REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*
30-01-2011

2. REPORT TYPE
Final Report

3. DATES COVERED *(From - To)*
April 1 2010-December 31 2010

4. TITLE AND SUBTITLE
Novel nonclassical-light-assisted protocols for quantum key distribution

5a. CONTRACT NUMBER
FA9550-10-C-0081

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Yurtsever, Ulvi
Dowling, Jonathan P.

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
MathSense Analytics, 1273 Sunny Oaks Circle, Altadena, CA 91001
Louisiana State University, Baton Rouge, LA 70803

8. PERFORMING ORGANIZATION REPORT NUMBER
FA9550-10-C-0081 Final Report

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Air Force Office of Scientific Research
875 N. Randolph Street Room 3112
Arlington, VA 22203

10. SPONSOR/MONITOR'S ACRONYM(S)
AFOSR/PKS

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
AFRL-OSR-VA-TR-2012-0813

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for Public Release

13. SUPPLEMENTARY NOTES

14. ABSTRACT

During our Phase I period of performance, we have investigated a competing technology to the decoy-state protocol for QKD (quantum key distribution) based on the use of entangled light pulses randomly mixed with Weak Laser Pulses (WLP), the so-named NCBB84 protocols, where the WLP are used exactly as in the standard BB84 (Bennett & Brassard 1984) protocol. Our theoretical work has identified a number of promising NCBB84 candidates, among which is the entangled decoy state protocol, which at this moment appears optimal. The entangled decoy state approach is especially promising from a practical standpoint because it allows a homodyne detection scheme to be used as opposed to photon-number-counting detectors needed by the standard decoy-state approach. Consequently, detectors with much
higher efficiencies and lower dark-count rates can be used with our new scheme, increasing the key generation rate.

15. SUBJECT TERMS
quantum cryptography, weak laser pulses, nonclassical light, entanglement

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** Ulvi Yurtsever
a. REPORT U	**b. ABSTRACT** U	**c. THIS PAGE** U	UU	7	**19b. TELEPHONE NUMBER** *(include area code)* 626-437-1604

Final Report for AIR FORCE STTR 09.B - Phase I
Novel nonclassical-light-assisted protocols for quantum key distribution

Principal Investigator: Dr. Ulvi Yurtsever
MathSense Analytics, 1273 Sunny Oaks Circle, Altadena, CA 91001
Phone: 626.437.1604, Email: ulvi@charter.net

Co-Investigator: Dr. Jonathan Dowling
Louisiana State University, Baton Rouge, LA 70803
Phone: 225.578.0887, Email: jdowling@phys.lsu.edu

1. STATEMENT AND SIGNIFICANCE OF THE PROBLEM

Quantum key distribution is an elegant application of quantum information theory with immense practical value. The security of classical cryptography is dependent on computational difficulty. However, the advent of quantum computing compromises classical encryption schemes. Fortunately, quantum information theory solves the exact problem it creates. If a transmitter, Alice, wants to exchange a message with a receiver, Bob, then the fundamental principles of quantum mechanics allow them to generate a key that cannot be obtained by an eavesdropper, Eve [1-3].

BB84 is a widely popular means of quantum key distribution. Theoretically, Alice sends a sequence of single photon pulses to Bob, and Alice randomly alternates between different bases for preparing the photons. In the receiving lab, Bob will randomly alternate between bases for measuring the incoming photons. For the sake of specificity, the key will be generated using orthogonal polarization bases. Alice will randomly prepare each photon as either horizontal, vertical, diagonal, or antidiagonal, and Bob will measure each randomly as either in the horizontal-vertical basis or the diagonal-antidiagonal basis. Therefore, if Eve tries measuring Alice's photon and then sending the result of her measurement to Bob, the eavesdropper will introduce errors into the key, since she does not know in which basis the photon is being sent nor does she know in which basis Bob will measure. Alice and Bob can then use these errors to detect the eavesdropper's presence and determine the security of the key [4].

