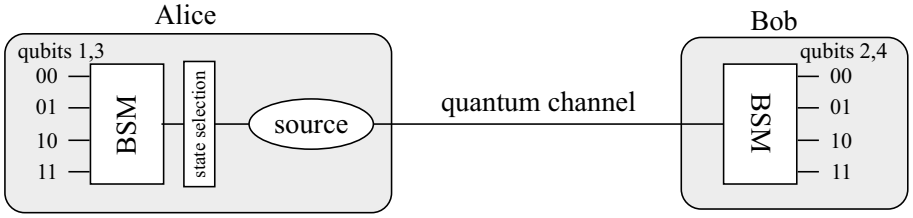

Fig. 4. Key distribution with hyperentangled Bell-states. "Source" represents the source of hyperentangled product states. BSM is the Bell-state measurement device discussed in section 4.

5 Two-photon quantum logic gates

It is well known that universal quantum computation can be performed using only single qubit rotations and two-qubit CNOT operations [26]. Using photons to encode qubits, it is a simple matter to implement single qubit rotations using phase shifters, beam splitters and wave plates. However, controlled logic operations involving two or more photons is a much more difficult task. Early proposals utilized non-linear materials to couple two or more fields [49] and consequently suffered from low efficiency. More recently, Knill, Laflamme and Milburn [50] (KLM) have shown that universal quantum computation can be performed using only linear optical elements, single-photon sources and photo-detectors. Their work utilizes the earlier results of Gottesman and Chuang [19], who showed that controlled quantum logic operations can be implemented using modified quantum teleportation procedures and ancillary entangled states. An interesting feature of the Gottesman-Chuang idea is that controlled quantum logic gates can be implemented non-locally, provided that parties involved share a certain amount of ancillary entangled states and can communicate classically [51, 52]. Several more recent proposals of two-photon controlled logic gates have followed [53, 54]. In all of these schemes the required nonlinearity is provided by post-selection of measurement results, and thus the gates operate probabilistically. For example, the (local) controlled-not (CNOT) gate proposed by Ralph *et. al* [54] and realized by O'brien *et. al* [55], which requires no ancillary photons,

operates with a success rate of 1/9, while the (non-local) CNOT gate proposed by Pittman *et. al* [53] and realized by Gasparoni *et. al* [56] has a success rate of 1/4, but requires an ancillary pair of entangled photons. Yoran and Reznik have proposed a method for deterministic quantum computation using single photons and components of the KLM scheme, however, their proposal requires entangled multi-photon "chain" states, which are currently difficult to realize experimentally [57].

Let us now present our hyperentangled CNOT gate. Consider an arbitrary two-photon hyperentangled state of the form

$$|\Psi_0\rangle = (\alpha\,|00\rangle_{12} + \beta\,|01\rangle_{12} + \gamma\,|10\rangle_{12} + \delta\,|11\rangle_{12})\,|\psi^-\rangle_{34}\,. \tag{10}$$

Here we show that the ancillary entangled state $|\psi^-\rangle_{34}$ can be used to implement a CNOT gate between qubits 1 and 2 with a 50% probability of success. We note that this gate is not scalable, since it requires post-selection of measurements on qubits 3 and 4. Qubits 3 and 4 are encoded into the same two photons as qubits 1 and 2, so measurement of qubits 3 and 4 inadvertently destroys qubits 1 and 2. Despite the fact that the gate presented here is probabilistic and non-scalable, there are still some interesting applications. For one, we show that our gate can be used to implement a two-photon version of the Deutsch algorithm. An interesting feature of this implementation is that due to the entanglement present in the initial state, the algorithm can be implemented non-locally.

For notational convenience, we will label two qubit gates with two subscripts, the first one is the control and the second is the target qubit. For example, CNOT_{13} is a CNOT gate where qubit 3 is flipped when qubit 1 is the logical 1 state. Single qubit gates will be labeled with a single subscript. For example, X_1 is the usual Pauli operator acting on qubit 1. For simplicity, we will use X_1 to represent $\mathsf{X}_1 \equiv \mathsf{X}_1 \otimes \mathsf{I}_2 \otimes \mathsf{I}_3 \otimes \mathsf{I}_4$.

