Entanglement sudden death: a threat to advanced quantum key distribution?

Gregg S. Jaeger & Alexander V. Sergienko

Natural Computing
An International Journal

ISSN 1567-7818

Nat Comput
DOI 10.1007/s11047-014-9452-7

Springer

Nat Comput
DOI 10.1007/s11047-014-9452-7

Entanglement sudden death: a threat to advanced quantum key distribution?

Gregg S. Jaeger · Alexander V. Sergienko

Abstract Entanglement is a global characteristic unique to quantum states that depends on quantum coherence and may allow one to carry out communications and information processing tasks that are either impossible or less efficient using classical states. Because environmental noise, even when entirely local in spatial extent, can fully destroy entanglement in finite time, an effect referred to as "entanglement sudden death" (ESD), it may threaten quantum information processing tasks. Although it may be possible to "distill" entanglement from a collection of noise-affected systems under appropriate circumstances, once entanglement has been completely lost no amount of distillation can recover it. It is therefore extremely important to avoid its *complete* destruction in times comparable to those of information processing tasks. Here, the effect of local noise on a class of entangled states used in entanglement-based quantum key distribution is considered and the threat ESD might pose to it is assessed.

Keywords Entanglement · Quantum information · Quantum state decoherence

1 Introduction

Entanglement and non-locality, which long have been of interest in the foundations of quantum theory, have become of interest for technological applications as the field of quantum information science has matured. The investigation of the effects of noise on entanglement and non-locality is of prime importance in practical situations, in some cases even more than the less subtle but often related effect of quantum state decoherence. The development of practical linear optical technology has also been important for both the exploration of foundational questions and quantum communication and information processing applications. One aspect of the latter is quantum decoherence mitigation as a means of furthering practical quantum optical networking tasks such as quantum key distribution (QKD) (Gisin et al. 2002) in which entanglement can be understood to play a role, either implicitly or explicitly, as in Ekert (1992); here the relation of the former to the latter is consider in relation to a practical example.

Under the influence of noise, the quantum coherence supporting entanglement and non-locality can disappear rapidly or, more typically, be lost asymptotically in time. The latter occurs when weak noise influences a quantum system due to interactions with the system's environment. However, even in the latter case, the entanglement and non-locality depending on it can still suddenly and completely disappear. Such phenomena are referred to as Entanglement Sudden Death (ESD) (Ann and Jaeger 2007; Yu and Eberly 2004, 2006, 2007) and Bell non-locality Sudden Death (BNSD) (Jaeger and Ann 2008), respectively. ESD and BNSD have recently been intensively explored in various contexts, especially theoretically but also experimentally (e.g. Almeida et al. 2007), in both continuous and discrete systems subject to noise of various sorts (Ann and Jaeger 2009, 2007, 2008; Gisin et al. 2002).

As a means for combating quantum decoherence effects, so-called decoherence-free subspaces (DFSs) involving entangled quantum states can be very helpful in practical

G. S. Jaeger
Division of Natural Sciences and Mathematics, Boston University, Boston, MA 02215, USA
e-mail: jaeger@bu.edu

A. V. Sergienko (✉)
Department of Electrical and Computer Engineering, Boston University, Boston, MA 02215, USA
e-mail: alexserg@engc.bu.edu

Published online: 10 August 2014

QKD, see for example (Walton et al. 2003). It is interesting to consider whether the mechanism of DFSs, which in most contexts are introduced to help protect processing tasks against the effects of noise, would be helpful or hurtful in light of ESD and BNSD, given that entanglement is more fragile than coherence itself. A passive entangled-photon detection method has previously been described in relation to this method, including a scheme using DFSs for QKD. We have recently proposed such a method realized in four-photon entangled states, which currently lie at the frontier of current investigations of quantum entanglement (Jaeger and Sergienko 2006). This technique involves a specially conceived basis of entangled states that results from the natural extension of concatenated coding techniques that support decoherence mitigation in simple phase noise scenarios (Jaeger and Sergienko 2006). It is important to understand the extent to which such techniques might be threatened by ESD despite the fact that complete decoherence is resisted for all finite times in simple noise models.

Here we consider the effect of ESD on this specific method for performing decoherence-mitigated QKD under a specific local noise model. Section 2 first describes details of the theory of quantum coherence and system evolution in the presence of environmental noise. Then, Sect. 3 considers ESD in both theoretical and experimental contexts for various sorts of such noise. Section 4 describes the application of DFSs in QKD. In the final section, we focus on the pertinence specifically of phase-noise-induced ESD for QKD by virtue of their effects on the above mentioned specific classes of state in the quantum optical context.

2 Quantum decoherence

Quantum decoherence, the significance of which here lies in the degradation of quantum properties it can cause, can be classified roughly into two sorts: intrinsic and extrinsic decoherence; here, we will follow the standard approach of considering decoherence as originating extrinsically (Jaeger 2007). Extrinsic decoherence involves standard quantum dynamics of the object system together with the environment of the system of interest with which it interacts, causing it to evolve non-unitarily. The environment is assumed to be described by a Hilbert space of far greater dimension than that of the system suffering decoherence, which we take to refer here both to dephasing and to zero-temperature relaxation.

