Quantum state engineering with ququarts: Application for deterministic QKD protocol


1 Faculty of Physics, Moscow State University - Russia
2 International Islamic University Malaysia - Kuala Lumpur, Malaysia
3 MIMOS Berhad - Kuala Lumpur, Malaysia

received 3 April 2009; accepted in final form 25 June 2009
published online 24 July 2009

PACS 03.67.Dd – Quantum cryptography and communication security
PACS 42.50.Dv – Quantum state engineering and measurements
PACS 03.67.Hk – Quantum communication

Abstract – We discuss the proof-of-principle demonstration of the extended deterministic Quantum Key Distribution (QKD) protocol based on ququarts. The experimental realization is based on the polarization degrees of freedom of two-mode biphotons, making the process of state preparation, transformation and measurement rather simple. The scheme uses only single nonlinear crystal for biphoton generation and linear optical elements for their following transformation and can be used as a base for further practical applications.

Copyright © EPLA, 2009

Introduction. – Unconditional security of QKD is limited in practical implementations by technical imperfections, such as non-perfect detectors efficiency and losses in the communication channel [1]. For example, in the standard BB84 protocol the key distribution is proven to be secure if the total quantum bit error rate (QBER) is less than approximately 11% [2]. In practice that results in limitations on the distance over which the secure communication can be established. One can look for a solution of the problem in different ways. The first one is straightforward and “technical” — it is to improve technical characteristics of the equipment used: increase detectors quantum efficiency, reduce losses in the channel and dark noise of the detectors, etc. The other way is a “physical” one and relies on properties of the physical system used to encode the information. One of the possible solutions following this way is to increase dimensionality of the system where information is encoded or/and to increase the number of bases used in the protocol [3].

Following this line of research, one faces the necessity to experimentally prepare, transform and measure the states of quantum systems with Hilbert space of more than two dimensions (qudits). In other words, one comes to, the so-called, “quantum state engineering” with qudits, an important branch for the whole quantum information science. Optical realizations of qudits are obviously preferable for the purposes of QKD, and much effort was made recently to study the properties of such systems [4–6]. Here we would like to stress on one of possible realizations of optical qudits, which turned out to be useful for quantum communication. It is the, so-called polarization ququarts, i.e. the four-dimensional optical qudits implemented using the polarization degrees of freedom of single-beam biphotons. This realization of ququarts seems to be promising, because the usage of polarization degrees of freedom allows one to perform unitary state transformations with linear optical elements. The tools for arbitrary polarization ququart state generation are developed in [6], giving the experimentalist a wide range of opportunities for state engineering. The way to realize a direct extension of BB84 protocol with polarization ququarts was discussed in [5]. It was shown that the polarization ququarts are easily controllable and the experimental scheme to distinguish the orthogonal states for different bases deterministically was proposed.

In this letter we discuss the implementation of polarization ququarts in the other group of QKD protocols, the deterministic ones. The first protocol of this kind, called “Ping-Pong” was proposed in [7] and, although proven to be insecure [8,9], gave rise to an elegant modification discussed in [10] and referred to as LM05. Except for the improved key transfer rate due to its deterministic nature, LM05 turned out to be more resilient to a wide class of individual attacks than standard BB84 [11].
The proof-of-principle experimental tests of LM05 were reported in [12].

The extension of LM05 involving a larger number of bases was recently proposed in [13]. This protocol, using 6 states out of three bases, which we will refer to as 6DP, seems to be more secure with respect to LM05 in the same way as BB84 extensions are more secure than the original one [3]. It turns out, that such extension requires two-qubit encoding, which makes polarization ququarts a natural object for the implementation of the protocol.

6DP protocol. – Let us first briefly describe the ideas underlying the LM05 protocol to make the notion of a deterministic QKD clearer. Let \( X, Y, Z \) be the Pauli matrices:

\[
X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},
\]

and \( |x_{\pm}\rangle, |y_{\pm}\rangle, |z_{\pm}\rangle \) their respective eigenvectors. We will identify these states with the polarization states of photons (circularly, diagonally and horizontally/vertically polarized, respectively). The protocol works as follows (fig. 1): the photon in one of the \( X \) or \( Z \) eigenstates is prepared at Bob’s side and sent to Alice. Alice performs a unitary polarization transformation described by one of the operators, either \( I \) (identity) or \( iY \) (bit-flip), and sends the photon back to Bob. In the first case the state of the qubit remains unchanged while in the second case it is changed to an orthogonal one. Identifying the identity of the qubit remains unchanged while in the second case it is flipped and the encoded pair of booleans.

