PHYSICAL REVIEW A **77**, 050301(R) (2008)

Simple and secure quantum key distribution with biphotons

I. Bregman,[1] D. Aharonov,[1] M. Ben-Or,[1] and H. S. Eisenberg[2]
[1]*Department of Computer Science, Hebrew University of Jerusalem, Jerusalem 91904, Israel*
[2]*Racah Institute of Physics, Hebrew University of Jerusalem, Jerusalem 91904, Israel*
(Received 24 September 2007; revised manuscript received 13 February 2008; published 7 May 2008)

The best qubit one-way quantum-key-distribution (QKD) protocol can tolerate up to 14.6% in the error rate. It has been shown how this rate can be increased by using larger quantum systems. The polarization state of a biphoton can encode a three-level quantum system—a qutrit. The realization of a QKD system with biphotons encounters several problems in generating, manipulating, and detecting such photon states. We define those limitations and find within them a few protocols that perform almost as well as the ideal qutrit protocol. One advantage is that these protocols can be implemented with minor modifications into existing single photon systems. The security of one protocol is proved for the most general coherent attacks and the largest acceptable error rate for this protocol is found to be around 17.7%. For comparison, the security of the best possible qutrit protocol of four mutually unbiased bases was also rigorously analyzed against general attacks, with a proven bound on the acceptable error rate of 21.1%.

DOI: 10.1103/PhysRevA.77.050301 PACS number(s): 03.67.Dd, 42.50.Ex

In order to establish an unconditionally secure communication channel between two parties (traditionally called Alice and Bob), they have to share a random sequence of bits known only to them—a one time pad. Quantum key distribution (QKD) is a scheme that exploits the details of quantum measurements for generating such a key. In the most basic protocol (referred to as BB84 after its inventors Bennett and Brassard in 1984 [1]), Alice sends Bob a series of two-level quantum systems, referred to as qubits. The states are randomly chosen from two sets, each of them contains two orthogonal states that represent the logical zero and one. The two sets relate to each other in a mutually unbiased way, i.e. the probability of measuring any particular state when given a state from a different set is 1/2. Thus, if Alice chooses to send a state from the first set, a measurement in the basis of the other, either by Bob or by an eavesdropper (called Eve), will give no information about Alice's choice.

To create the required secret key, a few more steps should be carried out through a classical channel, not necessarily secured. First, Alice and Bob compare their measurement bases and sift only those bits which were measured in identical bases. From the remaining key, they reveal a portion and compare the results in order to estimate the noise parameter. This noise can result either from a real physical noise in the channel as well as from Eve's measurements. Next, they perform two transformations on the key, one to correct for errors and the second, called privacy amplification, to reduce the amount of mutual information between them and Eve.

A QKD protocol is characterized by a few parameters. The ratio between the number of remaining bits after completing this procedure to the number of bits before it, is called the rate of the protocol. The merit function that characterizes a specific protocol shows its rate as a function of the disturbance, the error probability that the channel and Eve have created. The higher the critical disturbance, where the rate approaches zero, the more useful is the protocol. In recent years, the lower bound on the critical error rate of BB84 was improved several times and the best known result is about 12.9% [2].

The BB84 protocol can be extended in many ways. The first simple way is to add an extra base that is mutually unbiased with both others [3]. It can be easily shown that only one mutually unbiased base (MUB) can be added to the BB84 protocol. According to Ref. [4], the current critical error rate of this three MUB protocol is around 14.6%. Another approach is to use quantum systems of higher dimensionality [5]. A three-level system can represent a quantum trit (qutrit) and a general d-level system can represent a qudit. A possible advantage is the larger number of MUB, up to $d+1$ for a d-dimensional protocol [6]. Previously, generalized protocols that use qutrits and higher dimensional quantum systems have been suggested and their security was studied [5,7]. A potential advantage of improved rates for such protocols was shown by examining various attack schemes [8–13]. However, the values of the critical error rates for qutrit protocols subject to general attacks are still unknown.

There are a few approaches for the realization of more than two-level quantum systems with light. One is by discriminating between modes of different orbital angular momentum [14,15]. Another approach is to use several spatial modes [16] or time bins [17]. A different approach that has been studied extensively in recent years is the qutrit representation of the polarization state of two indistinguishable photons—a biphoton [18,19]. A general biphoton state can be written as

$$|\psi_2\rangle = \alpha_0|2,0\rangle + \alpha_1|1,1\rangle + \alpha_2|0,2\rangle, \quad (1)$$

where $|n_h, n_v\rangle$ is a Fock representation of n_h (n_v) horizontally (vertically) polarized photons. The general state ψ_2 is represented by a complex vector $\bar{\alpha}=(\alpha_0,\alpha_1,\alpha_2)$ with four degrees of freedom (three complex numbers less a general phase and normalization). This scheme can be also extended to higher dimensions by adding more photons, but in this paper we focus on qutrits.