Decoherence in such situations arises when correlations occur between the system and environment, due to their mutual interaction. The reduced system state, which is that of an open quantum system is obtained by averaging over the environmental degrees of freedom, typically exhibits decoherence, and in some cases also exhibits ESD or BNSD. The open quantum systems model considered here involves a quantum system of interest $\rho_{\rm sys}$ and an environment $\rho_{\rm env}$, beginning in a joint state $\rho_{\rm tot}$ in tensor product space $\mathscr{H}_{\rm sys} \otimes \mathscr{H}_{\rm env}$. The joint system, by contrast to the object system, always evolves unitarily. Each system evolves under its internal Hamiltonian, that is, $H_{\rm sys}(t)$ or $H_{\rm env}(t)$, together with the influence of the interaction $H_{\rm int}(t)$.

$$H_{\rm tot}(t) = H_{\rm sys}(t) \otimes \mathbb{I} + \mathbb{I} \otimes H_{\rm env}(t) + H_{\rm int}(t). \tag{1}$$

The joint system is described by a statistical density matrix $\rho_{\rm st}(t)$ that evolves unitarily: $\rho_{\rm st}(t) = U(t)\rho_{\rm tot}U^{\dagger}(0)$ according to the unitary transformation $U(t) = \exp\left[-i\int_0^t dt' H_{tot}(t')\right]$. The density operator averaged over noise fields is $\rho(t) = \langle \rho_{\rm st}(t) \rangle_{\rm noise}$, cf. (Yu and Eberly 2006).

As a result of mutual interaction, correlations develop between the system and the environment over the time interval $[0, t)$. The environment, appearing as noise to the system of interest, causes dephasing and/or amplitude damping often leading to complete decoherence only asymptotically of the system reduced state $\rho_{\rm sys} = {\rm tr}_{\rm env}\rho_{\rm tot}$. This process is represented using operator sum decomposition cf. (Kraus 1983; Yu and Eberly 2006). In particular, the time-evolved density matrix is given by the completely positive and trace preserving (CPTP) map,

$$\rho(t) = \mathscr{K}[\rho(0)] = \sum_{\mu=1}^{N} \overline{K}_{\mu}^{\dagger}(t)\rho(0)\overline{K}_{\mu}(t), \tag{2}$$

where the operators in the decomposition $\overline{K}_{\mu}$ satisfy the positivity and trace preserving relations via $\sum_{\mu} \overline{K}_{\mu}^{\dagger}(t)\overline{K}_{\mu}(t) = \mathbb{I}$ and $\sum_{\mu} \overline{K}_{\mu}(t)\overline{K}_{\mu}^{\dagger}(t) = \mathbb{I}$ (Kraus 1983). These two conditions enforce completeness and unitality, the latter ensuring that the identity, which corresponds to the fully mixed state, is unchanged by the map.

Even though environmental noise in some states causes the open subsystem of interest to fully decohere only in the limit $t \to \infty$ or, in the case of DFSs not at all, this noise for non-trivial classes of initial state destroys in finite time the non-classical properties such as entanglement or non-locality dependent on the maintenance of strong quantum coherence. The quantum state purity $\mathscr{P}(\rho) = {\rm tr}\,\rho^2$ is a readily computed measure of quantum coherence that proves useful in this contest. For a d-dimensional system, $1/d \le \mathscr{P}(\rho) \le 1$. The lower bound $1/d$ achieved only for the completely mixed state. The upper bound 1 is that of any any pure state, such as those typically prepared for using in quantum information processing and communication. The strongest decoherence effect is obviously that

in which such an initially purity 1 state later reaches minimum purity, that is, $1/d$.

In the study of quantum decoherence another valuable coherence measure for arbitrary mixed state density matrices ρ_1 and ρ_2, is the quantum state fidelity given by

$$\mathrm{F}(\rho_1,\rho_2)=\left[\mathrm{tr}\left(\sqrt{\sqrt{\rho_2}\,\rho_1\sqrt{\rho_2}}\right)\right]^2, \tag{3}$$

with $0\le \mathrm{F}(\rho_1,\rho_2)\le 1$. The upper bound 1 indicates that ρ_1 and ρ_2 are indistinguishable and the lower bound 0 indicates that ρ_1 and ρ_2 are orthogonal; the fidelity may be used in certain circumstances to find the time of the loss of coherence from that of an initial state of interest.

3 Disentanglement

Because entanglement is a global property of quantum states that is non-increasing under local operations (LOs), there are natural state classifications arising from the consideration of state behavior under local operations. Since classical communication (CC) also cannot affect entanglement, entangled state classification can likewise involve local operations in conjunction with classical communication (LO+CC). For bipartite states, there exists only one equivalence class of entangled pure states of two-level systems under such constraints, under LO+CC transformations, namely, that of the Bell states. In the tripartite case, the standard classification scheme identifies two distinct classes of genuinely tripartite entangled pure states. Pure states are of the same entanglement class in this sense if the parties involved have a chance of successfully mathematically converting one state into another under the stochastic LO+CC transformations (see Bennett et al. 2001 for more detail).

For studies involving bipartite entanglement, concurrence $C(\rho)$ and the closely related entanglement of formation $E_f(\rho)$ are most often used used as entanglement measures, because they are valid for both pure and mixed states. For a two-qubit density matrix ρ_{AB}, the concurrence is

$$C(\rho_{\mathrm{AB}})=\max\left[0,\sqrt{\lambda_1}-\sqrt{\lambda_2}-\sqrt{\lambda_3}-\sqrt{\lambda_4}\right], \tag{4}$$

