Error Models and Error Mitigation for Long-Distance, High-Fidelity Quantum Secret Sharing

Brent J. Yen and Jeffrey H. Shapiro

Research Laboratory of Electronics
Massachusetts Institute of Technology
Cambridge, MA 02139-4307

ABSTRACT

A quantum communication architecture is being developed for long-distance, high-fidelity transmission and storage of Greenberger-Horne-Zeilinger states. This system uses an ultrabright narrowband source of polarization-entangled photons plus trapped-atom quantum memories, and it is compatible with long-distance transmission over standard telecommunication fiber. An error model for the preceding architecture is derived, and the use of quantum error correction or entanglement purification protocols to improve the performance of this quantum communication system is also discussed.

Keywords: Greenberger-Horne-Zeilinger states, quantum communication, quantum error-correcting codes, entanglement purification protocols

1. INTRODUCTION

There has been much interest in Greenberger-Horne-Zeilinger (GHZ) states[1] because they can be used in a nonstatistical disproof of local hidden-variable theories of physics, and as resources for multiparty quantum communication protocols.[2] Shapiro[3] has recently described an architecture for long-distance transmission and storage of three-party GHZ states. His architecture uses an ultrabright narrowband source of polarization-entangled photons plus trapped-atom quantum memories, and it is compatible with long-distance transmission over standard telecommunication fiber. In the present paper we extend Shapiro's work in several ways. First, paralleling the approach taken by Aung,[4,5] we establish single-photon error models for two versions of the proposed GHZ quantum communication system: one using dual degenerate parametric amplifiers (dual-DPAs) for its entanglement source, and the other using a DPA plus a heralded source of single photons. We show that the density operators of the entangled mixed states stored in the quantum memories are diagonal in a simple logical basis. Using these error models, we develop performance analyses for two GHZ-state quantum communication systems. In particular, we consider quantum secret sharing (QSS) protocols[2] for both classical and quantum information distribution among multiple parties, i.e., communication protocols for which it is necessary for the receivers to cooperate in order to learn the secret information. We assess the QSS performance of our GHZ systems by evaluating the bit error rate of classical information sharing and the fidelity of quantum information sharing. We also describe the use of quantum error-correcting codes and entanglement purification protocols for improving the robustness of this GHZ-state quantum communication architecture.

2. GHZ-STATE SYSTEMS

Figure 1 is a schematic diagram for a long-distance quantum communication system that allows for the transmission and storage of the GHZ states required for multiparty quantum communication protocols such as QSS. This system uses an ultrabright source of polarization-entangled photons produced from optical parametric amplifiers. It employs quantum-state frequency conversion and time-division multiplexing polarization restoration[3] (not shown in Fig. 1) to transmit the entangled photons over standard telecommunications fiber to be loaded into ^{87}Rb trapped-atom quantum memories[6] for storage and processing. The GHZ system is run under a clocked

Send correspondence to J. H. Shapiro, E-mail: jhs@mit.edu, Telephone: 617-253-4179.

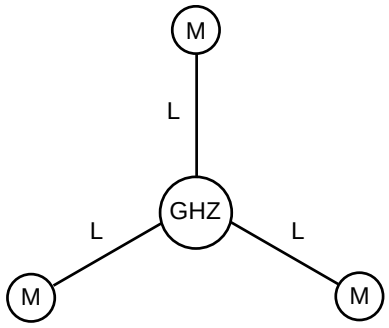

Figure 1. Schematic of long-distance GHZ communication system. GHZ = source of polarization-entangled photons from either Fig. 2(a) or (b); $L = L\,\mathrm{km}$ of standard telecommunications fiber; M = trapped-atom quantum memory.

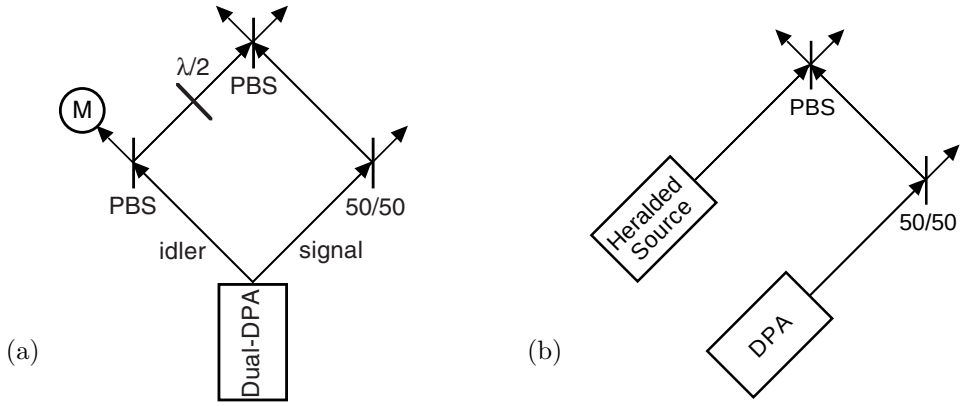

Figure 2. Source arrangements for the GHZ-state communication architecture in Fig. 1. (a) Dual-DPA GHZ system. The quantum memory in this figure represents a memory internal to the source block in Fig. 1; its loading is used as a trigger signal.[3] (b) Heralded single-photon source plus DPA system. PBS = polarizing beam splitter, $\lambda/2$ = half-wave plate.

loading protocol in which time slots of entangled photons are transmitted over optical fibers in the $1.55\,\mu$m low-loss window and gated into their respective quantum memories. We expect that the memory loading protocol can be run at cycling rates as high as $R = 500\,\mathrm{kHz}$, so that we can attempt to load a GHZ state once every $2\,\mu$s. By using this protocol to sequentially load an array of atomic memories at each location in Fig. 1, we can build up a reservoir of GHZ states that are shared by these memories.

We consider two possible source arrangements for the GHZ block in Fig. 1. The first is an ultrabright, narrowband variant of the source used by Bouwmeester et al. in an initial experimental demonstration of GHZ-state generation.[7] That experiment was an annihilative table-top measurement and had extremely low flux: 1 GHZ state every 150 sec. Our version of the Bouwmeester et al. source—shown in Fig. 2(a)—replaces their parametric downconverter with a pair of doubly-resonant, type-II phase matched DPAs. With this source, the Fig. 1 arrangement permits a throughput comparable to what Bouwmeester et al. produced in the laboratory to be realized at a source-to-memory radius of 10 km.[3] More important, though, is the fact that the memories in the Fig. 1 architecture allow the GHZ state to be stored for use in applications of three-party entanglement.

