AFRL-RI-RS-TR-2016-067

INVESTIGATING QUANTUM MODULATION STATES

MARCH 2016

FINAL TECHNICAL REPORT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

STINFO COPY

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE

■ **AIR FORCE MATERIEL COMMAND** ■ **UNITED STATES AIR FORCE** ■ **ROME, NY 13441**

NOTICE AND SIGNATURE PAGE

Using Government drawings, specifications, or other data included in this document for any purpose other than Government procurement does not in any way obligate the U.S. Government. The fact that the Government formulated or supplied the drawings, specifications, or other data does not license the holder or any other person or corporation; or convey any rights or permission to manufacture, use, or sell any patented invention that may relate to them.

This report was cleared for public release by the 88th ABW, Wright-Patterson AFB Public Affairs Office and is available to the general public, including foreign nationals. Copies may be obtained from the Defense Technical Information Center (DTIC) (http://www.dtic.mil).

AFRL-RI-RS-TR-2016-067 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

FOR THE CHIEF ENGINEER:

/ S /
RICHARD MICHALAK, Chief
Information Transmission Branch
Computing & Communications Division

/ S /
JOSEPH A. CAROLI
Acting Tech Advisor, Computing
& Communications Division
Information Directorate

This report is published in the interest of scientific and technical information exchange, and its publication does not constitute the Government's approval or disapproval of its ideas or findings.

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

1. REPORT DATE *(DD-MM-YYYY)* MARCH 2016	**2. REPORT TYPE** FINAL TECHNICAL REPORT	**3. DATES COVERED** *(From - To)* OCT 2012 – SEP 2015

4. TITLE AND SUBTITLE INVESTIGATING QUANTUM MODULATION STATES	**5a. CONTRACT NUMBER** IN-HOUSE
	5b. GRANT NUMBER N/A
	5c. PROGRAM ELEMENT NUMBER 61102F
6. AUTHOR(S) David H. Hughes, Reinhard Erdman, Vladimir Nikulin	**5d. PROJECT NUMBER** T1QD
	5e. TASK NUMBER IN
	5f. WORK UNIT NUMBER HO
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Air Force Research Laboratory/RITE 525 Brooks Road Rome NY 13441-4505	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Air Force Research Laboratory/RITE 525 Brooks Road Rome NY 13441-4505	**10. SPONSOR/MONITOR'S ACRONYM(S)** AFRL/RI
	11. SPONSOR/MONITOR'S REPORT NUMBER AFRL-RI-RS-TR-2016-067

12. DISTRIBUTION AVAILABILITY STATEMENT

Approved for Public Release; Distribution Unlimited. PA# 88ABW-2016-0953
Date Cleared: 2 MAR 2016

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This effort was primarily concerned with quantum aspects of optical communications. Two quantum communications technologies were studied: (1) Vulnerabilities in coherent state quantum data encryption, and (2) Quantum operations on entangled photon pairs using Lyot filters. Both operations enjoy security due to an eavesdropper's measurement disadvantage with respect to authorized users. This insures the authorized users enjoy an information advantage over the eavesdropper when measuring the quantum states, be they coherent state quantum data encryption or entangled photon pair quantum key distribution.

15. SUBJECT TERMS

Quantum Key Distribution, Quantum Data Encryption, Entangled Photons

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** **DAVID H. HUGHES**
a. REPORT U	**b. ABSTRACT** U	**c. THIS PAGE** U	UU	22	**19b. TELEPHONE NUMBER (*Include area code)*** **N/A**

Table of Contents

1.0 Summary

T1QDINHO was primarily concerned with quantum aspects of optical communications. Two quantum communications technologies were studied: (1) Vulnerabilities in coherent state quantum data encryption, and (2) Quantum operations on entangled photon pairs using Lyot filters. Both operations enjoy security due to an eavesdropper’s measurement disadvantage with respect to authorized users. This insures the authorized users enjoy an information advantage over the eavesdropper when measuring the quantum states, be they coherent state quantum data encryption or entangled photon pair quantum key distribution. A large part of authenticated users advantage resides in pre-shared knowledge of a measurement reference frame. In the case of entangled pair quantum key distribution, the simple fact that a measurement by an intruder in an intercept and resend attack incurs detectable correlation errors by the legitimate users.

2.0 Introduction

Prof. Nikulin focused his efforts on vulnerability analyses of coherent state data encryption begun with his student, Vigit Bedi, in FY 2013 and carried innovatively on through FY15. His work has been very productive. It is summarized in section 3.1.

FY14 and FY15 saw much more in-house focus on modeling entangled photon pair propagation through modified Lyot filter stages accomplished by Hughes and Erdman. Several circuits achieving related but distinct output states have been constructed, one of which has been submitted to the US Patent Office, and another will soon follow. Those circuits with brief explanation are presented in section 3.2.

3.0 Methods, Assumptions, and Procedures

3.1 Investigating Coherent State Quantum Data Encryption Confidentiality

Coherent state quantum data encryption is highly interoperable with current classical optical infrastructure in both fiber and free space optical networks. Coherent states are the most classical of quantum states. Generation and detection of their polarization and phase modulations are well understood and they can be amplified without disturbing too much the quantum nature of those modulations which possess noise. Shot noise in the detection process incurs ambiguity in the interpretation of measurement results. When the average photon number per transmission of a message bit grows sufficiently small, and the number of possible modulation states grows large, the variance of the information carrying modulation state increases. This causes uncertainty in the value of precisely what the modulated state is.