where the argument of the concurrence function, $\Lambda\equiv\sqrt{\lambda_1}-\sqrt{\lambda_2}-\sqrt{\lambda_3}-\sqrt{\lambda_4}$, is a function of the eigenvalues $\lambda_i\,(i=1,2,3,4)$, ordered by decreasing magnitude, of the matrix, $\tilde{\rho}_{\mathrm{AB}}=\rho_{\mathrm{AB}}\left(\sigma_y^{\mathrm{A}}\otimes\sigma_y^{\mathrm{B}}\right)\rho_{\mathrm{AB}}^{*}\left(\sigma_y^{\mathrm{A}}\otimes\sigma_y^{\mathrm{B}}\right)$, where ρ_{AB}^{*} is the complex conjugate of ρ_{AB}, $\sigma_y^{\mathrm{A(B)}}$ the standard Pauli matrix acting on qubit A(B) (Wootters 1998), and noting $C_{\mathrm{AB}}=C(\rho_{\mathrm{AB}})$ to simplify notation for later use; the more conceptual measure of entanglement, the entanglement of formation, can be written in terms of the concurrence as

$$E_f(\rho_{\mathrm{AB}})=h\left[\left(1+\sqrt{1-C_{\mathrm{AB}}^2}\right)/2\right], \tag{5}$$

where $h(x)=-x\log_2 x-(1-x)\log_2(1-x)$.

For systems beyond the 2×2- and 2×3-dimensional cases, good entanglement measures are known to exist so far only in special circumstances, for example, when extra symmetries are present. For this reason, studies of ESD are not easily extendible and focus must shift to BNSD (Jaeger and Ann 2008). Furthermore, entanglement must be understood as differing from non-locality in principle. For example, already in the two-qubit system, there exist situations in which entanglement and non-locality appear to differ, the Werner states can exhibit entanglement without violating a Bell inequality (Werner and Wolf 2001; Werner 1989). The next largest bipartite system, by dimensionality, that can be considered is the symmetric 3×3-dimensional case.

Although there is no generalized entanglement measure known to exist so far for arbitrary mixed-state two-qutrit entanglement, the separability condition for a two-qutrit Werner-like state, ρ_ϵ, composed of the maximally mixed component $\mathbb{I}_9/9$, and a maximally entangled component $|\Psi\rangle=(|11\rangle+|22\rangle+|33\rangle)/\sqrt{3}$,

$$\rho_\varepsilon=\frac{(1-\varepsilon)}{9}\mathbb{I}_9+\varepsilon|\Psi\rangle\langle\Psi|, \tag{6}$$

with $0\le\varepsilon\le 1$ has been found (Caves and Milburn 2000). The above state is separable, that is, not entangled, if and only if $\varepsilon\le 1/4$.

Addressing the relationship between decoherence and disentanglement, that is, the nature of the loss of entanglement in relation to the loss of state coherence, was an important step toward the discovery of ESD and BNSD. ESD is the extreme case in which coherence may persist, or be lost only asymptotically, whereas the entanglement is entirely eliminated in finite time. In particular, the discovery that they may decay at different rates was an indication that ESD is possible. A discrete-variable model of spatially separated atoms in a cavity subjected to vacuum noise leading to spontaneous emission was shortly thereafter used in the search for additional examples of ESD (Yu and Eberly 2004). In the two-qubit basis

$$\begin{aligned}|1\rangle_{\mathrm{AB}}&=|++\rangle_{\mathrm{AB}}\,,|2\rangle_{\mathrm{AB}}=|+-\rangle_{\mathrm{AB}},|3\rangle_{\mathrm{AB}}\\&=|-+\rangle_{\mathrm{AB}}\,,|4\rangle_{\mathrm{AB}}=|--\rangle_{\mathrm{AB}}\end{aligned} \tag{7}$$

an important class of initial states of the form

$$\rho(t) = \frac{1}{3}\begin{pmatrix} a(t) & 0 & 0 & 0 \\ 0 & b(t) & z(t) & 0 \\ 0 & z(t)^* & c(t) & 0 \\ 0 & 0 & 0 & d(t) \end{pmatrix} \tag{8}$$

is that for which with $a \geq 0$, $d = 1 - a$, and $b = c = z = 1$. Yu and Eberly considered the evolution of states in the operator-sum representation under noise described by

$$\rho(t) = \sum_{\mu=1}^{4} K_\mu(t)\rho(0)K_\mu^\dagger(t) \ , \tag{9}$$

where the operators representing amplitude damping noise, which satisfy the CPTP relations, can be written

$$K_1 = \begin{pmatrix} \gamma_A & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} \gamma_B & 0 \\ 0 & 1 \end{pmatrix} , \ K_2 = \begin{pmatrix} \gamma_A & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 0 \\ \omega_B & 0 \end{pmatrix} , \tag{10}$$

$$K_3 = \begin{pmatrix} 0 & 0 \\ \omega_A & 0 \end{pmatrix} \otimes \begin{pmatrix} \gamma_B & 0 \\ 0 & 1 \end{pmatrix} , \ K_4 = \begin{pmatrix} 0 & 0 \\ \omega_A & 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & 0 \\ \omega_B & 1 \end{pmatrix} , \tag{11}$$

where $\gamma_{A(B)} = \gamma_{A(B)}(t) = e^{-\Gamma_{A(B)}t}$ characterizes the decay for subsystem A(B), described by the rate parameter $\Gamma_{A(B)}$ and $\omega_{A(B)} = \sqrt{1 - \gamma_{A(B)}^2}$.