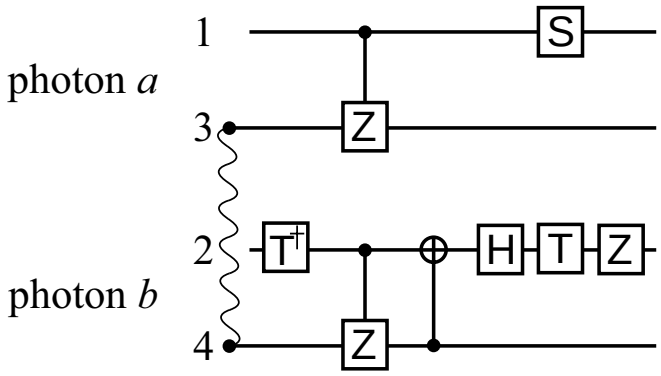

Fig. 5. Quantum circuit diagram of hyperentangled CNOT gate. All the quantum gates used are single photon (one and two qubit) gates and are defined in the text. The curvy line is used to show that qubits 3 and 4 are entangled.

We now present our hyperentangled CNOT gate. A quantum circuit diagram is shown in Fig. 5. The gate consists of single qubit operations and 3 controlled-logic operations on qubits encoded in the same photon. Thus, all the necessary gates can be implemented deterministically and are well within the bounds of current quantum optics experiments, as discussed in section 3.

We use the $\mathsf{T}^\dagger$ gate, where

$$\mathsf{T} \equiv \begin{pmatrix} e^{i\pi/4} & 0 \\ 0 & e^{-i\pi/4} \end{pmatrix}. \tag{11}$$

Applying this gate to the second qubit, the state $|\Psi_0\rangle$ becomes

$$\begin{aligned} \mathsf{T}_2^\dagger |\Psi_0\rangle &\longrightarrow |\Psi_1\rangle \\ &= (\alpha e^{-i\pi/4} |00\rangle_{12} + \beta e^{i\pi/4} |01\rangle_{12} + \gamma e^{-i\pi/4} |10\rangle_{12} + \delta e^{i\pi/4} |11\rangle_{12}) \left|\psi^-\right\rangle_{34}. \end{aligned} \tag{12}$$

We then perform a pair of controlled-Z gates (CZ) on qubits 1 and 3 and 2 and 4, where Z is the usual Pauli operator [26]. The state evolves as

$$\begin{aligned} \mathrm{CZ}_{13}\mathrm{CZ}_{24} |\Psi_1\rangle &\longrightarrow |\Psi_2\rangle \\ &= \alpha e^{-i\pi/4} |00\rangle_{12} \left|\psi^-\right\rangle_{34} - \beta e^{i\pi/4} |01\rangle_{12} \left|\psi^+\right\rangle_{34} \\ &+ \gamma e^{-i\pi/4} |10\rangle_{12} \left|\psi^+\right\rangle_{34} - \delta e^{i\pi/4} |11\rangle_{12} \left|\psi^-\right\rangle_{34}. \end{aligned} \tag{13}$$

The next step is a CNOT_{42} gate, which gives

$$\begin{aligned} \mathrm{CNOT}_{42} |\Psi_2\rangle &\longrightarrow |\Psi_3\rangle \\ &= \frac{\alpha}{\sqrt{2}} e^{-i\pi/4} (|01\rangle_{12} |01\rangle_{34} - |00\rangle_{12} |10\rangle_{34}) \\ &+ \frac{\beta}{\sqrt{2}} e^{i\pi/4} (-|00\rangle_{12} |01\rangle_{34} - |01\rangle_{12} |10\rangle_{34}) \\ &+ \frac{\gamma}{\sqrt{2}} e^{-i\pi/4} (|11\rangle_{12} |01\rangle_{34} + |10\rangle_{12} |10\rangle_{34}) \\ &+ \frac{\delta}{\sqrt{2}} e^{i\pi/4} (-|10\rangle_{12} |01\rangle_{34} + |11\rangle_{12} |10\rangle_{34}). \end{aligned} \tag{14}$$

