Decoherence-Free Subspaces in Quantum Key Distribution

Zachary D. Walton,* Ayman F. Abouraddy, Alexander V. Sergienko, Bahaa E. A. Saleh, and Malvin C. Teich
Quantum Imaging Laboratory†, Department of Electrical & Computer Engineering, Boston University, 8 Saint Mary's Street, Boston, Massachusetts 02215-2421, USA
(Received 26 March 2003; published 20 August 2003)

We demonstrate that two recent innovations in the field of practical quantum key distribution (one-way autocompensation and passive detection) are closely related to the methods developed to protect quantum computations from decoherence. We present a new scheme that combines these advantages, and propose a practical implementation of this scheme that is feasible using existing technology.

DOI: 10.1103/PhysRevLett.91.087901 PACS numbers: 03.67.Hk, 03.65.Yz, 03.67.Dd, 42.65.Ky

Decoherence has been a principal impediment in quantum information processing applications. In quantum computing, decoherence-induced deviations from the desired computational trajectory at the single-qubit level will quickly accumulate if left uncorrected. Thus, techniques such as decoherence-free subspaces (DFSs; for a review, see Ref. [1]) have been developed as tools for protecting quantum computations. In quantum key distribution (QKD; for a review, see Ref. [2]), single-qubit errors are also deleterious; however, sufficiently infrequent single-qubit errors are tolerable, since the resulting errors can be corrected by classical error correction protocols. This has led many QKD experimentalists to forego the complexity of decoherence-mitigation techniques such as DFSs in favor of more conventional methods to improve the precision of single-qubit operations (periodic alignment of polarization axes, temperature stabilization of interferometers, etc.). In this Letter, we consider the applicability of DFSs to QKD.

This Letter is organized as follows. We begin by demonstrating that a recently proposed QKD implementation (one-way autocompensating quantum cryptography [3]) is, in fact, equivalent to a well-known DFS. We then pursue a suggestion in Ref. [2] to consider a single-qubit, phase-time coding QKD scheme in which Bob is not required to actively switch between conjugate measurement bases. We show that both one-way autocompensation (OWA) and passive detection are achieved by embedding the logical Hilbert space in a larger physical Hilbert space. Next, we describe a new scheme that combines OWA and passive detection. Finally, we propose an experimental implementation of this new scheme that is feasible using existing technology.

Relating OWA and DFSs.—In Ref. [3], Klyshko's "advanced wave interpretation" [4] was used to describe OWA as a variation on round-trip autocompensation [5,6]. These schemes are called autocompensating because they allow high-visibility quantum interference without calibration or active stabilization of the receiver's (Bob's) apparatus. In the context of quantum computation theory [7], a more natural explanation of OWA is provided by DFSs. Palma *et al.* [8] have shown that a single logical qubit encoded in two physical qubits according to

$$|\bar{0}\rangle \rightarrow |01\rangle, \qquad |\bar{1}\rangle \rightarrow |10\rangle \tag{1}$$

will be protected against collective dephasing. Collective dephasing describes a noise model in which each physical qubit is subject to the same transformation

$$|0\rangle \rightarrow |0\rangle, \qquad |1\rangle \rightarrow e^{i\phi}|1\rangle, \tag{2}$$

where ϕ is an uncontrolled degree of freedom. Under this transformation, the states $|01\rangle$ and $|10\rangle$ acquire the same phase factor ($e^{i\phi}$). Thus, a qubit encoded according to Eq. (1) will be immune to collective dephasing.

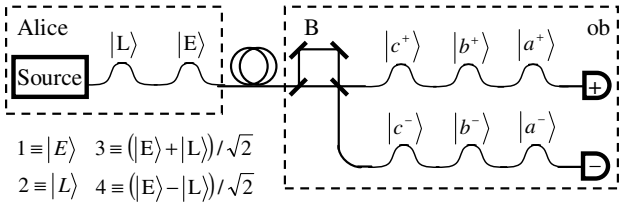
To link this DFS to OWA, we consider time-bin photonic qubits [9], in which the physical basis states $|0\rangle$ and $|1\rangle$ correspond to early ($|\mathrm{E}\rangle$) and late ($|\mathrm{L}\rangle$) single-photon wave packets, respectively. Two-qubit states (e.g., $|\mathrm{EL}\rangle$) may be created in which the two time-bin qubits are distinguished by some convenient degree of freedom (e.g., polarization, or a time delay much longer than that used to define the individual time-bin qubits themselves).

