2-8-2007

Large-Alphabet Quantum Key Distribution Using Energy-Time Entangled Bipartite States

Irfan Ali-Khan
University of Rochester

Curtis J. Broadbent
University of Rochester

John C. Howell
Chapman University, johhowell@chapman.edu

Recommended Citation

I. Ali-Khan, C. J. Broadbent, and J. C. Howell, *Large-Alphabet Quantum Key Distribution Using Energy-Time Entangled Bipartite States*, Phys. Rev. Lett. **98**(6), 060503. https://doi.org/10.1103/PhysRevLett.98.060503

Large-Alphabet Quantum Key Distribution Using Energy-Time Entangled Bipartite States

Large-Alphabet Quantum Key Distribution Using Energy-Time Entangled Bipartite States

Irfan Ali-Khan, Curtis J. Broadbent, and John C. Howell

Department of Physics and Astronomy, University of Rochester, Rochester, New York 14627, USA

(Received 14 July 2006; revised manuscript received 27 November 2006; published 8 February 2007)

We present a protocol for large-alphabet quantum key distribution (QKD) using energy-time entangled biphotons. Binned, high-resolution timing measurements are used to generate a large-alphabet key with over 10 bits of information per photon pair, albeit with large noise. QKD with 5% bit error rate is demonstrated with 4 bits of information per photon pair, where the security of the quantum channel is determined by the visibility of Franson interference fringes. The protocol is easily generalizable to even larger alphabets, and utilizes energy-time entanglement which is robust to transmission over large distances in fiber.

DOI: 10.1103/PhysRevLett.98.060503 PACS numbers: 03.67.Dd, 03.67.Hk, 42.50.Dv

Quantum key distribution (QKD) has continued to progress toward the goal of practical and provably secure key distribution operating at high bandwidths and over large distances [1,2]. Achieving high bandwidths over large distances remains a challenge to researchers, and it is for this reason that recent studies have focused on the possibility of increasing the information content of each transmitted quantum state by using states with higher dimensionality d [3–8], i.e., qudits instead of qubits. Higher dimensional quantum states also have the attractive properties of an increased sensitivity to eavesdropping and a decreased sensitivity to noise [9,10].

Higher dimensional states for QKD have been investigated previously. Artificial discretization of entangled transverse position-momentum quantum states with $d = 6$ [5] and $d = 37$ [6] has been demonstrated. However, such spatially encoded states are not well suited to QKD over large distances owing to the difficulties of preserving the phase fronts in free space or optic fiber. Hyperentangled states of polarization, spatial mode, and energy time have also been achieved with $d = 36$ [8]. Lastly, time-bin entangled states having $d = 3$ have been implemented in a QKD scheme operable over large distances. Unfortunately, time-bin entangled states are not easily generalized to larger dimensions [7].

In a recent publication [11] some of the authors demonstrated that time-energy entangled photons can have very large information content per biphoton. In this Letter we show experimentally that the continuously entangled time-energy system can be discretized in order to achieve an alphabet of over 1024 characters, i.e., over 10 bits per photon (albeit with large noise). We demonstrate that a real advantage in transmission rates is obtained by incorporating more information per photon. For a bit error rate (BER) bound of 5%, an optimum transmission rate in our system is obtained by incorporating 4 bits of information per photon pair.

Consider the unnormalized biphoton state

$$|\Psi\rangle \propto \int dt_1 dt_2 A(t_1, t_2) B(t_1, t_2) \times e^{-i(\omega_p/2)(t_1+t_2)} \hat{a}_1^\dagger(t_1) \hat{a}_2^\dagger(t_2)|0\rangle, \quad (1)$$

