AFRL-RD-PS
TP-2009-1027

AFRL-RD-PS
TP-2009-1027

FREE-SPACE QUANTUM KEY DISTRIBUTION USING MULTILEVEL ENCODING VIA TRANSVERSE FIELD MODULATION: PREPRINT

Mark T. Gruneisen

Air Force Research Laboratory
3550 Aberdeen Ave SE
Kirtland AFB, NM 87117

1 August 2009

Technical Paper

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.

AIR FORCE RESEARCH LABORATORY
Directed Energy Directorate
3550 Aberdeen Ave SE
AIR FORCE MATERIEL COMMAND
KIRTLAND AIR FORCE BASE, NM 87117-5776

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-0188*

1. REPORT DATE *(DD-MM-YYYY)* 01-08-2009	**2. REPORT TYPE** Technical Paper	**3. DATES COVERED** *(From - To)* *1 August 2009*

4. TITLE AND SUBTITLE Free-Space Quantum Key Distribution using Multilevel Encoding via Transverse Field Modulation; Preprint	**5a. CONTRACT NUMBER** NONE **5b. GRANT NUMBER** NONE **5c. PROGRAM ELEMENT NUMBER** NONE
6. AUTHOR(S) Mark T. Gruneisen	**5d. PROJECT NUMBER** NONE **5e. TASK NUMBER** NONE **5f. WORK UNIT NUMBER** NONE
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Air Force Research Laboratory 3550 Aberdeen Ave SE Kirtland AFB, NM 87117	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) Air Force Research Laboratory 3550 Aberdeen Ave SE Kirtland AFB NM 87117-5776	**10. SPONSOR/MONITOR'S ACRONYM(S)** AFRL/RDSE **11. SPONSOR/MONITOR'S REPORT NUMBER(S)** AFRL-RD-PS-TP-2009-1027

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release.

13. SUPPLEMENTARY NOTES

Accepted for publication at the Topical meeting on Applications of Lasers for Sensing and Free Space Communications; http://www.osa.org/meetings/topicalmeetings/LSC/default/.aspx. 1-3 Feb 2010. San Diego, CA. 377ABW-2009-1159; 11 Sep 2009. "Government Purpose Rights"

14. ABSTRACT

Transverse modulation of the complex optical field defines sets of orthogonal states for multilevel quantum key distribution. Principles of holography are evaluated as a means of generating and sorting the single photon states.

15. SUBJECT TERMS

Quantum cryptography; Quantum communications; Diffractive optics; Volume gratings; Wave propagation

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** Mark Gruneisen
a. REPORT Unclassified	**b. ABSTRACT** Unclassified	**c. THIS PAGE** Unclassified	SAR	6	**19b. TELEPHONE NUMBER** *(include area code)* 505- 846-9298

Free-Space Quantum Key Distribution using Multilevel Encoding via Transverse Field Modulation

Mark T. Gruneisen
Air Force Research Laboratory, Directed Energy Directorate
AFRL/RDSE Kirtland AFB, NM 87117-5776

Abstract: Transverse modulation of the complex optical field defines sets of orthogonal states for multilevel quantum key distribution. Principles of holography are evaluated as a means of generating and sorting the single photon states.

OCIS codes: 270.5568 Quantum cryptography; 270.5565 Quantum communications; 050.1970 Diffractive optics; 050.7330 Volume gratings; 070.7345 Wave propagation

1. Introduction

Quantum key distribution (QKD) refers to a technique for sharing encryption keys that utilizes principles of quantum uncertainty to detect eavesdropping [1,2]. The BB84 protocol introduced by Bennett and Brassard in 1984 utilizes two orthogonal polarization states in a given basis to define the quantum bit, or qubit, values. Polarization is described by two dimensions and may be represented in any of three complementary bases; namely vertical/horizontal, +/-45-degrees, and right-hand/left-hand circular polarization. In the BB84 protocol, sensitivity to eavesdropping is ensured by randomly changing the polarization basis. Figure 1 shows the sender, Alice, and the receiver, Bob, randomly switching between two complementary bases. When Alice and Bob choose the same basis, a qubit may be unambiguously transmitted and measured. Measurements with complementary bases however yield random outcomes and a sifting process discards these qubits. Should an eavesdropper, Eve, attempt to discretely divert, measure, clone, and resend photons, she will sometimes choose the wrong bases and the thereby introduce bit errors that alert Alice and Bob to her presence. Polarization encoding offers many compelling benefits for free-space QKD including insensitivity to atmospheric propagation and availability of inexpensive and robust optics for creating and sorting polarized photons.