In OWA quantum cryptography, Alice superposes the two-qubit time-bin states $|\mathrm{EL}\rangle$ and $|\mathrm{LE}\rangle$ with one of four relative phases ($0, \pi/2, \pi, 3\pi/2$) and sends the two-qubit state to Bob. Note that the superposition of $|\mathrm{EL}\rangle$ and $|\mathrm{LE}\rangle$ entails time-bin entanglement, an idea introduced in Ref. [9]. Bob applies one of two relative phase shifts ($0, \pi/2$) to the superposed terms and makes his measurement. In this way, they may effect the familiar four-state QKD protocol (BB84) [10].

The equivalence of OWA and the DFS in Eq. (1) may be seen by carefully following Bob's detection process. After applying his phase shift, Bob analyzes the state using a Mach-Zehnder interferometer (MZI) with optical delay equal to the time delay separating $|\mathrm{E}\rangle$ and $|\mathrm{L}\rangle$. Using the notation of Fig. 1, the action of the interferometer on a single time-bin qubit is

$$\begin{aligned} |\mathrm{E}\rangle &\rightarrow i|a^-\rangle + ie^{i\phi}|b^-\rangle - e^{i\phi}|b^+\rangle + |a^+\rangle, \\ |\mathrm{L}\rangle &\rightarrow i|b^-\rangle + ie^{i\phi}|c^-\rangle - e^{i\phi}|c^+\rangle + |b^+\rangle, \end{aligned} \tag{3}$$

 0031-9007/03/91(8)/087901(4)$20.00



		Time of Detection		
		$\|a^{\pm}\rangle$	$\|b^{\pm}\rangle$	$\|c^{\pm}\rangle$
Detector	+	{2,3,4}	{1,2,4}	{1,3,4}
	−	{2,3,4}	{1,2,3}	{1,3,4}

FIG. 1. A single-photon implementation of BB84 suggested in Ref. [2]. The kets $|\mathrm{E}\rangle$ and $|\mathrm{L}\rangle$ correspond, respectively, to an advanced (early) and a delayed (late) single-photon wave packet. Alice sends one of the four states listed below the diagram of the apparatus. The chart indicates which of Alice's states are consistent with a given measurement event at Bob's side. As described in the text, Bob's apparatus does not require active change of measurement basis.

where ϕ is the relative phase along the two paths. Here, and for the remainder of this Letter, normalizing constants and overall phase factors have been suppressed. By postselecting those cases in which both photons are detected at time slots corresponding to $|b^{+}\rangle$ or $|b^{-}\rangle$, Bob achieves the following effective transformation:

$$\begin{aligned} |\mathrm{EL}\rangle &\rightarrow |b^{+}b^{+}\rangle + |b^{-}b^{-}\rangle + i(|b^{+}b^{-}\rangle - |b^{-}b^{+}\rangle), \\ |\mathrm{LE}\rangle &\rightarrow |b^{+}b^{+}\rangle + |b^{-}b^{-}\rangle - i(|b^{+}b^{-}\rangle - |b^{-}b^{+}\rangle), \end{aligned} \tag{4}$$

where a common factor of $e^{i\phi}$ has no consequence.

The crucial assumption in going from Eq. (3) to Eq. (4) is that the MZI transforms each of the two time-bin qubits identically. For time-bin qubits distinguished by a time delay that is short compared to the characteristic time of interferometric drift (though long compared to the time separating $|\mathrm{E}\rangle$ and $|\mathrm{L}\rangle$), this assumption is certainly valid. The probability of Bob detecting two photons on the same output arm ($|b^{+}b^{+}\rangle$ or $|b^{-}b^{-}\rangle$) depends on the relative phase between the $|\mathrm{EL}\rangle$ and $|\mathrm{LE}\rangle$, and similarly for the probability of detecting two photons on different arms ($|b^{+}b^{-}\rangle$ or $|b^{-}b^{+}\rangle$). The critical point is that each of these probabilities is independent of the interferometer's phase delay, ϕ. Thus, just as the DFS described in Eq. (1) protects a logical qubit encoded in two physical qubits from collective dephasing, OWA enables Bob to measure high-visibility two-photon interference with a MZI that does not require initial calibration or active phase stabilization.