Rewriting qubit 2 in the $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$ basis, the above expression becomes

$$\begin{aligned} |\Psi_3\rangle &= \frac{\alpha}{\sqrt{2}} e^{-i\pi/4} (|0+\rangle_{12} \left|\psi^-\right\rangle_{34} - |0-\rangle_{12} \left|\psi^+\right\rangle_{34}) \\ &- \frac{\beta}{\sqrt{2}} e^{i\pi/4} (|0-\rangle_{12} \left|\psi^-\right\rangle_{34} + |0+\rangle_{12} \left|\psi^+\right\rangle_{34}) \\ &- \frac{\gamma}{\sqrt{2}} e^{-i\pi/4} (|1-\rangle_{12} \left|\psi^-\right\rangle_{34} - |1+\rangle_{12} \left|\psi^+\right\rangle_{34}) \\ &- \frac{\delta}{\sqrt{2}} e^{i\pi/4} (|1+\rangle_{12} \left|\psi^-\right\rangle_{34} + |1-\rangle_{12} \left|\psi^+\right\rangle_{34}). \end{aligned} \tag{15}$$

Performing a Hadamard rotation H_2 rotates qubit 2 back to the computational basis, which gives

$$\begin{aligned} |\Psi_4\rangle &= \frac{\alpha}{\sqrt{2}} e^{-i\pi/4} (|00\rangle_{12} \left|\psi^-\right\rangle_{34} - |01\rangle_{12} \left|\psi^+\right\rangle_{34}) \\ &- \frac{\beta}{\sqrt{2}} e^{i\pi/4} (|01\rangle_{12} \left|\psi^-\right\rangle_{34} + |00\rangle_{12} \left|\psi^+\right\rangle_{34}) \\ &- \frac{\gamma}{\sqrt{2}} e^{-i\pi/4} (|11\rangle_{12} \left|\psi^-\right\rangle_{34} - |10\rangle_{12} \left|\psi^+\right\rangle_{34}) \\ &- \frac{\delta}{\sqrt{2}} e^{i\pi/4} (|10\rangle_{12} \left|\psi^-\right\rangle_{34} + |11\rangle_{12} \left|\psi^+\right\rangle_{34}). \end{aligned} \tag{16}$$

Using the gates $\mathsf{S}_1 \otimes \mathsf{T}_2$, where

$$\mathsf{S} \equiv \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \tag{17}$$

results in

$$\begin{aligned} |\Psi_5\rangle &= \frac{1}{\sqrt{2}}(\alpha\,|00\rangle_{12} - \beta\,|01\rangle_{12} - \gamma\,|11\rangle_{12} + \delta\,|10\rangle_{12})\,|\psi^-\rangle_{34} \\ &+ \frac{i}{\sqrt{2}}(\alpha\,|01\rangle_{12} - \beta\,|00\rangle_{12} + \gamma\,|10\rangle_{12} - \delta\,|11\rangle_{12})\,|\psi^+\rangle_{34}. \end{aligned} \tag{18}$$

A final Z_2 gate gives the required result:

$$\begin{aligned} |\Psi_6\rangle &= \frac{1}{\sqrt{2}}(\alpha\,|00\rangle_{12} + \beta\,|01\rangle_{12} + \gamma\,|11\rangle_{12} + \delta\,|10\rangle_{12})\,|\psi^-\rangle_{34} \\ &- \frac{i}{\sqrt{2}}(\alpha\,|01\rangle_{12} + \beta\,|00\rangle_{12} - \gamma\,|10\rangle_{12} - \delta\,|11\rangle_{12})\,|\psi^+\rangle_{34}. \end{aligned} \tag{19}$$