An eavesdropper intercepting the ciphertext, or some portion of it, can perform a coherent measurement in an attempt to measure the phase and amplitude of the signal – the first step in an attempt to exploit the resulting estimates to gain the information conveyed therein. Is the message bit sent a one or zero? That eavesdropper's minimum probability of error converges to ½, a coin toss, when the average photon number and the number of possible states satisfy the aforementioned conditions. The eavesdropper suffers a measurement disadvantage relative to authorized users, which translates to an information advantage for the users when they are confronted with the same modulation uncertainty in their measurements.

Mitigating uncertainties in legitimate user's measurements of ciphertext states exchanged between them is the fact that they share a short secret key that is expanded into very long running keys by a highly complex block stream cipher. The stream cipher maps message bits onto random blocks of bits producing modulated states that are intrinsically noisy. The ciphertext so generated is equally noisy to eavesdropper and legitimate users. Since legitimate users share the short secret key and the algorithm generating the ciphertext, they can invert that transformation and perform a well discriminated binary decision. They don't have to estimate the modulation by performing a coherent detection estimate with ambiguous results, for they each know what modulation block is used to perform the transformation in each bit sent. Thus, if legitimate user A encrypts a stream of message bits and sends them to partner B, B does not know what the message bit is. But B does know how to invert the modulation and reveal the best estimate on that modulation. They share a measurement advantage over E, the eavesdropper. Since E does not share the transformation, A and B enjoy an information advantage over E.

This situation is under assault. Ever better technology is beginning to encroach upon the uncertainty of the shot noise limit, diminishing the variance masking security at the heart of coherent state quantum data encryption. However, that trend toward achieving the so-called Heisenberg limit of uncertainty, which is smaller than the shot noise limit by a factor proportional to the square root of the average photon number, is not the only threat to quantum data encryption.

In each transmission event, it might be possible for E to estimate not the message bit sent, but some of the bits in the stream cipher block specifying the modulation state. Why? Think of a point on a circle. It resides at an angle to some reference angle. That angle is specified by an integer whose binary representation in terms of a bit string is comprised of an alphabet, {1,0}. For example, suppose the possible number of states available to legitimate users is N. An angle specified by another integer b is given by its position in along the half-circle as

$$\theta_n = \frac{\pi}{N-1} b_n \tag{1}$$

In (1), b is chosen by a stream cipher block, which is a pseudo-random bit stream generated by the stream cipher, say AES. Its binary representation is $\{b_n\} = (b_{N-1}, b_{N-2}, \ldots, b_1, b_0)$, b_j Ɛ {0,1}. If the mapping of the message bit, m, is done by simple XOR with the least significant bit of the block, b_0, by the legitimate sender, the nth message modulated angle is specified as,

$$\begin{aligned} \theta_n &= \frac{\pi}{N-1} b_n + 0, \quad \text{if } m_n \oplus b_0 = 0 \\ &= \frac{\pi}{N-1} b_n + \pi, \quad \text{if } m_n \oplus b_0 = 1 \end{aligned} \tag{2}$$

In (2), depending on the XOR between m and the least significant bit of b, the modulation angle for the message bit sent is in one plane or the plane diametrically opposed. All the legitimate user must do is invert the shared transformation and measure which "base band" angle is detected, 0 or π, which is logically 0 or 1. E cannot perform the inverse transformation even if E knows what stream cipher is used, say AES. E does not know the secret seed key used by A and B.

Exploitation attempts then focus on imperfect measurements and the estimation of the more significant bits used in each block specifying θ_n . These significant bits can be estimated, sometimes accurately. Knowing them, and the stream cipher used, with side channel knowledge about the message, a known plain text for example, E can execute an attack on the seed key itself. How effective such attacks are is the subject of Prof. Nikulin's recent research at AFRL. His research focused primarily on ascertaining via modeling and simulation the number of bits per block that can be estimated as a function of the mean number of photons per message bit and the number of possible modulation states extant per message bit sent. That is the starting point to exploitation on an intercepted message by intruder E.

3.2 Quantum Operations on Entangled Photon Pairs Using Lyot Filters

Quantum data encryption involves several to many photons per use of the quantum channel. Quantum key distribution, on the other hand, typically involves just one or two photons to engender secret keys. Those keys can be used to seed stream ciphers, as one time pads for session keys involving short messages such as distributing other secret keys to authorized users, etc. One of the oldest methods engendering secret keys using the quantum mechanical principles is BB84. Shared secret keys generated via BB84 utilize just one photon whose information carrier degree of freedom is typically its polarization observable in free space optical instantiations.

Two possible polarizations exist in each photon relative to a chosen frame of reference. Logical assignments of 1 or 0 are assigned to a polarization state. In a transmission event from A to B, say, in order to ensure maximum ambiguity to an eavesdropper E, two frames oriented at 45^{o} to one another are often used. A randomly chooses one of the two dimensional frames in which to encode a photon's polarization and sends that photon to B, who randomly chooses one of the two frames in which to measure the received polarization state. These frames can be switched by polarization modulators. They then perform basis, or frame reconciliation. Half the time they will agree. Those events wherein their basis choices differ are dropped, because they cannot be sure if in their separate frames they have measured the same polarization state. Only when their basis choices reside in the same frame can they be assured that polarization measurements made by B will agree with polarization states sent by A. Errors can exist, even when their reference frames agree. Hence, the foregoing activity is followed by error correction and then privacy distillation resulting in a shared secret key.