Passive detection via enlarging the Hilbert space.—The two-photon quantum key distribution scheme described in Ref. [9] has the remarkable property that both Alice and Bob use passive detection (i.e., they are not required to switch between conjugate measurement bases). In Ref. [2], Gisin *et al.* suggest applying Klyshko's advanced wave interpretation to generate an associated one-photon scheme. We present a specific implementation of this one-photon scheme here to show that it achieves passive detection by enlarging the Hilbert space (see Fig. 1). Let the advanced and delayed single-photon wave packets be associated with the poles of the Poincaré sphere. The four states required for BB84 are typically taken from the equator, since a single MZI can be used to generate any of the equatorial states. Instead, we imagine using two antipodal points on the equator and the poles themselves. Bob analyzes the signal from Alice with a MZI, recording which detector fired (one of two possibilities) at which time (one of three possibilities). When Bob's detection is in the first or third time positions, he can reliably distinguish between the pole states based on the time of detection. When his detection is in the second time position, he can reliably distinguish between the equatorial states based on which detector fired. Thus, Bob is no longer obliged to make an active change to his apparatus to effect the requisite change of basis [11].

To see how this passive detection is derived from enlargement of the Hilbert space, consider the quantum state of Alice's signal after Bob's MZI. Alice's four states of one qubit are mapped onto four mutually nonorthogonal states of a six-state quantum system (see Fig. 1). Thus, by mapping a two-state quantum system into a six-state quantum system, Bob is able to perform his part of the BB84 protocol with a fixed-basis measurement in the six-state Hilbert space [13].

Combining OWA and passive detection.—OWA and passive detection have been previously presented in separate proposals (Refs. [3,9], respectively). Here we present a new scheme that combines these two beneficial features in a single implementation (see Fig. 2). The new scheme follows from that presented in Ref. [3], just as the preceding single-photon scheme follows from the traditional phase-coding implementation. Let the states $|1\rangle$ and $|2\rangle$ in Fig. 2 be associated with the poles of the Poincaré sphere. Instead of using equatorial states and forcing Bob to postselect those cases for which the advanced (delayed) amplitudes take the long (short) path, we use two equatorial points ($|3\rangle$ and $|4\rangle$) and the poles themselves to make up Alice's four signal states. Signal states that are consistent with a given joint detection are presented in the chart. As seen in Fig. 1, each photon can lead to six different detection events. Thus, since the new protocol involves two photons, there are 36 possible detection events (see Fig. 2).

The protocol operates as follows. As in BB84, Alice and Bob publicly agree on an association of each of the four signal states (see Fig. 2) with logical values "0" or "1" (i.e., $1 \rightarrow$ "0", $2 \rightarrow$ "1", $3 \rightarrow$ "0", $4 \rightarrow$ "1"). For each run of the experiment, Alice randomly chooses one of the four signal states and sends it to Bob. When Bob detects both photons in their respective middle time slots, he has