Recent work has shown that it may be possible to construct heralded single-photon sources.[8] With such a source, we can design a GHZ system with a substantially higher throughput than the configuration discussed above. In Fig. 2(b), the heralded source places a single photon in the proper spatio-temporal mode for coupling to the trapped-atom quantum memory during each loading cycle. With the heralded-plus-DPA GHZ source, throughput rises by three orders of magnitude over the dual-DPA system, to about 15 GHZ states/sec at a 10 km source-to-memory radius.[3]

2.1. Dual-DPA GHZ System

The first GHZ system uses a dual-DPA source of polarization-entangled photon pairs.[9] Assume the DPA sources have cavity linewidth Γ, output-coupling rate γ, and anti-phased, continuous-wave pumps with normalized gain $G > 0$. Then the signal (S) and idler (I) output beams of DPAs 1 and 2 are each in zero-mean Gaussian states with normally-ordered and phase-sensitive correlation functions

$$\langle \hat{A}^{\dagger}_{k_j}(t+\tau)\hat{A}_{k_j}(t)\rangle = \frac{G\gamma}{2}\left[\frac{e^{-(1-G)\Gamma|\tau|}}{1-G} - \frac{e^{-(1+G)\Gamma|\tau|}}{1+G}\right], \tag{1}$$

$$\langle \hat{A}_{S_j}(t+\tau)\hat{A}_{I_j}(t)\rangle = \frac{(-1)^{j-1}G\gamma}{2}\left[\frac{e^{-(1-G)\Gamma|\tau|}}{1-G} + \frac{e^{-(1+G)\Gamma|\tau|}}{1+G}\right], \tag{2}$$

for $k = S, I$ and $j = 1, 2$, where $\hat{E}_S(t) = \hat{A}_S(t)e^{-i\omega_P t/2}$ and $\hat{E}_I(t) = \hat{A}_I(t)e^{-i\omega_P t/2}$ are photon-units, positive-frequency signal and idler field operators, and ω_P is the pump frequency. Fiber transmission loss does not change the Gaussian nature of the joint signal/idler states; it merely multiplies the DPA correlation functions by the transmission factor $\eta_L < 1$. The signal and idler output beams of DPAs 1 and 2 are combined into vector fields, $\hat{\boldsymbol{A}}_S(t) = \begin{pmatrix}\hat{A}_{S_1}(t) & \hat{A}_{S_2}(t)\end{pmatrix}^T$ and $\hat{\boldsymbol{A}}_I(t) = \begin{pmatrix}\hat{A}_{I_2}(t) & \hat{A}_{I_1}(t)\end{pmatrix}^T$, and transmitted along the signal and idler paths in Fig. 2(a) where they are gated into the quantum memories.

We use a cold-cavity loading analysis to derive the state that is loaded into the quantum memories. Let $\{\,\hat{a}_l(T_c) : l = T_y, A_x, A_y, B_x, B_y, C_x, C_y\,\}$, be the intracavity annihilation operators after a T_c-second long loading interval for the y-polarized mode of the trigger memory and the x- and y- polarized modes of the quantum memories $\{A, B, C\}$, viz., a clockwise labeling of the quantum memories in Fig. 1. If the memory cavities have cavity linewidth Γ_c and input-coupling rate γ_c, then the intracavity operators are related to the input fields by

$$\hat{\boldsymbol{a}}_k(T_c) = \hat{\boldsymbol{a}}_k(0)e^{-\Gamma_c T_c} + \int_0^{T_c} e^{-\Gamma_c(T_c-t)}\left[\sqrt{2\gamma_c}\hat{\boldsymbol{A}}_k(t) + \sqrt{2(\Gamma_c-\gamma_c)}\hat{\boldsymbol{A}}_{k_v}(t)\right]dt, \tag{3}$$

for $k = A, B, C$, where the initial internal annihilation operators and loss operators $\{\hat{\boldsymbol{a}}_k(0), \hat{\boldsymbol{A}}_{k_v}(t)\}$ are in vacuum states.

It is not hard to show that the joint anti-normally ordered characteristic function for the Gaussian state of the quantum memory modes is

$$\begin{aligned}\chi_A^{T_y ABC}(\boldsymbol{\zeta}) = \exp\Bigg[&-\left(\frac{1+\bar{n}}{2}\right)\left(|\zeta_{A_x}+\zeta_{B_y}|^2 + |\zeta_{A_y}+\zeta_{C_y}|^2 + |\zeta_{B_x}+\zeta_{C_x}|^2 + 2|\zeta_{T_y}|^2\right)\\ &-\frac{1}{2}\left(|\zeta_{A_x}-\zeta_{B_y}|^2 + |\zeta_{A_y}-\zeta_{C_y}|^2 + |\zeta_{B_x}-\zeta_{C_x}|^2\right)\\ &+\tilde{n}\mathrm{Re}[(\zeta_{A_x}+\zeta_{B_y})(\zeta_{A_y}+\zeta_{C_y})] - \sqrt{2}\tilde{n}\mathrm{Re}[\zeta_{T_y}(\zeta_{B_x}+\zeta_{C_x})]\Bigg],\end{aligned} \tag{4}$$

where

$$\bar{n} = I_- - I_+, \tag{5}$$

$$\tilde{n} = I_- + I_+, \tag{6}$$

$$I_\pm = \frac{\eta_L\gamma\gamma_c}{\Gamma\Gamma_c}\frac{G}{(1\pm G)(1\pm G+\Gamma_c/\Gamma)}. \tag{7}$$

2.2. Heralded-plus-DPA GHZ System

The heralded-plus-DPA GHZ system uses a single DPA and a heralded source of single photons. The heralded source makes it possible to place a photon at the half-wave plate in each loading cycle, which improves the throughput of the overall system. Let the transmission factor for the heralded photon be $\eta = \eta_L\gamma\gamma_c/\Gamma\Gamma_c$. The

joint anti-normally ordered characteristic function of the quantum memory modes for the heralded-plus-DPA source GHZ system is

$$\chi_A^{ABC}(\boldsymbol{\zeta}) = \left(1 - \frac{\eta}{2}|\zeta_{A_x} + \zeta_{B_y}|^2\right) \exp\Bigg[-\left(\frac{1+\bar{n}}{2}\right)\left(|\zeta_{A_y} + \zeta_{C_y}|^2 + |\zeta_{B_x} + \zeta_{C_x}|^2\right) - \frac{1}{2}\left(2|\zeta_{A_x}|^2 + 2|\zeta_{B_y}|^2 + |\zeta_{A_y} - \zeta_{C_y}|^2 + |\zeta_{B_x} - \zeta_{C_x}|^2\right) + \tilde{n}\mathrm{Re}[(\zeta_{B_x} + \zeta_{C_x})(\zeta_{A_y} + \zeta_{C_y})]\Bigg]. \quad (8)$$

3. SINGLE-PHOTON ERROR MODEL

A procedure for nondestructively detecting whether a quantum memory has absorbed a photon has been described in Ref. 3. This procedure makes it possible to isolate erasure events, i.e., loading intervals in which any of the atomic memories fails to absorb a photon. A method has also been proposed[4, 5] for converting multiphoton events, i.e., loading intervals in which any of the memory cavities absorbs two or more photons, into erasure events. After eliminating erasures, the only remaining loading events are those in which a single photon entered one of the memories at each end of the quantum communication system. In this section, we derive the single-photon error model density matrices for the dual-DPA and heralded-plus-DPA GHZ-state systems.