However, in experimental settings, Alice does not have a true single photon source. Instead, the photons are sent using weak laser pulses. This coherent light follows a Poisson distribution that gives rise to the state

$$\rho = \sum_n \frac{\mu^n}{n! e^{\mu}} \mid n\rangle\langle n \mid \tag{1}$$

Here μ is the mean photon number which will be a positive number less than one to avoid pulses with more than one photon. However, multiple photon pulses will still occur with probability of $P_M = 1 - e^{-\mu} - \mu e^{-\mu}$ This exposes the scheme to the photon number splitting attack, which can be rather dangerous when Alice and Bob are communicating over a channel with high loss, particularly since in a security analysis Alice and Bob are restricted to currently available technology. However, Eve's technological resources are only restricted by the laws of physics. This prevents a scheme's security from becoming obsolete due to the emergence of new technology and allows quantum cryptography to avoid one of classical cryptography's great dangers. Therefore, to perform this attack on a practical BB84 setup, which is using an attenuated coherent source, Eve can replace the high loss channel that Alice and Bob are using with a lossless channel without Alice and Bob realizing it. Eve then performs a quantum non-demolition (QND) measurement on each pulse to obtain number information without perturbing the photon polarization. When she measures a single photon, Eve simulates the loss of the original line by blocking a fraction of these pulses. When Eve measures a pulse with multiple photons, she splits the pulse and stores a photon in a quantum memory. Eve then sends the rest of the pulse to Bob. After Alice and Bob perform public discussion and announce the bases used for each pulse, Eve can then retrieve the photons from her quantum memory and obtain a significant fraction of the key without being detected by Alice and Bob [5-9].

Decoy states are a potent solution to this attack. In the photon number splitting attack described above, Alice's photon source had a constant mean photon number. However, if Alice randomly alters the mean photon number of her source in a way that is known to her, but not perceivable to Eve, then she can detect the photon number splitting attack. Pulses from the source with a higher mean photon number will contain a greater fraction of multi-photon pulses, which Eve will not block. Therefore, when Alice and Bob discuss the protocol, Alice can compare the loss in the line for when different mean photon numbers were used. If there is a marked difference between the loss for the decoy states and the loss for the signal states, then Alice can conclude that Eve is using the photon number splitting attack [10-14]. The decoy state method has had multiple experimental successes [15-22].

The crux of the decoy state solution is that Eve is manipulating photon number statistics in a way that is detectable by Alice. However, if Eve is able to gain information, which allows her to not alter the statistics in a detectable manner, then the decoy state technique will not be a successful solution. Moreover, the decoy state approaches assume a stable source, when this may not be the case in practice. Monitoring the source can hurt the efficiency of the protocol in practical free-space settings. In this project, we proposed alternatives to the decoy state schemes by augmenting weak laser pulse BB84 with entangled light to detect an eavesdropper. For convenience and clarity, we refer to this entanglement enhanced WLP BB84 as NCBB84 (Non-Classical Light Assisted BB84). Most entanglement based quantum key distribution schemes rely on violations of Bell's inequalities to ensure security [23]. But, there are multiple differences between schemes like E91 and NCBB84. In our new scheme, the entangled states are not used to distribute key bits. Instead, they are used like decoy states and the only goal of these pulses is to detect the presence of an eavesdropper. More specifically, the entangled pulses are sent randomly mixed with the weak laser pulses to guard against the use of a quantum non-demolition measurement device. Sending entangled decoy states allows Alice and Bob to obtain phase information. When Eve measures photon number in the photon number splitting attack on weak laser pulse BB84, she avoids detection, because the number operator commutes with polarization. However, phase and number do not commute. Therefore, Alice and Bob can use the phase information provided by entangled decoy states to the detect Eve whenever she chooses an attack scheme that involves measuring number.

2. NOVEL ENTANGLEMENT-ASSISTED NCBB84 PROTOCOLS STUDIED IN THIS PROJECT

An implementation of NCBB84 would have Alice run WLP BB84 protocol with frequency f_s. The entangled state decoy ancilla would be implemented with frequency f_d. However, it is important to note that Bob's detection scheme for the entangled pulses will be different from his detection scheme for the signal states. This is problematic, because if the mode that Alice and Bob are operating in at any given time is not random, then the security of the entire protocol is compromised. If Eve can predict whether a signal state or a decoy state is being sent, then she can adjust her attack plan accordingly and render the decoy states useless. Therefore, it is critical that the decoy states are not distinguishable from the signal states. Additionally, Alice and Bob will have to randomly alternate between the signal and decoy modes. Felicitously, the decoy mode will not need to be run with very high frequency in order to detect the use of a quantum non-demolition attack. Nevertheless, since Alice and Bob must each run separate modes for the signal states and the decoy states, a fraction of the pulses they exchange will be worthless. Alice and Bob will exchange key information with frequency f_s^2, and the pulses will yield information about the presence of a quantum non-demolition measurement device with frequency f_d^2. With frequency $2f_sf_d$, Alice and Bob will be operating in different modes, and these exchanges will provide no valuable information. This loss is not decimating for the scheme. Nevertheless, it is indicative of the tradeoff in quantum cryptography between speed and security.