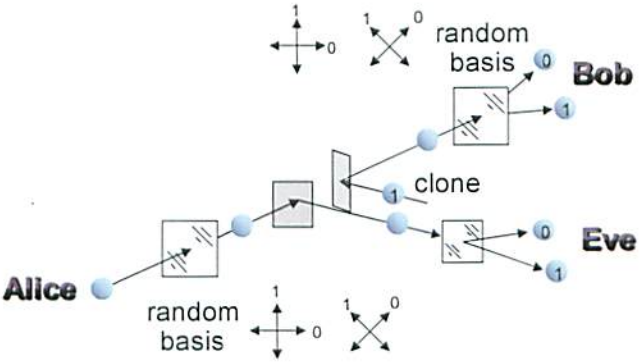

Fig. 1 Schematic of a BB84 quantum key distribution system.

It has been proposed that implementing QKD in dimensions greater than binary can result in increased security and bandwidth [3]. As the dimension d increases, the number of complementary bases increases correspondingly with as many as d+1 bases possible. With increasing number of bases, the probability that Eve will randomly choose the correct basis decreases and the bit error rate due to eavesdropping increases enhancing the detectability of eavesdropping. If fewer than all of the bases are utilized, the increased information content of the d-level "qudit" may be, at least partially, realized.

Polarization is a vector characteristic of the optical field and intrinsically two-dimensional. However, the scalar properties of the complex field (i.e. transverse modulation of the amplitude and phase) can be utilized to define arbitrarily large sets of orthonormal complex fields in which free-space QKD could be implemented. For example, the Laguerre-Gaussian and Hermite-Gaussian functions each provide a complete basis set of orthogonal functions in which one can represent solutions to the paraxial wave equation [4]. While polarization is understood to be a manifestation of the photon's spin angular momentum, the azimuthal phase component of the Laguerre-Gaussian polynomials is understood to be a manifestation of the photon's orbital angular momentum [5,6].

2. Components of a free-space d-level QKD system based on transverse field modulation

Practical implementation of free-space QKD based on transverse field modulation (TFM) poses several challenges. From an initial basis comprised of orthonormal complex optical fields, it is straightforward to define the additional complementary bases [7]. The amplitude and phase modulation associated with these complex fields are to be imparted to photons with fidelity sufficient to establish orthogonality among the states of each basis. Corruption of these states due to atmospheric and diffractive propagation is to be considered and, finally, a robust technology for sorting the photons with high efficiency and low cross talk is needed. In the discussion that follows, we take the complex field of classical optics to be representative of the quantum probability amplitude of the photon state [8].

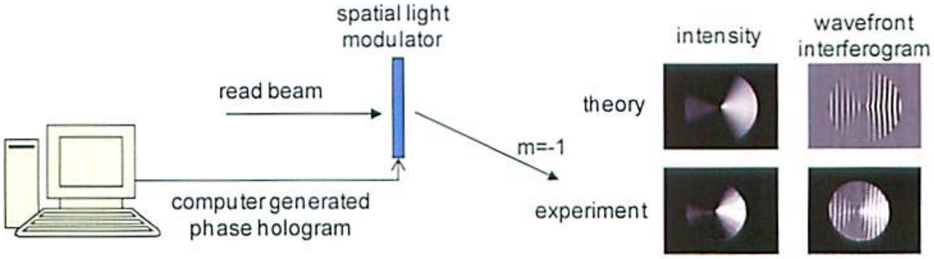

Fig. 2 Generation of d-level states with computer-generated holography and a spatial light modulator.

The Leith-Upatnieks approach to holography utilizes interference between an optical field and a reference wave to encode both amplitude and phase information in the hologram. We have shown that computer-generated holography (CGH) implemented with high-resolution liquid-crystal spatial light modulators (SLMs) is a promising technique for creating the required amplitude and phase modulation with sufficient fidelity [7]. Figure 2 shows an excerpt from ref. [7] in which an initial basis comprised of three azimuthal phase functions is used to generate the 3 additional complementary bases. The Leith-Upatnieks interference function associated with one state in one of the complementary bases is calculated, scaled and displayed on a 512x512 element phase modulator. The figure shows the calculated intensity and wavefront interferogram associated with the theoretical state and that achieved experimentally in the m=-1 diffracted order.

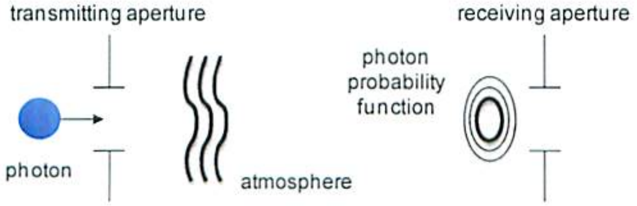

Fig. 3 Propagation effects include atmospheric turbulence and diffraction.

Figure 3 illustrates propagation phenomena that can corrupt the amplitude and phase modulated photon states. These include both atmospheric aberrations and diffraction. The effects of atmospheric turbulence on the optical phase associated with azimuthal phases has been evaluated analytically and shown to randomize the photon states adaptive optics technologies can mitigate the effects of turbulence on optical phase. However, the fidelity with which one can compensate turbulence may be limited by many parameters. These include atmospheric parameters associated with range, altitude and elevation as well as the performance characteristics of the adaptive optics system.