3.1. Dual-DPA GHZ System

We develop an error model for the dual-DPA source GHZ system conditioned on the event that each memory loads a single photon. Define the computational basis of the quantum memories as

$$|0\rangle_A = |01\rangle_{A_xA_y} \quad \text{and} \quad |1\rangle_A = |10\rangle_{A_xA_y}, \quad (9)$$
$$|0\rangle_B = |01\rangle_{B_xB_y} \quad \text{and} \quad |1\rangle_B = |10\rangle_{B_xB_y}, \quad (10)$$
$$|0\rangle_C = |10\rangle_{C_xC_y} \quad \text{and} \quad |1\rangle_C = |01\rangle_{C_xC_y}, \quad (11)$$

in terms of the number-ket representations for the x- and y-polarized photons that loaded these memories. With this computational basis, the GHZ state loaded by the Fig. 1 system is $|\psi_{\mathrm{GHZ}}\rangle_{ABC} = (|000\rangle_{ABC} + |111\rangle_{ABC})/\sqrt{2}$.

To study the success and error events in our GHZ system, we consider an equivalent system model in which the effects of memory cavity loading are included in the DPA source state. This means we can assume that the sources generate outputs $\{\,\hat{a}_{S_j}, \hat{a}_{I_j} : j = 1, 2\,\}$, in the two-mode Gaussian states described by the characteristic functions

$$\chi_A^{S_1I_1}(\zeta_{S_1}, \zeta_{I_1}) = \exp\left[-(1+\bar{n})(|\zeta_{S_1}|^2 + |\zeta_{I_1}|^2) + 2\tilde{n}\mathrm{Re}(\zeta_{S_1}\zeta_{I_1})\right], \quad (12)$$

and

$$\chi_A^{S_2I_2}(\zeta_{S_2}, \zeta_{I_2}) = \exp\left[-(1+\bar{n})(|\zeta_{S_2}|^2 + |\zeta_{I_2}|^2) - 2\tilde{n}\mathrm{Re}(\zeta_{S_2}\zeta_{I_2})\right]. \quad (13)$$

In Table 1, we list the seven possible combinations of source photons that, ignoring beam splitter losses, will load exactly one photon in each quantum memory.* This table also lists the quantum memory state that each such source combination loads. We can use Table 1, together with source number-state probabilities, to compute the success and error probabilities of the GHZ-state memory loading protocol. Let $\Pr(|mn\rangle_{SI}) = {}_{SI}\langle mn|\hat{\rho}_{SI}|mn\rangle_{SI}$, where $|mn\rangle_{SI}$ is the product number state of the DPA output signal and idler modes, and $\hat{\rho}_{SI}$ is the density

*Note that the desired entry in this table, $|\psi_{\mathrm{GHZ}}\rangle_{ABC}$, occurs when one signal/idler pair from each DPA provides the four photons that load the $\{T, A, B, C\}$ memories. For the other memory states shown in Table 1, one of the DPAs must produce more than one signal/idler pair to achieve the memory load. Such memory loads occur through a combination of multiple-pair emission from a DPA and source-to-memory loss.

DPA_1 Photons	DPA_2 Photons	Memory State Loaded
S_1, I_1	S_2, I_2	$\|\psi_{\text{GHZ}}\rangle_{ABC}$
S_1, S_1, I_1	S_2	$\|101\rangle_{ABC}$
S_1, I_1, I_1	S_2	$\|001\rangle_{ABC}$
S_1	S_2, I_2, I_2	$\|110\rangle_{ABC}$
I_1	S_2, I_2, I_2	$\|010\rangle_{ABC}$
S_1, S_1	S_2, I_2	$\|100\rangle_{ABC}$
I_1, I_1	S_2, I_2	$\|011\rangle_{ABC}$

Table 1. Combinations of dual-DPA source photons that, ignoring beam splitter losses, load a single photon in each quantum memory of Fig. 1. Also shown is the state of memories A, B, and C that results from each such source combination. Photons S_j and I_j, $j = 1, 2$, represent signal and idler photons from the jth DPA.

operator corresponding to either (12) or (13). In Appendix A, we derive the following source number-state probabilities:

$$\Pr\left(|01\rangle_{SI}\right) = \frac{N}{D^2}, \tag{14}$$

$$\Pr\left(|02\rangle_{SI}\right) = \frac{N^2}{D^3}, \tag{15}$$

$$\Pr\left(|11\rangle_{SI}\right) = \frac{N^2 + \tilde{n}^2}{D^3}, \tag{16}$$

$$\Pr\left(|12\rangle_{SI}\right) = \frac{N(N^2 + 2\tilde{n}^2)}{D^4}, \tag{17}$$

where $N \equiv \bar{n}(1 + \bar{n}) - \tilde{n}^2$ and $D \equiv (1 + \bar{n})^2 - \tilde{n}^2$.

In the single-photon error model, the quantum memories can load the GHZ state only if the dual-DPA source generates the four photons $\{S_1, S_2, I_1, I_2\}$, i.e., each DPA outputs exactly one signal and one idler photon. We compute the probability of loading the GHZ state by conditioning on the event that the dual-DPA source generates the four photons $\{S_1, S_2, I_1, I_2\}$ as follows:

$$\Pr\left(|\psi_{\text{GHZ}}\rangle_{ABC}\right) = \Pr\left(\,|\psi_{\text{GHZ}}\rangle_{ABC} \mid \{S_1, S_2, I_1, I_2\}\,\right) \Pr\left(\{S_1, S_2, I_1, I_2\}\right) \tag{18}$$

$$= \frac{1}{4}\Pr\left(|11\rangle_{SI}\right)^2 = \frac{1}{4}\left(\frac{N^2 + \tilde{n}^2}{D^3}\right)^2 = \frac{(N^2 + \tilde{n}^2)^2}{4D^6}. \tag{19}$$

The factor of 1/4 after the second equality represents factor-of-two losses at the top PBS and at the 50/50 beam splitter in Fig. 2(a).

For each source combination in Table 1, there is a factor of 1/4 loss arising from the beam splitters in our setup, so that the probabilities of the error components are

$$\Pr\left(|101\rangle_{ABC}\right) = \Pr\left(|001\rangle_{ABC}\right) = \Pr\left(|110\rangle_{ABC}\right) = \Pr\left(|010\rangle_{ABC}\right) \tag{20}$$

$$= \frac{1}{4}\Pr\left(|01\rangle_{SI}\right)\Pr\left(|12\rangle_{SI}\right) = \frac{N^2(N^2 + 2\tilde{n}^2)}{4D^6}, \tag{21}$$

and

$$\Pr\left(|100\rangle_{ABC}\right) = \Pr\left(|011\rangle_{ABC}\right) = \frac{1}{4}\Pr\left(|11\rangle_{SI}\right)\Pr\left(|02\rangle_{SI}\right) = \frac{N^2(N^2 + \tilde{n}^2)}{4D^6}. \tag{22}$$

Using the basis,

$$\left\{\frac{|000\rangle_{ABC} \pm |111\rangle_{ABC}}{\sqrt{2}}, |001\rangle_{ABC}, |110\rangle_{ABC}, |010\rangle_{ABC}, |101\rangle_{ABC}, |011\rangle_{ABC}, |100\rangle_{ABC}\right\}, \tag{23}$$