WLP BB84 does not require further description here, because there are already firmly established protocols related to its performance. However, the entanglement auxillary system requires further description. We will generate two time entangled photons using Spontaneous Parametric Down Conversion (SPDC). One photon in the pair will be measured to obtain an accurate time of emission for the other photon. The non-measured photon will then be sent through a system similar to a Franson interferometer. However, an analogy could also be made to a Mach-Zehnder interferometer. The photon will encounter a beam splitter and become the $|\Psi\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle)$ state. Half of the state will travel down the longer arm, while the other half will travel down the shorter arm. The halves will recombine at the second beam splitter where there will be a probability for the state to not continue along the main system path. A detector will be placed to consume these possibilities. However, when the pulse does follow the main system path, there is an entangled pulse, where half is delayed in time due to extra path length of the long arm. This pulse is then sent out of Alice's lab to Bob along their quantum channel.

When Bob receives the test pulse from Alice in his lab, he will detect the pulse by sending it through a beam splitter which will put the pulse through long and short arms identical to the setup in Alice's lab. The pulse will then encouter the final beam splitter. In this process, there are three distinguishable possibilities for the pulse, once it is detected by Bob after exiting the final beamsplitter. One possibility is for the delayed part of the pulse to take the long path and the other part to take the short path, once the first beam splitter is reached. Two other possibilities are for both portions of the pulse to take the same path. The final possibility and the only one of interest for this protocol is when the delayed part of the pulse takes the short path and the other part takes the long path. For this outcome, the temporal overlap of the pulses at the second beam splitter will trigger the Hong-Ou-Mandel effect. This will not occur for the other three possibilities. However, because of the time measurement taken in Alice's lab, the first three possibilities can be ignored when processing the data. For the outcome of interest, only one detector will fire at a time. However, if Eve performs a quantum non-demolition measurement on the line, then the Hong-Ou-Mandel effect will not present itself. Therefore, in a situation with a lossless channel and perfect detectors, if two detectors fire at once, then Alice and Bob can deduce that Eve is performing quantum non-demolition measurement as part of her eavesdropping attack. The strong time information from the photon initially detected by Alice allows for the differentiation between these three outcomes. One possibility is that the photon took the short path both times. Another outcome is that the photon took the long path both times. These two possibilities do not yield strong information about Eve's activities. However, the other possibility is that the photon travels down one long path and one short path. This possibility can then be used to detect the use of a quantum non-demolition measurement device. In this scenario, the photon's self-interference, will result in a bright port and a dark port in Bob's detection apparatus. Yet, if Eve is measuring number, so that she can perform the photon number splitting attack, then Bob's dark port will not be completely dark. Obviously, it will not be completely dark even without an eavesdropper, since a practical system will have imperfections and not identically mirror the ideal case. Nevertheless, the eavesdropper's actions will still introduce additional error, which can be used to detect her presence, using Chernoff hypothesis testing.

For the Chernoff hypothesis testing, we want to determine the error in detecting Eve, when using any of the protocols in the NCBB84 class. For this test, we have two symmetric hypotheses. The null hypothesis is that Eve is not measuring number using a quantum non-demolition measurement device. The alternative hypothesis is that Eve is using such a device to measure number. We are only investigating the photons that reach Bob with the proper time information, so loss is not the key quantity to investigate here. Instead, dephasing is the primary concern. In an ideal scenario, with no dephasing from the environment, we can easily construct the situations of the two hypotheses. For the null hypothesis, the probability that the photon will enter the bright port is 1, and there is 0 probability for the photon to enter the dark port. When Eve is acting on the system in the alternative hypothesis, there is an equal probability for the photon to enter either of Bob's detectors. This results in a Chernoff distance of .69. In this situation, detecting Eve at the 95% confidence level will require an exchange of 4 photons between Alice and Bob. Obviously, this is not a realistic scenario, even with environmental dephasing, the number of photons required to detect Eve is still relatively low, which means that the apparatus does not place an extremely high burden on the rate of key distribution.