where ω_p is the down-conversion pump frequency and $\hat{a}_i^\dagger(t_i)$ is the photon creation operator in mode i at time t_i [12]. After passing through spectral filters, a Gaussian correlation function $A(t_1, t_2) = e^{-(t_1-t_2)^2/4\tau^2}$ provides a good approximation for the biphoton temporal correlation function, where the correlation time τ is on the order of $\sim$100 fs, as determined by the 10 nm bandwidth of the spectral filters. The biphoton temporal correlation function $A(t_1, t_2)$ can be understood as the correlation between the time at which the two photons exit the nonlinear crystal. Also, $B(t_1, t_2) = e^{-(t_1+t_2)^2/16T^2}$ represents the biphoton envelope function, where the biphoton envelope T is given by the coherence time of the pump photon of frequency ω_p that was destroyed in the creation of the entangled biphoton. The biphoton coherence time is on the order of $\sim$500 ns corresponding to the inverse laser linewidth. For mathematical simplicity it is straightforward to show that for $T \gg \tau$, $A(t_1, t_2)B(t_1, t_2) \simeq e^{-(t_1-t_2)^2/4\tau^2} e^{-t_1^2/4T^2}$. The Schmidt number, or number of information eigenmodes, of Eq. (1) is given by $K \sim T/\tau$ [11,13].

Suppose that a party, Alice, sends another party, Bob, one photon of the entangled state discussed above, and keeps the other photon under her control. Suppose now that an eavesdropper, Eve, makes a positive operator value measurement (POVM) on the arrival time of the photon sent to Bob [14]. We model Eve's measurement as a projective filter function, $\hat{M}_e = \int dt f(t, T_E) \hat{a}_e^\dagger(t)|0\rangle \times \langle 0|\hat{a}_e(t)$, where $f(t, T_E)$ is a general filter function and T_E is related to the resolution of Eve's POVM. A Gaussian filter function $f(t, T_E) = e^{-t^2/4T_E^2}$ gives

$$|\Psi_M\rangle \propto \int dt_1 dt_2 e^{-(t_1-t_2)^2/4\tau^2} \times e^{-(t_1^2/4)[(1/T^2)+(1/T_E^2)]} \hat{a}_1^\dagger(t_1) \hat{a}_2^\dagger(t_2)|0\rangle, \quad (2)$$

which represents the biphoton wave function after Eve's POVM. For $T_E \ll T$ we get $(\frac{1}{T^2} + \frac{1}{T_E^2}) \sim \frac{1}{T_E^2}$, which gives us $K \sim T_E/\tau$. This implies that Eve's POVM results in a decrease in the Schmidt number; eavesdropping has decreased the number of information eigenmodes.

It has been shown that the Franson interference visibility [15] can be used as a Bell-type entanglement measure for energy-time entanglement [16,17]. We find that the Franson fringe visibility, along with the known path mismatch, can also be used to measure the biphoton envelope width T (or T_E after Eve's POVM). If Alice and Bob send the state in Eq. (2) through a Franson interferometer, the post-selected coincidence rate is given by

$$R_M \propto \int dt_a dt_b |\langle 0|\hat{\alpha}(t_a, t_b, \delta t, \Delta t)|\Psi_M\rangle|^2 \quad (3)$$

$$\cong 1 + \cos\left[\frac{\omega_p}{2}(2\Delta t + \delta t)\right] e^{-\delta t^2/8\tau^2} e^{-\Delta t^2/8T_E^2}, \quad (4)$$

where $\hat{\alpha}(t_a, t_b, \delta t, \Delta t) = [\hat{a}_1(t_a + \Delta t + \delta t)\hat{a}_2(t_b + \Delta t) + \hat{a}_1(t_a)\hat{a}_2(t_b)]$, where $\hat{a}_{1,2}(t)$ is the destruction operator for Alice's and Bob's detectors, respectively, Δt is the path mismatch in Bob's arm of the Franson interferometer, and δt is the difference in path mismatches between Alice's and Bob's arms of the Franson interferometer. A strong drop in Franson fringe visibility is observed when $T_E \lesssim \Delta t$. Therefore, we can detect the presence of Eve's POVM by observing a reduction in the visibility of Alice's and Bob's Franson fringes, as predicted by the exponential function in Eq. (4). Note that a larger path mismatch Δt provides a more sensitive test against Eve's POVM.