Heralded Photon	DPA Photons	Memory State Loaded
H	S, I	$\|\psi_{\rm GHZ}\rangle_{ABC}$
H	I, I	$\|001\rangle_{ABC}$
H	S, S	$\|110\rangle_{ABC}$
—	S, S, I	$\|010\rangle_{ABC}$
—	S, I, I	$\|011\rangle_{ABC}$

Table 2. Combinations of source photons that, ignoring beam splitter losses, load a single photon into each quantum memory for the heralded GHZ system. H represents a photon from the heralded source, and S, I are signal and idler photons from the DPA source.

we now find the joint conditional density matrix for memories A, B, and C, given that an erasure has not occurred. For the dual-DPA GHZ system, this density matrix turns out to be diagonal in the Eq. (23) basis, and given by

$$\hat{\rho}_{ABC} = \mathrm{diag}\big(P_{G_d} \quad 0 \quad P_{e1_d} \quad P_{e1_d} \quad P_{e1_d} \quad P_{e1_d} \quad P_{e2_d} \quad P_{e2_d}\big)\,, \tag{24}$$

where

$$P_{G_d} = \frac{(N^2+\tilde{n}^2)^2}{7N^4+12N^2\tilde{n}^2+\tilde{n}^4}, \tag{25}$$

$$P_{e1_d} = \frac{N^2(N^2+2\tilde{n}^2)}{7N^4+12N^2\tilde{n}^2+\tilde{n}^4}, \tag{26}$$

$$P_{e2_d} = \frac{N^2(N^2+\tilde{n}^2)}{7N^4+12N^2\tilde{n}^2+\tilde{n}^4}. \tag{27}$$

3.2. Heralded-plus-DPA GHZ System

We now develop the single-photon error model for the heralded-plus-DPA GHZ system. We begin by examining the ways in which exactly one photon can be loaded at each quantum memory. To do so requires exactly three photons from the heralded-plus-DPA source; Table 2 shows the source combinations that can load each of the memories with a single photon, ignoring the beam splitter losses.

To compute the probabilities of the events in Table 2, we use the DPA source probabilities listed in Eqs. (14)–(17) and let η be the probability of receiving a heralded photon. Then,

$$\Pr\left(|\psi_{\rm GHZ}\rangle_{ABC}\right) = \Pr\left(\,|\psi_{\rm GHZ}\rangle_{ABC} \mid \{H,S,I\}\,\right)\Pr\left(\{H,S,I\}\right) = \frac{1}{4}\eta\Pr\left(|11\rangle_{SI}\right) = \frac{\eta(N^2+\tilde{n}^2)}{4D^3}. \tag{28}$$

The error components are computed similarly:

$$\Pr\left(|001\rangle_{ABC}\right) = \Pr\left(|110\rangle_{ABC}\right) = \frac{1}{4}\Pr\left(H\right)\Pr\left(|02\rangle_{SI}\right) = \frac{\eta N^2}{4D^3}, \tag{29}$$

$$\Pr\left(|010\rangle_{ABC}\right) = \Pr\left(|011\rangle_{ABC}\right) = \frac{1}{4}[1-\Pr\left(H\right)]\Pr\left(|12\rangle_{SI}\right) = (1-\eta)\frac{N(N^2+2\tilde{n}^2)}{4D^4}. \tag{30}$$

For the heralded-plus-DPA source, the conditional density matrix in the basis (23) is therefore,

$$\hat{\rho}_{ABC} = \mathrm{diag}\big(P_{G_h} \quad 0 \quad P_{e1_h} \quad P_{e1_h} \quad P_{e2_h} \quad 0 \quad P_{e2_h} \quad 0\big)\,, \tag{31}$$

where

$$P_{G_h} = \frac{\eta(N^2+\tilde{n}^2)D}{\eta(3N^2+\tilde{n}^2)D + 2(1-\eta)N(N^2+2\tilde{n}^2)}, \tag{32}$$

$$P_{e1_h} = \frac{\eta N^2 D}{\eta(3N^2+\tilde{n}^2)D + 2(1-\eta)N(N^2+2\tilde{n}^2)}, \tag{33}$$

$$P_{e2_h} = \frac{(1-\eta)N(N^2+2\tilde{n}^2)}{\eta(3N^2+\tilde{n}^2)D + 2(1-\eta)N(N^2+2\tilde{n}^2)}. \tag{34}$$

In calculating these matrix elements we have used the same transmission loss factor, $\eta = \eta_L\gamma\gamma_c/\Gamma\Gamma_c$, for each source-to-memory path in Figs. 1 and 2(b).

4. QUANTUM SECRET SHARING

Secret sharing refers to cryptographic protocols that allow Alice to share secret information with Bob and Charlie in such a way that individually they have no means for learning Alice's secret, but by working together can they gain access to Alice's secret information. One classical implementation of secret sharing requires Alice to send Bob a random bit string r and to send Charlie the modulo-2 sum, $r \oplus m$, of the random bit string r and her message m. If Bob and Charlie act together, they can recover Alice's message m simply by adding their bit strings together. Of course, this protocol presumes that Bob cannot monitor Alice's transmission to Charlie and, likewise, that Charlie cannot intercept Alice's transmission to Bob.

Quantum secret sharing (QSS) protocols divide into two types, depending on whether Alice's secret information is classical or quantum. We will look at how GHZ states can be used to share classical and quantum secrets[2] and analyze the performance of our GHZ systems in the single-photon error model.

4.1. QSS for Classical Secrets

Hillery et al. presented a QSS protocol in Ref. 2 that allows Alice to send classical secret messages to Bob and Charlie by using GHZ states. The three parties first share N GHZ states, i.e., their joint state is $|\psi_{\rm GHZ}\rangle_{ABC}^{\otimes N}$.[†] For each shared GHZ state,

$$|\psi_{\rm GHZ}\rangle_{ABC} = \frac{1}{\sqrt{2}}(|000\rangle_{ABC} + |111\rangle_{ABC}), \tag{35}$$

Alice, Bob, and Charlie measure on their own memories randomly in either the x basis or the y basis, where

$$|x\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle), \quad |y\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm i|1\rangle). \tag{36}$$

After making these measurements, Alice, Bob, and Charlie publicly announce their measurement bases. Bob and Charlie individually have no information about Alice's measurement outcomes, but in half of the cases—i.e., when Bob and Charlie used the same basis and Alice used the x basis, or when Bob and Charlie used different bases and Alice used the y basis—they can work together to determine Alice's results by using the lookup table in Table 3. For example, if they all measure in the x basis and Bob and Charlie both obtain the result $x-$, then they know that Alice has the result $x+$.

Alice, Bob, and Charlie keep the measurement results from the cases in which they choose appropriate bases and discard the others. By associating $x+, y+$ results with bit 0 and $x-, y-$ results with bit 1, Alice now shares a joint key with Bob and Charlie with which she can encode classical messages.

In our error model, Alice, Bob, and Charlie will sometimes carry out the QSS protocol with an incorrect state from the ensemble of states in the basis (23). In an error event, it is possible for Bob and Charlie to obtain incorrect results from the lookup table. Shared key bits created with error states have error probability 1/2.

[†]Reference 2 does not present an architecture for establishing this shared entanglement over a long distance; we described just such an architecture, however, in Sec. 2.