<table>
<thead>
<tr>
<th>( I )</th>
<th>( X )</th>
<th>( iY )</th>
<th>( Z )</th>
</tr>
</thead>
<tbody>
<tr>
<td>(</td>
<td>y_{\pm}\rangle,</td>
<td>z_{\pm}\rangle )</td>
<td>(</td>
</tr>
<tr>
<td>(</td>
<td>x_{\pm}\rangle,</td>
<td>z_{\pm}\rangle )</td>
<td>(</td>
</tr>
<tr>
<td>(</td>
<td>x_{\pm}\rangle,</td>
<td>y_{\pm}\rangle )</td>
<td>(</td>
</tr>
<tr>
<td>(</td>
<td>x_{\pm}\rangle,</td>
<td>y_{\pm}\rangle )</td>
<td>(</td>
</tr>
</tbody>
</table>

Encoded value 00 01 10 11

Table 1: 6DP protocol: the possible combinations of qubits sent by Bob, the operations on them with the resulting number of bits flipped and the encoded pair of booleans.

Experimental realization. – In the proposed implementation 6 states from table 1 are realized as polarization states of photon pairs generated in SPDC process. SPDC may be phenomenologically described as a process of spontaneous decay of a pump photon into a pair of correlated photons with lower frequency due to nonzero quadratic susceptibility [15]. We will consider the, so-called, type-I SPDC, when pump is extraordinary and downconverted photons are ordinary waves in the birefringent nonlinear crystal. Let us choose the orientation of the crystal axis and the polarization of the pump to be horizontal, so both photons would have vertical polarization. In this case the state of the downconverted field, calculated in the first order of perturbation theory has the following form:

\[
|\Psi\rangle = |\text{vac}\rangle + \int dk_1 dk_2 \Psi(k_1, k_2)|V\rangle_1|V\rangle_2.
\]

Here \( k_1, k_2 \) are wave vectors of the downconverted photons and \( \Psi(k_1, k_2) \) is the biphoton amplitude characterizing the frequency-angular spectrum of SPDC radiation. In the stationary case the photon’s frequencies satisfy the condition \( \omega_1 + \omega_2 = \omega_p \) due to the energy conservation. After fixing the frequency-angular degrees of freedom (by using narrow-band filters and pinholes) and postselection induced by coincidence measurement eliminating the vacuum component, the polarization state of the biphoton can be described by a state vector \( |\Psi\rangle = |V_1 V_2\rangle \), where indexes 1,2 correspond to different wavelengths and/or different propagation directions. An arbitrary biphoton polarization state can be expressed as a ququart:

\[
|\Psi\rangle = c_1|1\rangle + c_2|2\rangle + c_3|3\rangle + c_4|4\rangle = c_1|H_1 H_2\rangle + c_2|H_1 V_2\rangle + c_3|V_1 H_2\rangle + c_4|V_1 V_2\rangle.
\]

Here \( c_j = \alpha_j e^{i\phi_j} \) are complex probability amplitudes, whereas polarization states are produced by corresponding creation operators acting upon the vacuum state: \( |H_i\rangle = a_i|0\rangle, |V_i\rangle = b_i|0\rangle, \) \( i = 1, 2 \). The choice of above representation in terms of product polarization states (2) is rather natural. Indeed each basic state in (2)
can be directly achieved in SPDC process from a single crystal. We will identify the states of table 1 with polarization states of photons as follows:

\[ |z^+\rangle = |H\rangle, \quad |z^-\rangle = |V\rangle, \]
\[ |x^+\rangle = |D\rangle, \quad |x^-\rangle = |A\rangle, \quad (3) \]
\[ |y^+\rangle = |R\rangle, \quad |y^-\rangle = |L\rangle. \]

According to the protocol, we should be able to prepare the 6 states of the form

\[ |D_1 R_2\rangle, |R_1 D_2\rangle, |D_1 V_2\rangle, |V_1 D_2\rangle, |R_1 V_2\rangle, |V_1 R_2\rangle \quad (4) \]

(on Bob’s side), and to apply the transformations, described by Pauli operators \( X, Y, Z \) (on Alice’s side). These 6 states can be easily generated out of initial \( |V_1 V_2\rangle \) state by means of local transformations. In particular we used the quarter- and half-wave plates applied to each of the photons in a pair independently. The setup is depicted in fig. 2.