The energy-time entanglement QKD protocol we present here is accomplished in 6 steps. (1) Alice sends Bob one photon of an energy-time entangled biphoton and keeps one for herself. (2) Alice and Bob randomly and independently measure arrival times of their incoming photon either directly with low-jitter (FWHM ~50 ps, $1/e^2$ width ~350 ps) detectors (timing detector) or after sending their photon through an unbalanced Michelson interferometer acting as one-half of a Franson interferometer (see Fig. 1). These timing measurements of Alice and Bob are accurately synchronized to each other by using a shared, public synchronization pulse signal. This sync signal has a period of 64 ns between consecutive pulses in our experiment, where each pulse is measured, counted, and recorded. During the entirety of the QKD process Alice privately scans one arm of her unbalanced interferometer between two neighboring Franson interference maximum and minimum locations (predetermined during initial calibration). (3) After all the photons have been detected, Bob publicly sends Alice the exact arrival times of the photons that were detected in the output of his Michelson interferometer. Alice uses this information, along with her own Franson timing measurements and respective interferometer scan locations, to determine the visibility of the Franson fringes. (4) Using the measured visibility, Alice determines the security of the system and communicates the status of security to Bob. If the system is measured to be secure then Alice and Bob can proceed with the QKD protocol. (5) Alice and Bob privately bin their remaining (non-Franson) timing measurements, where each bin corresponds to a character of the QKD alphabet (see Fig. 3). Details of the binning procedure are explained below. For our experiment, the bin size, σ, is varied between 48 ps–30.6 ns, where a trade-off between alphabet size and BER is explored. The first bin of the alphabet begins with each sync pulse, and the alphabet extends over the period of the sync signal (64 ns for our experiment). (6) Alice and Bob publicly publish the relevant sync periods in which they measure the arrival of non-Franson photons; however, they keep the precise binning information from step (5) private. Alice and Bob discard the non-Franson photon arrival events that do not occur in the same sync periods, and keep the rest. Alice and Bob are thus left with identical photon events, where both photons of a down-conversion pair are measured in the same time bin by Alice and Bob. The unpublished, precise arrival times for the accepted photon detection events thus give Alice and Bob a common key.

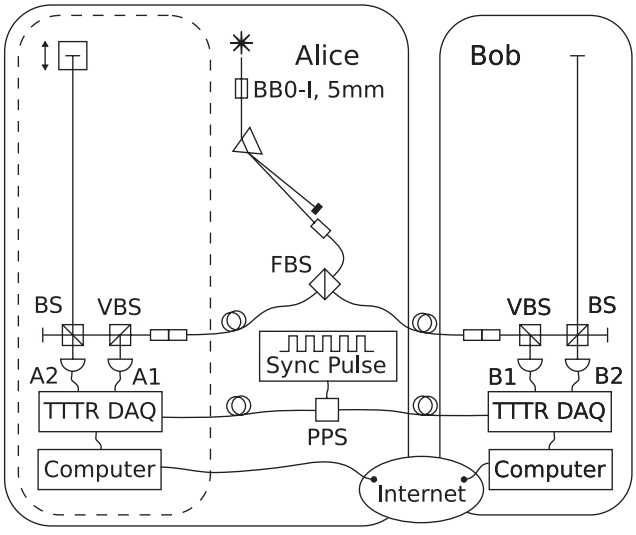

FIG. 1. Experimental setup. BS, FBS, VBS, and PPS, refer to a 50:50 beam splitter, a fiber 50:50 beam splitter, a variable beam splitter made with a half wave plate and a polarizing beam splitter, and a passive power splitter, respectively.

An outline of the experiment is shown in Fig. 1. Alice uses a 50 mW, 390 nm, cw laser having a bandwidth of 2 MHz to pump 5 mm of beta-barium borate (BBO)-I cut for collinear, degenerate down-conversion (with measured raw singles rate ~800 kHz and coincidence rate ~60 kHz using PerkinElmer single photon counting mode (SPCM) with single mode fiber). The down-converted photons are coupled into a single mode, 50:50, fiber beam splitter, where one photon is sent to Alice and the other to Bob. The instances where both photons travel to either Alice or Bob can presently be ignored. Using a variable beam splitter, Alice and Bob randomly and independently send their photons either to a high-resolution timing detector ($A1/B1$, Micro Photon Devices (MPD) PMD, background dark-count rate ~250 Hz, background light-count rate ~1 kHz, singles rate ~20 kHz, coincidence rate ~24 Hz, accidental-to-correlated coincidence ratio of 1:88 for a 1 ns