Inspection shows that post-selecting the $|\psi^-\rangle_{34}$ portion of the state (19) results in a CNOT operation on qubits 1 and 2. Similarly, post-selecting the $|\psi^+\rangle_{34}$ portion results in the $\mathsf{Z}_1\mathsf{X}_1\mathrm{CNOT}_{12}\mathsf{X}_1$ gate up to a global phase. $\mathsf{X}_1\mathrm{CNOT}_{12}\mathsf{X}_1$ is a logic operation similar to the usual CNOT gate, however the target bit is flipped when the control is in the logical 0 state. In summary, the CNOT gate is composed of the following sequence of logic operations: (*i*) single-qubit $\mathsf{T}_2^\dagger$ gate, (*ii*) (single photon controlled gates) controlled$-\mathsf{Z}_{13} \otimes$ controlled$-\mathsf{Z}_{24}$, (*iii*) (single photon) CNOT_{42}, (*iv*) single qubit Hadamard gate H_2, (*v*) single qubit S_1 and T_2 gates, (*vi*) single qubit Z_2 gate.

The hyperentangled CNOT gate has a success probability of 1/2. However, despite the fact that the gate is probabilistic, we will show that it can be used to implement a two-photon version of the Deutsch algorithm deterministically.

5.1 Deutsch Algorithm

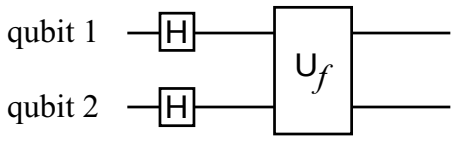

Fig. 6. Quantum circuit used to implement the Deutsch algorithm.

A simple example of the utility of the hyperentangled CNOT gate is the experimental implementation of Deutsch's algorithm [59, 60], one of the first examples of a quantum algorithm. The general problem is as follows. Suppose that one is in possession of a black box which takes a bit x into another bit $f(x)$. There are four possible outcomes: two corresponding to each of the two possible input bits 0 and 1. Now suppose that it would suffice to know if f is constant: $f(0) = f(1)$ or balanced: $f(0) \neq f(1)$. Obviously, to characterize the function f using classical computation requires two black-box computations, one to compute $f(0)$ and one to compute $f(1)$. However, as Deutsch showed, using quantum computation we can run

Table 2. Controlled logic operations U_f and U'_f associated to the possible values of $f(x)$.

$f(x)$	U_f
$f(0) = f(1) = 0$ (constant)	$\mathsf{I}_1 \otimes \mathsf{I}_2$
$f(0) = f(1) = 1$ (constant)	$\mathsf{I}_1 \otimes \mathsf{X}_2$
$f(0) = 0, f(1) = 1$ (balanced)	CNOT_{12}
$f(0) = 1, f(1) = 0$ (balanced)	$\mathsf{X}_1\mathrm{CNOT}_{12}\mathsf{X}_1$

the black box only one time. To do so requires a quantum oracle operator which implements the unitary transformation

$$\mathsf{U}_f \left|x\right\rangle \left|y\right\rangle \longrightarrow \left|x\right\rangle \left|y \oplus f(x)\right\rangle . \tag{20}$$

In order for U_f to implement $f(x)$ and still be unitary, it is necessary that U_f act on two qubits. However, we note that $f(x)$ is evaluated for only one input qubit. In general, implementation of U_f is non trivial, since it is a controlled logic operation. Table 2 shows the controlled logic operations U_f required for the possible values of $f(x)$. Using the quantum circuit shown in Fig. 6, it is a simple matter to show that the initial state $\left|0\right\rangle_1 \left|1\right\rangle_2$ evolves as [26]

$$\begin{aligned} \left|\Phi\right\rangle &= \mathsf{U}_f \mathsf{H}_1 \mathsf{H}_2 \left|0\right\rangle_1 \left|1\right\rangle_2 \\ &= \frac{1}{\sqrt{2}} \left[(-1)^{f(0)} \left|0\right\rangle_1 + (-1)^{f(1)} \left|1\right\rangle_1\right] \left|-\right\rangle_2 . \end{aligned} \tag{21}$$