There are a few difficulties with generating arbitrary biphoton states [20] as well as when trying to manipulate [21] and detect them. Optical parametric down conversion (PDC) is the obvious choice as a generating scheme, but there are only two types of processes available; type I that creates states of the $|2,0\rangle$ and $|0,2\rangle$ forms, and type II that creates $|1,1\rangle$ (both in a collinear scheme). If a noncollinear scheme is used, type I can create the $|1,1\rangle$ type as well. In order to create a general state as in Eq. (1), a sensitive interferometer that includes both type I and II crystals is required. Moreover, as we will show later, it is impossible to transform efficiently by means of linear optics a state created with one PDC process into an arbitrary biphoton state. Finally, as transformations are limited, efficient detection is only possible for the three basic vectors [the components of Eq. (1), defined as the "measurement basis"] and their available transformations within those limits. Detection of a general state is only possible with a beam-splitter setup that detects a general state only 1 out of 4 attempts.

In this paper, we define the subset of biphoton states, which is easily generated, manipulated and detected. We find biphoton QKD protocols within these limits that are more secure and efficient than the best single photon protocol. Critical error rates are derived for various one-way qutrit protocols subject to general attacks, and compared to the best possible qutrit protocol of 4 MUB [5].

First, we shall define the set of allowed transformations. When a biphoton is transmitted through a linear optics setup, the polarization state of both of its photons experience the same single photon unitary transformation. The set of all possible unitary transformations on a single photon polarization can be mapped onto the Poincaré sphere (or the Bloch sphere for a general qubit realization), such that $\hat{U}(\theta,\varphi)$ describes the operation that transforms the state at the north pole to the coordinates (θ,φ). Thus, if we position the state $|1,0\rangle$ at the north pole, a general operation will transform it into

$$\hat{U}(\theta,\varphi)|1,0\rangle = \cos(\theta/2)|1,0\rangle + \sin(\theta/2)e^{i\varphi}|0,1\rangle. \qquad (2)$$

We name the north pole state as the "anchor" state and the set of $\hat{U}$ operators as the single photon operations. In this single photon case it is trivial to show that whatever anchor state is chosen, the $\hat{U}$ operators will always cover the whole single photon polarization space. There are a few simple rules to note. A trivial 2π rotation along any great circle will bring any state to itself, while a π rotation will transform any state to its orthogonal state. Moreover, a rotation by only $\pi/2$ along such a path always transforms between two mutually unbiased states.

We shall now find the set of states that can be reached by applying $\hat{U}$ to the biphoton measurement basis. Choosing the states $|2,0\rangle$ and $|1,1\rangle$ as the anchors and applying the single photon operations, we get

$$\hat{U}(\theta,\varphi)(1,0,0) = \left(\cos^2\left(\frac{\theta}{2}\right),\frac{1}{\sqrt{2}}\sin(\theta)e^{i\varphi},\sin^2\left(\frac{\theta}{2}\right)e^{2i\varphi}\right), \qquad (3)$$

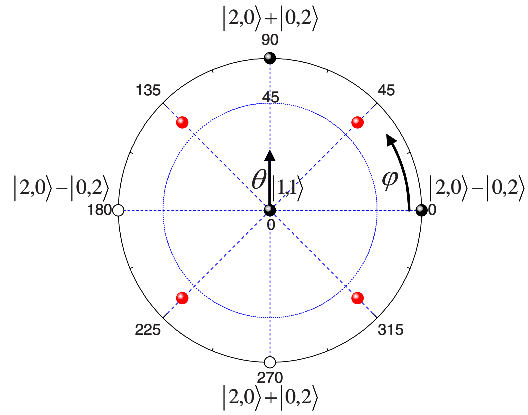

FIG. 1. (Color online) A top projection from the north pole of an orthogonal triplet basis on the $|1,1\rangle$ dome. The empty circles are states identical to their 180° opposites. Four states on this manifold are mutually unbiased to the triplet. These four states are not orthogonal between themselves.

$$\hat{U}(\theta,\varphi)(0,1,0) = \left(\frac{1}{\sqrt{2}}\sin(\theta),\cos(\theta)e^{i\varphi},\frac{-1}{\sqrt{2}}\sin(\theta)e^{2i\varphi}\right), \qquad (4)$$

as the new $\bar{\alpha}$ vectors, respectively. By allowing only two parameter operations from a finite set of anchor states, we defined a two-dimensional subset of the general biphoton four-dimensional space. As the $|0,2\rangle$ state appears at the south pole of the sphere defined by the $|2,0\rangle$ anchor, there is a full overlap between spheres defined by these two states. On the other hand, the $|1,1\rangle$ state does not appear on the $|2,0\rangle$ sphere, thus defining a non-overlapping sphere that cannot be reached from the $|2,0\rangle$ sphere by single photon operations.