		Charlie			
		$x+$	$x-$	$y+$	$y-$
Bob	$x+$	$x+$	$x-$	$y-$	$y+$
	$x-$	$x-$	$x+$	$y+$	$y-$
	$y+$	$y-$	$y+$	$x-$	$x+$
	$y-$	$y+$	$y-$	$x+$	$x-$

Table 3. QSS for classical information distribution. Lookup table for determining Alice's measurement outcome.

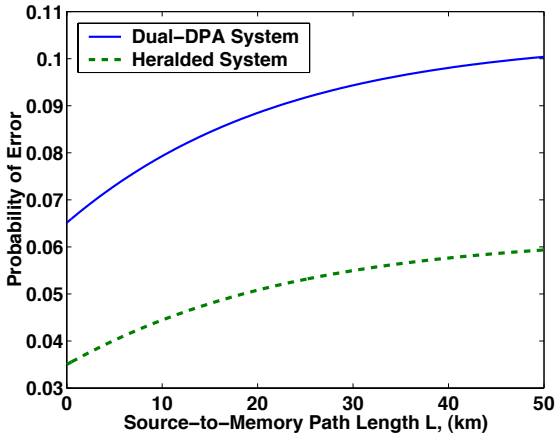

Figure 3. QSS bit error probabilities for dual-DPA and heralded-plus-DPA GHZ systems in the QSS protocol. These plots assume each DPA operates at 1% of its oscillation threshold, 5 dB excess loss in each source-to-memory path, 0.2 dB/km loss in each fiber, and $\Gamma_c/\Gamma = 0.5$ ratio of memory-cavity linewidth to source-cavity linewidth.

From the density matrices (24) and (31), we find that the bit error probability for classical information transmission via the QSS protocol is

$$P_e = 2P_{e1_d} + P_{e2_d}, \tag{37}$$

for the dual-DPA system, and

$$P_e = P_{e1_h} + P_{e2_h}, \tag{38}$$

for the heralded-plus-DPA system. The bit error probabilities (37) and (38) are plotted in Fig. 3. Possible methods for improving the performance of our GHZ systems include purifying the three-party entangled state to reduce the number of error events or using classical error correction to transmit Alice's message.

4.2. QSS for Quantum Secrets

We now consider the performance of our GHZ systems for transmission of quantum information using the QSS protocol proposed in Ref. 2. In this protocol, Alice, Bob, and Charlie share a GHZ state $|\psi_{\rm GHZ}\rangle_{ABC} = (|000\rangle_{ABC} + |111\rangle_{ABC})/\sqrt{2}$, and Alice's secret is the qubit $|\psi\rangle_S = \alpha|0\rangle_S + \beta|1\rangle_S$, which she wishes to send to Bob and Charlie in such a way that they must cooperate to obtain this quantum information. The joint state of Alice, Bob, and Charlie—including Alice's portion of the GHZ state *and* her quantum secret—at the start of the QSS protocol is $|\psi\rangle_S|\psi_{\rm GHZ}\rangle_{ABC}$.

Alice initiates the QSS protocol by making the Bell-state measurements, $\{|\psi^{\pm}\rangle_{SA}, |\phi^{\pm}\rangle_{SA}\}$, on her secret and her portion of the GHZ state. Alice then labels as (m, n) the two classical bits she derives from these measurements, using the following scheme: $\psi^+ = (0,1), \psi^- = (1,1), \phi^+ = (0,0), \phi^- = (1,0)$. She sends m to

Shared State	QSS Output	Fidelity	Dual-DPA	Heralded
$\|\psi_{\rm GHZ}\rangle_{ABC}$	$\|\phi\rangle_S$	1	P_{G_d}	P_{G_h}
$\|001\rangle_{\rm ABC}$	$\|\beta\|^2\|0\rangle_{SS}\langle 0\| + \|\alpha\|^2\|1\rangle_{SS}\langle 1\|$	1/3	P_{e1_d}	P_{e1_h}
$\|110\rangle_{ABC}$	$\|\beta\|^2\|0\rangle_{SS}\langle 0\| + \|\alpha\|^2\|1\rangle_{SS}\langle 1\|$	1/3	P_{e1_d}	P_{e1_h}
$\|010\rangle_{ABC}$	$\|\alpha\|^2\|0\rangle_{SS}\langle 0\| + \|\beta\|^2\|1\rangle_{SS}\langle 1\|$	2/3	P_{e1_d}	P_{e2_h}
$\|101\rangle_{ABC}$	$\|\alpha\|^2\|0\rangle_{SS}\langle 0\| + \|\beta\|^2\|1\rangle_{SS}\langle 1\|$	2/3	P_{e1_d}	0
$\|011\rangle_{ABC}$	$\|\beta\|^2\|0\rangle_{SS}\langle 0\| + \|\alpha\|^2\|1\rangle_{SS}\langle 1\|$	1/3	P_{e2_d}	P_{e2_h}
$\|100\rangle_{ABC}$	$\|\beta\|^2\|0\rangle_{SS}\langle 0\| + \|\alpha\|^2\|1\rangle_{SS}\langle 1\|$	1/3	P_{e2_d}	0

Table 4. For each three-party state that might be shared by Alice, Bob, and Charlie, this table lists the output state that will result from application of the QSS protocol—in which Alice, Bob, and Charlie *assume* that they have shared the GHZ state $|\psi_{\rm GHZ}\rangle_{ABC}$—the average fidelity that is achieved with this output state when the quantum secret $|\psi\rangle_S$ is uniformly distributed over the Bloch sphere, and the occurrence probabilities [from Eqs. (24) and (31), for the dual-DPA and heralded-plus-DPA sources, respectively] of these output states.

Bob and $m \oplus n$ to Charlie, using secure classical channels so that Bob cannot intercept $m \oplus n$ and Charlie cannot obtain m. It follows that neither Bob nor Charlie has any information about Alice's secret—even after receiving the classical information from Alice—because their marginal density operators at this point in the protocol can be shown to be $\hat{\rho}_B = \hat{I}_B/2$ and $\hat{\rho}_C = \hat{I}_C/2$, respectively, where $\hat{I}$ is the identity operator.

For Bob and Charlie to learn Alice's secret qubit $|\psi\rangle_S$, they must cooperate. Because the no-cloning theorem precludes making two copies of this state, either Bob or Charlie—but *not* both of them—will possess a replica of $|\psi\rangle_S$ at the end of the QSS protocol. Let us arbitrarily assume that Bob and Charlie have agreed to let Charlie be the recipient of this replica. Having made that agreement, Bob measures his portion of the GHZ state in the x basis, $\{|\pm x\rangle_B \equiv (|0\rangle_B \pm |1\rangle_B)/\sqrt{2}\}$, and he sends Charlie the result of this measurement along with Alice's m bit. Together with Alice's $m \oplus n$—which he received earlier—Charlie now has all the information he needs to turn his portion of the GHZ state into a replica of Alice's secret via a local unitary operation.