If $f(0) = f(1)$, we have

$$\left|\Phi\right\rangle = \pm \left|+\right\rangle_1 \left|-\right\rangle_2 , \tag{22}$$

while if $f(0) \neq f(1)$ then

$$\left|\Phi\right\rangle = \pm \left|-\right\rangle_1 \left|-\right\rangle_2 . \tag{23}$$

Thus, measuring qubit 1 in the $\left|\pm\right\rangle$ basis provides information as to whether the function f is constant or balanced in only one run of the quantum black box operator U_f.

We will now show that the CNOT gate described in section 5 can be used to implement the Deutsch algorithm deterministically, with 100% success probability. If the initial hyperentangled state is $\left|\Psi_i\right\rangle = \left|0\right\rangle_1 \left|1\right\rangle_2 \left|\psi^-\right\rangle_{34}$, implementing the initial H_1 and H_2 gates along with the four possible values of the U_f operator listed in Table 2 gives the following output states:

$$\left|\Psi_{\mathrm{con}}\right\rangle = \pm \left|+\right\rangle_1 \left|-\right\rangle_2 \left|\psi^-\right\rangle_{34} , \tag{24}$$

if $f(x)$ is constant and

$$\left|\Psi_{\mathrm{bal}}\right\rangle = \pm \frac{1}{\sqrt{2}} \left|-\right\rangle_1 \left|-\right\rangle_2 \left|\psi^-\right\rangle_{34} \pm \frac{i}{\sqrt{2}} \left|+\right\rangle_1 \left|-\right\rangle_2 \left|\psi^+\right\rangle_{34} , \tag{25}$$

if $f(x)$ is balanced. Detecting qubit 1 in the $\left|+\right\rangle$ state and qubits 3 and 4 in the $\left|\psi^-\right\rangle$ state indicates that $f(x)$ is constant while detecting qubit 1 in the $\left|-\right\rangle$ state and qubits 3 and 4 in the $\left|\psi^-\right\rangle$ state *or* qubit 1 in the $\left|+\right\rangle$ state and qubits 3 and 4 in the $\left|\psi^+\right\rangle$ state implies that $f(x)$ is balanced. Thus, despite the fact that the CNOT gate operates probabilistically, the Deutsch algorithm can be implemented deterministically.

It is interesting to notice that the Deutsch algorithm can in principle be implemented non-locally, provided that it is possible to implement a non-local oracle operator U_f. Using

the CNOT gate proposed in section 5, all operations in U_f are single-photon operations. Thus, a non-local oracle can easily be constructed provided the two parts (one which operates on photon a and one which operates on photon b) can communicate classically. The cost of a non-local oracle is 2 bits of classical communication, since it is necessary to determine the operator U_f, which can take one of four values.

6 Conclusion

Hyperentangled multi-photon states can be used to construct larger dimensional systems. Here we have shown some possible applications of these types of states to quantum information tasks such as Bell-state measurements and quantum dense coding. We have proposed a quantum key distribution protocol based on Bell-state measurement of hyperentangled states, as well as a two-photon controlled-not (CNOT) gate which operates probabilistically with a success rate of 50%. Despite its probabilistic nature, we have shown that this gate can be used to implement a two-photon version of the Deutsch algorithm. A two-photon implementation may be interesting in quantum communication as it can be realized non-locally. Experimental realization of this protocol is well within the bounds of current quantum optics experiments and is underway in our laboratory.

Acknowledgements

Financial support was provided by Brazilian agencies CNPq, PRONEX, CAPES, FAPERJ, FUJB and the Instituto do Milênio de Informação Quântica.

