World Academy of Science, Engineering and Technology
International Journal of Nuclear and Quantum Engineering
Vol:7, No:1, 2013

Higher-Dimensional Quantum Cryptography

Bradley Christensen, Kevin T. McCusker, Daniel J. Gauthier, Daniel Kumor, Venkat Chandar, and P. G. Kwiat

***Abstract*—**We report on a high-speed quantum cryptography system that utilizes simultaneous entanglement in polarization and in "time-bins". With multiple degrees of freedom contributing to the secret key, we can achieve over ten bits of random entropy per detected coincidence. In addition, we collect from multiple spots on the downconversion cone to further amplify the data rate, allowing us to achieve over 10 Mbits of secure key per second.

***Keywords*—**Downconversion, Hyper-entanglement, Quantum Cryptography.

I. Introduction

THE nonclassical features of single and entangled photons can be used to establish a provably secure quantum communication channel – in fact, this is the only provably secure means of encryption. There have been many proof-of-principle quantum key distribution (QKD) experiments, and now even a few vendors of first-wave commercial systems. However, in all of these the final secret key rates are much lower than one would like for an ideal practical system, where, e.g., one might want to encode at video rates. The protocols for the commercial systems only use a single qubit, which results in generating at most a single bit of key data per detection. To optimize the data rate of these QKD systems, each photon should carry the maximum information that can be detected. For instance, instead of only entangling the photons in polarization (as is the case in BB84), we can also entangle the photon in additional degrees of freedom through hyper-entanglement [1]. Using these other entangled degrees of freedom, we can encode additional bits per photon (bpp). As an example, if each photon is allowed to appear in one of 1024 time-bins or spatial 'pixels,' then a single detection event in principle could yield $\log_2 1024=10$ bits [2], with up to an additional bit of shared entropy from the polarization degree of freedom, for up to 11 bbp. We are currently pursuing this technique to thereby realize a system with over 10 bpp and a total data rate of at least 10^9 bits per second after multiplexing many channels.

II. Higher-Dimensional QKD

To achieve the high data rate, we need to efficiently use every photon by accessing the full parameter space. The timing DOF is used to encode the majority of the bits per photon. By using a PBS and a delay line to create additional laser pulses, we can increase the repetition rate of the pump to increase the number of available time-bins that the photon can arrive in. Each doubling of the laser pulse rate adds up to an additional bit of random information (the photon has twice as many time-bins it can appear in). However, we cannot raise the repetition rate indefinitely, since the detectors have an intrinsic timing jitter; we can thus only increase the pump until the jitter in the detectors blur which time-bin the photon was produced in (see Fig. 1).

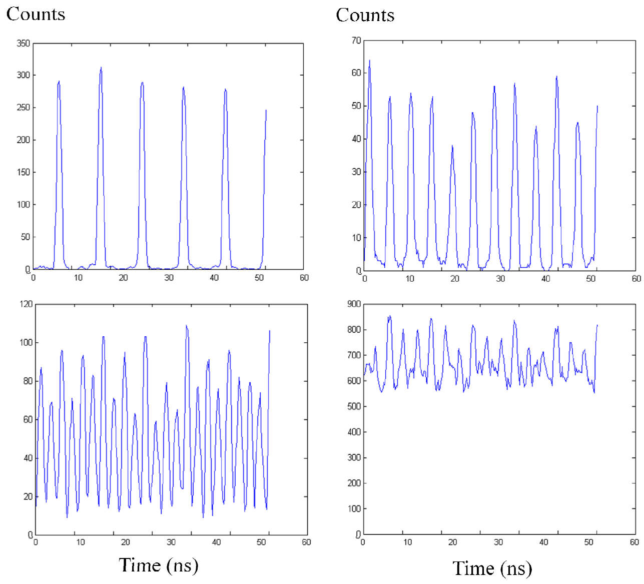

Fig. 1 The autocorrelation of the single-photon detectors shows how well the detectors can distinguish neighboring pulses. As we increase the repetition rate of the laser (120 MHz, 240 MHz, 480 MHz, 960 MHz), the pulses begin to merge together and can no longer be distinguished. There is extra broadening in these figures from taking the autocorrelation (the pulses are broadened by a factor of √2). When two neighboring pulses cannot be distinguished, there will be no additional shared entropy between Alice and Bob for additionally increasing the repetition rate of the laser.