4.2.1. Uncoded Performance

Let F be the average fidelity of the preceding QSS protocol when Alice's secret, $|\psi\rangle_S$, is selected from a uniform distribution over the Bloch sphere. Using Table 4, we compute the average QSS fidelity for the dual-DPA GHZ system to be,

$$F = P_{G_d} + 2P_{e1_d} + 2P_{e2_d}/3, \tag{39}$$

and for the heralded-plus-DPA GHZ system,

$$F = P_{G_h} + 2P_{e1_h}/3 + P_{e2_h}. \tag{40}$$

4.2.2. Coded Performance

Quantum error correction can be used to improve the performance of the QSS protocol. We will illustrate this improvement by considering use of the five-qubit error-correcting code:[10]

$$|0_L\rangle = |00000\rangle + |00110\rangle + |01001\rangle + |01111\rangle + |10101\rangle - |10011\rangle + |11100\rangle + |11010\rangle, \tag{41}$$

$$|1_L\rangle = -|00101\rangle - |00011\rangle + |01100\rangle - |01010\rangle - |10000\rangle + |10110\rangle + |11001\rangle + |11111\rangle. \tag{42}$$

Table 4 lists the output states that result from application of the QSS protocol—in which Alice, Bob, and Charlie *assume* that they have shared the GHZ state $|\psi_{\rm GHZ}\rangle_{ABC}$—when in fact they have shared one of the states from the basis (23). From this table, we see that applying the QSS protocol, when a particular basis state has been shared, is equivalent to sending a qubit over one of the following three channels:

$$\mathcal{E}_I(\hat{\rho}) = \hat{\rho}, \tag{43}$$

$$\mathcal{E}_A(\hat{\rho}) = \hat{P}_0\hat{\rho}\hat{P}_0^\dagger + \hat{P}_1\hat{\rho}\hat{P}_1^\dagger, \tag{44}$$

$$\mathcal{E}_B(\hat{\rho}) = \hat{P}_2\hat{\rho}\hat{P}_2^\dagger + \hat{P}_2^\dagger\hat{\rho}\hat{P}_2, \tag{45}$$

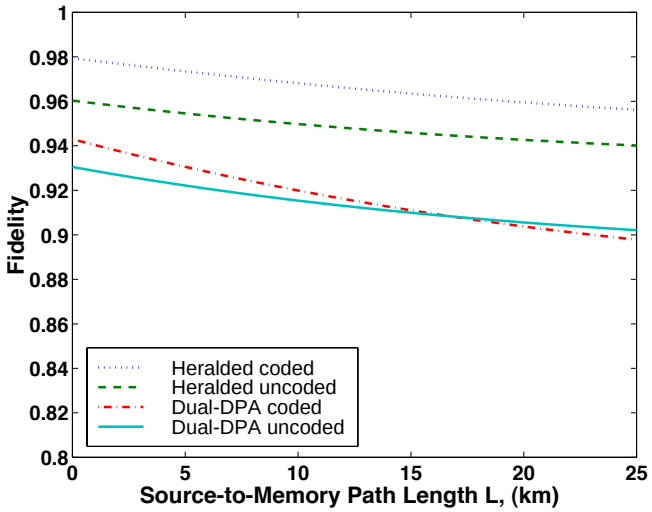

Figure 4. Average fidelity in the QSS protocol. We compare the performance of the dual-DPA and heralded-plus-DPA GHZ systems with and without coding. We assume the same operating conditions as in Fig. 3.

where $\hat{P}_0 = |0\rangle\langle 0|$, $\hat{P}_1 = |1\rangle\langle 1|$, and $\hat{P}_2 = |0\rangle\langle 1|$. Channel $\mathcal{E}_A$ takes an input qubit $\alpha|0\rangle + \beta|1\rangle$ to the mixed state $|\alpha|^2|0\rangle\langle 0| + |\beta|^2|1\rangle\langle 1|$, and channel $\mathcal{E}_B$ gives the output state $|\beta|^2|0\rangle\langle 0| + |\alpha|^2|1\rangle\langle 1|$. Because the density matrix for the $\{A, B, C\}$ quantum memories is diagonal in the Eq. (23) basis, these three channel possibilities, $\{\mathcal{E}_I, \mathcal{E}_A, \mathcal{E}_B\}$, occur with probabilities

$$P_I = P_{G_d}, \tag{46}$$
$$P_A = 2P_{e1_d}, \tag{47}$$
$$P_B = 2P_{e1_d} + 2P_{e2_d}, \tag{48}$$

for the dual-DPA system, and

$$P_I = P_{G_h}, \tag{49}$$
$$P_A = P_{e2_h}, \tag{50}$$
$$P_B = 2P_{e1_h} + P_{e2_h}, \tag{51}$$

for the heralded-plus-DPA system.

The five-qubit coded QSS channel has the form

$$\mathcal{E}_1 \otimes \mathcal{E}_2 \otimes \mathcal{E}_3 \otimes \mathcal{E}_4 \otimes \mathcal{E}_5(\hat{\rho}_{\rm enc}), \tag{52}$$

where $\hat{\rho}_{\rm enc}$ is the encoded qubit state and $\mathcal{E}_i \in \{\mathcal{E}_I, \mathcal{E}_A, \mathcal{E}_B\}$. We used simulations to evaluate the average fidelity for each of the 243 possible coded QSS channels. For each coded QSS channel, let n_k be the number of $\mathcal{E}_k$ components, $k = I, A, B$. The 243 channels were divided into 21 different cases, according to the distribution (n_I, n_A, n_B). The simulation results are displayed in Table 5. The average fidelity of the coded QSS channel is then calculated, using the multinomial distribution for (n_I, n_A, n_B), as follows,

$$F = \sum_{j=1}^{21} \Pr(\text{case } j) F_j = \sum_{j=1}^{21} \binom{5}{n_I, n_A, n_B} P_I^{n_I} P_A^{n_A} P_B^{n_B} F_j, \tag{53}$$

where F_j is the average fidelity of the five qubit code given that a coded QSS channel in case j occurs; the j-dependence of (n_I, n_A, n_B) is as given in Table 5.

Figure 4 shows the average QSS fidelity for the dual-DPA and heralded-plus-DPA GHZ systems with and without coding. We see that the heralded-plus-DPA GHZ system has significantly better performance than the

Case	(n_I, n_A, n_B)	F_j	# of channels
1	$(5,0,0)$	1	1
2	$(4,1,0)$	1	5
3	$(4,0,1)$	1	5
4	$(3,2,0)$	5/6	10
5	$(3,1,1)$	2/3	20
6	$(3,0,2)$	1/3	10
7	$(2,3,0)$	7/10	10
8	$(2,2,1)$	47/90	30
9	$(2,1,2)$	19/45	30
10	$(2,0,3)$	7/15	10
11	$(1,4,0)$	37/60	5
12	$(1,3,1)$	29/60	20
13	$(1,2,2)$	17/36	30
14	$(1,1,3)$	31/60	20
15	$(1,0,4)$	11/20	5
16	$(0,5,0)$	7/12	1
17	$(0,4,1)$	29/60	5
18	$(0,3,2)$	29/60	10
19	$(0,2,3)$	31/60	10
20	$(0,1,4)$	31/60	5
21	$(0,0,5)$	5/12	1
total			243

Table 5. Coded QSS channel simulation results. The 243 coded QSS channels are divided into 21 cases according to component distribution (n_I, n_A, n_B). For each case, we list the average fidelity F_j and the number of coded QSS channels belonging to that case.

dual-DPA system in the QSS protocol in both uncoded and coded operation. Coding improves the performance of the heralded-plus-DPA system for all path lengths shown in this figure, but beyond about 16 km source-to-memory path length coding reduces the fidelity of the dual-DPA system. The dual-DPA curves with and without error correction cross because the five-qubit code degrades performance when the incidence of multi-qubit errors is too high; the same thing occurs for the heralded-plus-DPA system, but at a much longer path length. Even when coding improves the fidelity, there is still a price to be paid: use of the five-qubit code reduces throughput by a factor of five.