coincidence window) or an unbalanced Michelson interferometer. The output of the unbalanced Michelson interferometer is sent to a correlation detector ($A2/B2$, PerkinElmer SPCM, dark-count rate ~450 Hz, background light-count rate ~600 Hz, singles rate ~67 KHz, coincidence rate ~58 Hz). Signals from the detectors ($A1/B1/A2/B2$) are routed to two high-resolution data acquisition devices (DAQ, PicoQuant PicoHarp run at $\xi =$ 16 ps resolution), one DAQ for $A1$ and $A2$, and the other DAQ for $B1$ and $B2$. The two DAQs are synchronized to each other via a clock signal (with period $T_{\text{sync}} = 64$ ns) that is generated by Alice. Alice's and Bob's unbalanced Michelson interferometers both have a path mismatch of $\tau \simeq 10$ ns. Alice's unbalanced Michelson interferometer has an automated 20 nm resolution translation stage in the long arm that she scans as part of the key generation protocol outlined above.

Ideally, for the duration of the QKD process, Alice need only randomly measure the predetermined maximum and minimum locations of the Franson fringes. However, due to phase drifts, for the duration of the experiment Alice's stage is scanned from $c\Delta\tau = 0$ to $c\Delta\tau = 600$ nm $\cong 3\frac{\lambda_p}{2}$ in 50 nm steps with 3 s integral periods. After taking data for a nominal duration of 60 s, Bob sends Alice his Franson event arrival times. Alice uses Bob's Franson event arrival times along with her own Franson event arrival times to obtain a measured visibility $V = 93 \pm 7\%$ [see Fig. 2(a)]. The error in measured visibility is due to phase instabilities (we require 10 nm stability over 3 m path lengths), which can be improved with an all-fiber setup. The measured visibility is used to estimate the resolution of Eve's POVM in the intercept-resend-type attack discussed previously. Assume that Eve performs a POVM on every photon pair. A theoretical plot of Franson fringe visibility versus Eve's POVM resolution is shown in Fig. 2(b). A Gaussian POVM and a rectangular POVM are analyzed, where the POVM resolution corresponds to 4 standard deviations for a Gaussian POVM (corresponding to 99.99% of the distribution) and the FWHM for the rectangular POVM. As seen in Fig. 2(b), a measured Franson fringe visibility of ~93% corresponds to Eve's POVM resolution of $\gtrsim 50$ ns. As discussed below, the optimal alphabet obtained in our experiment spans a period of 21 ns. Hence Eve does not gain any detailed information about the key, demonstrating security of the quantum channel. A more rigorous security analysis is beyond the scope of this Letter, and shall be presented in a later publication. Alice communicates to Bob that the quantum channel is secure and they proceed with the key sifting process of the protocol.

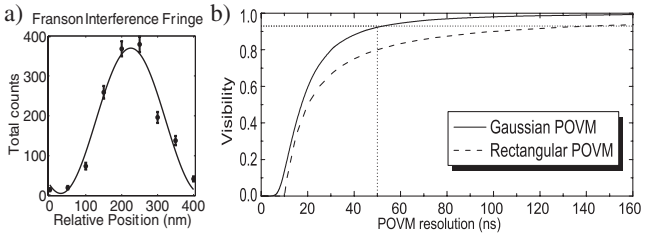

FIG. 2. (a) Franson fringe visibility is measured to be 93%. (b) Franson fringe visibility vs Eve's POVM resolution. The solid curve represents a Gaussian POVM, while the dashed curve represents a rectangularform POVM. A measured visibility of 93% corresponds to a POVM resolution of $\gtrsim 50$ ns, demonstrating security (details in text).

