Quantum Key Distribution Using Hyperentangled Time-Bin States

Daniel J. Gauthier,[1] Christoph F. Wildfeuer,[1] Hannah Guilbert,[1] Mario Stipčević,[1,2] Bradley Christensen,[3] Daniel Kumor,[3] Paul Kwiat,[3] Kevin McCusker,[4] Thomas Brougham[5] and Stephen M. Barnett[5]

[1]*Duke University, Department of Physics, Box 90305, Durham, North Carolina 27708 USA*
[2]*Rudjer Boskovic institute, Bijenicka 54, 10002 Zagreb, Croatia*
[3]*University of Illinois, Urbana-Champaign, Department of Physics, 1110 W. Green St., Urbana, Illinois 61801, USA*
[4]*Northwestern University, Department of EECS, 2145 Sheridan Rd., Evanston, Illinois 60208, USA*
[5]*University of Strathclyde, Department of Physics, Glasgow G4 0NG, United Kingdom*
gauthier@phy.duke.edu

Abstract: We describe our progress on achieving quantum key distribution with high photon efficiency and high rate using hyperentanglement. Methods of securing time-bin states and classical error correction protocols appropriate for our high-dimension protocols are discussed.

OCIS codes: (270.5565) Quantum communications, (270.5568) Quantum cryptography, (270.5585) Quantum information and processing

We describe our recent progress on developing a quantum key distribution (QKD) system based on hyperentanglement. Two parties, Alice and Bob, share pairs of hyperentangled photons [1] from spontaneous parametric downconversion (SPDC) in a pair of nonlinear optical BiBO crystals, where the photons are simultaneously entangled in polarization, spatial mode, and time-bin degrees of freedom (DOF). Each DOF plays a different role in the overall QKD protocol: most of the randomness is encoded in the photon timing, polarization entanglement is used to check for eavesdropping, and the spatial modes realize independent quantum communication channels.

As shown in Fig. 1 for a single spatial channel of the QKD system, the SPDC source is pumped by a high-repetition-rate (pulse period δt), high-power modelocked laser (355 nm, 5 ps pulse width, Coherent Paladin) so that each photon pair is emitted in a superposition of many different time bins (but both photons are always detected in the same time bin in a perfect system). By measuring the photon arrival time relative to a classically synchronized and publicly shared master clock, they generate a shared random key with many bits per photon [2, 3]. The quantum state of the generated light for each spatial mode is described approximately by

$$|\psi\rangle \propto \left(|t_0 t_0\rangle + |t_1 t_1\rangle + |t_2 t_2\rangle + \ldots + |t_N t_N\rangle\right) \otimes \left(|HH\rangle + |VV\rangle\right) . \qquad (1)$$

(More precisely, there is a Poisson probability distribution to create a pair in each time bin for the case when the time bin is longer than the first-order coherence time of the down converted and spectrally filtered light.)

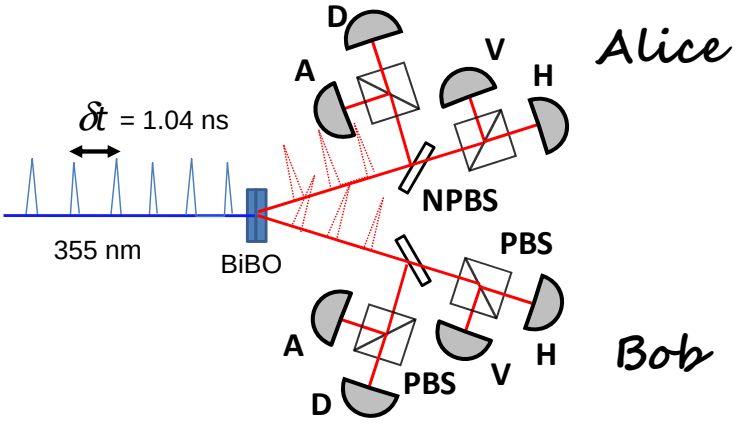

Fig. 1 Experimental setup for our QKD system for one spatial mode. The non-polarizing beam splitter (NPBS) in Alice and Bob's setup randomly direct the photonic states to either the Horizontal (H)/Vertical (V) basis or the Diagonal (D)/Anti-Diagonal (A) polarization bases, where single-photons are detected and their time of arrival recorded.