References

1. P. G. Kwiat (1997), *Hyperentangled states*, J. Mod. Optics, 44, 2173–2184.
2. J.G. Rarity and P.R. Tapster (1990), *Experimental Violation of Bell's Inequality Based on Phase and Momentum*, Phys. Rev. Lett., 64, 2495.
3. Paul G. Kwiat, Klaus Mattle, Harald Weinfurter, Anton Zeilinger, Alexander V. Sergienko, and Yanhua Shih (1995), *New High-Intensity Source of Polarization-Entangled Photon Pairs*, Phys. Rev. Lett., 75, 4337.
4. Paul G. Kwiat, Edo Waks, Andrew G. White, Ian Appelbaum, and Phillipe H. Eberhard (1999), *Ultrabright source of polarization-entangled photons*, Phys. Rev. A., 60, R773.
5. P.R. Tapster, J.G. Rarity, and P.C.M. Owens (1994), *Violation of Bell-s Inequality over 4 km of Optical Fiber*, Phys. Rev. Lett., 73, 1923.
6. Alois Mair, Alipasha Vaziri, Gregor Weihs, and Anton Zeilinger (2001), *Entanglement of the orbital angular momentum states of photons*, Nature, 412, 313.
7. John C. Howell, Ryan S. Bennink, Sean J. Bentley, and R. W. Boyd (2004), *Realization of the Einstein-Podolsky-Rosen Paradox Using Momentum- and Position-Entangled Photons from Spontaneous Parametric Down Conversion*, Phys. Rev. Lett. 92, 210403.
8. Milena D'Angelo, Yoon-Ho Kim, Sergei P. Kulik, and Yanhua Shih (2004), *Identifying Entanglement Using Quantum Ghost Interference and Imaging*, Phys. Rev. Lett. 92, 23360.
9. S. P. Walborn, S. Pádua, and C. H. Monken (2005). *Conservation and entanglement of Hermite-Gaussian modes in parametric down-conversion*, quant-ph/0407216.
10. Adán Cabello (2003), *Supersinglets*, J. Mod. Optics, 50, 6–7.
11. Zeng-Bing Chen, Jian-Wei Pan, Yong-De Zhang, C. Brukner, and Anton Zeilinger (2003), *All-Versus-Nothing Violation of Local Realism for Two Entangled Photons*, Phys. Rev. Lett., 90, 160408.