Indeed, the purpose of this entanglement ancilla is to increase the rate of secure key distribution relative to other schemes. The transmittivity of the quantum channel shared by Alice and Bob is typically the primary factor in determining the rate of secure key generation. In true single photon BB84, this rate is linearly related to the transmittivity. However, for weak laser pulse BB84 without any more sophisticated augmentations, the secure key rate is related to the square of the channel's transmittivity, and, since the transmittivity is in practical situations a number much less than 1, this presents a major problem. However, for WLP BB84 schemes which eliminate the photon number splitting attack as a viable mode of eavesdropping, the linear relationship between secure key rate and transmittivity can be salvaged. This is the case for NCBB84. Additionally, the secure key rate has a linear relationship with transmittivity for coherent decoy state protocols as well as schemes that utilize strong phase reference pulses that eliminate Eve's ability to send Bob vacuum signals.

3. PROGRESS ON PHASE-I OBJECTIVES

During the nine months (April 1 – December 31, 2010) of our Phase I period of performance we honed in on a variant of our proposed protocol based on entangled decoy states which is particularly promising from a practical standpoint. A brief description of this protocol can be given as follows:

Entangled Decoy States: As with the number splitting attack, Eve can always do a non-demolition measurement in a basis which does not affect or commutes with the state of the signal photons. In the case of BB84, doing a number measurement on the signal photons will not affect the polarization of them. Eve's number measurement will not be detected. If we use decoy states sensitive to QND measurements, then we can detect Eve. An easy number and phase entangled state to produce is a low NOON state, specifically the state $|\Psi >= \frac{1}{\sqrt{2}}(|10 > +|01 >)$. SPDC can be used to produce a pair of time entangled photons. One of the pair of photons is measured to get an accurate time of emission of the other photon in the pair. The non-measured photon is then sent through a beam splitter to produce a low NOON state. This state is sent through the signal line and Bob does a phase measurement. If Eve

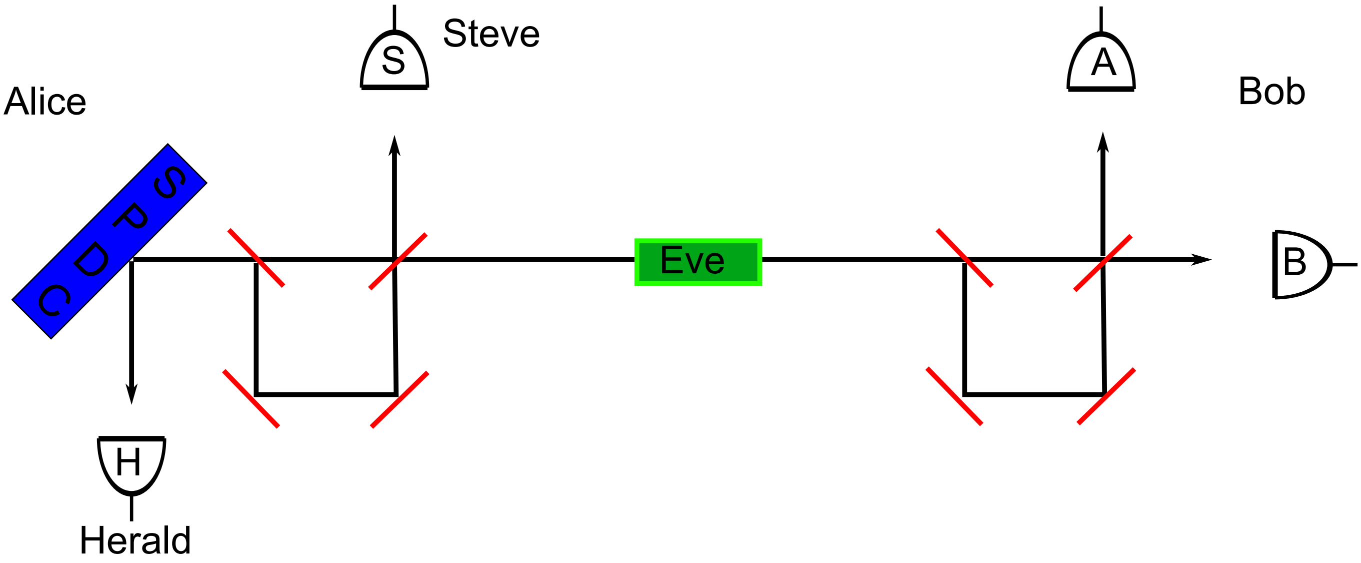

FIG. 1:

does a number measurement on the state, then the phase information will be scrambled and Bob can detect this, and therefore, detect Eve.

