High-dimensional time-energy entanglement-based quantum key distribution using dispersive optics

Catherine Lee[1,2†], Zheshen Zhang[1], Jacob Mower[1], Greg Steinbrecher[1], Hongchao Zhou[1], Ligong Wang[1], Robert D. Horansky[3], Varun B. Verma[3], Michael S. Allman[3], Adriana E. Lita[3], Richard P. Mirin[3], Francesco Marsili[4], Andrew D. Beyer[4], Matthew D. Shaw[4], Sae Woo Nam[3], Gregory Wornell[1], Franco N. C. Wong[1], Jeffrey H. Shapiro[1], and Dirk Englund[1]

[1] *Research Laboratory of Electronics, Massachusetts Institute of Technology; 77 Massachusetts Ave, Room 36-575; Cambridge, MA 02139, USA*
[2] *Department of Physics, Columbia University; 538 West 120th St; New York, NY 10027, USA*
[3] *National Institute of Standards and Technology; 325 Broadway St; Boulder, CO 80305, USA*
[4] *NASA Jet Propulsion Laboratory; 4800 Oak Grove Dr; Pasadena, CA 91109, USA*

[†] *cath@mit.edu*

Abstract: We implement a high-dimensional quantum key distribution protocol secure against collective attacks. We transform between conjugate measurement bases using group velocity dispersion. We obtain > 3 secure bits per photon coincidence.

OCIS codes: (270.5568) Quantum cryptography, (060.5565) Quantum communications.

1. Introduction

High-dimensional quantum key distribution (QKD) allows two parties, Alice and Bob, to establish a secret key at a potentially higher rate and photon information content than that afforded by two-level QKD protocols. Alice and Bob can generate secure infomation based on the correlations between a pair of entangled photons. Energy-time entanglement is particularly appealing because the photon correlations are well-preserved over tranmission through both single-mode optical fiber and free space. We report the first implementation of dispersive-optics QKD (DO-QKD), a high-dimensional protocol based on energy-time entanglement of pairs of photons, with proven security against collective attacks [1].

2. Theory

In DO-QKD, entangled photon pairs are generated by a spontaneous parametric downconversion (SPDC) source held by Alice. Alice retains one photon in the pair and sends the other to Bob. Alice and Bob detect their photons in two conjugate measurement bases — either directly or after normal/anomalous group-velocity dispersion (GVD). If Alice applies normal dispersion and Bob applies anomalous dispersion of equal magnitude to their respective halves of an entangled pair, then the original correlations between their photons can be recovered [2]. A schematic of this setup is presented in Fig. 1.

To show security against collective attacks, we calculate the secure key capacity, i.e., Alice and Bob's information advantage over Eve. The secure key capacity, in terms of bits per detected coincidence (bpc), is defined in the asymptotic regime (for infinitely long keys) as

$$r = \beta I(A;B) - \chi(A;E), \tag{1}$$

where β is the reconciliation efficiency, $I(A;B)$ is Alice and Bob's Shannon information, and $\chi(A;E)$ is Alice and Eve's Holevo information. By measuring the covariance matrix, we can bound the information accessible to Eve, and any information that Alice and Bob share in excess of this bound will be secure.

3. Experiment

We implemented the setup shown in Fig. 1 using a periodically-poled potassium titanyl phosphate (PPKTP) waveguide-based SPDC source, WSi superconducting nanowire single-photon detectors (SNSPDs), and dispersion compensators providing 600 ps/nm of dispersion.

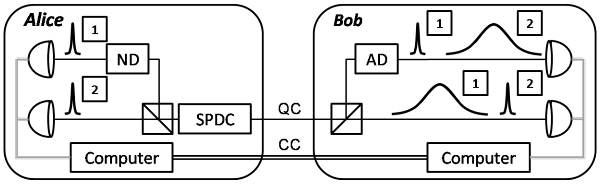

Fig. 1. Schematic of the DO-QKD setup. Alice holds the SPDC source, keeps one photon, and sends the other to Bob. In case 1, Alice measures in the dispersed arrival-time basis, and in case 2, she measures in the arrival-time basis. Bob must measure in the same basis as Alice for their measurements to be correlated. QC is quantum communication, CC is classical communication, ND is normal dispersion, and AD is anomalous dispersion.

If Alice and Bob both measure their photons directly, they see narrow timing correlations, as pictured in Fig. 2(a). However, if only one party applies dispersion and the other does not, the timing correlations are lost or severely diminished, depending on the magnitude of the dispersion applied. This is pictured in Fig. 2(b) and (c). If Alice and Bob both apply dispersion, then the original correlations between their photons are recovered, as pictured in Fig. 2(d).

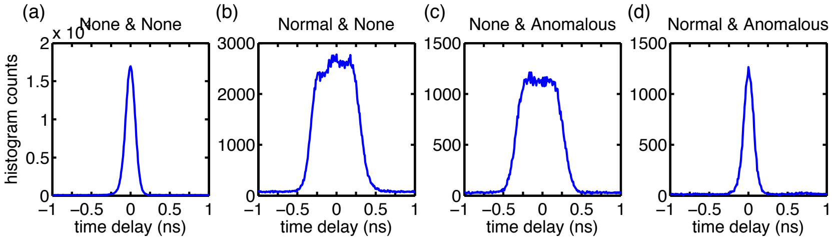

Fig. 2. (a) If Alice and Bob measure their photons directly, they see a narrow coincidence peak. (b, c) If only one party applies group-velocity dispersion, Alice and Bob see a broadened coincidence peak. (d) If Alice applies normal dispersion and Bob applies anomalous dispersion, they again see a narrow coincidence peak.

Following the acquisition of time-tagged data from the SNSPDs, we sifted the time-tagged data into time frames composed of d bins, where d is the dimension of the protocol. We keep only data from the frames in which Alice and Bob both recorded one detection event in the same basis. The sifted keys are sequences of characters $0,1,2,\ldots,d-1$, representing the bin within each frame when the photon was detected. The sifted keys were not identical, mainly due to timing jitter in the SNSPDs, so Alice and Bob correct their errors by employing a layered low density parity check (LDPC) code [3] such that Alice and Bob agree on an identical random sequence.

4. Results

Based on our setup, we bounded Eve's information to <1 bpc. This led to a maximum of 3.2 secure bpc with low SPDC pump power (0.16 photons/frame). Increasing the pump power leads to a larger entangled pair generation rate but also to a larger probability of multipair events, which lower the information per coincidence. At high SPDC pump power (1.1 photons/frame), we generated secure information at a maximum rate of 260 kbps, with 1.7 secure bpc.

References

1. J. Mower, Z. Zhang, P. Desjardins, C. Lee, J. H. Shapiro, and D. Englund, "High-dimensional quantum key distribution using dispersive optics," Phys. Rev. A **87**, 062,322 (2013).
2. J. D. Franson, "Nonlocal cancellation of dispersion," Phys. Rev. A **45**, 3126–3132 (1992).
3. H. Zhou, L. Wang, and G. Wornell, "Layered schemes for large-alphabet secret key distribution," in "Information Theory and Applications Workshop (ITA), 2013," (IEEE, 2013), pp. 1–10.