Due to deleterious rotational effects on polarization by random refraction index imperfections in most deployed optical fibers, phase shifting by A and then B in the quantum channel connecting legitimate users can be used as measurement bases. The quantum channel configuration is equivalent to a Mach-Zender interferometer and has two paths for transit from A to B. Phase modulators at each node, A and B, act just like the polarization modulators in the polarization case.

Another method generating secret keys is utilization of the manifestation of conserved quantities between two photons, both of which are engendered in a sufficiently compact space-time event. Degrees of freedom, or observables such as frequency and polarization, possessed by these photons are correlated due to conservation of energy and photon spin. This entanglement leads to non-local correlations and can be made manifest by measuring the relevant degrees of freedom at two displaced locations. One example of such a configuration is a server sends correlated photon pairs to users A and B who measure the relevant observables and infer the values of the other when the frames in which they measure agree, just like in BB84. A and B must also reconcile their measurement bases, and they must also perform error reconciliation and privacy distillation. The former must be done in order to ensure inferences they make on the state they measure about the state the other has measured agree.

Basis, or frame reconciliation induces a reduction by one half of the prospective shared keys. Horace Yuen proposes using Keyed Communication in Quantum Noise to mitigate this operational loss in throughput. If frame reconciliation is done prior to all transmission events by each relevant party sharing a long running key that was generated by one short, shared secret key and a stream cipher in order to choose subsequent shared frames, frame reconciliation is not necessary in fresh secret key generation. Moreover, a shared frame between users in each transmission event authenticates their legitimacy. The sharing of such information starts with trust. An eavesdropper is not a legitimate user, possessing no authenticating shared keys for frame choices, and this obtains whether using one photon or two entangled photons.

Wavelength division multiplexing is used in multi-access communications wherein K nodes are linked simultaneously with one master node in a hub and spokes configuration. One way to accomplish this in earth-centric free space is to deploy a hub node in some high earth orbit enjoying line-of-sight to assets at lower earth orbits to include the earth's surface. A technology we have been exploring is a hub possessing one aperture whose field of regard includes some number of spokes, each a field of view. The hub is comprised of a birefringent Lyot filter stage tree that simultaneously routes incoming and outgoing frequencies to and from each spoke. Each spoke within the hub's field of regard has a transmit/receive module that are endpoints of the Lyot filter stage tree within the hub's backend electro-optics control suite.

Designed for high rate multi-access laser communications, we became interested in entangled photon pairs propagating through at minimum one Lyot filter stage for quantum information applications. Such applications include entanglement routing and quantum key distribution. Thus we asked the questions can polarization entanglement be preserved in transit through the device? If not, can it be modified to do so? We answer the questions posed, in principle, in the affirmative. Reported here are two such modifications, a hyper-entangled photon server for quantum key distribution and an entangled photon router.

4.0 Results and Discussion

4.1.1 Design and Analysis of Receiver for Measuring Coherent States of Light in Free-space Quantum Encryption Channels - FY13-Nikulin and Bedi[[1]

Quantum communication (QC) is a form of laser communication technology that was developed to assure encrypted data transfer in applications that require additional security features. It uses quantum processes at the physical layer of encryption to hide the signal in irreducible quantum noise. By doing so and avoiding the extra mathematical complexity associated with traditional cryptography, this technology achieves very competitive performance characteristics. The range of potential applications for QC systems is broad and includes both free-space and waveguide links in secure banking operations, ground vehicles, mobile airborne and space-borne networking. Just like any laser communication technology, QC links are affected by several sources of distortions. Under practical conditions, atmospheric turbulence creates spatial and temporal fields of the refractive index that alter the phase of the signal. In addition, the hardware imperfections, such as phase noise of the laser sources, imprecise control of the drive electronics, etc., can affect the properties of the transmitted signal. As a result, not only normal signal detection by authorized parties, but also exploitation of quantum communication links becomes extremely difficult. Within the scope of this project, we work on the design and analysis of a coherent (heterodyne) receiver. Basic results of the laboratory measurements are combined with simulation studies of quantum systems with different number of encryption bases and operating at different power levels. This project complements other AFRL-funded research efforts in this area, including the design of optical communication transceivers and the development of encryption systems, including Alpha-Eta.

4.1.2 Statistical Analysis of the Secrecy of the Running Key in Quantum Encryption Channels Using Coherent States of Light - FY14 – Nikulin [2]

Optical quantum communication (QC) technology is based on the principles of quantum processes at the physical layer of encryption that can be used to hide signals in irreducible quantum noise. It was developed to assure encrypted data transfer in the applications that require additional security features, but without the extra mathematical complexity associated with traditional cryptography. Under practical conditions, QC links are affected by several sources of distortions including both external, e.g. atmospheric turbulence, and internal, such as phase noise of the laser sources, imprecise control of the drive electronics, etc. As a result, not only normal signal detection by authorized parties, but also exploitation of quantum communication links becomes extremely difficult. This year’s goal was to use our practical coherent receiver to develop enhanced statistical techniques for assessment of potential vulnerability of the running key. Basic results of the laboratory measurements are combined with simulation studies to develop the techniques can be used for both conceptual improvement of the encryption approach and for quantitative comparison of secrecy of different quantum communication protocols. This project complements other AFRL-funded research efforts in this area, including the design of optical transceivers and development of encryption systems.