Alice and Bob bin the arrival times of their timing photons. Since the arrival times of each photon is measured with respect to the clock cycle immediately preceding it, the first level of binning is accomplished by Alice and Bob publicly communicating the respective clock cycle, denoted n_a for Alice's clock cycle and n_b for Bob's, during which each photon detection event occurs. Coarse-grained coincidence events are those for which $n_a = n_b$. The simplest form of binning in order to obtain a D-character alphabet involves dividing each 64 ns sync period into D, equally sized bins. Each bin has an equal chance of containing a photon event since a cw pump is used. Using a bin size of $\sigma = 3\xi = 48$ ps gives us an alphabet of $D = \frac{64 \text{ ns}}{48 \text{ ps}} \sim 1278$ characters, i.e., over 10 bits per photon. However, the detector electronics jitter has a $1/e^2$ width of 350 ps that results in a very high quantum dit error rate (QDER) of 86%, due to one photon registering in the dth bin with Alice while the other photon registers in the $d \pm$ 1th bin with Bob. Converting dits to bits, we find that this corresponds to a BER of ~30%. Error correction codes can be used to reduce the BER, but are only effective for a raw BER of less than 11% [18].

In order to reduce the raw BER, a process of indexing and redundancy is performed on the bins. Each of the 1278 bins are consecutively indexed from $i = 1$ to $i = I$, with every I consecutive bins representing the same character (see Fig. 3). Alice and Bob publicly announce the index i of their binned photons (but keep the character private). Alice and Bob keep those coarse-grained correlation events that also have the same index, and discard the rest. For example, an index parameter of $I = 5$ reduces the alphabet to $\frac{1278}{5} = 255$ characters, but also reduces the BER to ~21%. This process reduces the BER due to the jitter in the detector electronics; however, a sizeable BER remains due to erroneous coincidences that are caused by low collection and detection efficiency, ambient room light, fluorescence in the optics, and dark counts in the detectors.

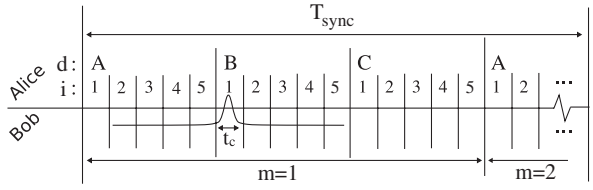

FIG. 3. Example of the binning procedure as outlined in the text. In this example we have used $I = 5$, $M = 2$, and $D = 3$.

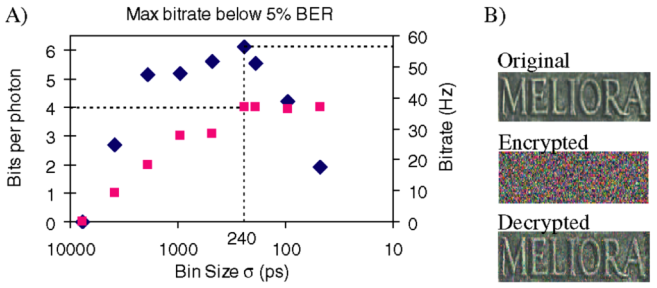

FIG. 4 (color online). (a) Diamonds represent optimal bit-rate vs σ (optimized for I and M). Squares represent information per photon pair for each optimization. Overall optimum bit rate is obtained for $\sigma = 240$ ps, with 4 bits per photon pair. (b) Demonstration of cryptography using optimal key. Image size 32 KB. Key reused 58 times.

The BER due to these accidental coincidences can be further reduced by reducing the coarse-grained coincidence window of 64 ns. This is done by dividing the sync period (64 ns) into M, separate periods, denoted n_a^m and $n_b^{m'}$ for Alice and Bob, respectively. Alice and Bob publicly announce the sync division, m, during which a photon is measured, and keep only those coarse-grained coincidences for which $n_a^m = n_b^{m'}$. This reduces the BER due to accidental coincidences, but also reduces the alphabet size $D = 1278$ by a factor M. For example, for $M = 2$, the alphabet size is reduced to 639 characters (assuming $I = 1$). It should be noted that the security of the system, determined by the Franson fringe visibility, is independent of the BER.