The 10mm LiIO₃ crystal, cut for non-collinear, non-degenerate type-I phase-matching, is pumped by a 50 mW diode laser operating at 405 nm wavelength. The crystal axis is oriented horizontally, the pump is linearly polarized in the same plane which is ensured by the Glan-Thompson prism (H). The wavelengths of the down-converted photons are selected to be \( \lambda_1 = 750 \text{ nm} \) and \( \lambda_2 = 880.4 \text{ nm} \). The two beams are combined on the dichroic beamsplitter (DBS) transmitting 880 nm and reflecting 750 nm. The initially non-collinear regime is chosen only for the reasons of experimental simplicity, allowing to transform each photon independently when they are spatially separated. At the exit of Bob’s setup both photons propagate collinearly to achieve the state of ququart \( |\Psi_{meas}\rangle \) — one of the states in (4). It worths mentioning, that the setup was designed in a specific “triangular” shape (fig. 2) in order to minimize the incident angles for all mirrors, reducing the depolarization effects. A set of quarter- and half-wave plates for appropriate wavelengths is inserted in each arm of the setup to realize the polarization transformations.

![Diagram of Bob's station](image)

The action of a wave plate on each of the photons is described by a unitary \( SU(2) \) transformation:

\[ G_{1,2} = \left( \begin{array}{cc} t_{1,2} & r_{1,2} \\ -r_{1,2}^* & t_{1,2}^* \end{array} \right), \quad (5) \]
where \( \delta = \pi(n_\alpha(\lambda_{1,2}) - n_\beta(\lambda_{1,2}))h/\lambda_{1,2} \) is the plate’s optical thickness, and \( \chi_{1,2} \) is the angle of plate’s optical axis rotation with respect to vertical direction. One can easily show that an arbitrary polarization transformation of a single photon can be implemented using a sequence of quarter- and half-wave plates rotated at appropriate angles:

\[ G_{1,2} = G_{1,2}^{(\lambda/4)}(\beta_{1,2})G_{1,2}^{(\lambda/2)}(\alpha_{1,2}). \]

The total transformation of the biphonon field is an outer product of transformations of each photon in pair: \( G = G_1(\alpha_1, \beta_1) \otimes G_2(\alpha_2, \beta_2) \) [16]. As well as the required six states are product states, exhibiting no entanglement, this type of transformations is enough to prepare them all. Let us describe the transformations explicitly. The states and corresponding orientation of quarter- and half-wave plates in both arms of Bob’s setup are listed in table 2.

<table>
<thead>
<tr>
<th>State</th>
<th>( \alpha_1 )</th>
<th>( \beta_1 )</th>
<th>( \alpha_2 )</th>
<th>( \beta_2 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>(</td>
<td>D_1 R_2\rangle )</td>
<td>+22.5°</td>
<td>+45°</td>
<td>0°</td>
</tr>
<tr>
<td>(</td>
<td>R_1 D_2\rangle )</td>
<td>0°</td>
<td>+45°</td>
<td>+22.5°</td>
</tr>
<tr>
<td>(</td>
<td>D_1 V_2\rangle )</td>
<td>+22.5°</td>
<td>+45°</td>
<td>0°</td>
</tr>
<tr>
<td>(</td>
<td>V_1 D_2\rangle )</td>
<td>0°</td>
<td>0°</td>
<td>+22.5°</td>
</tr>
<tr>
<td>(</td>
<td>R_1 V_2\rangle )</td>
<td>0°</td>
<td>+45°</td>
<td>0°</td>
</tr>
<tr>
<td>(</td>
<td>V_1 R_2\rangle )</td>
<td>0°</td>
<td>0°</td>
<td>0°</td>
</tr>
</tbody>
</table>

In particular the transformations on Alice’s side can be realized in a single-beam configuration, using a set of two specifically cut quartz plates, acting as half-wave plates on both wavelengths (but of different order, of course). In our setup we used two identical quartz plates of 545 mkm length (fig. 3b). The phase shift introduced by these plates was \( \delta_1 = 6\pi + \pi/2 \) and \( \delta_2 = 5\pi + \pi/2 \) for the chosen wavelengths \( \lambda_{1,2} \), respectively. To perform identity transformation \( I \) nothing is to be inserted into the beam. For \( Z \) and \( X \) transformations only one plate, rotated at
0° or 45° respectively, is used. The iY transformation is a superposition of Z and X and is performed when both plates are inserted.