4.1.3 Eavesdropping Detection Based on Statistical Analysis of the Estimates of the Running Key in Quantum Encryption Channels - FY15 – Nikulin [3]

Quantum communication (QC) signals present an extreme challenge to an eavesdropper who needs to inspect many decrypted cipher text possibilities to find a plaintext message, especially as the number of encryption bases N_b is increased and the mean photon-number $|\alpha|^2$ is decreased. Fig. 1 illustrates well-separated theoretical phase constellations and our experimental data that demonstrates a lot of uncertainty.

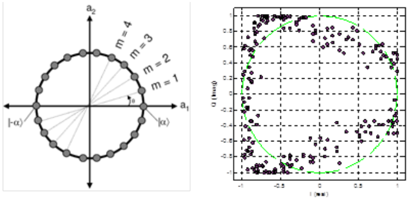

Figure 1. Phase constellations and measurements

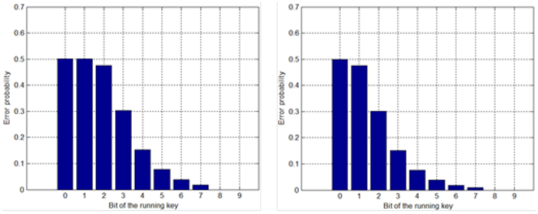

Figure 2. Running key error probability distributions

Under these conditions, the most practical kind of attack is intercept and resend (I&R), when each signal coming from Alice is measured by Eve in an attempt to determine the actual phase and the corresponding value of the running key. Then a new signal is prepared based on the result of the measurement and sent to the legitimate recipient Bob. It can be expected that when Eve tampers with the signal, she introduces artifacts that can be detected as follows. Each value of the running key that designates a particular phase encryption base can be expressed by the following bit sequence: (a^{m-1} a^{m-2} … a^0). Due to the quantum noise, only a certain number of the most significant bits (a^{m-1} a^{m-2} … a^n…) can be measured precisely. In addition, probabilities of correct measurement of the remaining bits (a^{n-1} a^{n-2} … a^0) can also be estimated from statistical analysis of the measurement errors. An example in Fig. 2 shows error probability distributions for each bit in the binary representation of the running key. With no eavesdropper present, this kind of distribution constitutes a “normalcy profile” (left subplot). When Eve tampers with a signal, additional distortions are introduced and the bit-wise distribution of errors is expected to change (right subplot). The main goals of this year’s effort include the development of an approach that establishes a normalcy profile for a quantum communication link and analyzes any deviations from it to identify potential attacks.

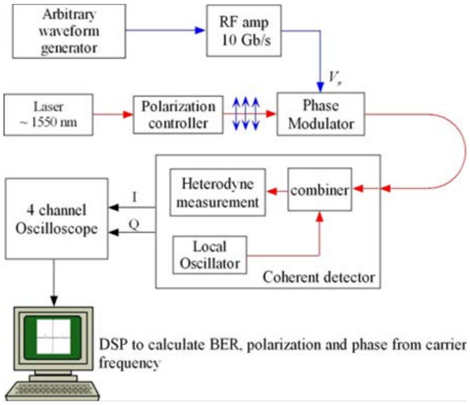

Figure 3. The experimental setup

Most of the work is being performed in the simulation environment with the plans to conduct experimental demonstration. With our laboratory system shown in Fig. 3 it is possible to perform measurements of the original encrypted signal (intercept part of the I&R attack). The results can also be used to verify the normalcy profile. Then the obtained estimates can be used to perform the second phase modulation of the optical signal and another set of measurements can be taken emulating Bob's signal received from Eve (resend part of the I&R attack). By obtaining the running key error probability distribution we can experimentally verify if our eavesdropping detection algorithm is capable of catching an attack in progress by analyzing this "signature" of the system.

The following tasks are identified for this phase of the project.

1. Research of the types of attacks in practical quantum communication channels and their effects on the received signal.

2. Mathematical modeling of the effects of eavesdropping on characteristics of the received signal.

3. Development of statistical analysis techniques and establishing the normalcy profile based on the binary representation of the running key.

4. Development of an analysis algorithm to detect deviation from the normalcy profile and detection of attacks.

5. Assessment of the accuracy of phase estimation for different numbers of encryption bases and different power levels (based on simulations and basic experimental results).

6. Re-design of the eavesdropping detection algorithm to reflect the findings during the summer phase of the program.

7. Adapting our coherent detection test bed to the experiments that emulate I&R attacks.

8. Performing measurements to establish normalcy profile and attack signatures.

9. Assessment of the accuracy of the eavesdropping detection algorithm for different experimental conditions of the QC systems with different numbers of encryption bases.

4.2.1 Multi-Frequency Entanglement Router System - Hughes and Erdmann [4]

A high performance free-space Wavelength Division Multiplexed (WDM) transceiver system is assessed as to its viability for routing collinear entangled photons in place of the classical optical signals for which it was designed. Explicit calculations demonstrate that entanglement in the Input State is retained throughout transit of the system, without intrinsic loss. Introduction of spatial degrees of freedom (DOF) altered the entanglement such that it could be manifested at remote locations, as required in Non-local Bell test measurements or Quantum Key Distribution (QKD) Protocols. It was also found that by adding another set of components, the system’s exit state was changed from being entangled in frequency to being polarization entangled. Finally it was found possible to route a complete entangled state to either of the two remote users by proper selection of the (discreet) frequencies at the input state. Each entanglement in the photon states was maximal, hence suited for Quantum Information Processing (QIP) applications. The device has been submitted for a patent and is shown in figure (4).