12. Zeng-Bing Chen, Qiang Zhang, Xiao-Hui Bao, Jörg Schiedmayer, and Jian-Wei Pan (2005, *Deterministic and Efficient Quantum Cryptography Based on Bell's Theorem*, quant-ph/0501171.
13. Paul G. Kwiat and Harald Weinfurter (1998), *Embedded Bell-state analysis*, Phys. Rev. A, 58, R2623.
14. S. P. Walborn, S. Pádua, and C. H. Monken (2003), *Hyperentanglement-assisted Bell-state analysis*, Phys. Rev. A, 68, 042313.
15. Lev Vaidman and Nadav Yoran (1999), *Methods for reliable teleportation*, Phys. Rev. A, 59, 116.
16. N. Lütkenhaus, J. Calsamiglia, and K.-A. Suominen (1999), *Bell measurements for teleportation*, Phys. Rev. A, 59, 3295.
17. J. Calsamiglia and N. Lütkenhaus (2001), *Maximum efficiency of a linear-optical Bell-state analyzer*, Appl. Phys. B, 72, 67–71.
18. D. Boschi, S. Branca, F. DeMartini, L. Hardy, and S. Popescu (1998), *Experimental Realization of Teleporting an Unknown Pure Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels*, Phys. Rev. Lett., 80, 1121.
19. Daniel Gottesman and Isaac L. Chuang (1999), *Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations*, Nature, 402, 390.
20. Yun-Feng Huang, Xi-Feng Ren, Yong-Sheng Zhang, Lu-Ming Duan, and Guang-Can Guo (2004), *Experimental Teleportation of a Quantum Controlled-*NOT *Gate*, Phys. Rev. Lett., 93, 240501.
21. C. Cinelli, M. Barbieri, F. De Martini, and P. Mataloni (2004). *Experimental realization of hyperentangled two-photon states*, quant-ph/0406148.
22. Julio T. Barreiro, Nathan K. Langford, Nicholas A. Peters, Paul G. Kwiat (2005), *Generation of Hyper-entangled Photon Pairs*, Phys. Rev. Lett., 95, 260501.
23. N. J. Cerf, C. Adami, and P. Kwiat (1998), *Optical simulation of quantum logic*, Phys. Rev. A, 57, R1477.
24. Berthold-Georg Englert, Christian Kurtsiefer, and Harald Weinfurter (2003), *Universal unitary gate for single-photon two-qubit states*, Phys. Rev. A, 63, 032303.
25. Robin Blume-Kohout, Carlton M. Caves, and Ivan H. Deutsch (2002), *Climbing Mount Scalable, Physical Resource Requirements for a Scalable Quantum Computer*, Foundations of Physics, 32, 1641.
26. M.A. Nielsen and I.L. Chuang. *Quantum Computation and Quantum Information.* Cambridge, Cambridge (2000).
27. Marco Fiorentino and Franco N. C. Wong (2004), *Deterministic Controlled-NOT Gate For Single-Photon Two-Qubit Quantum Logic*, Phys. Rev. Lett. 93, 070502.
28. A. N. de Oliveira, S. P. Walborn, and C. H. Monken (2005), *Implementation of the Deutsch Algorithm using Polarization and Transverse Modes*, J. of Opt. B: Quantum and Semiclass. Opt. 7 (2005) 288292.
29. C.H. Bennett and S.J. Weisner (1992), *Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states*, Phys. Rev. Lett., 69, 2881.
30. Klaus Mattle, Harald Weinfurter, P.G. Kwiat, and Anton Zeilinger (1996), *Dense Coding in Experimental Quantum Communication*, Phys. Rev. Lett., 76, 4656.
31. C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wooters (1993), *Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels*, Phys. Rev. Lett., 70, 1895.
32. D. Bouwmeester, J. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger (1997), *Experimental quantum teleportation*, Nature, 390, 575.
33. Jian-Wei Pan, Dik Bouwmeester, Harald Weinfurter, and Anton Zeilinger (1998), *Experimental Entanglement Swapping, Entangling Photons That Never Interacted*, Phys.Rev. Lett., 80, 3891.
34. Thomas Jennewein, Gregor Weihs, Jian-Wei Pan, and Anton Zeilinger (2002), *Experimental Nonlocality Proof of Quantum Teleportation and Entanglement Swapping*, Phys. Rev. Lett., 88, 017903–1.
35. Sibasish Ghosh, Guruprasad Kar, Anirban Roy, Aditi Sen(De), and Ujjwal Sen (2001), *Distinguishability of Bell States*, Phys. Rev. Lett., 87, 277902–1.