In the Markov approximation with the two subsystems decohering at the same rate, so that $\Gamma_A = \Gamma_B = \Gamma$ with analogous relations, $\gamma_A(t) = \gamma_B(t) = \gamma(t)$ and $\omega_A(t) = \omega_B(t) = \omega(t)$. The concurrence is given by $C(\rho(t)) = \frac{2}{3}\max\left\{0, \gamma(t)^2 f(t)\right\}$, with $f(t) = 1 - \sqrt{a(1 - a + 2\omega^2 + \omega^4 a)}$. The satisfaction of the inequality, $1 - a(1 - a + 2\omega^2 + \omega^4 a) \leq 0$, is a sufficient condition for concurrence to be zero, which is readily satisfied. Thus, for example, take the case of an initial state

$$\rho(t) = \frac{1}{3}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \tag{12}$$

that is, where $a = 1$. For this example, one finds that ESD occurs in the timescale $t_{dis} = \frac{1}{\Gamma}\ln\left[\frac{2+\sqrt{2}}{2}\right]$, which is finite for nonzero finite values of Γ (Yu and Eberly 2004).

Besides the effect of quantum vacuum noise leading to spontaneous emission as above, one can also examine the effects of "classical" noise, that is, phase damping in a large class of two-qubit mixed states that often arise in physical contexts and includes the pure EPR-Bell states and the Werner mixed states. Two types of noise effects can be considered, both global and multi-local. One can also consider both weak dephasing noise and weak amplitude damping noise, each independently as well as when acting jointly (Yu and Eberly 2006, 2007). For Werner states given by

$$\rho_W = \frac{1 - F}{3}\mathbb{I}_4 + \frac{4F - 1}{3}|\Psi^-\rangle\langle\Psi^-| \ , \tag{13}$$

with $1/4 \leq F \leq 1$, where $|\Psi^-\rangle$ is the Bell singlet state, it can be shown that when subject to amplitude damping noise, there is entanglement sudden death in a state of this form only when the state is equal to or less than a critical fidelity of $F_{crit} \approx 0.714$. This state is more robust against amplitude damping noise than to dephasing noise. The existence of ESD in larger systems has also been shown in other cases. For example, a compound system composed of a two-level and a three-level system, as well as for composite systems having any finite dimension (Ann and Jaeger 2008).

The demonstration of ESD in a bipartite system of a pair of identical subsystems of arbitrarily large finite dimensions has been shown under depolarizing noise (Ann and Jaeger 2007). This is possible when considering the only known case in which a mixed state entanglement measure exists for arbitrary $d > 2$, namely, the $d \times d$ isotropic states. The isotropic states are those that are invariant under $U \otimes U^*$ transformations and are of the form

$$\rho_{iso}(d) = \left(\frac{1 - F}{d^2 - 1}\right)I_{d^2} + \left(\frac{Fd^2 - 1}{d^2 - 1}\right)P(|\Psi(d)\rangle). \tag{14}$$

This state is separable when $F(\rho_{iso}(d), P(|\Psi\rangle)) \leq F_{critical}(d) \equiv d^{-1}$.

The isotropic states must satisfy $F(\rho_{iso}(d), P(|\Psi(t = 0)\rangle)) > F_{critical}(d)$, as well as $F(\rho_{iso}(d), P(|\Psi(t < \infty)\rangle)) \leq F_{critical}(d)$ for some finite time t for there to be ESD in the case of arbitrary finite dimensions $d > 2$. These conditions were both shown to be satisfied for an isotropic state subject to depolarizing noise; an initially entangled state becomes separable in finite time despite the persistence of state coherence. The existence of ESD for ranges of initial states in such a wide variety of contexts strongly suggests that ESD is a generic phenomenon in all quantum systems in specific classes of states.

Experimental evidence for ESD has been found in a variety of physical contexts including optical setups and atomic ensembles. Most significantly for our considerations, confirmation of the existence of entanglement sudden death for a pair of two-level systems due to multi-local dephasing and amplitude damping noise in a straightforward optical interferometric experiment has been carried out (Almeida et al. 2007); this study was the first experimental confirmation of ESD. In the realization, one system is denoted by the horizontal and vertical

polarizations of a photon, the other is the ground and excited state of an atom, and the environment acting upon these is the momentum of the photon. The general photon polarization Bell-state

$$|\Phi\rangle = |\alpha||HH\rangle + |\beta|\exp(i\delta)|VV\rangle, \tag{15}$$

where H is horizontal polarization and V is the vertical, is considered. Two initial states $|\psi_I\rangle$ defined by $|\beta|^2 = |\alpha|^2/3$ and $|\psi_{II}\rangle$ defined by $|\beta|^2 = 3|\alpha|^2$ have been considered. Entanglement can be quantified in this case by the concurrence, which there is

$$C(\rho) = \max\{0, 2(1-p)|\beta|(|\alpha| - p|\beta|)\}. \tag{16}$$

These initial states both have a concurrence of $C(\rho) \approx 0.8$ and similar purity, respectively, $\mathscr{P}_I \approx 0.91$ and $\mathscr{P}_{II} \approx 0.97$. $|\alpha|$, $|\beta|$, and δ are modified physically by a combination of quarter- and half-wave plates put in the pump beam path.

The evolution of the system for the amplitude damping channel is given by $|H\rangle \otimes |a\rangle \rightarrow |H\rangle \otimes |a\rangle$, $|V\rangle \otimes |a\rangle \rightarrow \sqrt{1-p}|V\rangle \otimes |a\rangle + \sqrt{p}|H\rangle \otimes |b\rangle$, where $|a\rangle(|b\rangle)$ denote orthogonal spatial modes. Under this map, the horizontal polarization state $|H\rangle$ is unaffected whereas the vertical state $|V\rangle$ has a probability of flipping to $|H\rangle$ with probability p, in which case the spatial mode occupied also changes, *or* remaining unchanged, with probability $1-p$. For the case of $|\beta| \leq |\alpha|$, there is no entanglement if $p = 1$. By contrast, for $|\beta| > |\alpha|$, finite-time disentanglement occurs for $p = |\alpha/\beta|$. Then $|\psi_I\rangle$ undergoes asymptotic disentanglement, with complete disentanglement occurring only when $p = 1$, the case where each individual subsystem state is also completely incoherent. For $|\psi_{II}\rangle$, the concurrence goes to zero for $p<1$, showing ESD. A comprehensive analysis of quantum optical experiments exploring further ESD for the amplitude damping channel has more recently also been carried out (Salles et al. 2008).