Figure (1) shows how the Eavesdropper detector would be implemented in the lab. A laser beam pumps a crystal to produce SPDC photons entangled in time. One photon is measured at detector H for the pairs emission time. The other photon is sent through what is basically a Franson interferometer. First the photon is split into the $|\Psi>=\frac{1}{\sqrt{2}}(|10>+|01>)$ state. Then half of the state follows the longer arm and the other half follows the shorter arm. At the second beam splitter there is a %50 chance that the state will not enter the signal beam. Detector S can be placed there to eliminate these possibilities. If both halves of the state do go the correct way, then we have an entangled state traveling through the line that has one half of it delayed in time by the extra time it took to go through the longer arm. The state going through the beam is a superposition of a photon followed by vacuum AND vacuum followed by a photon. If Eve does a number measurement on one half of the state, then the phase information in the state will be scrambled and the state will collapse into a photon followed by vacuum OR vacuum followed by a photon. At Bob's half of the Franson interferometer, the state is reconstituted in time. Three things can happen on Bob's side: (A) The delayed half of the state can take the longer arm, and the other can take the shorter arm. (B) Both halves can take the longer or shorter arms. (C) The delayed half can take the shorter arm, and the other the longer arm. For both A and B, the state is not reconstituted in time, but for C, the input to the last beam splitter is a $|\Psi>=\frac{1}{\sqrt{2}}(|10>+|01>)$ state. The output of choice C is determined by the Hong-Mandel effect. One detector should be dark, while the other detector will receive a photon %100 of the time. Because we have such accurate time information from Alice's side, we know when C should occur, and the other events can be ignored. If Eve did a number measurement between Alice and Bob, then Hong-Mandel no longer is in effect and the output to the detectors will be a %50 chance of a photon going to either detector. So, if a photon is detected in the dark port, then there is a %100 chance that Eve is there. Since the photon detected in the light port could possibly be a photon that was measured by Eve, there is a %50 chance that Eve sent it.

Chernoff Bounds: In order to quantify a maximum error is detecting eve, P^{Max}_{Error}, we will use hypothesis testing formalism. The two hypothesis we are comparing are: H_0: Eve is NOT QND measuring photon-number on the BB84 photons. H_E: Eve is QND measuring photon-numbers (PNS attack). Since we are only counting in coincidence, the photons that get lost on the way to Bob are discarded. So instead of loss, we will calculate the effect of de-phasing instead of loss. The environment or Eve using a weak measurement, could possibly weaken the phase information in the decoy state. If this happens then the probability for a photon entering the dark port when Eve is absent will go up to a max of %50. For no de-phasing, the hypothesis H_0, no Eve, has the probability for detecting a photon at detector A of $p=1$ and the probability for detecting a photon at detector B is $\overline{p}=1-p=0$. For hypothesis H_E, Eve is listening, the probability for detecting a photon at detector A is $q=\frac{1}{2}$ and the probability for detecting a photon at detector B is $\overline{q} = 1 - q = \frac{1}{2}$. The Chernoff distance equation for testing these symetric hypothesis is:

$$C(p,q) = \xi Ln(\frac{\xi}{p}) + \overline{\xi} Ln(\frac{\overline{\xi}}{\overline{p}}) \tag{2}$$

Where $\xi = \frac{Ln(\frac{\overline{q}}{\overline{p}})}{Ln(\frac{p}{\overline{p}})+Ln(\frac{\overline{q}}{q})}$ and $\overline{\xi} = 1 - \xi$. The Chernoff distance in the case with no de-phasing is 0.69. The maximum probability of an error in choosing the correct hypothesis is given by:

$$P^{Max}_{Error} = \frac{1}{2} e^{-nC(p,q)} \tag{3}$$

where the actual error $P_{Error} \leq P^{Max}_{Error}$. This means that to have %5 error (%95 confidence) that Eve would be detected will take about 4 photons.

In the case with de-phasing the problem turns into that of determining whether a coin is fair or not. The question becomes; how many coincidence counts (coin flips) does it take to be confident that Eve is there or not (the coin is fair or not)? Figure (2) shows how the Chernoff distance changes with increasing probability of finding a photon in the dark port for H_0. Figure (3) shows how many photons are needed to have a %95 confidence of determining if Eve is listening. There is an additional requirement we must place on the protocol and Eve. The time between signal photons must be shorter than the time delay inserted into the decoy state. If this were not so, then Eve could do a number measurement of both halves of the decoy state in a time interval that encompasses the whole decoy state. If Eve did this, the decoy state would not collapse. If the time delay in the decoy state is large enough to let many key photons pass, and Eve was measuring over this long time, then Eve would not get good information about the key.