Input frequencies are non-degenerate and fall into two classes with respect to the Lyot filter stacks: (1) Congruent and (2) Incongruent. Polarization states of congruent frequencies remain invariant in transit through the Lyot filters, which are the blue rectangles in figure 4. Incongruent frequencies have their polarization states rotated by 90^{o}.

Under unitary evolution, input states and output states for congruent/incongruent frequencies, congruent/congruent frequencies, and incongruent/incongruent frequencies are shown in table 1.

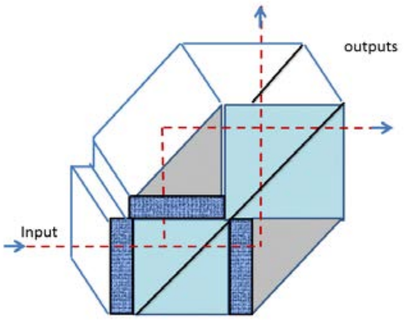

Figure 4. Multi-Frequency Entanglement Router System. The squares with diagonals crossing through their faces are polarization beam splitters.

Table 1 Input/Output Entanglement Router States

	1: Congruent/Incongruent
IN	$\left\|\psi_{in}\right\rangle = \frac{1}{\sqrt{2}}\left\| f_1, s_1, a;\ f_2, s_2, a\right\rangle + \frac{1}{\sqrt{2}}\left\| f_1, p_1, a;\ f_2, p_2, a\right\rangle$
OUT	$\left\|\psi_{PBS2}\right\rangle = \frac{1}{\sqrt{2}}\left\| f_1, s_1, b;\ f_2, s_2, a\right\rangle + \frac{1}{\sqrt{2}}\left\| f_1, p_1, b;\ f_2, p_2, a\right\rangle$
	2: Congruent/Congruent
IN	$\left\|\psi_{in}\right\rangle = \frac{1}{\sqrt{2}}\left\| f_1, s_1, a_1;\ f_2, s_2, a\right\rangle + \frac{1}{\sqrt{2}}\left\| f_1, p_1, a;\ f_2, p_2, a\right\rangle$
OUT	$\left\|\psi_{in}\right\rangle = \frac{1}{\sqrt{2}}\left\| f_1, s_1, b;\ f_2, s_2, b\right\rangle + \frac{1}{\sqrt{2}}\left\| f_1, p_1, b;\ f_2, p_2, b\right\rangle$
	3: Incongruent/Incongruent
IN	$\left\|\psi_{PBS2}\right\rangle = \frac{1}{\sqrt{2}}\left\| f_1, s_1, a;\ f_2, s_2, a\right\rangle + \frac{1}{\sqrt{2}}\left\| f_1, p_1, a;\ f_2, p_2, a\right\rangle$
OUT	$\left\|\psi_{PBS2}\right\rangle = \frac{1}{\sqrt{2}}\left\| f_1, H_1, a;\ f_2, H_2, a\right\rangle + \frac{1}{\sqrt{2}}\left\| f_1, \mathrm{V}_1, a;\ f_2, \mathrm{V}_2, a\right\rangle$

Polarization states denoted by s are perpendicular to the planes of incidence. They reflect at the polarization beam splitter interface. Polarization states denoted by p, travel through the polarization beam splitter interface, ideally without reflection. Congruent frequencies are the bluish colored states in table 1, while incongruent frequencies are signified by reddish color. Two congruent or two incongruent frequencies do not have to be the same frequency in each case. They simply have their polarizations either remain invariant for congruent and rotated by 90^o for incongruent. In all cases, the frequency/polarization entangled state arrives collinearly at the device along path/direction 'a'. For case 1, the exiting amplitude states split up by frequency to go in distinct directions a and b. Case 2 has both frequencies exiting in direction b, and case 3 just the opposite, with both frequencies exiting in direction a. In all cases, the amplitudes remain entangled in polarization and frequency. In case 1, however, path entanglement with frequency is not made manifest since there is no frequency randomness associated with a particular exit path. Polarization does exit randomly in both paths, however; frequency and path are entangled. Frequency and polarization are entangled in the remaining cases, but taken separately they are not manifestly entangled with path. Taken as two possibilities in one event, however, those states are entangled with path, because subject to the frequency compositions, which may arrive randomly at the entrance, the state can go in either direction, a or b.

4.2.2 Hyper-entangled Photon Server - Hughes and Erdmann [5]

Optical Physics Company's hyperspectral Lyot filter stage is designed for multi-access high capacity wavelength division multiplexing between a communications hub and spatially separated spokes. We asked the question, can polarization entanglement be preserved in transit through the device? If not, can it be modified to do so? We answer the questions posed, in principle, in the affirmative. Reported here and shown in figure (5) is one such modification. It employs a hyper-entangled bipartite input state possessing non-degenerate frequencies for advanced quantum communications.