It is possible to identify a few great circle rotation rules for the two new spheres, that would be useful later when we will look for possible QKD protocols in this subset. First, the $|2,0\rangle$ sphere inherited all of the properties from the $|1,0\rangle$ single photon sphere. A 2π rotation returns to the original state, a π rotation transforms between two orthogonal states and $\pi/2$ between two states whose projection on each other is 1/2. In the case of the $|1,1\rangle$ sphere, there is an interesting difference. The same rules still apply, but for half the angles. A π rotation returns to the original state, a $\pi/2$ rotation transforms between two orthogonal states and $\pi/4$ between two states whose projection on each other is $1/\sqrt{2}$. We can identify an orthogonal vector triplet on the $|1,1\rangle$ sphere as three states with $\pi/2$ in between them. A simple example for such a triplet is the $|1,1\rangle$ state and two "bunched" states such as $|2,0\rangle+|0,2\rangle$ and $|2,0\rangle-|0,2\rangle$ [22]. Curiously, the state that is exactly in the middle of any such triplet (at the tetrahedral point, about 54.7° from all the triplet states) is mutually unbiased with them (see Fig. 1). As opposite points on the $|1,1\rangle$ sphere are identical, it is enough to consider only the upper half of the sphere (a dome).

The rotation rules convert the task of finding MUB to a packaging problem. Is it possible to pack two triplet bases together on the $|1,1\rangle$ dome and preserve a mutually unbiased

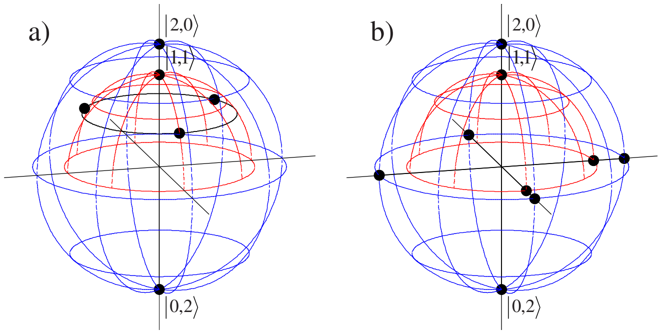

FIG. 2. (Color online) (a) The umbrella protocol: two mutually unbiased bases within the single-photon operation subspace. (b) The three rays protocol: three ray-type bases that are not perfectly mutually unbiased.

relationship? By examining Fig. 1 it is easy to see that it is impossible. On the other hand, we recognize a second general type of an orthogonal basis. If we position the dome concentrically inside the $|2,0\rangle$ sphere such that both of their north poles point in the same direction, every ray that passes through the sphere center will cut the subspace at three points, two on the sphere and one on the dome. This ray triplet contains three orthogonal states. The simplest example is the vertical ray that defines the measurement basis.

We define two possible protocols whose security will be checked here. The first protocol has two perfectly MUB and the second has three (or more) which are not. Apart from the measurement basis that is included in both protocols, the additional basis of the first protocol is

$$\left\{\frac{1}{\sqrt{3}}(1,1,-1),\frac{1}{\sqrt{3}}(1,\tau,-\tau^2),\frac{1}{\sqrt{3}}(1,\tau^2,-\tau)\right\}, \qquad (5)$$

where $\tau = e^{2i\pi/3}$. Notice how this basis is equivalent to the second Fourier basis in Ref. [5], up to a minus sign at the last position. We name this protocol after its umbrella shape [see Fig. 2(a)]. The two additional bases of the second protocol are of the ray type:

$$\left\{\frac{1}{2}(1,\sqrt{2},1),\frac{1}{\sqrt{2}}(1,0,-1),\frac{1}{2}(1,-\sqrt{2},1)\right\},$$

$$\left\{\frac{1}{2}(1,\sqrt{2}i,-1),\frac{1}{\sqrt{2}}(1,0,1),\frac{1}{2}(-1,\sqrt{2}i,1)\right\}. \qquad (6)$$