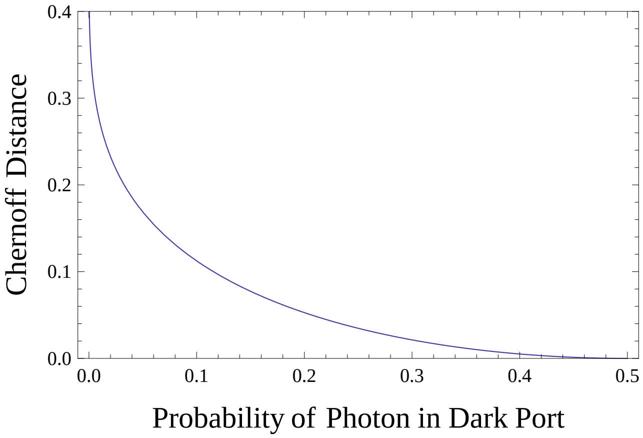

FIG. 2:

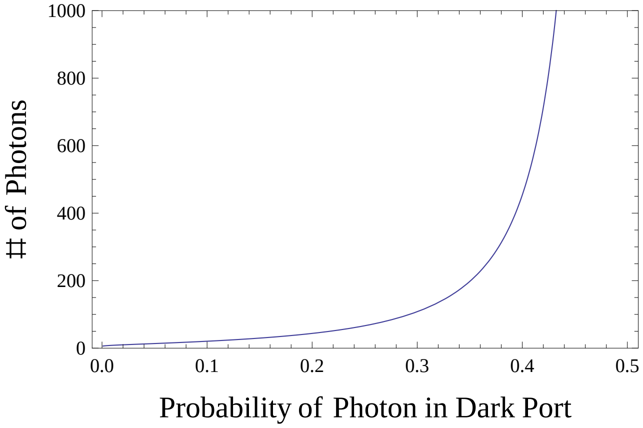

FIG. 3:

Analysis of the distinguishability of eavesdropping from photon loss: The quantum Chernoff bound is an established method for quantifying the distiguishability of various state density matrices dependent on specific states, measurement schemes, and predicted hypotheses. Here, the two hypothesis have been stated above and each correspond to a unique mixed state. Henceforth, a secure key (absence of an eavesdropper, but assuming photon loss in the transmission line) will be referred to as the the null hypothesis (H_0), and the presence of an eavesdropper as the alternative hypothesis H_1. Likewise, the mixed states corresponding to these two hypotheses are ρ_0 and ρ_1, respectively. The states must be measured by way of a positive operator valued measurement (POVM), which implies an intrinsic randomness of the measurement outcome. It directly follows that a measurement resulting in $\rho_{0,1}$ does not necessarily guarantee knowledge of the hypothesis. Rather, the probability of hypothesis H_b given a measured ρ_i is given by $p_i(b) = Tr[\rho_i E_b]$ for a single copy of the quantum state. The probability of concluding the incorrect hypothesis (probability of error), is given by

$$P_e = \frac{1}{2}[p_0(1) + p_1(0)] = \frac{1}{2}[Tr(\rho_0 E_1) + Tr(\rho_1 E_0)] \tag{4}$$

where $E_{0,1}$ are element of the POVM scheme, and $E_0 + E_1 = \hat{I}$. For this binary hypothesis scenario, the Helstrom matrix aids in elimination of varialbes: $\Gamma \equiv \rho_0 - \rho_1$. The probability of error is now

$$P_e = \frac{1}{2}(1 - Tr[E_1 \Gamma]) \tag{5}$$

The traceless property of Γ implies the existence of negative eigenvalues. Examination of 5 indicates that error is minimized by choosing a POVM that acts a projector on the positive eigenvalue subspace of the Helstrom matrix (i.e., $Tr[E_1\Gamma] = Tr\|\Gamma\|/2 = Tr\left[\sqrt{\Gamma^\dagger\Gamma}\right]/2$). Assuming this detection scheme, the error probability becomes

$$P_e = \frac{1}{2}\left(1 - \frac{1}{2}Tr\|\rho_1 - \rho_0\|\right). \tag{6}$$

The scope of the above analysis is limited to a single copy of the quantum state. For multiple copies, the full quantum Chernoff bound analysis is more computationally intensive and more insightful. This generalized analysis has been carried out recently, and the results will be published in a forthcoming paper which is under preparation.