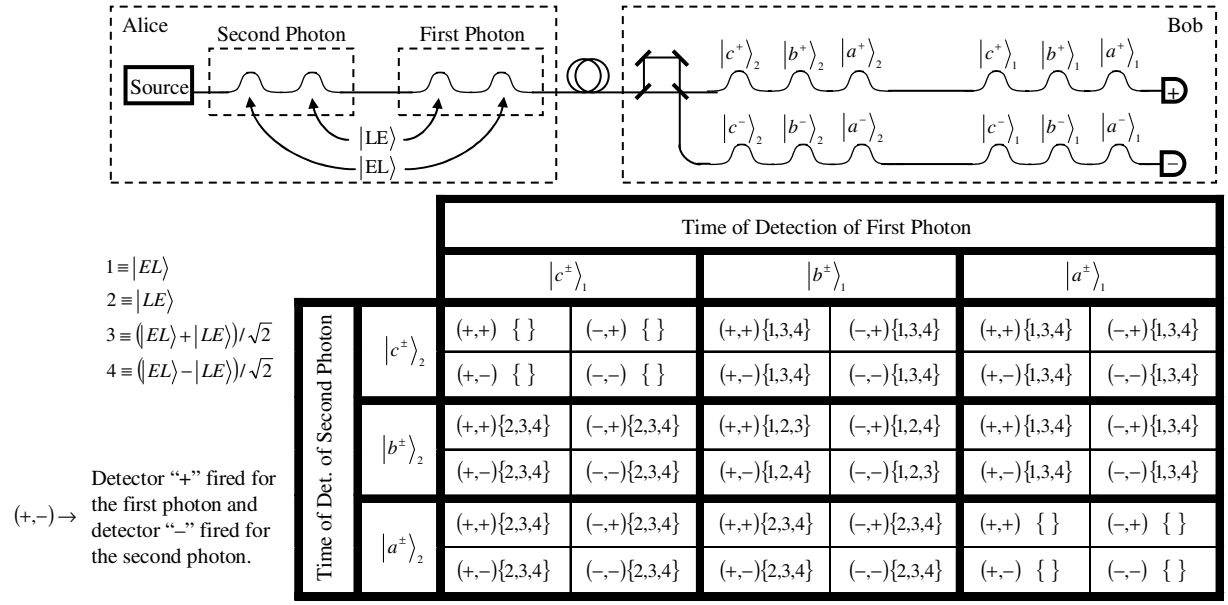


FIG. 2. A new scheme for quantum key distribution that combines OWA with passive detection. Two time-bin qubits are sent from Alice to Bob in one of the four quantum states on the left of the figure. The chart on the right uses two levels of structure to describe the detection pattern at Bob's side. The coarse structure is defined by the bold lines. Each of the nine bold-lined rectangles corresponds to a specification of the joint time of detection of the two photons. The fine structure is defined by the thin lines. Each of the four thin-lined rectangles within the bold-lined rectangles corresponds to a specification of which detector fired for each of the two photons (this coding is illustrated by an example at the bottom left of the figure). The numbers in the curly brackets in each thin-lined rectangle indicates which (if any) of the four quantum states on the left are consistent with the corresponding detection pattern.

effectively measured in the $\{3, 4\}$ basis (the "phase" basis). When Bob detects both photons in their early time slots, or both photons in their late time slots, he has effectively measured in the $\{1, 2\}$ basis (the "time" basis) [15]. After the quantum transmission, Alice and Bob publicly announce their bases. On the occasions when their bases match, Bob is able to infer the state that Alice sent, based on his detection pattern using the chart in Fig. 2. As in single-qubit BB84, the occasions in which their bases do not match are discarded. The scheme achieves passive detection (Bob is not required to make any active changes to his apparatus) and autocompensation (the phase delay in Bob's interferometer does not affect any measured probabilities). The intrinsic efficiency of the scheme is 1/4, compared to 1/2 for single-qubit BB84.

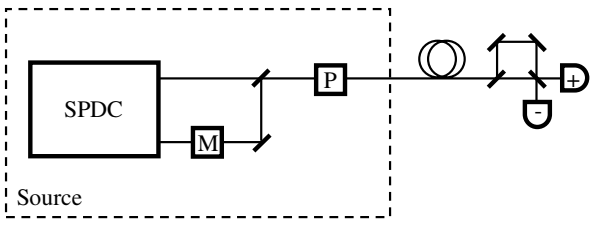


FIG. 3. A proposed implementation for the source employed in Fig. 2. "SPDC" is a nonlinear crystal pumped by a brief pulse to produce a noncollinear, polarization-entangled two-photon state via spontaneous parametric down-conversion. The action of elements "M" and "P" is described in the text.

A feasible implementation.—A proposed implementation for the source employed in Fig. 2 is presented in Fig. 3. First, a pair of noncollinear, polarization-entangled photons is produced via type-II spontaneous parametric down-conversion from a nonlinear crystal pumped by a brief pulse [16]. Second, the modulating element "M" performs one of four functions (filter one of the two polarization modes, or introduce one of two relative phases between the two polarization modes), based on Alice's choice of signal states. Third, the two beams are combined with a relative temporal delay that matches the temporal delay Bob will subsequently introduce with his MZI. This stage converts the photon pair from a pair of spatially defined polarization-entangled qubits to a pair of polarization-defined time-bin entangled qubits. Finally, the element labeled "P" (for polarization) delays and rotates one of the polarization modes by a duration much greater than the delay of the third step, such that the delayed portion of the state in the same polarization as the nondelayed portion. Thus, the two photons sent from Alice to Bob have the wave packet structure illustrated at the top of Fig. 2.