Although the three bases are only close to mutually unbiased, this protocol is appealing because of its symmetry and similarity to the three bases protocol for qubits [3] [see Fig. 2(b)]. Additionally, we considered a protocol with seven ray bases in order to check whether adding rays improves the protocol. The seven rays are the three of the previous protocol, plus the four rays through the tetrahedral points (the directions are identical to the seven solid circles in Fig. 1)

The simplest eavesdropping attack scheme is the "intercept and resend" approach. Showing that a protocol is secure against this limited attack does not imply security against general attacks. It is only used here for comparison between different protocols. We calculated Bob and Eve mutual information with Alice with the method of Ref. [5] and plotted the difference between them as a function of the error rate for a few protocols (see Fig. 3). There is a clear hierarchy between qubit and qutrit protocols. The umbrella protocol is better than any other using qubits, while the three rays protocol is even better than the umbrella protocol even though it does not include perfectly MUB. As expected, the best performance belongs to the four MUB protocol, that marks the upper limit for any qutrit protocol. Surprisingly, the seven rays protocol performs very close to ideal. All critical values are much higher than the real limits as this attack scheme is far from ideal.

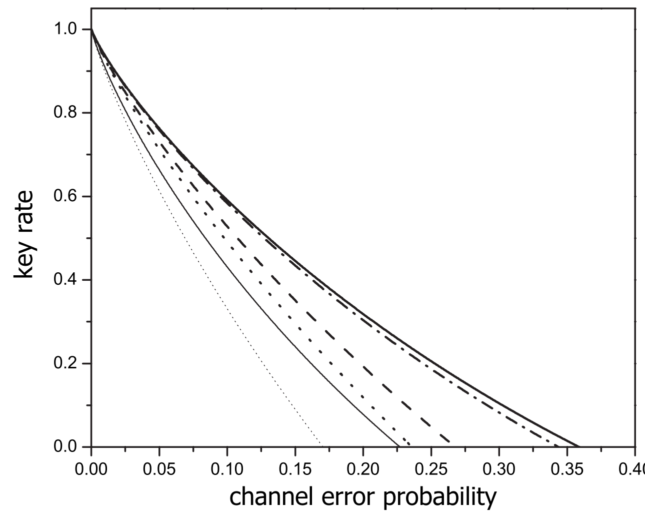

FIG. 3. Key rate analysis under intercept and resend attack of a few QKD protocols. Qubit protocols are in thin lines, dotted lines for BB84, and solid lines for the 3 MUB extension. Thick lines are for qutrit protocols. Dotted, dashed, dotted-dashed, and solid lines are for the umbrella, three rays, seven rays, and four MUB, respectively.

In order to prove the ultimate security that is required from a QKD protocol, we use the general method for one-way protocols introduced in Refs. [23,24]. The advantage of this method over other previous security proofs is its easy extendability to higher dimension while proving security against the most general coherent attacks. The scheme results in a convex nonlinear optimization problem for every error rate value. Here, we only prove unconditional security for the four MUB and the umbrella protocols as they correspond to simpler sets of constraints than the ray protocols. Nevertheless, it is only reasonable to assume that as the performance of the ray type protocols according to intercept and resend analysis is between the four MUB and umbrella protocols, their performance against general coherent attacks will be in this range as well.

After deriving the constraints, we optimized numerically the target function (the protocol rate) with the CVXOPT convex optimization package [25]. Both procedures, with and without noise addition, were calculated. The results are plotted in Fig. 4. For the three MUB qubit protocol we reproduced the known critical values of 14.1% (12.7%) (with and without noise optimization). We find proven lower bounds of 17.7% (16.0%), 20.3% (18.25%) and 21.1% (19.1%) for the

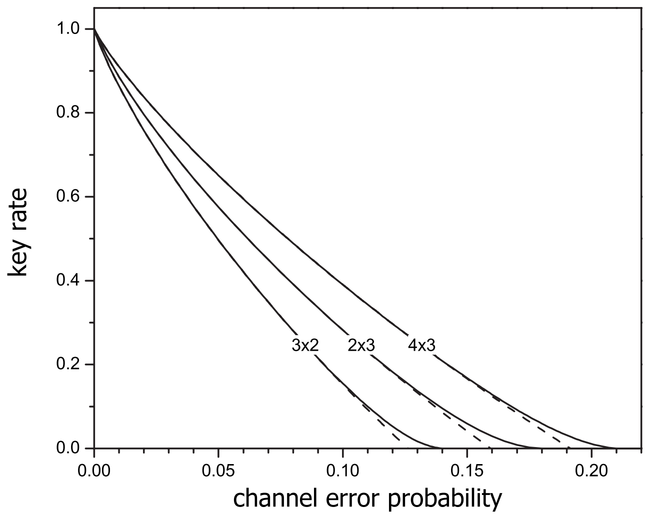

FIG. 4. Key rate analysis for a general coherent attack. Solid (dashed) lines are for calculation with (without) noise optimization. Presented results are for three qubit and two and four qutrit MUB (3×2, 2×3, and 4×3 respectively).