The polarization degree of freedom adds an additional ½ bit of information (Alice and Bob must randomly choose between two measurement bases, only half of the measurements result in any shared information – this can be increased by biasing one basis choice over the other [3]) and is used as a security check. Currently, we assume that there exist no quantum non-

B. G. Christensen is with the Department of Physics, University of Illinois, Urbana, IL 61801 USA (phone: 217-244-1608; e-mail: bgchris2@ illinois.edu).

P. G. Kwiat and D. Kumor are also with Department of Physics, University of Illinois.

K. T. McCusker, was with the Department of Physics, University of Illinois, Urbana, IL 61801 USA. He is now with the Department of Physics & Astronomy, Northwestern University, Evanston, IL 60208 USA.

D. J. Gauthier is with the Department of Physics, Duke University, Durham, NC 27708 USA.

V. Chandar is with the Department of Physics, Massachusetts Institute of Technology, Cambridge, MA 02139 USA.

demolition (QND) measurements that can detect the time-bin of the photon without disturbing the polarization. To our knowledge no such experimental capability exists at present; currently realized QND methods thus far only work with microwave photons in ultra-high finesse superconducting cavities, and still disturb polarization. However, to be secure against any eavesdropper without assuming technological constraints, we need to eventually be able to completely secure the timing DOF. One option, similar to the polarization implementation, is to measure in a mutually unbiased basis (MUB). One possible MUB is the Fourier Transform basis,

$$|\phi_k\rangle = \frac{1}{\sqrt{M}}\sum_{n=0}^{M-1}\exp\left(\frac{2\pi nk}{M}\right)|t_n\rangle .$$

Measuring in this basis, however, requires an extremely large array of stable interferometers if we want to check the full 10 timing bits of each photon. We are still exploring other more efficient, stable, and secure ways of detecting an eavesdropper (Eve). For instance, by measuring the coherence between different sets of time-bins (e.g., the phase between |t = 0> and |1> as well as the phase between |0> and |10>) we can infer the maximum amount of information Eve could have detected, setting an upper bound on the amount of privacy amplification necessary. Another option is to measure the spectral correlations between Alice and Bob's photons. Any measurement made that localizes the photon in time, will alter the spectral bandwidth of the photons. We are still exploring these options to determine which will require the least amount of additional (and potentially unnecessary) privacy amplification from the inferred information taken by Eve. Finally, the spatial degree of freedom for the photons will be used to multiplex multiple channels together to maximize the data rate.

III. Experimental Setup

For the experiment, we use a 4-Watt, 120-MHz repetition rate laser (see Fig. 2). The laser pumps two orthogonal BiBO nonlinear crystals to produce polarization entanglement in the downconversion photons. The long coherence time of the laser enables the temporal entanglement. By using beamsplitters, we can increase the pulse rate of the laser to 960 MHz. Two locations on the downconversion cones are collected into independent single-mode fibers for spatial filtering. The polarization entanglement is verified by subsequently passing the photons from both channels through a polarization analysis. A nonpolarizing beamsplitter randomly sends the photons to be measured in the H/V or the D/A basis as a check for an eavesdropper. We use AR-coated, low-crosstalk Brewster angle polarizing beamsplitters (extinction ratio greater than 8700:1) to make the polarization measurement. The photons then pass through custom interference filters that create a 20-nm transmission band before being detected by single-photon-counting modules. The two polarization analysis channels share the same optical components (by being spatially separated), but are sent to different detectors as depicted in Fig. 2. The detector outputs are sent to a time-to-digital converter to measure the relative arrival time of the photons.