4.2.3. Entanglement Purification

In this section an alternative approach for improving the performance of the GHZ system is studied: the use of an entanglement purification protocol. Let Alice, Bob, and Charlie possess a block of n mixed entangled three-party states. Through the use of local operations and classical communications, they can produce a smaller number $m < n$ of GHZ states with arbitrarily small probability of error for large n. The yield of an entanglement purification protocol is defined as $D = m/n$ in the limit $n \to \infty$.

The entanglement purification scheme we shall consider is the multiparty hashing protocol.[11] Define the cat basis as the set of orthonormal states

$$|\psi_{p,i_1 i_2}\rangle_{ABC} = \frac{|0 i_1 i_2\rangle_{ABC} + (-1)^p |1 \bar{i}_1 \bar{i}_2\rangle_{ABC}}{\sqrt{2}}, \tag{54}$$

where $p, i_1, i_2 = 0, 1$. We call p the phase bit and i_1, i_2 the amplitude bits. Given an initial mixed entangled state $\hat{\rho}_{ABC}$, let $H(p), H(i_1)$, and $H(i_2)$ be the entropies of the phase and amplitude bits with respect to the diagonal

Cat State	p	i_1	i_2	Dual-DPA	Heralded
$\|000\rangle + \|111\rangle$	0	0	0	P_{G_d}	P_{G_h}
$\|000\rangle - \|111\rangle$	1	0	0	0	0
$\|001\rangle + \|110\rangle$	0	0	1	P_{e1_d}	P_{e1_h}
$\|001\rangle - \|110\rangle$	1	0	1	P_{e1_d}	P_{e1_h}
$\|010\rangle + \|101\rangle$	0	1	0	P_{e1_d}	$P_{e2_h}/2$
$\|010\rangle - \|101\rangle$	1	1	0	P_{e1_d}	$P_{e2_h}/2$
$\|011\rangle + \|100\rangle$	0	1	1	P_{e2_d}	$P_{e2_h}/2$
$\|011\rangle - \|100\rangle$	1	1	1	P_{e2_d}	$P_{e2_h}/2$

Table 6. The distribution for each bit of the unknown cat state is determined by the single-photon density matrices (24) and (31). The distributions can be used to compute the entropies $H(p), H(i_1)$, and $H(i_2)$.

cat-basis matrix entries of $\hat{\rho}_{ABC}$. From Table 6, we find that the entropies of the phase and amplitude bits for the dual-DPA GHZ system are

$$H(p) = H(P_{G_d} + 2P_{e1_d} + P_{e2_d}), \tag{55}$$
$$H(i_1) = H(P_{G_d} + 2P_{e1_d}), \tag{56}$$
$$H(i_2) = H(P_{G_d} + 2P_{e1_d}), \tag{57}$$

and for the heralded-plus-DPA GHZ system,

$$H(p) = H(P_{G_h} + P_{e1_h} + P_{e2_h}), \tag{58}$$
$$H(i_1) = H(P_{G_h} + 2P_{e1_h}), \tag{59}$$
$$H(i_2) = H(P_{G_h} + P_{e2_h}). \tag{60}$$

Maneva and Smolin[11] have shown that the yield of the multiparty hashing protocol is

$$Y = 1 - H(p) - \max\{H(i_1), H(i_2)\}, \tag{61}$$

if the right-hand side is a positive quantity, and it is zero otherwise.

Figure 5 compares the performance of the GHZ-state systems with and without the use of the multiparty hashing protocol. The left panel shows normalized throughput, DN_{success}, versus source-to-memory path length, where $N_{\text{success}} = R \Pr(\psi_{GHZ})$ is the throughput of successful GHZ memory loadings/sec and yield $Y = 1$ when no entanglement purification is employed. The initial fidelities of the dual-DPA and heralded GHZ systems are quite high, so the throughput lost through the application of the hashing protocol is quite modest. Assuming perfect measurements at the transmitter and perfect qubit logic at the receiver in implementing the hashing protocol, the average QSS fidelity is unity in the limit of large block sizes. The major drawback of utilizing entanglement purification, as compared to the much simpler five-qubit error correction code, is the enormous amounts of quantum memory that are needed at the transmitter and receiver to realize the large block sizes that valildate use of the asymptotic yield expression (61).

5. CONCLUSION

A quantum communication architecture for long-distance, high-fidelity transmission and storage of GHZ states for quantum secret sharing has been studied. We derived the single-photon loading event model for the GHZ system for two different source configurations, and developed performance analyses for the GHZ-based quantum secret sharing of either classical or quantum information. We evaluated the classical bit error rate of classical information sharing and examined the fidelity of quantum information sharing. A preliminary assessment of the application of quantum error correction or entanglement purification showed that these techniques can improve the performance of the baseline architecture. In the case of a simple quantum error-correcting code, this improvement comes at the cost of a substantial reduction in throughput. In the case of entanglement purification, the cost is a dramatic increase in the amount of quantum memory that will be needed at each location.

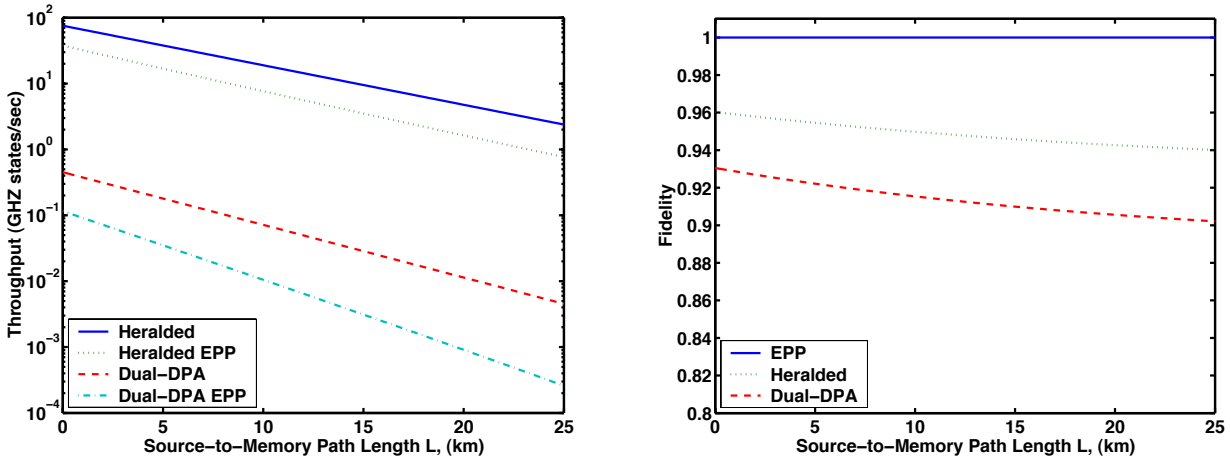

Figure 5. Performance of dual-DPA and heralded GHZ systems with the multiparty hashing protocol. Left plot: Throughput of GHZ states with and without the hashing protocol. Right plot: Average fidelity for quantum secret sharing. With the hashing protocol, the fidelity of QSS approaches one as the block size $n \to \infty$. We assume the same operating conditions as in Fig. 3. EPP = entanglement purification protocol.