36. M. G. A. Paris and M. B. Plenio and S. Bose and D. Jonathan and G. M. D' Ariano (2000), *Optical Bell Measurement by Fock Filtering*, Phys. Lett. A, 273, 153.
37. Y.-H Kim, S. P. Kulik and Y. Shih (2001), *Quantum Teleportation of a Polarization State with a Complete Bell State Measurement*, Phys. Rev. Lett., 86, 1370.
38. Kae Nemoto and W. J. Munro (2004), *Nearly Deterministic Linear Optical Controlled-NOT Gate*, Phys. Rev. Lett., 93, 250502.
39. M.O. Scully, B.-G. Englert, and C.J. Bednar (1999), *Two-Photon Scheme for Detecting the Bell Basis Using Atomic Coherence*, Phys. Rev. Lett., 83 4433.
40. E. Del Re, B. Crosignani, and P. DiPorto (2000), *Scheme for Total Quantum Teleportation*, Phys. Rev. Lett., 84, 2989.
41. J. D. Franson, B.C. Jacobs, T.B. Pittman (2004),*Quantum Computing Using Single Photons and the Zeno Effect, quant-ph/0408097.*
42. *S. P. Walborn, A. N. de Oliveira, S. Pádua, and C. H. Monken (2003),* Optical Bell-state analysis in the coincidence basis, *Europhys. Lett, 62, 161–167.*
43. *Mohamed Bourennane, Anders Karlsson, and Gunnar Björk (2001),* Quantum key distribution using multilevel encoding , *Phys. Rev. A, 64, 012306.*
44. *Adán Cabello (2000),* Quantum Key Distribution in the Holevo Limit, *Phys. Rev. Lett., 85, 5635.*
45. *G. L. Long and X. S. Liu (2002),* Theoretically efficient high-capacity quantum-key-distribution scheme, *Phys. Rev. A., 65, 032302.*
46. *Kim Boström and Timo Felbinger (2002),* Deterministic Secure Direct Communication Using Entanglement, *Phys. Rev. Lett., 89, 187902.*
47. *Antoni Wójcik (2003),* Eavesdropping on the "Ping-Pong" Quantum Communication Protocol, *Phys. Rev. Lett., 90, 157901.*
48. *I. P. Degiovanni, I. Ruo Berchera, S. Castelletto, M. L. Rastello, F. A. Bovino, A. M. Colla, and G. Castagnoli (2004),* Quantum dense key distribution, *Phys. Rev. A, 69, 032310.*
49. *G. J. Milburn (1989),* Quantum optical Fredkin gate, *Phys. Rev. Lett., 62, 2124–2127.*
50. *E. Knill, R. Laflamme, and G. J. Milburn (2001),* A scheme for efficient quantum computation with linear optics, *Nature, 409, 46–52.*
51. *J. Eisert, K. Jacobs, P. Papadopoulos and M. B. Plenio (2000),* Optimal local implementation of nonlocal quantum gates, *Phys. Rev. A, 62, 052317.*
52. *Daniel Collins, Noah Linden and Sandu Popescu (2001),* Nonlocal content of quantum operations, *Phys. Rev. A, 64, 032302.*
53. *T. B. Pittman, B. C. Jacobs, and J. D. Franson (2001),* Probabilistic quantum logic operations using polarizing beam splitters, *Phys.Rev. A, 64, 062311.*
54. *T. C. Ralph, N. K. Langford, T. B. Bell, and A. G. White (2002),* Linear optical controlled-NOT gate in the coincidence basis, *Phys. Rev. A, 65, 062324.*
55. *J. L. O'Brien, G. J. Pryde, A. G. White, T. C. Ralph, and D. Branning (2003),* Demonstration of an all-optical quantum controlled-NOT gate, *Nature, 426, 264.*
56. *Sara Gasparoni, Jian-Wei Pan, Philip Walther, Terry Rudolph, and Anton Zeilinger (2004),* Realization of a Photonic Controlled-NOT Gate Sufficient for Quantum Computation, *Phys.Rev. Lett., 93, 020504.*
57. *N. Yoran and B. Reznik (2003),* Determinisitc Linear Optics Quantum Computation with Single Photon Qubits, *Phys. Rev. Lett., 91, 037903.*
58. *G. J. Pryde, J. L. O'Brien, A. G. White, S. D. Bartlett, and T. C. Ralph (2004),* Measuring a Photonic Qubit without Destroying It, *Phys.Rev. Lett., 92, 190402.*
59. *D. Deutsch (1985),* Quantum theory, the Church-Turing Principle and the universal quantum computer, *Proc. R. Soc. Lond. A, 400, 97–117.*
60. *D. Deutsch (1989),* Quantum computational networks, *Proc. R. Soc. Lond. A, 425, 73–90.*