By varying σ, I, and M, it is possible to find an optimal transmission rate within a desired error bound. As seen in Fig. 4(a), the optimal transmission rate for our system, within a BER bound of 5%, corresponds to $\sigma = 240$ ps with 4 bits per photon pair (using $I = 5$ and $M = 3$, not shown). Hence, a real advantage is achieved by incorporating more information per photon pair. Note that this result was obtained for an estimated eavesdropping POVM resolution of $\gtrsim 50$ ns, larger than the $\frac{64}{3} = 21$ ns period of the optimal alphabet, thus demonstrating security. An added benefit of this time-energy system is that this optimization can easily be performed in post-processing, since $\frac{\sigma}{\xi}$, I, and M are all computational (as opposed to physical) parameters. Hence, it is very easy to perform a unique optimization for different systems. Further, even if the measured visibility of the Franson fringes is reduced, e.g., due to the presence of an eavesdropper, a new optimization can immediately be performed so as to maintain security. For completeness, an image is encrypted and decrypted using the key obtained for $\sigma = 240$ ps, $I = 5$, and $M = 3$, as shown in Fig. 4(b).

We have presented a protocol for large-alphabet QKD using energy-time entangled photons generated by a cw pump, as motivated in [11]. In this QKD protocol, one conjugate basis is used exclusively for key generation while the other conjugate basis is used exclusively for measuring security of the quantum channel. It is possible to maintain secure QKD even in the presence of eavesdropping by monitoring the Franson fringe visibility and reoptimizing $\frac{\sigma}{\xi}$, I, and M. We have demonstrated an alphabet of over 10 bits per photon, albeit with a 30% BER. Within a BER bound of 5%, an optimal transmission rate was achieved by using 4 bits per photon. Even larger alphabets can be obtained by using longer sync pulse intervals or higher resolution timing detectors, while the BER would need to be significantly reduced by reducing losses and noise in the system. Energy-time entanglement has previously been demonstrated to be well preserved over large distances in fiber [16,17], which makes the application of this protocol an exciting prospect for practical QKD.

We acknowledge J. D. Franson for useful discussions and helpful suggestions. We gratefully acknowledge support from the ARO under Grant No. W911NF-05-1-0018, NSF under Grant No. EIA-0323463, ARDA under Grant No. W911NF-05-1-0197, DOD Quantum Imaging MURI, and the University of Rochester.

[1] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, New J. Phys. **4**, 41 (2002).
[2] X. Li, P. L. Voss, J. E. Sharping, and P. Kumar, Phys. Rev. Lett. **94**, 053601 (2005).
[3] L. Neves, G. Lima, J. G. A. Gómez, C. H. Monken, C. Saavedra, and S. Pádua, Phys. Rev. Lett. **94**, 100501 (2005).
[4] A. Mair, A. Vaziri, G. Weihs, and A. Zeilinger, Nature (London) **412**, 313 (2001).
[5] M. N. O'Sullivan-Hale, I. Ali-Khan, R. W. Boyd, and J. C. Howell, Phys. Rev. Lett. **94**, 220501 (2005).
[6] S. P. Walborn, D. S. Lemelle, M. P. Almeida, and P. H. S. Ribeiro, Phys. Rev. Lett. **96**, 090501 (2006).
[7] H. de Riedmatten, I. Marcikic, V. Scarani, W. Titel, H. Zbinden, and N. Gisin, Phys. Rev. A **69**, 050304(R) (2004).
[8] J. T. Barreiro, N. K. Langford, N. A. Peters, and P. G. Kwiat, Phys. Rev. Lett. **95**, 260501 (2005).
[9] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002).
[10] G. M. Nikolopoulos, K. S. Rande, and G. Alber, Phys. Rev. A **73**, 032325 (2006).
[11] I. Ali Khan and J. C. Howell, Phys. Rev. A **73**, 031801(R) (2006).
[12] W. P. Grice and I. A. Walmsley, Phys. Rev. A **56**, 1627 (1997).
[13] C. K. Law and J. H. Eberly, Phys. Rev. Lett. **92**, 127903 (2004).
[14] G. J. Pryde, J. L. O'Brien, A. G. White, T. C. Ralph, and H. M. Wiseman, Phys. Rev. Lett. **94**, 220405 (2005).
[15] J. D. Franson, Phys. Rev. Lett. **62**, 2205 (1989).
[16] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, Phys. Rev. Lett. **81**, 3563 (1998).
[17] I. Marcikic, H. de Riedmatten W. Tittel, H. Zbinden, M. Legre, and N. Gisin, Phys. Rev. Lett. **93**, 180502 (2004).
[18] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).