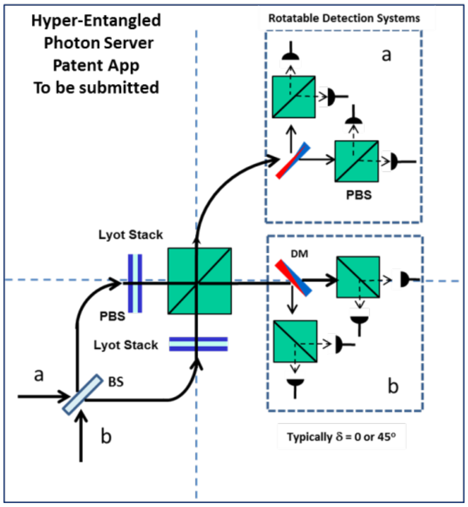

Figure 5. Hyper-entangled photon circuit

Table 2: Input/Output Hyper-Entangled Photon Server

Input State
$\left\vert\Psi_{in}\right\rangle=\frac{1}{\sqrt{2}}\left(\left\vert f_1,S_1,0,1\right\rangle\left\vert f_2,S_2,0,1\right\rangle+\left\vert f_1,P_1,1,0\right\rangle\left\vert f_2,P_2,1,0\right\rangle\right)$
Measurement Bases of Output State
$\left\vert\Psi_{Meas}\right\rangle=\frac{1}{2\sqrt{2}}\left(\left\vert f_1,s_1,10;f_2,s_2,01\right\rangle-\left\vert f_1,p_1,10;f_2,p_2 01\right\rangle+\left\vert f_1,s_1,01;f_2,s_2,10\right\rangle-\left\vert f_1,p_1,01;f_2,p_2,10\right\rangle\right)\sin\left(2\delta\right)$ $+\frac{1}{2\sqrt{2}}\left(\left\vert f_1,s_1,10;f_2,p_2,01\right\rangle+\left\vert f_1,p_1,10;f_2,s_2,01\right\rangle+\left\vert f_1,s_1,01;f_2,p_2,10\right\rangle+\left\vert f_1,p_1,01;f_2,s_2,10\right\rangle\right)\cos\left(2\delta\right)$ $+\frac{1}{2\sqrt{2}}\left(\left(\left\vert f_1,s_1,10;f_2,p_2,10\right\rangle+\left\vert f_1,p_1,10;f_2,s_2,10\right\rangle\right)\cos\left(2\delta\right)+\left(\left\vert f_1,p_1,01;f_2,s_2,01\right\rangle+\left\vert f_1,s_1,01;f_2,p_2,01\right\rangle\right)\cos\left(2\delta\right)\right)$ $+\frac{1}{2\sqrt{2}}\left(\left(\left\vert f_1,s_1,10;f_2,s_2,10\right\rangle-\left\vert f_1,p_1,10;f_2,p_2,10\right\rangle\right)\sin\left(2\delta\right)+\left(\left\vert f_1,s_1,01;f_2,s_2,01\right\rangle-\left\vert f_1,p_1,01;f_2,p_2,01\right\rangle\right)\sin\left(2\delta\right)\right)$

Degrees of freedom in table (2) within the kets are frequency, polarization, occupation number in path/direction ‘a’, and lastly path/direction ‘b’. Photon amplitudes within the composite state kets are separated by semi-colons. One input state is given in the first row of table (2), shown also in figure 5. Output states from the system, expressed in possible measurements at displaced locations, comprise two classes of state amplitudes: bunched and anti-bunched for both congruent and incongruent frequency states. The top set of amplitudes in the row (2) of table (2) are anti-bunched states, wherein both a and b receive a photon. The bottom set are bunched states; both photons arrive at either a or b, not at a and b.

Angle δ specifies the agreed upon frame in which to perform measurements by authorized users. These are shared key choices before any QKD session occurs and unknown to any prospective eavesdropper. In order to present minimal ambiguity to authorized users, angle δ is restricted to the set {0,45^{o}}.

Anti-bunched states: When δ = 0, polarization measurements are anti-correlated; if a measures s polarization, b measures p polarization. For δ=45^{o}, polarization measurements are correlated; when a measures s polarization, so does b, and likewise for p polarized states. These events, after error correction and privacy distillation, are shared fresh key material.

Bunched states: When δ = 0, polarization measurements are anti-correlated; if dichroic mirrors are in place, as they are in figure 5, represented by the red/blue rectangles, a or b measure anti-correlated polarizations. For δ=45^{o}, a or b measure correlated polarizations. If a is the receiver of both photons, b has no knowledge of the measurement a performs, and the same holds for b. Either node not receiving at least one photon can conclude the event is a photon loss or the other node received both. Some reconciliation must occur for them to utilize the bunched states toward a common random bit stream to contribute to the shared fresh key material.

4.2.3 Non-local Correlations in a Hyper-entangled Circuit - Hughes and Erdmann [6]

An authorized user receiving bunched photon states from the output of a hyper-entangled photon server can make use on average of one fourth of the total transmitted events to gain situational awareness of the communications channel. Another user receiving bunched states can do the same. Both users then gain a common operating picture of the confidentiality and integrity of the remaining half of the total transmission events by making non-local correlated measurements on anti-bunched photon states. Employing Keyed Communication in Quantum Noise, they know the keyed logic assignment their respective paths represent, the keyed logic assignment their respective frequencies represent, and they have agreed in which polarization basis to measure for each transmission event. Then, in each anti-bunched transmission, they share a random bit stream to use as fresh secret key material of at least eight bits; maybe more; some people have been utilizing the orbital angular momentum of light which, in principle, can be used to gain greater information capacity in each transmission event.

