Quantum Key Distribution Using Hyperentangled Time-Bin States

Daniel J. Gauthier,[1] Christoph F. Wildfeuer,[1] Hannah Guilbert[1] and Mario Stipčević[1,2]
[1]Duke University, Department of Physics, Box 90305, Durham, North Carolina 27708 USA
[2]Rudjer Boskovic institute, Bijenicka 54, 10002 Zagreb, Croatia
gauthier@phy.duke.edu
Bradley Christensen, Daniel Kumor and Paul Kwiat
University of Illinois, Urbana-Champaign, Department of Physics, 1110 W. Green St., Urbana, Illinois 61801, USA
Kevin McCusker
Northwestern University, Department of EECS, 2145 Sheridan Rd., Evanston, Illinois 60208, USA
Thomas Brougham and Stephen M. Barnett
University of Strathclyde, Department of Physics, Glasgow G4 0NG, United Kingdom

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 appropriate for our high-dimension protocols will be 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. Alice and Bob share pairs of hyperentangled photons [1] from spontaneous parametric downconversion (SPDC) in BiBO, 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 protocol: most of the randomness is encoded in the photon timing (the quantum pulse-position-modulation protocol), polarization entanglement is used to check for eavesdropping, and the spatial modes realize independent QC channels. The SPDC source is pumped by a high-repetition-rate (rate R), high-power laser at 355 nm, 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

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

where N=1,024 for encoding 10 bits per photon (bpp), for example. (More precisely, there is a Poisson probability distribution to create a pair in each time bin.) To increase the key generation rate, we duplicate this basic setup and this quantum state at many different azimuthal directions around the down conversion cone (different parallel spatial channels).

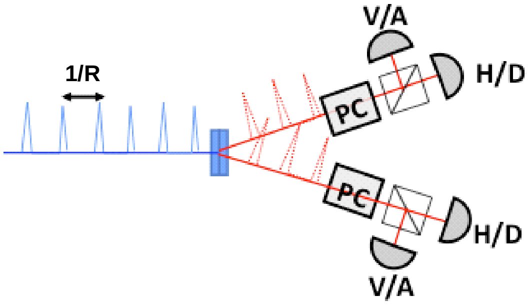

Fig. 1 Experimental setup for our QKD system for one spatial mode. PC is a polarization controller and single-photon-counting detectors measure in the Horizontal (H)/Vertical (V) basis or the Diagonal (D)/Anti-Diagonal (A) polarization basis.

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 manufactured by Laser Components (SAP 500) mated with custom active quenching electronics [4]. Initial performance estimates are: temporal jitter ~150 ps, ~40 Mcps saturation flux, and ~65% quantum efficiency at 710 nm (and over 80% at shorter wavelengths). We also require high heralding efficiency (ratio of coincidence counts to single counts) of the overall detection system. We have obtained efficiencies over 50% into single-mode fibers using proper mode matching and high-efficiency spectral filters using standard Perkin-Elmer avalanche photodiodes, 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. With R=960 MHz 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 are currently using what appears to be an efficient approach to this problem where we create “frames” of temporal data [5]. Based on a public discussion between Alice and Bob, frames that are empty are deleted from the data, which overcomes most of the deletion errors. The data remaining in the non-empty frames are then processed using a low-density parity-check error correcting code. We will discuss theoretical approaches for determining the efficiency of this error correcting protocol.

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 QND measurement. We are investigating methods for securing all time bins so that our system is secure against all known attacks. We show that phase-states form a basis that is mutually-unbiased with respect to the time-bin basis, which can be measured using a cascaded tree of Franson interferometers. While this approach achieves full security, it is difficult to realize experimentally. Recently, we explored the use of a smaller number of Franson interferometers than required to fully perform a measurement in the phase-state basis and quantify 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].

In the presentation, we will discuss our current results, including the leakage of information to Eve through the experimental imperfections, our current understanding of optimal error correction methods, and techniques that will allow for absolute security.

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

[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,” arXiv:1210.4501.