critical error rates of the two (the umbrella), three, and four MUB qutrit protocols, respectively. The three qutrit MUB graph is not presented here as it can't be realized within the borders of our subset. These values are considerably higher than the best value for qubit protocols to date. Just two MUB gives most of the gain between qubits and qutrits, as previously suggested by weaker security analysis [12,13].

We have left open an important issue regarding any qutrit protocol with biphotons. Namely, what is the relation between the single photon (qubit) error rate of a certain channel and the qutrit error probability when transmitting biphotons? This issue will be addressed in a later work.

In conclusion, we defined the single photon operation subspace of the polarized biphoton representation of qutrits. This subspace includes states which are easy to generate and detect, and thus are easy to implement in a QKD protocol. We suggested a few possible protocols within this subspace. The security of these protocols was rigorously analyzed and compared to standard one-way qubit protocols. A large improvement was shown compared to qubits, even for the umbrella protocol, which has only two MUB. The unconditional security of the umbrella and the four MUB protocols was proved by extending a previous proof for qubits.

H.S.E. and I.B. would like to thank the Israeli Science Foundation for supporting this work under Grants No. 366/06 and No. 1057/05, respectively. The authors wish to thank B. Kol and N. Gisin for helpful discussions.

[1] Ch. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175.
[2] G. Smith, J. M. Renes, and J. A. Smolin, e-print arXiv:quant-ph/0607018.
[3] D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998).
[4] O. Kern and J. M. Renes, e-print arXiv:quant-ph/0712.1494.
[5] H. Bechmann-Pasquinucci and A. Peres, Phys. Rev. Lett. **85**, 3313 (2000).
[6] W. K. Wootters and B. D. Fields, Ann. Phys. (N.Y.) **191**, 363 (1989).
[7] V. Karimipour, A. Bahraminasab, and S. Bagherinezhad, Phys. Rev. A **65**, 052331 (2002).
[8] H. Bechmann-Pasquinucci and W. Tittel, Phys. Rev. A **61**, 062308 (2000).
[9] M. Bourennane, A. Karlsson, and G. Björk, Phys. Rev. A **64**, 012306 (2001).
[10] D. Bruß and C. Macchiavello, Phys. Rev. Lett. **88**, 127901 (2002).
[11] M. Bourennaneet *et al.*, J. Phys. A **35**, 10065 (2002).
[12] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002).
[13] F. Caruso, H. Bechmann-Pasquinucci, and C. Macchiavello, Phys. Rev. A **72**, 032340 (2005).
[14] A. Mair, A. Vaziri, G. Weihs, and A. Zeilinger, Nature (London) **412**, 313 (2001).
[15] S. Gröblacher *et al.*, New J. Phys. **8**, 75 (2006).
[16] L. Bartůšková *et al.*, Phys. Rev. A **74**, 022325 (2006).
[17] R. T. Thew, A. Acín, H. Zbinden, and N. Gisin, Phys. Rev. Lett. **93**, 010503 (2004).
[18] A. V. Burlakov, M. V. Chekhova, O. A. Karabutova, D. N. Klyshko, and S. P. Kulik, Phys. Rev. A **60**, R4209 (1999).
[19] M. V. Chekhova, L. A. Krivitsky, S. P. Kulik, and G. A. Maslennikov, Phys. Rev. A **70**, 053801 (2004).
[20] Yu. I. Bogdanov *et al.*, Phys. Rev. A **70**, 042303 (2004); Yu. I. Bogdanov *et al.*, Phys. Rev. Lett. **93**, 230503 (2004).
[21] B. P. Lanyon *et al.*, Phys. Rev. Lett. **100**, 060504 (2008).
[22] C. K. Hong, Z. Y. Ou, and L. Mandel, Phys. Rev. Lett. **59**, 2044 (1987).
[23] B. Kraus, N. Gisin, and R. Renner, Phys. Rev. Lett. **95**, 080501 (2005).
[24] R. Renner, N. Gisin, and B. Kraus, Phys. Rev. A **72**, 012332 (2005).
[25] http://abel.ee.ucla.edu/cvxopt