The polarization dephasing channel is described by $|H\rangle \otimes |a\rangle \rightarrow |H\rangle \otimes |a\rangle, |V\rangle \otimes |a\rangle \rightarrow \sqrt{1-p}|V\rangle \otimes |a\rangle + \sqrt{p}|V\rangle \otimes |b\rangle$. In that case, the polarization states are unchanged but coherent superpositions of polarization have reduced coherence. Here, both states $|\psi_I\rangle$ and $|\psi_{II}\rangle$ exhibit the same behavior; for, but only for, $p = 1$ they completely disentangle.

In the next section we consider what might be expected when pursued with qubits transmittable using time-bin "levels," and how the above results impact a specific implementation of them.

4 Decoherence free subspaces in a quantum key distribution

In practical quantum key distribution (QKD), traditional interferometric techniques have thus far been almost exclusively relied upon to improve cryptographic system performance rather than quantum methods; in particular, these have made no use of quantum entanglement for noise mitigation. The relative complexity of decoherence-mitigation techniques such as decoherence-free subspaces (DFSs) involving entangled quantum states has typically limited their use in QKD due to their then often being a need for addition qubits to implement them. However, this is changing. Here, we will both discuss a practical means of realizing DFS methods involving entangled states (Gisin et al. 2002; Walton et al. 2003) and consider the effect of dephasing noise on their entanglement. In particular, a recent quantum key distribution scheme using phase-time encoding and passive photo-detection is discussed that is designed to allow quantum signaling to be free from decoherence arising from the collective dephasing of pairs of two-level systems to discover any limitations due to other noise effects.

In order to understand the operation of this QKD scheme, let us first review the two-level systems ('qubits') formed from probability amplitudes of a single photon separated into two distinct time bins, a method and apparatus for creating which has been recently been provided (Jaeger 2003). Such a set of states is measurable via early and late time of photon arrival. The corresponding quantum amplitudes then form the computational basis. These qubits have been proposed for the realization of BB84 QKD, in particular (Gisin et al. 2002). This method eliminates the need to make active choices of bit encoding/decoding basis of signal states because it is fully compatible with passive detection methods. Consider a single time-bin qubit encountering a specific passive-detection apparatus realized by enlarging the range of possible space-time paths of the two qubit amplitudes (Gisin et al. 2002; Jaeger 2003; Walton et al. 2003).

In the scheme, under the preferred interferometric decoding arrangement, amplitudes emerge in three separate time bins for each photon in each of the two output ports of a Mach–Zehnder interferometer (MZI). The MZI in the receiver's laboratory introduces a fixed phase shift corresponding to that introduced by the time delay between amplitudes $|E\rangle$ and $|L\rangle$ for early and late time of arrival of the photon at any point on the segment of their trajectory up to the MZI. These respectively result in quantum amplitudes for early, intermediate and late photon arrivals at photon detectors, that is, $-1, 0, +1$ and $-1', 0', +1'$ in the two output ports. Using the appropriate choices of amplitude and relative phase of the initial key-bit encoding qubit amplitudes $|E\rangle$ and $|L\rangle$, the sender, Alice, can realize the two complementary bases needed for carrying out the BB84 protocol, the signal states of which are then decoded by the receiver.

In addition to the "computational basis" states $|E\rangle$ and $|L\rangle$, Alice can create the "diagonal" basis states, in which

the early and late amplitudes are placed in balanced superpositions: $|\nearrow\rangle = \frac{1}{\sqrt{2}}(|E\rangle + |L\rangle)$, $|\searrow\rangle = \frac{1}{\sqrt{2}}(|E\rangle - |L\rangle)$. The effect of the MZI of the receiving lab on the computational basis states is then to produce three possible arrival times for the signal photon out of *each* of the two available output ports of the MZI. The computational basis states are the transformed into a larger Hilbert space, where the three post-MZI time bins are labeled $-1, 0, +1$ as above:

$$|E\rangle \rightarrow i|-1'\rangle + ie^{i\phi}|0'\rangle - e^{i\phi}|0\rangle + |-1\rangle \tag{17}$$

$$|L\rangle \rightarrow i|0'\rangle + ie^{i\phi}|+1'\rangle - e^{i\phi}|+1\rangle + |0\rangle, \tag{18}$$

where the two output trajectory segments leading out of the two MZI ports are distinguished using primes. ϕ is then arranged to be zero. Each computational basis state then results in a coherent superposition of four possible space-time locations, because each beam splitter in the photon trajectory contributes two possibilities. Each initial amplitude can take long or short paths through the MZI and emerge though one of two ports, providing six quantum possibilities (as two of $8 = 2 \times 4$ possibilities become indistinguishable in the intermediate final time bins, due to the matching of the path-difference with the timing difference between early and late initial amplitudes, and labeled as 0 and $0'$). The effect of introducing the decoding MZI can be seen as an embedding of the four signal states $|E\rangle, |L\rangle, |\nearrow\rangle, |\searrow\rangle$ in the larger Hilbert space containing the six states $|-1\rangle, |0\rangle, |+1\rangle, |-1'\rangle, |0'\rangle, |+1'\rangle$.