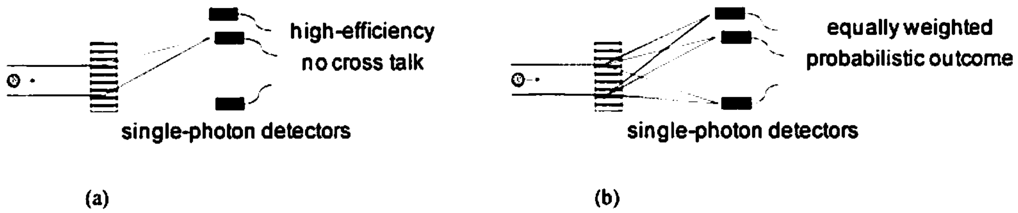

Fig. 4 An ideal photon sorter in a 3-level QKD system showing sorting with (a) correct basis and (b) incorrect basis.

Figure 4 shows a schematic representation of an ideal photon sorter in a 3-level system. An incident photon is described by one of three states in as many as four bases. When the sorting element and photon are associated with the same basis, the photon is binned to one of three detectors that reveal the state within that basis as shown in Fig. 4(a). When the sorting element and photon are associated with different bases, there is equal probability of measuring any state within the measurement basis as shown in Fig. 4(b). Proposed approaches to photon sorting include interferometry [11], cascaded volume holograms [12], and volume multiplexed holograms [13]. In the multiplexed hologram approach, one hologram is prepared per basis. Each state of the basis is recorded with a unique reference wave in a separate exposure. Upon readout, the matched hologram efficiently diffracts light from each state of the basis to reconstruct the appropriate reference wave. Holograms associated with other bases will disperse light uniformly among all reference waves associated with the hologram. A coupled mode theory analysis of volume multiplexed holograms generated from plane-wave-derived bases captures the phenomenology of phase and amplitude modulation and indicates that the ideal sorting characteristics described above should be achievable [13]. Demonstrations of volume Bragg gratings as angular magnifiers with high efficiency and low cross talk also indicate that such technology may be realizable [14].

Acknowledgements

The author wishes to acknowledge collaborations with Raymond Dymale, Glenn Tyler, and Warner Miller.

References

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," in Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India (IEEE, New York, 1984) 175-179

[2] G. Brassard, "A brief history of quantum cryptography: a personal perspective," proc. IEEE (2005)

[3] M. Bourennane, A. Karlsson, G. Björk, N. Gisin, and N. J. Cerf, "Quantum key distribution using multilevel encoding: security analysis," J. Phys. A: Math. Gen. 35 (2002) 10065-10076

[4] A. E. Siegman, *Lasers*(University Science Books, 1986), Chap. 16.

[5]. L. Allen, M. W. Beijersbergen, R. J. C. Spreeuw, and J. P. Woerdman, "Orbital angular momentum of light and the transformation of Laguerre-Gaussian laser modes," Phys. Rev. A 45, 8185-8189 (1992).

[6] *Optical Angular Momentum*, L. Allen, S. M. Barnett, and M. J. Padgett (IOP Publishing Ltd., London, 2003)

[7] M. T. Gruneisen, W. A. Miller, R. C. Dymale, and A. Sweiti, "Holographic generation of complex fields with spatial light modulators: Application to quantum key distribution," App. Opt. 47(4), A33-A42 (2008).

[8] C. Cohen-Tannoudji, B. Diu, and F. Laloë, *Quantum Mechanics*(John Wiley & Sons, 1977), Chap. 1.

[9] C. Paterson, "Atmospheric turbulence and orbital angular momentum of single photons for optical communication," PRL 94, 153901 (2005).

[10] G. A. Tyler and R. W. Boyd, "Influence of atmospheric turbulence on the propagation of quantum states of light carrying orbital angular momentum," Opt. Lett. 34, 142-144 (2009).

[11] J. Leach, J. Courtial, K. Skeldon, S. M. Barnett, S. Franke-Arnold, and M. J. Padgett, "Interferometric methods to measure orbital and spin, or the total angular momentum of a single photon," Phys. Rev. Lett. 92, 013601 1-4 (2004).

[12] J. A. Anguita, M. A. Neifeld, and B. V. Vasic, "Turbulence-induced channel crosstalk in an orbital angular momentum-multiplexed free-space optical link," App. Opt. 47, 2414-2429 (2008).

[13] W. A. Miller and M. T. Gruneisen, "Efficient photon sorter in a high-dimensional Hilbert space," arXiv:0810.0336v2 [quant-ph] 3 Oct 2008.

[14] L. Glebov, "Volume Bragg Gratings in PTR glass – new optical elements for laser design," abstr-240-2, 2008, Nara, Japan.

DISTRIBUTION LIST

DTIC/OCP
8725 John J. Kingman Rd, Suite 0944
Ft Belvoir, VA 22060-6218 1 cy

AFRL/RVIL
Kirtland AFB, NM 87117-5776 2 cy

Mark Gruneisen
Official Record Copy
AFRL/RDSE 1 cy