The overall secure communication rate for the system is given by

$$R = M\eta^2\left(\frac{\langle n\rangle\xi}{\delta t}\right), \tag{2}$$

where M is the number of independent communication channels (M=1 in Fig. 1), η is the total efficiency of the channel (assumed the same for Alice and Bob) and includes the spatial collection efficiency of the optics, spectral efficiency of the filters, other losses, and the quantum efficiency of the detectors, $\langle n\rangle$ is the mean generated photon number per time bin, and ξ is the photon efficiency in bits per generated coincidence, which includes the mutual information in the photon arrival time and the polarization. Here, ξ includes the efficiency of the sifting on polarization bases, the error correction efficiency for both the timing and polarization mutual information, and privacy amplification due to leakage of information to an eavesdropper. For the case when the $\langle n\rangle$ is small, the photon efficiency can be substantial as shown in Fig. 2. The shared mutual information between Alice and Bob associated with the timing part of the entropy increases with decreasing photon rate, eventually turning around and dropping to zero due to the effects of detector dark counts. For reasonable parameters, it is seen that many bits of information can be encoded on a single correlated photon pair, one benefit of using hyperentanglement.

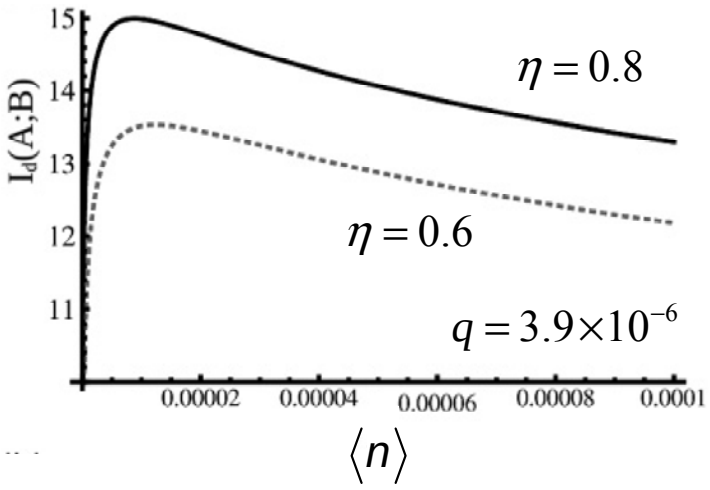

Fig. 2 Mutual information per detected photon pair shared between Alice (A) and Bob (B) as a function of mean photon number per time bin. Here, $I_d(A;B) = \xi/\left(\eta^2\langle n\rangle + q^2\right)$, where q is the probability of a dark count per time bin. Adapted from Ref. [3].

Clearly, Fig. 2 shows that the photon efficiency increases as $\langle n\rangle$ decreases, albeit slowly, but Eq. (2) shows that the overall rate decreases because R is proportional to $\langle n\rangle$. Thus, there is a trade-off between photon efficiency and rate in a QKD system that relies on the entropy associated with the photon time of arrival. To increase the key generation rate, we duplicate this basic setup, thereby increasing M, at many different azimuthal directions around the down conversion cone [1].

To obtain the highest entropy rate shared between Alice and Bob requires detectors with small timing jitter, high saturation flux, and high quantum efficiency. We are currently developing a new line of avalanche photodiodes (APDs) manufactured by Laser Components (SAP 500) mated with commercial low-jitter electronics (MPD PDM). The SAP 500 detectors are large area silicon APDs (500 μm diameter active area) with a ~65% quantum efficiency at 710 nm (and over 80% at shorter wavelengths) and jitter well below 200 ps (FWHM) when the light is focused to a small (<50 μm) spot in the center of the detector. Figure 3 shows the jitter distribution when two SAP 500 + MPD PMD single-photon counting detection systems are illuminated by correlated photon pairs from our SPDC source.

The full width at half maximum of this correlation probability distribution is ~230 ps, implying an average jitter for each detector of ~230 ps/$2^{1/2}$ = 160 ps. The effective dead time of this system is ~60 ns, limiting the saturation rate to below 20 MHz. The dead time is largely governed by the PDM electronics module to reduce the after-pulsing probability of the detector. To increase this rate, we are developing custom active quenching electronics [4]. Initial performance estimates of the custom circuit indicate that a dead time of ~20 ns can be obtained with an after-pulsing probability less than 2%.

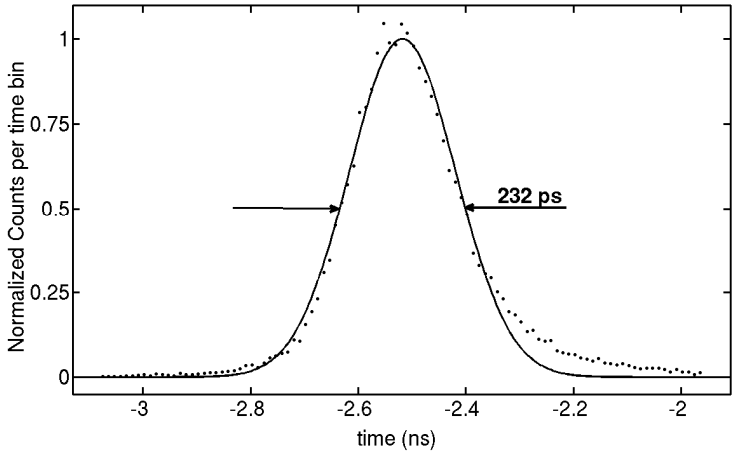

Fig. 3 Temporal correlation distribution of two SAP 500 + MPD PDM detectors in our SPDC setup at a wavelength of 710 nm.