Several ways exist to encode the degrees of freedom within a ket. For example, we can include the frequency, the polarization, and the path as follows. Let f_1=1, f_2=0, s=1, p=0, and retain the path occupation numbers in the state in table (2) row (2). We can arbitrarily collect the terms as follows,

$$\begin{aligned}\left|\Psi_{\text{out}}\right\rangle = {} & \frac{\sin(2\delta)}{2\sqrt{2}}\left(\left|1,1,1,0;0,1,0,1\right\rangle - \left|1,0,1,0;0,0,0,1\right\rangle + \left|1,1,0,1;0,1,1,0\right\rangle - \left|1,0,0,1;0,0,1,0\right\rangle\right) \\ & + \frac{\cos(2\delta)}{2\sqrt{2}}\left(\left|1,1,1,0;0,0,0,1\right\rangle + \left|1,0,1,0;0,1,0,1\right\rangle + \left|1,1,0,1;0,0,1,0\right\rangle + \left|1,0,0,1;0,1,1,0\right\rangle\right) \\ & + \frac{\cos(2\delta)}{2\sqrt{2}}\left(\left|1,1,1,0;0,0,1,0\right\rangle + \left|1,0,1,0;0,1,1,0\right\rangle + \left|1,0,0,1;0,1,0,1\right\rangle + \left|1,1,0,1;0,0,0,1\right\rangle\right) \\ & + \frac{\sin(2\delta)}{2\sqrt{2}}\left(\left|1,1,1,0;0,1,1,0\right\rangle - \left|1,0,1,0;0,0,1,0\right\rangle + \left|1,1,0,1;0,1,0,1\right\rangle - \left|1,0,0,1;0,0,0,1\right\rangle\right)\end{aligned} \qquad (3)$$

This in base 10 is

$$\begin{aligned}\left|\Psi_{\text{out}}\right\rangle = {} & \frac{\sin(2\delta)}{2\sqrt{2}}\left(\left|229\right\rangle - \left|161\right\rangle + \left|214\right\rangle - \left|146\right\rangle\right) + \frac{\cos(2\delta)}{2}\left(\left|225\right\rangle + \left|165\right\rangle + \left|210\right\rangle + \left|150\right\rangle\right) \\ & + \frac{\cos(2\delta)}{2}\left(\left|226\right\rangle + \left|166\right\rangle + \left|149\right\rangle + \left|209\right\rangle\right) + \frac{\sin(2\delta)}{2}\left(\left|230\right\rangle - \left|162\right\rangle + \left|213\right\rangle - \left|145\right\rangle\right)\end{aligned} \qquad (4)$$

In (4), the degrees of freedom in each ket have been represented by a bit stream and translated into a base 10 number. Measurements collapse the wave function to just one composite ket, so the base 10 number translated back to decimal and decoded gives the state of the system measured by a and b in the anti-bunched state case, and a or b in the bunched state case. Anti-bunched states in (4) are the top row and bunched states the bottom row.

Suppose in 'a' the authorized users have been keyed to measure in the $\delta = 45^{o}$ frame. Then suppose 'a' measures f_1, s, and of course a, and 'b' measures f_2, s, and of course b. In the absence of error, the prospective bit stream authorized users share is 11100101, the binary representation of 229, an anti-bunched state. That is a shared bit stream and starting point from which secret key material is distilled.

A bit stream utilizing the anti-bunched states thus far shared is not entirely random. In it, 'a' is always 1 and 'b' is always 1. That can change, and do so at random. Suppose they have agreed to switch logic assignments at random on the basis of which user receives or does not receive both photons. That is, along with their keyed basis sharing, they can key their logical identities by employing another key, derived from the reception of bunched states. They may also agree to flip their frequency and even polarization logical assignments in the same keyed random way, using the bunched state arrivals to activate the switch in processing after the measurements. Bunched state switching alerts, derived from a current common QKD engenderment, can be used for future QKD engenderment sessions or even in the same measurement session depending upon the particular mapping used in post processing.

A map utilizing the bunched state occupations to switch logic assignments is a random function. Part of the protocol, it resides at all nodes and is activated by the reception of ciphertext from stream ciphers. Stream ciphers, examples of which are AES, or coherent state quantum data encryption, take in relatively short secret seed keys and spit out very long running keys in which to encrypt messages. As Yuen points out, even when authorized users share keys for basis selection, error corrections and privacy amplification must still be performed. This can be done hub to spokes via stream ciphers, which are classical or quasi-classical encrypted communications. Bunched state logic switch flags can be a part of messages sent between authorized users and the hub. In such a protocol, security is a hybrid of classical mathematical complexity and quantum mechanical randomness.

Bunched states can also be used to diagnose both legs of the channel. If one user receives both photons in an event the users have agreed to measure in, say, the PBS basis, that user expects to find 100% anti-correlated polarization states. If not, the local channel has errors and possibly an intruder executing an intercept/resend attack, or other correlation integrity busting intrusion. That intruder knows not the current common basis shared by server and users, nor the PBS measurement basis defined within it. In other words, an intruder's touch is discernable because, if an intruder does not share the common server-user reference frame defining δ, on average the intruder could be wrong in their polarization measurement a discernible fraction of the events. A standard feature of quantum communications, this will incur polarization correlation errors over and above the channel noise in legitimate users' correlations.

The dichroic mirror, or DM, in figure (5) allows them to make polarization correlation measurements at each of their locations. They will individually arrive at a common operating picture of the integrity, and thus the confidentiality of their key sifting communication when they correct errors and perform privacy amplification. If the disturbance is too great to reasonably surmount, the users can simply abort. The intruder's denial of service attack is then a success. In free space, however, such a bold attack could place the intruder into harm's way in a very real kinetic sense.