In the cases for which Alice chooses signal states in the diagonal basis, the states output from the MZI are obtained by appropriately adding the right hand sides of Expressions 17 and 18. The central arrival time bins of the two ports can result from either early or late initial amplitudes entering one output port or the other depending on the relative sign of superposition states of these amplitudes, that is, the diagonal basis of the BB84 protocol; when this signal basis is chosen, the state amplitude for the central arrival time bin arising from $|\nearrow\rangle$ can only enter the lower port and that arising from the state $|\searrow\rangle$ can enter only in the upper port. When the computational basis of states $|E\rangle$ and $|L\rangle$ is chosen instead and these states take the short or long paths, respectively, through the MZI they produce signal states that arrive early or late, respectively, whichever output arm is involved.

Alternatively, by the encoding of signal qubits into logical basis states of an even larger subspace, namely, that in the Hilbert space of a photon pair, quantum keys can be transmitted in a manner that is decoherence-free relative to collective local dephasing (Palma et al. 1996; Walton et al. 2003). Making use of such a scheme, with the two photons being temporally well separated, that is, separated by a time longer than that used between the time-bin amplitudes $|E\rangle_i$ and $|L\rangle_i$ $(i = 1, 2)$ of the individual photons, two-sign capacity can be achieved.

A collective local dephasing model is one that assumes that computational basis states acquire the same uncontrollable phase shift, χ, relative to each other, *i.e.* when the environment induces (on average) the transformation $|E\rangle \rightarrow |E\rangle, |L\rangle \rightarrow e^{i\chi}|L\rangle$ for every subsystem. To mitigate this simple effect, one can use a two-qubit signal encoding to logical basis states $|0\rangle_L \equiv |EL\rangle, |1\rangle_L \equiv |LE\rangle$, which are not affected by dephasing: the physical qubit dephasing corresponds to the transformation $|EL\rangle \rightarrow e^{i\chi}|EL\rangle$, $|LE\rangle \rightarrow e^{i\chi}|LE\rangle$. Thus, the dephasing process above will have an identical net effect on the two logical states. In effect, one has both $|0\rangle_L \rightarrow |0\rangle_L$ and $|1\rangle_L \rightarrow |1\rangle_L$, since only a relative phase difference is observationally relevant, by contrast with the incoherent behavior of non-encoded physical basis states $|0\rangle$ and $|1\rangle$; coherence protection under such noise similarly follows for the relevant superpositions of these two states $|\nearrow\rangle_L = \frac{1}{\sqrt{2}}(|0\rangle_L + |1\rangle_L), |\searrow\rangle_L = \frac{1}{\sqrt{2}}(|0\rangle_L - |1\rangle_L)$ by linearity. For future reference, note that these logical states are simply two Bell states - that is, $|\nearrow\rangle_L = |\Psi^+\rangle$ and $|\searrow\rangle_L = |\Psi^-\rangle$. The sender, Alice, can then realize the BB84 protocol in this decoherence-free subspace by using polarization entangled photon pairs produced by spontaneous parametric down-conversion (SPDC) converted into phase-time qubit pairs at random in the appropriate four states comprised by states of this logical basis together with their positive and negative balanced superpositions in the complementary, "diagonal" logical basis, each with equal probability (see Walton et al. 2003 for a concrete realization). The same MZI is used in the laboratory of the receiver as was used in the single-photon arrangement, again allowing for passive state decoding/detection. Now, the effect of the MZI is to allow three possible arrival times (early, intermediate, and late) for each photon in *each* of the two available output ports of the MZI, much as before; the effect of the MZI on the physical basis states of both qubits is the same transformation described above. Each photon will be involved in one of each of the two sets of six events, with a corresponding early, intermediate or late arrival time.

After detection, using a classical channel, both Alice and Bob disclose the "choices" of encoding and decoding bases in their respective local laboratories. When the two basis choices are appropriate, Bob receives a key bit from Alice; otherwise, his result provides no useful key material. When Bob detects both photons in the intermediate time bins he will be making a useful measurement in the diagonal logical signal basis, defined by an intermediate-length arrival time difference. For example, the components of the

two-qubit basis vectors (serving as logical qubit computational basis states) of corresponding to intermediate arrival times only are thus transformed as

$$|0\rangle_L \rightarrow |00\rangle + |0'0'\rangle + i|00'\rangle - i|0'0\rangle \tag{19}$$

$$|1\rangle_L \rightarrow |00\rangle + |0'0'\rangle - i|00'\rangle + i|0'0\rangle, \tag{20}$$

up to a physically irrelevant overall global phase factor, that describe appropriately post-selected pure ensembles. Thus, when these two photons arrive in the same detector, a detection of one bit (say 0) value is obtained; when they arrive in two different detectors a detection of the other bit value (say 1) is obtained, regardless of the detector(s) in which the first photon and second photon arrive. Alternatively, when the two photons arrive one in an early time bin and one in a late time bin, so that the time separation between their arrivals is either the shortest possible or the longest possible of the three possible relative arrival intervals, a useful measurement in the computational signal basis is obtained. In the former case, a detection of one key binary value is shared, whereas in the latter the other other key value 1 is shared.