The QKD rate also depends on the overall system efficiency, as mentioned above, which is quantified by the system heralding efficiency (ratio of coincidence counts to single counts). We have obtained heralding efficiencies over 50% into single-mode fibers using proper mode matching and high-efficiency spectral filters and standard Perkin-Elmer avalanche photodiodes (65% typical quantum efficiency, 800 ps typical jitter), and comparable heralding efficiencies using multi-mode fibers. The output of Alice and Bob's detectors are sent to independent high-speed time-tagging units that have an RMS jitter of ~50 ps and high transfer rate to a personal computer.

Consistent with theoretical expectations on the trade-off between photon efficiency and entropy rate, we obtain higher photon efficiency (entropy rate) at lower (higher) detected photon flux. Interestingly, we find that running the system at higher photon efficiency allows us to extract more bits from a system that is constrained by non-ideal detector characteristics, especially the saturated detection rate. With δt = 1.04 ns and at low pump power, we obtain a polarization bit error rate of 0.4%, 10.4 timing bits-per-photon (bpp) and 0.4 polarization bpp at a rate of 580 kb/s after error correction using two parallel spatial channels, and a bit error rate of 0.8%, 5.5+0.4 bpp and 12.8 Mb/s after error correction at higher power.

We find that standard error correcting schemes are not well suited for our situation where we are dominated by deletion errors (where Alice, say, detects a photon but Bob does not because of the non-unit detection probability). We find that most error correction codes fail when the deletion errors are too high in that too much information needs to be exchanged over the pubic channel and hence is potentially revealed to an eavesdropper, resulting in zero secret key rate.

To overcome this problem, we are currently using what appears to be an efficient approach where we create "frames" of temporal data [5] as illustrated in Fig. 4. Here, a frame consists of N contiguous time bins. In the simplest approach, Alice and Bob disclose over a public channel the number of photons they measure in each frame (but do not reveal which time bins the photons appear within a frame). Frames for which Alice and/or Bob do not observe at least one photon are deleted from the data, which overcomes most of the deletion errors. The data remaining in the non-empty frames is then processed using a low-density parity-check error-correcting code.

Interestingly, we find that a substantial fraction of the mutual information is contained in the frames where Alice and Bob each see one photon in a frame (denoted by 1:1 frames) if N is sufficiently large. A theoretical estimate of the entropy partitioning is shown in Fig. 5, where we account only for the deletion errors and do not consider detector

jitter or dark counts. For small frame sizes, most of the entropy is contained in the fluctuations in the photon number from frame-to-frame (denoted by the fame occupancy). As N increases, the information in the 1:1 frames rises quickly and the frame-occupancy entropy drops. For much larger values of N, the information in the 2:2 frames begins to grow, but is always a small fraction of the total entropy over the range shown here. The entropy in the 1:1 frames is approximately 70% of the total (detected) entropy and is rather insensitive to the choice of N about its maximum value. For moderate frame sizes, nearly 90% of the entropy is contained in just the 1:1 frames and the frame occupancy. Thus, a greatly simplified error-correction strategy is to discard all but the 1:1 frames. We note that the frame occupancy entropy is lost to the eavesdropper if we publicly announce the frame occupancy number; we are investing methods for using error-correcting methods for coding this information so that most of it can be kept secret from the eavesdropper.

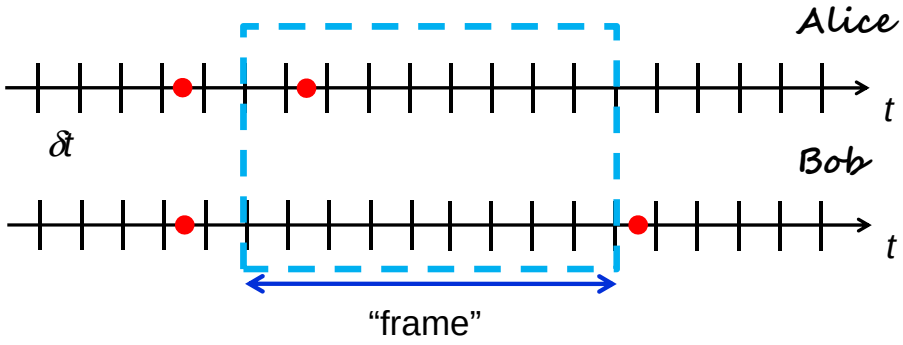

Fig. 4 Creating frames of time bins. Alice and Bob share a public master clock, which allows them to define temporal bins (one for each pump laser pulse) of duration δt. The solid circles represent the detection of a photon and the dashed line defines a frame of N contiguous time bins. In some cases, shown at the left, both Alice and Bob receive the correlated photon pair. In many cases, finite transmission and detection efficiency "erases" a photon detection event so that Alice or Bob receives a photon, but the other does not. Dark counts also create uncorrelated events in either of Alice or Bob's temporal stream of data.