APPENDIX A. NUMBER STATE PROBABILITIES

Here we provide a derivation of the product number-state probabilities (14)–(17). The mixed Gaussian state of the signal and idler is given by the anti-normally ordered characteristic function

$$\chi_A(\zeta_S,\zeta_I) = \exp\left[(1+\bar{n})(|\zeta_S|^2+|\zeta_I|^2) + 2\tilde{n}\mathrm{Re}(\zeta_S\zeta_I)\right]. \tag{62}$$

The density operator of the Gaussian state can be expressed as the operator-valued inverse Fourier transform of its characteristic function:

$$\hat{\rho}_{SI} = \iint \chi_A(\zeta_S,\zeta_I) e^{-\zeta_S\hat{a}_S^\dagger - \zeta_I\hat{a}_I^\dagger} e^{\zeta_S^*\hat{a}_S + \zeta_I^*\hat{a}_I} \frac{d^2\zeta_S d^2\zeta_I}{\pi^2}. \tag{63}$$

It is easy to show, via series expansion, that,

$$\langle n|e^{-\zeta\hat{a}^\dagger+\zeta^*\hat{a}}|n\rangle = L_n(|\zeta|^2), \tag{64}$$

where $L_n(\cdot)$ is the Laguerre polynomial of order n. The probability of the product number state $|mn\rangle_{SI}$ is then

$$\Pr(|mn\rangle_{SI}) = {}_{SI}\langle mn|\hat{\rho}_{SI}|mn\rangle_{SI} = \iint \chi_A(\zeta_S,\zeta_I) L_m(|\zeta_S|^2) L_n(|\zeta_I|^2) \frac{d^2\zeta_S\, d^2\zeta_I}{\pi^2} \tag{65}$$

$$= \int_0^\infty\int_0^\infty\int_0^{2\pi}\int_0^{2\pi} \exp\left[-(1+\bar{n})(r_S^2+r_I^2) + 2\tilde{n}r_S r_I\cos(\theta_S+\theta_I)\right] \times L_m(r_S^2)L_n(r_I^2)\frac{r_S r_I}{\pi^2}\, d\theta_S d\theta_I dr_S dr_I \tag{66}$$

$$= 4\int_0^\infty\int_0^\infty \exp\left[-(1+\bar{n})(r_S^2+r_I^2)\right] L_m(r_S^2)L_n(r_I^2)J_0(2i\tilde{n}r_S r_I) r_S r_I dr_S dr_I \tag{67}$$

$$= \frac{\bar{n}^m}{(1+\bar{n})^{m+1}}\int_0^\infty \exp\left[-\frac{\left((1+\bar{n})^2-\tilde{n}^2\right)R_I}{1+\bar{n}}\right] L_n(R_I) L_m\left(\frac{\tilde{n}^2 R_I}{\bar{n}(1+\bar{n})}\right) dR_I \tag{68}$$

$$= \binom{m+n}{m}\frac{N^{m+n}}{D^{m+n+1}} F[-m,-n;-m-n;D(\bar{n}^2-\tilde{n}^2)/N^2], \tag{69}$$

where $F[\alpha, \beta; \gamma; z]$ is the hypergeometric function. In this derivation, we introduced polar coordinates in (66), and used (7.421.1) from Ref. 12 to evaluate the inner integral in that expression, followed by the change of variables $R_I = r_I^2$, and application of (7.414.4) from Ref. 12 to get (69). Special cases of (69) are

$$\Pr(|0n\rangle_{SI}) = \frac{N^n}{D^{n+1}}, \tag{70}$$

$$\Pr(|1n\rangle_{SI}) = \frac{N^{n-1}(N^2 + n\tilde{n}^2)}{D^{n+2}}. \tag{71}$$

We obtain the number state probabilities (14)–(17) by substituting $n = 1, 2$ into Eqs. (70) and (71).

ACKNOWLEDGMENTS

This research was supported by the DoD Multidisciplinary University Research Initiative (MURI) program administered by the Army Research Office under Grant DAAD19-00-1-0177, by the Quantum Information Science and Technology program under Army Research Office Grant DAAD19-01-1-0647, and by the National Reconnaissance Office under Contract NRO000-C-0158.

REFERENCES

1. D. M. Greenberger, M. Horne, and A. Zeilinger, "Going beyond Bell's theorem," in *Quantum Theory, and Conceptions of the Universe*, M. Kafatos, ed., pp. 73–76, Kluwer Academic, 1989.
2. M. Hillery, V. Buzek, and A. Berthiaume, "Quantum secret sharing," *Phys. Rev. A* **59**, pp. 1829–1834, 1999.
3. J. H. Shapiro, "Architectures for long-distance quantum communication," *New J. of Phys.* **4**, pp. 47.1–47.18, 2002.
4. J. Aung, "Quantum error modeling and correction in long distance teleportation using singlet state," S. M. thesis, Massachusetts Institute of Technology, 2002.
5. J. H. Shapiro, J. Aung, and B. J. Yen, "Quantum error models and error mitigation for long-distance teleportation architectures," in *Proceedings of the Feynman Festival*, (College Park, MD, August 2002), quant-ph/0211086.
6. S. Lloyd, M. S. Shahriar, J. H. Shapiro, and P. R. Hemmer, "Long-distance unconditional teleportation of atomic states via complete Bell state measurements," *Phys. Rev. Lett.* **87**, art. 167903, 2001.
7. D. Bouwmeester, J-W. Pan, M. Daniell, H. Weinfurter, and A. Zeilinger, "Observation of three-photon Greenberger-Horne-Zeilinger entanglement," *Phys. Rev. Lett.* **82**, pp. 1345–1349, 1999.
8. C. Santori, M. Pelton, G. Solomon, Y. Dale, and Y. Yamamoto, "Triggered single photons from a quantum dot," *Phys. Rev. Lett.* **86**, pp. 1502–1505, 2001.
9. J. H. Shapiro and N. C. Wong, "An ultrabright narrowband source of polarization-entangled photon pairs," *J. Opt. B: Quantum and Semiclass. Opt.* **2**, pp. L1–L4, 2000.
10. R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, "Perfect quantum error correcting code," *Phys. Rev. Lett.* **77**, pp. 198–201, 1996.
11. E. N. Maneva and J. A. Smolin, "Improved two-party and multi-party purification protocols." quant-ph/0003099.
12. I. Gradshteyn and I. Ryzhik, *Table of Integrals, Series, and Products*, Academic Press, 2000.