The extreme entanglement properties of Bell states follow from nonseparability arising from their symmetry or antisymmetry under the binary exchange of subsystems, each half the (two qubit) size of the composite system. By carrying out for one additional step an encoding procedure similar to that described above, concatenating the code with itself—that is, going from using two-photon states to using four-photon states—elements of a recently delimited basis of larger entangled states, which lie in a different, yet more robust decoherence-free subspace, are obtained. The symmetry of the Bell basis states has been used to define a new, broader class of bases, "Bell gems," that generalize the Bell basis (Jaeger 2004). Bell gem $\mathcal{G}_4$, at the bottom of this hierarchy, is the Bell basis itself. Those basis states, rather than merely serving to encode logical qubits from physical qubits, can be viewed as physical 16-its constructed from 4-its: since the Bell gem basis elements at each level form a basis, each of these 16 states is orthogonal to the 15 others.

For QKD applications, however, one will not need all the subspaces spanned by pairs elements that are available in the Bell gem $\mathcal{G}_{16}$—a pair of complementary subspace bases, one of which is taken from the eight pairs of states discussed in Jaeger (2004) suffices. In particular, one needs only

$$|0\rangle_{\bar{L}} = (1/\sqrt{2})(|\nearrow\rangle_L|\searrow\rangle_L + |\searrow\rangle_L|\nearrow\rangle_L) \tag{21}$$

$$|1\rangle_{\bar{L}} = (1/\sqrt{2})(|\nearrow\rangle_L|\searrow\rangle_L - |\searrow\rangle_L|\nearrow\rangle_L), \tag{22}$$

which are elements of the Bell gem $\mathcal{G}_{16}$, because $|\nearrow\rangle_L = |\Psi^+\rangle$ and $|\searrow\rangle_L = |\Psi^-\rangle$. Typically DFS are tailored to specific noise models. Note, in particular, that the two-photon DFS above spanned by $\{|0\rangle_L, |1\rangle_L\}$ does not protect its logical states from "higher-order" dephasing. However, it turns out that elements of above Bell gem can be used in situations described by a more complex noise model where even the two-photon DFS above is insufficient to protect against such decoherence effects (Jaeger and Sergienko 2006). In a more complicated environment than one merely inducing dephasing as described immediately above, such four-photon states can thus provide an appropriate decoherence-free subspace. Note, that the larger Hilbert space spanned by $\mathcal{G}_{16}$ readily provides 8 orthogonal subspaces and that, in an environment described by a noise model including additional dephasing of the form $|0\rangle_L \rightarrow |0\rangle_L$, $|1\rangle_L \rightarrow e^{i\bar{\chi}}|1\rangle_L$, with $\bar{\chi}$ being another average random phase, the two-photon logical states will themselves be susceptible to decoherence analogous to that in the initial single physical-qubit case but occurring at the two-qubit level. By carrying out *two* logical qubit encoding steps to arrive at elements of $\mathcal{G}_{16}$, such higher-order decoherence can be seen to be avoided.

5 ESD and quantum key distribution

The first DFS described above was designed to operate under the simple local collective random phase noise model introduced in this section. The above QKD scheme may also face noise as described by the open-system dephasing noise model described in Section 2 that also pertains to the quantum optical experiments described in Section 3. Therefore, let us now consider the question of whether such noise presents difficulties for the proposed QKD scheme, based on what is known about its effects in the quantum interferometer setting. We find that despite having not been designed for such noise, unlike the case for more fragile states, ESD poses no threat to them.

The behavior of the class of states of the generalized (*i.e.* possibly unequally weighted) $|\Phi\rangle$ form under such noise was discussed in Section 3. Such states suffer from both decoherence and disentanglement. Under both multilocal dephasing and amplitude damping noise, there can be decoherence and disentanglement. For example, we saw that the relatively fragile states, ESD can occur under amplitude damping noise if $|\beta| > |\alpha|$ and the noise parameter $p = |\frac{\alpha}{\beta}|$. This takes place, for example, when the squared amplitude of the damped basis state $|11\rangle$ is three times that of the orthogonal state $|00\rangle$ of the superposition while identifying 0 with H and 1 with V. Even for such relatively noise-fragile states, with the

inverse of this ratio of squared amplitudes both decoherence and disentanglement occur only in the infinite-time limit, that is *without* ESD, while the infinite-time limit is not relevant to QKD because it is only one step of an overall cryptographic process which must be carried out itself in finite time. For QKD based on the latter such state, the reliability of the scheme might be reduced but it would not fail.

Nonetheless, for greater reliably, one can use a logical-qubit state encoding based on pairs of Bell singlet states as in the DFS schemes described above, that is, of pairs each of the form

$$|\Psi\rangle = |\alpha||01\rangle + |\beta|\exp(i\delta)|10\rangle \ , \tag{23}$$

with $|\alpha| = |\beta|$. These can be used with a phases $\exp(i\delta)$ of $+1$ or -1 alone or pairwise, in order to produce the Bell gem states of Eqs. 21 and 22. In either case, the DFS property protects these against entanglement sudden death under collective phase noise, so long as the photon pairs are truly prepared in pure states. This is because all effects on joint states occur identically on the two elements of the superposition.