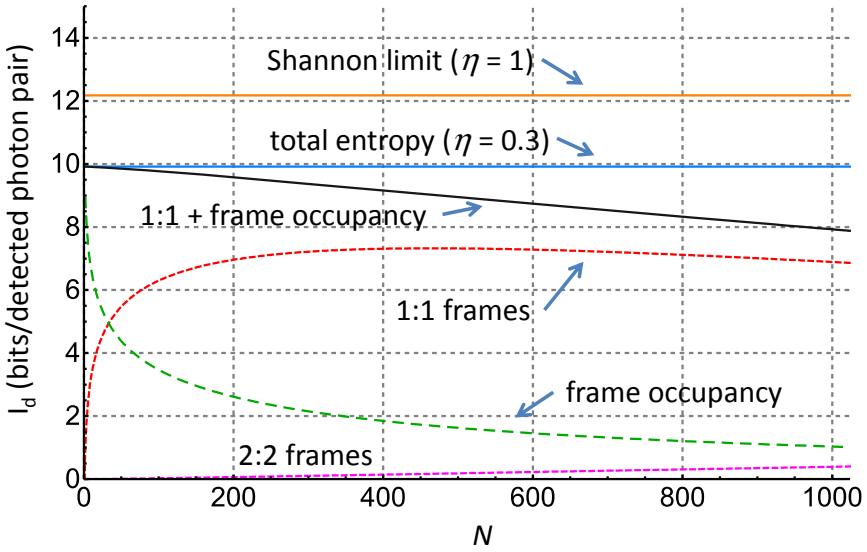

Fig. 5 Distribution of the detected mutual information among different frames as a function of the frame size. The efficiency of Alice and Bob's channel is assumed to be the same and the average photon number per time bin is $\langle n \rangle = 5.3\times10^{-4}$.

Our current scheme is not secure against an attack by Eve equipped with a polarization preserving quantum non-demolition measurement of photon timing, although the sensitivity and bandwidth required for such an attack on our system is many orders of magnitude away from the current state of the art in quantum non-demolition (QND) measurements. We are investigating methods for securing all time bins so that our system is secure against all known attacks and find that the so-called phase-states are particularly interesting. The phase states are mutually unbiased with respect to the time-bin basis and can be measured using a cascaded tree of Franson interferometers.

While this approach achieves full security, it is difficult to realize experimentally because it requires a large number of path-length-stabilized interferometers and N detectors. Recently, we explored the use of a smaller number of Franson interferometers than that required to fully perform a measurement in the phase-state basis and quantified the susceptibility of this approach to some eavesdropping attacks [6]. We are also exploring methods based on group velocity dispersion that transforms frequency information of a quantum state to the temporal domain, thereby substantially reducing the number of detectors required to perform a security check [7, 8].

We gratefully acknowledge the financial support of the DARPA DSO InPho program.

References

[1] P. G. Kwiat, "Hyper-entangled states," J. Mod. Opt. **44**, 2173 (1997).

[2] 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**, 060503 (2007).

[3] T. Brougham and S. M. Barnett, "Information communicated by entangled photon pairs," Phys. Rev. A **85**, 032322 (2012).

[4] M. Stipčević, H. Skenderović, and D. Gracin, "Characterization of a novel avalanche photodiode for single photon detection in VIS-NIR range," Opt. Express **18**, 17448 (2010).

[5] Y. Kochman and G. W. Wornell, "On high-efficiency optical communication and key distribution," Information Theory and Applications Workshop (ITA), pp. 172-179, 5-10 Feb. 2012.

[6] T. Brougham, S. M. Barnett, K. T. McCusker, P. G. Kwiat, and D. J. Gauthier, "Security of high-dimensional quantum key distribution protocols using Franson interferometers," J. Phys. B: At. Mol. Opt. Phys. **46**, 104010 (2013).

[7] J. Mower, Z. Zhang, P. Desjardins, C. Lee, J. H. Shapiro, D. Englund, "High-dimensional quantum key distribution using dispersive optics," Phys. Rev. A **87**, 062322 (2013).

[8] J. Nunn, L. J. Wright, C. Söller, L. Zhang, I. A. Walmsley, and B. J. Smith, "Large-alphabet time-frequency entangled quantum key distribution by means of time-to-frequency conversion," Opt. Express **21**, 15959-15973 (2013).