There are two noteworthy aspects of the configuration in Fig. 3. First, the technique introduced in Ref. [9] for

creating time-bin entangled photon pairs leads only to superpositions of the correlated possibilities (i.e., $|EE\rangle$ and $|LL\rangle$). The source presented in Fig. 3 enables arbitrary superpositions of the anticorrelated possibilities (i.e., $|EL\rangle$ and $|LE\rangle$). Furthermore, the correlated states can easily be created from this source by rotating the polarization axes at element M in Fig. 3. In this way, all four time-bin entangled Bell states can be conveniently generated with this source. Second, the interference in Bob's interferometer results from the indistinguishability of photon amplitudes that were initially in the same polarization mode. This is in contrast to configurations in which photon amplitudes from different polarization modes are made indistinguishable by use of a polarization analyzer. Thus, the reduction in visibility that has come to be associated with extremely brief pump pulses [19] will not be present in this scheme. Note that a symmetrization method has been developed to restore visibility for experiments using polarization-entangled photons created by such a short pulse pump [17,20].

In conclusion, we have demonstrated that two recent innovations in the field of practical quantum key distribution (autocompensation and passive detection) are closely related to the methods developed to protect quantum computations from decoherence. Pursuing this conceptual link between techniques from quantum computation and advances in practical QKD, we have developed a new QKD scheme (Fig. 2) that combines autocompensation and passive detection. Furthermore, we have proposed a practical implementation of the scheme (Fig. 3) that is feasible using existing technology.

We thank Matthew D. Shaw and Magued B. Nasr for valuable conversations, and Jean C. Boileau for constructive criticism on an early draft. This work was supported by the National Science Foundation; the Center for Subsurface Sensing and Imaging Systems (CenSSIS), an NSF Engineering Research Center; and the Defense Advanced Research Projects Agency (DARPA).

*Electronic address: walton@bu.edu
†Electronic address: Quantum Imaging Laboratory: http://www.bu.edu/qil

[1] D. A. Lidar and K. B. Whaley, quant-ph/0301032.
[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[3] Z. D. Walton, A. F. Abouraddy, A. V. Sergienko, B. E. A. Saleh, and M. C. Teich, Phys. Rev. A **67**, 062309 (2003).
[4] A. V. Belinsky and D. N. Klyshko, Laser Phys. **2**, 112 (1992).
[5] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, Appl. Phys. Lett. **70**, 793 (1997).
[6] D. S. Bethune and W. P. Risk, in *IQEC'98 Digest of Postdeadline Papers* (Optical Society of America, Washington, DC, 1998), Vol. 12-2.
[7] M. A. Nielsen and I. L. Chuang, *Quantum Computing and Quantum Information* (Cambridge University Press, New York, 2001).
[8] G. M. Palma, K.-A. Suominen, and A. K. Ekert, Proc. R. Soc. London A **452**, 567 (1996).
[9] J. Brendel, N. Gisin, W. Tittel, and H. Zbinden, Phys. Rev. Lett. **82**, 2594 (1999).
[10] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, New York, 1984), pp. 175–179.
[11] The idea of using pole states is explored in Ref. [12]; however, that paper does not mention the possibility of passive detection.
[12] H. Bechmann-Pasquinucci and W. Tittel, Phys. Rev. A **61**, 062308 (2000).
[13] A similar idea is presented in Ref. [14]. In that paper, Alice uses four states of a three-state quantum system, and Bob achieves passive detection by mapping Alice's three-state quantum system into an eight-state quantum system.
[14] K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. Lett. **89**, 037902 (2002).
[15] On the occasions when Bob's detection pattern is (early, middle), (middle, early), (middle, late), or (late, middle), he has also effectively measured in the time basis. However, to simplify the analysis by making the probability of successful bit-sharing independent of the basis in which Alice sent, we consider only the extreme cases (early, early) and (late, late) as valid time-basis detections.
[16] A femtosecond pump pulse is typically desired for experiments involving the simultaneous creation of multiple down-converted photon pairs [17]. Our implementation does not require such a brief pump pulse, and will work with a picosecond laser, such as that used in Ref. [18].
[17] F. De Martini, G. Di Giuseppe, and S. Pádua, Phys. Rev. Lett. **87**, 150401 (2001).
[18] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, Phys. Rev. Lett. **84**, 4737 (2000).
[19] T. E. Keller and M. H. Rubin, Phys. Rev. A **56**, 1534 (1997).
[20] Y.-H. Kim and W. P. Grice, J. Mod. Opt. **49**, 2309 (2002).