The transformed ququart state is measured deterministically by Bob by means of the setup shown in fig. 4. Dichroic beam-splitter separates the photons of different wavelengths, and two sets of quarter- and half-wave plates followed by polarizing beam-splitters allow one to chose the measurement basis. Measurement results in clicks of a pair of detectors, which are registered with a 4-input double-coincidence scheme. The scheme produces only pairwise clicks of the detectors, and no coincident clicks of D1 and D2 (as well as of D3 and D4) are possible, since there is only one photon in each arm after the DBS.

Results and discussion. – To analyze quality of prepared and transformed states the tools of quantum state tomography (QST) were used [16]. The ququart state |Ψ\text{in}\rangle is subjected to the linear transformations that are done by a set of the retardation plates. Then projective measurements of the transformed state are performed onto the states with vertical polarizations. The state can be statistically reconstructed using the data obtained in the series of measurements with varying combinations of optical elements such as variances in quartz plates thickness and small depolarizing effects of dichroic mirrors. Basically the error rate accumulates errors arising both from Bob’s preparation scheme and Alice’s transformation. In any case, the achieved fidelity is well above the error limit which is expected to be critical for protocol’s security.

Conclusion. – As a conclusion, we have demonstrated the ability to implement the six-state deterministic QKD protocol using polarization ququarts as information carriers. The experimental results clearly demonstrate that the proposed method allows one to prepare the states used in the protocol and to perform all the necessary unitary transformations with high quality. The simplicity of the protocol implementation is based mainly on the fact that only product states of two qubits are involved in ququart engineering. The reported experiment is a proof-of-principle, and some parts of the 6DP protocol stayed beyond the scope of this work, particularly the Control Mode was not actually realized. Nevertheless, there are no principal problems with implementing it using the deterministic measurement scheme presented in the work. It is worthy to mention, that all manipulations with ququarts described above can be implemented with fast polarization transformers, whereas no principal problems are to be expected when using this scheme for free-space key distribution. In that sense the biphoton implementation of qudits seems to be an attractive tool for further research.

Table 3: Experimentally measured fidelity for the states prepared at Bob’s station (I column) and the states after Alice’s transformations (X, iY and Z columns, respectively).

<table>
<thead>
<tr>
<th>State</th>
<th>I</th>
<th>X</th>
<th>iY</th>
<th>Z</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>D1\text{L2}\rangle</td>
<td>97.93</td>
<td>98.25</td>
<td>98.08</td>
</tr>
<tr>
<td></td>
<td>D1\text{D2}\rangle</td>
<td>98.45</td>
<td>98.86</td>
<td>98.78</td>
</tr>
<tr>
<td></td>
<td>D1\text{V2}\rangle</td>
<td>98.60</td>
<td>94.90</td>
<td>97.76</td>
</tr>
<tr>
<td></td>
<td>V1\text{D2}\rangle</td>
<td>98.40</td>
<td>96.99</td>
<td>96.93</td>
</tr>
<tr>
<td></td>
<td>L1\text{V2}\rangle</td>
<td>99.53</td>
<td>98.25</td>
<td>97.21</td>
</tr>
<tr>
<td></td>
<td>V1\text{L2}\rangle</td>
<td>99.13</td>
<td>98.15</td>
<td>98.06</td>
</tr>
</tbody>
</table>

Fig. 3: (Color online) Alice’s station.

Fig. 4: (Color online) Deterministic measurement scheme.

\begin{table}[h]
\centering
\begin{tabular}{|c|c|c|c|c|}
\hline
State & I & X & iY & Z \\
\hline
D1L2 & 97.93 & 98.25 & 98.08 & 97.20 \\
D1D2 & 98.45 & 98.86 & 98.78 & 98.99 \\
D1V2 & 98.60 & 94.90 & 97.76 & 96.94 \\
V1D2 & 98.40 & 96.99 & 96.93 & 97.89 \\
L1V2 & 99.53 & 98.25 & 97.21 & 99.18 \\
V1L2 & 99.13 & 98.15 & 98.06 & 96.51 \\
\hline
\end{tabular}
\caption{Experimentally measured fidelity for the states prepared at Bob’s station (I column) and the states after Alice’s transformations (X, iY and Z columns, respectively).}
\end{table}
Quantum state engineering with ququarts: Application for deterministic QKD protocol

REFERENCES