5.0 Conclusions

5.1 Investigating Coherent State Quantum Data Encryption Confidentiality: Conclusions

A simulation testbed developed in this project is a result of our continuing work in the field of quantum communication systems. The model developed as a part of our previous efforts includes the effects of atmospheric attenuation, phase noise, the number of encryption bases, and photon count on a free-space Alpha-Eta optical link. The model was further refined and the results presented in this report also reflect some of the experimental work conducted in the quantum communication laboratory at the AFRL. It includes a newly developed coherent receiver that underwent preliminary testing and correlation of the results with the model. We have demonstrated how security of a system that uses quantum phase encryption increases as we decrease the number of photons per symbol, or increase the number of phase bases and signal noise. In addition, the effects of wavelength mismatch between the signal source and the local oscillator has been observed and will be addressed in more detail in the near future. The results are presented for a particular hardware unit that implements synchronous demodulation; however, the approach developed and discussed in this report can be very useful to extending this modeling technique to various heterodyne detection systems.

A simulation and analysis test bed has been developed within the scope of this project. It is based on laboratory experimentation combined with mathematical algorithms that perform statistical analysis of the secrecy of the running key. This report presents the results of our continuing work in the field of quantum communication systems. The coherent detection system developed as a part of our previous efforts was used to emulate an Alpha-Eta optical link. The statistical processing algorithm was developed to quantify our capabilities to accurately measure each bit of the running key. The results were obtained using experimental data from a particular hardware setup; however, the approach developed and discussed in this report can be very useful for extending to any practical heterodyne detection systems for assessing potential vulnerability of the running key.

The results obtained in the course of this research can be used for conceptual improvement of the encryption protocols. This is direct continuation of our efforts from the last several years that included problems in optical connectivity, signal propagation, sensing/detection and secrecy of the running key. It is expected that this project will complement other AFRL-funded research efforts in this area, including the design of optical transceivers and development of encryption systems.

5.2 Quantum Operations on Entangled Photon Pairs Using Lyot Filters: Conclusions

We have designed a customized optical system that can be fabricated in compact integrated format, (cemented) prisms, plates and cubes. The system can function to route and or exchange entangled photon states and properties. Using a co-linear entangled source the system selectively manifests maximally frequency entangled or polarization entangled photons, both suited for QKD applications (shared keys with provable security). It also allows a complete entangled state to be routed to either user by selecting both input frequencies congruent, or in-congruent (with respect to the Lyot stages). Unique features are selectable entanglement and routing, compact size and integrated construction for telescopic compatibility. To the best of our awareness no existing systems can provide this in a single system without incurring polarization projection losses of half of the entangled input states.

We asked the questions, can polarization entanglement be preserved in transit through a single stage hyperspectral multi-access Lyot filter and, if not, can it be modified to do so? We answered the questions posed, in principle, in the affirmative. Assuming perfect, lossless linear optical elements in our circuit, our modification entailed adding a beam splitter and an additional Lyot filter stack to the existing Lyot filter stage to ensure an initially entangled input state remained so, but additionally evolved into a hyper-entangled state. This allows quantum key distribution to ensue, wherein authorized users choose from two, two dimensional bases at the outset, using half of the transmission events for secret sharing and the other half for channel diagnostics. A companion paper to the current one analyzes entanglement between the system's degrees of freedom using Perez-Horodecki, or positive partial transpose criteria, in addition to the Clauser, Horne, Shimony, and Holt Bell test inequality. Another modification to the Lyot stage has been designed by us, directly handling a collinear input state. This latter modification, to be reported on in another paper, is also relatively simple and doesn't require a beam splitter, but uses two additional Lyot filter stacks instead of just one. It could find application in entanglement routing. A salient point in this paper, and not originating with us, is that exploiting non-degenerate frequency degrees of freedom allow an additional modicum of information flow control in quantum optical circuits, just as it does in classical optical devices. We emphasize that the foregoing analysis only *indicates* the efficacy of the hyper-entangled photon server's operation. Linear optical elements are not perfect, spectral distributions are not delta functions, and dispersion exists in all paths. Moreover, its efficiency is as problematic as BB84 in that half the transmission events that make it through the channel are not shared by both parties to distill fresh secret keys. Yet, unlike BB84 where basis reconciliation between the two users discard on average one half the events for lack of basis agreement, here we use the bunched states to gain a common operating picture of a possibly adverse channel.

A user receiving bunched states from the output of a hyper-entangled photon server can make use of a quarter of the total transmitted events to gain situational awareness of the communications channel. Another user receiving bunched states can do the same. This allows them both to gain a common operating picture of the confidentiality and integrity of the remaining half of the total events wherein they each receive one photon of an entangled pair. They know the keyed logic assignment their respective paths represent, the keyed logic assignment their respective frequencies represent, and they have agreed in which polarization basis to measure for each transmission event. Then they share a random bit stream to use as fresh secret key material of at least eight bits that might be extensible to more.

6.0 References

[1] Vladimir Nikulin and Vigit Bedi, Final Report for VFRP (2013).

[2] Vladimir V. Nikulin, David H. Hughes, John Malowicki, and Vijit Bedi, Proceedings of SPIE Vol. 9500-8 SPIE (2015).

[3] Vladimir V. Nikulin, Final Report for VFRP (2015).

[4] Reinhard K. Erdman and David H. Hughes, paper in process.

[5] David H. Hughes and Reinhard Erdman, paper in submission.

[6] David H. Hughes and Reinhard Erdman, paper in submission.

7.0 Acronym List

AES: Advanced Encryption Standard

AFRL: Air Force Research Lab

BB84: Bennet and Brassard quantum key distribution protocol published in 1984

DM: Dichroic Mirror

DOF: Degrees of Freedom

I&R: Intercept and Resend

QC: Quantum Communications

QIP: Quantum Information Processing

QKD: Quantum Key Distribution