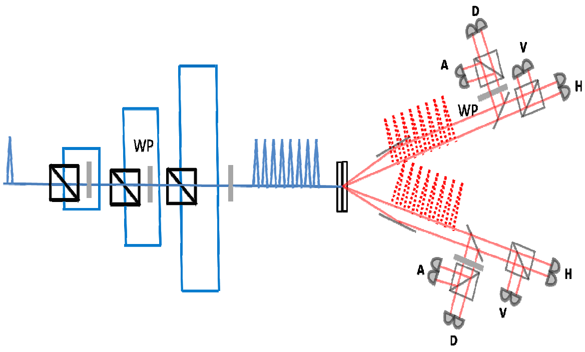

Fig. 2 Each laser pulse (at 120 MHz) is split into 8 pulses via 3 different delay lines (roughly 1-ns, 2-ns, and 4-ns delay loops). After each delay loop, the pulse is passed through a waveplate to keep equal amplitudes in each pulse. These delay loops increase the laser repetition rate so that more information is sent per photon. All of these pulses are within the coherence length of the laser, so the resulting dowconversion is time-bin entangled. We collect from two spots on the same downconversion cone (the same wavelength range is used for both channels). Each channel shares the same beamsplitters, waveplates, and filters, but is sent to independent detectors.

IV. Data

Current data is shown in Table I. The singles and coincidence rates given are the average of the count rates over all 8 channels. The bit error rate (BER) is the percent of the data where Alice and Bob measure different polarizations in the same basis, and represents the fraction of information Eve

TABLE I
Higher-Dimensional QKD System Statistics

	High Data Rate (High Power)	High Bits Per Photon (Low Power)
Singles Rate	5.8 MHz	150 kHz
Coincidence Rate	1.9 MHz	45 kHz
Bit Error Rate (Polarization)	0.8%	0.4%
Entropy Per Second	10.4 Mbits	470 kbits
Bits Per Coincidence	5.5 bpp	10.4 bpp
Expected Secure Entropy Per Second	5.9 Mbits	270 kbits

The two sets of data were generated by changing the laser power to increase (or decrease) the average number of photon pairs created per second. With lower singles rate, the number of time-bins in which each photon could have been born is increased, thus increasing the bits per photon. The entropies listed include both the data from the timing and polarization degree of freedom. Bits per coincidence is calculated in terms of shared entropy per coincidence (instead of secure entropy per coincidence). The excepted secure entropy is the entropy retained after decoding the two data strings along with privacy amplification from the BER. This table is for one of the two channels, the second channel operates at approximately 80% of the capacity of the displayed channel.

potentially knows, and therefore determines the amount of privacy amplification necessary. As the pump power increases, the probability of generating two uncorrelated pairs of photons also increases. If Alice and Bob detect photons from the different pairs, an uncorrelated polarization coincidence results, increasing in the bit error rate. As the pump repetition rate increase, there is less energy per pulse, and therefore the probability of generating multiple pairs per pulse is reduced (and the BER is thus decreased). Utilizing detectors with reduced jitter, we expect to be able to increase the laser repetition rate to 1.92 GHz, and potentially even to 3.84 GHz. The entropy per coincidence and entropy per second are calculated directly from the singles and coincidences. A low-density parity-check (LDPC) code is used to decode the two data strings at approximately 60% of the Shannon limit. The resultant code will be sent through privacy amplification to secure the secret key from any eavesdropper.

V. Conclusion

We have demonstrated a high-speed quantum cryptography system that uses hyper-entangled photons to operate at a secure key rate of 10.6 Mbits/s. By decreasing the pump power, we can also generate over 10 bits of shared entropy per coincidence. Currently the data rate is limited by detector saturation, and the bits per photon are limited by detector jitter. We are currently characterizing improved detectors to further enhance the system. Future work also includes removing the need to assume a technologically limited eavesdropper, in addition to collecting from additional locations on the downconversion cone.

Acknowledgment

This research was supported by the DARPA InPho program through the US Army Research Office award W911NF-10-1-0395.

References

[1] Julio T. Barreiro, et. al., Phys. Rev. Lett. **95**, 26051 (2005).
[2] I. Ali-Khan, C. J. Broadbent, and J. C. Howell, Phys. Rev. Lett. 98, 060503 (2007).
[3] H.-K. Lo, H. F. Chau, and M. Ardehali, J. Cryptol. **18**, 133 (2005).