Lossy state propagation: When photon loss is modeled as the limiting case of an infinite number of discrete beam splitters along the transmission mode (H_0), the output state is then given by

$$\rho_0(x) = \frac{1}{2}\left(|N,0\rangle\langle N,0| + \sum_{n=0}^{N}\binom{N}{n}\left(e^{-n\mu x}\left(1-e^{-\mu x}\right)^{N-n}\right)|0,n\rangle\langle 0,n| + e^{-\frac{N}{2}\mu x}\left(e^{-i\eta x}|N,0\rangle\langle 0,N| + e^{i\eta x}|0,N\rangle\langle N,0|\right)\right) \tag{7}$$

where μ is the loss coefficient and η is the accumulated phase rotation. For the alternate hypothesis H_1 in which an eavesdropper measures exactly one photon from the transmission mode (disregarding, for simplicity, the effects of loss and assuming only one of the N total photons are lost from the state), with eavesdropping on transmission mode "b" the output state and density matrix are

$$|\text{out}\rangle_1 = \frac{1}{\sqrt{2}}\left(|N,0\rangle + |0,N-1\rangle\right) \tag{8}$$

$$\rho_1 = \frac{1}{2}\left(|N,0\rangle\langle N,0| + |0,N-1\rangle\langle 0,N-1| + |N,0\rangle\langle 0,N-1| + |0,N-1\rangle\langle N,0|\right) \tag{9}$$

Investigation of the error boundss (upper and lower bounds) for distinguishing the density matrices $\rho_{0,1}$ corresponding the the hypotheses $H_{0,1}$ continued in the last three months, but has not yet been completed. Study of other distinguishability metrics and modified entangled state configurations are continuing. We are developing a complete theoretical framework to discuss the optimum measurement schemes—shown here as simply the projection on the positive eigenvalue subspace of the Helstrom matrix relating the measured output states. Some new results of this general framework will be included in our forthcoming publication (under preparation).

4. PLANS FOR A POSSIBLE PHASE II FOLLOW-ON

We are in planning discussions for a future collaboration with the University of Maryland Baltimore County (UMBC) Quantum Technologies group led by Profs. Jim Franson and Todd Pittmann for follow-on experimental work beyond our Phase I theory effort. The entangled decoy state approach, which at this moment appears optimal, is especially promising from a practical standpoint because it allows a homodyne detection scheme to be used as opposed to photon-number-counting detectors needed by the standard decoy-state approach. Consequently, detectors with much higher efficiencies and lower dark-count rates can be used with our new scheme, increasing the key generation rate. It will be relatively straightforward for the UMBC group o prepare the infrastructure for a homodyne detection scheme coupled with entangled ($N = 1$ N00N) decoy-state free-space QKD, culminating in a proof-of-principle demonstration, and we are excited about this opportunity. Upon invitation, we have recently proposed a Phase II follow-on to our Phase-I project involving a collaboration between MathSense Analytics, our Phase-I research institution partner Louisiana State University, and the UMBC group. Our proposed Phase-II objectives are to complete the theoretical development reported above, to experimentally demonstrate the efficacy of the new protocols in a laboratory setting, and to carry out numerical and simulation analyses in support of the experimental work, culminating in the design, breadboarding, and production of a table-top demonstration QKD system.