In particular, for this state and a phase factor of -1, the time-bin dephasing noise can still be simply described by the effect

$$|\Psi^{\pm}\rangle \rightarrow e^{i\langle\phi_0\rangle}|0\rangle e^{i\langle\phi_1\rangle}|1\rangle \pm e^{i\langle\phi_1\rangle}|1\rangle e^{i\langle\phi_0\rangle}|0\rangle \tag{24}$$

$$= e^{i(\langle\phi_0\rangle+\langle\phi_1\rangle)}(|0\rangle|1\rangle \pm |1\rangle|0\rangle) \tag{25}$$

$$= e^{i(\langle\phi_0\rangle+\langle\phi_1\rangle)}|\Psi^{\pm}\rangle, \tag{26}$$

the resulting global phase factor being unobservable. A similar global phase will clearly result in the case of such noise for whichever Bell state $|\Psi^{\pm}\rangle$, that is, $|\Psi^{+}\rangle$ or $|\Psi^{-}\rangle$ and therefore on the even linear combinations of the two. This sort of noise will accordingly have no relevant effect on the logical states of this decoherence-free subspace, because $|0\rangle_L \rightarrow e^{i(\langle\phi_0\rangle+\langle\phi_1\rangle)}|0\rangle_L$ and $|1\rangle_L \rightarrow e^{i(\langle\phi_0\rangle+\langle\phi_1\rangle)}|1\rangle_L$; the logical states remain orthogonal despite the noise, as can be seen by taking their inner product. Analogous phase noise acting on the Bell gem states (cf. Eqs. 21 and 22) at between two-photon states have the analogous effect, one need only consider the logical basis states $|0\rangle_L$ and $|1\rangle_L$ in place of $|0\rangle$ and $|1\rangle$ and "higher order" phase shifts $e^{i\langle\phi_{Li}\rangle}$ in place of $e^{i\langle\phi_0\rangle}$ $(i = 0, 1)$ in the expressions immediately above.

Such choices of readily producible DFS states are an elegant solution to the problems of decoherence and disentanglement in entanglement distribution networks in such local noise conditions.

6 Conclusion

Both already realized and potential uses of entangled photon states in quantum key distribution and quantum networks in the presence of environmental noise were investigated here. In particular, the use of quantum decoherence mitigation techniques involving entangled quantum states were discussed, including a scheme that uses decoherence free subspaces in a practical implementation viable with linear optical equipment. This demonstrates the value of theoretical quantum computing tools in emerging real-world quantum technologies such as QKD networks, where uniquely quantum mechanical properties such as higher-order quantum entanglement may soon be practically distributed in noisy environments. Special attention was paid to situations in which entanglement sudden death could appear to be a serious threat. Our investigation suggests that although this threat is a real one, specific decoherence-mitigating methods such as that considered in detail here are available that allow one to protect entanglement-based QKD from the threat of entanglement sudden death by exploiting decoherence-free subspaces.

Acknowledgments This research was supported by the DARPA QUINESS program through U.S. Army Research Office Award No. W31P4Q-12-1-0015.

References

Almeida MP, de Melo F, Hor-Myell M, Salles A, Walborn SP, Souto Ribero PH, Davidovich L (2007) Environment-induced sudden death of entanglement. Science 316:579

Ann K, Jaeger G (2007) Local-dephasing-induced entanglement sudden death in two-component finite-dimensional systems. Phys Rev A 76:044101

Ann K, Jaeger G (2008) Entanglement sudden death in qubit-qutrit systems. Phys Lett A 372:579

Ann K, Jaeger G (2009) Finite-time destruction of entanglement and non-locality by environmental influences. Found Phys 39:790

Bennett CH, Popescu S, Rohrlich D, Smolin JA, Thapliyal AV (2001) Exact and Asymptotic Measures of multipartite pure state entanglement. Phys Rev A 63:012307

Caves CM, Milburn GJ (2000) Qutrit entanglement. Opt Commun 179:439

Ekert AK (1992) Quantum cryptography based on Bell's theorem. Phys Rev Lett 67:661

Gisin N, Ribordy G, Tittel W, Zbinden H (2002) Quantum cryptography. Rev Mod Phys 74:145

Jaeger G (2003) Method and apparatus for creating at least one qubit in a quantum computing device. US Patent No. 6,633,053

Jaeger G (2004) Bell gems: the Bell basis generalized. Phys Lett A 329:425

Jaeger G, Sergienko AV (2006) Entangled states in quantum key distribution. AIP Conf Proc 810:161

Jaeger G (2007) Quantum information: an overview (chapter 10). Springer, Heidelberg

Jaeger G, Ann K (2008) Generic tripartite Bell nonlocality sudden death under local phase noise. Phys Lett A 372:6853

Kraus K (1983) States, effects, and operations. Springer, Berlin
Palma GM, Suominen K-A, Ekert AK (1996) Quantum computers and dissipation. Proc R Soc Lond A 452:567
Salles A, de Melo F, Almeida MP, Hor-Meyll M, Walborn SP, Souto Ribeiro PH, Davidovich L (2008) Experimental investigation of the dynamics of entanglement: Sudden death, complementarity, and continuous monitoring of the environment. Phys Rev A 78:022322
Walton ZD, Abouraddy AF, Sergienko AV, Saleh BEA, Teich MC (2003) Decoherence-free subspaces in quantum key distribution. Phys Rev Lett 91:087901
Werner RF (1989) Quantum states with Einstein–Podolsky–Rosen correlations admitting a hidden-variable model. Phys Rev A 40:4277
Werner RF, Wolf MM (2001) Bell inequalities and entanglement. Quantum Inf Comput 1(3):1
Wootters WK (1998) Entanglement of formation of an arbitrary state of two qubits. Phys Rev Lett 80:2245–2248
Yu T, Eberly JH (2004) Finite-Time disentanglement via spontaneous emission. Phys Rev Lett 93:140404
Yu T, Eberly JH (2006) Quantum open system theory: bipartite aspects. Phys Rev Lett 97:140403
Yu T, Eberly JH (2007) Evolution from entanglement to decoherence. Quantum Inf Comp 7:459