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum Cryptography, Rev. Mod. Phys. 74 (2002)
[2] V. Scarani et al., "The Security of Practical Quantum Key Distribution", Rev. Mod. Phys. 81 (2009)
[3] B. Qi, L. Qian, and H. Lo, A brief introduction of quantum cryptography for engineers
[4] C. H. Bennett and G. Brassard, Proceedings of IEEE International Conference on Computers, Systems, and Signal processing, pp. 175-179, IEEE New York (1984)
[5] B. Huttner, N. Imoto, N. Gisin, and T.Mor, Quantum cryptography with coherent states, Phys. Rev. A 51, 1863 (1995)
[6] G. Brassard, N. Lütkenhaus, T.Mor, and B.C. Sanders, Limitations on Practical Quantum Cryptography, Phys. Rev. Lett. 85, 1330 (2000)
[7] N. Lütkenhaus, Security against individual attacks for realistic quantum key distribution, Phys. Rev. A 61, 052304 (2000)
[8] N. Lütkenhaus and M. Jahma, Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack, New J. Phys. 4, 44 (2002)
[9] H.P. Yuen, "Quantum amplifiers, quantum duplicators and quantum cryptography", Quantum Semiclass. Opt. 8, 939 (1996)
[10] X.B. Wang, Beating the photon-number-splitting attack in practical quantum cryptography, Phys. Rev. Lett. 94, 230503 (2005)
[11] H. Lo, X. Ma, K. Chen, Physical Review Letters, 94 (2005) 230504
[12] X.B. Wang, T. Hiroshima, A. Tomita, and M. Hayashi, "Quantum information with Gaussian states," Phys. Rep. 448, 1 (2007)
[13] W.Y. Hwang, "Quantum key distribution with high loss: toward global secure communication", Phys. Rev. Lett. 91, 057901 (2003)
[14] J.W. Harrington, J.M Ettinger, R.J. Hughes, J.E. Nordholt, "Enhancing practical security of quantum key distribution with a few decoy states"
[15] T.Y. Chen, et al. http://arxiv.org/abs/0908.4063, "200 km Decoy-state quantum key distribution with photon polarization"
[16] C.-Z. Peng et al., Experimental Long-Distance Decoy-State Quantum Key Distribution Based on Polarization Encoding, Phys. Rev. Lett. 98, 010505 (2007)
[17] T. Schmitt-Manderbach et al., Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km, Phys. Rev. Lett. 98, 010504 (2007)
[18] D. Rosenberg et al., "Practical long-distance quantum key distribution system using decoy levels", New J. Phys. 11, 045009 (2009)
[19] T.Y. Chen et al., "Field test of a practical secure communication network with decoy-state quantum cryptography", Opt. Exp. 17, 6450 (2009)
[20] Q. Wang et al., "Experimental Decoy-State Quantum Key Distribution with a Sub-Poissionian Heralded Single-Photon Source", Phys. Rev. Lett. 100, 090501 (2008)
[21] Z.Q. Yin et al., "Experimental Decoy State Quantum Key Distribution Over 120 km Fibre", Chin. Phys. Lett. 25, 3547 (2008)
[22] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, "Experimental Quantum Key Distribution with Decoy States", Phys. Rev. Lett. 96, 070502 (2006)
[23] A.K. Ekert, "Quantum cryptography based on Bell's theorem," Phys. Rev. Lett. 67, 661-663 (1991)
[24] H. Inamori, N. Lutkenhaus, D. Mayers, Unconditional security of practical quantum key distribution, Eur. Phy. J. D 41, 599 (2007)
[25] D. Gottesman, H.-K. Lo, N. Lutkenhaus, and J. Preskill, Security of quantum key distribution with imperfect devices, Quantum Inf. Comput. 4, 325 (2004)
[26] J.G. Raty et al, New J. Phys. 4, 82 (2002)
[27] R.J. Hughes et al, New J. Phys. 4, 43 (2002)
[28] P.W. Shor and J. Preskill, Phys. Rev. Lett. 85, 441 (2000)
[29] H.K. Lo and H.F. Chau, Science 283, 2050 (1999)
[30] D. Mayers, J. Assoc. Comput. Mach. 48, 351 (2001)
[31] A.K. Ekert, Phys. Rev. Lett. 67, 661 (1991)
[32] C.H. Bennett, D.P. DiVincenzo, J.A. Smolin, and W.K. Wootters, Phys. Rev. A 54, 3824 (1996)
[33] A.K. Ekert, J.G. Rarity, P.R. Tapster, and G. Massimo, Palma, Phys. Rev. Lett. 69, 1293 (1992)
[34] J. Brendel, W. Tittel, H. Zbinden and N. Gisin, Phys. Rev. Lett. 82, 2594 (1999)
[35] J.D. Franson, Phys. Rev. Lett. 62, 2205 (1989)
[36] C.K. Hong, Z.Y. Ou, and L. Mandel, Phys. Rev. Lett. 59, 2044 (1987)
[37] Y.H. Shih and C.O. Alley, Phys. Rev. Lett. 61, 2921 (1988)
[38] Ch.H. Bennett et al., J. Cryptology 5, 3 (1992)
[39] A. Acín, N. Gisin, and V. Scarani, Phys. Rev. A 69, 012309 (2004)
[40] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, Phys. Rev. Lett. 92, 057901 (2004)
[41] J. Liang, S.M. Hendrickson, and T.B. Pittman, arXiv:1012.4434v1 [quant-ph]
[42] J. Hu, X. Wang, http://arxiv.org/abs/1004.3730
[43] N. Gisin, et al. http://arxiv.org/abs/quant-ph/0411022