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

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.

In Ref. [1], Klyshko's "advanced wave interpretation" [2] was used to describe one-way autocompensating (OWA) quantum key distribution (QKD) as a variation on round-trip autocompensating QKD [3, 4]. These schemes are called autocompensating because they allows high-visibility quantum interference without calibration or active stabilization of the receiver's (Bob's) apparatus. In the context of quantum computation theory [5], a more natural explanation of OWA is provided by decoherence-free subspaces (DFSs, for a review, see Ref. [6]). Palma *et al.* [7] have shown that a single logical qubit encoded in two physical qubits according to

$$\begin{aligned} |\bar{0}\rangle &\rightarrow |01\rangle \\ |\bar{1}\rangle &\rightarrow |10\rangle \end{aligned} \tag{1}$$

will be protected against collective dephasing.

To link this DFS to OWA, we consider time-bin photonic qubits [8], in which the physical basis states $|0\rangle$ and $|1\rangle$ correspond to early ($|\mathrm{E}\rangle$) and late ($|\mathrm{L}\rangle$) single-photon wavepackets, 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 QKD, Alice superposes the two-qubit time-bin states $|\mathrm{EL}\rangle$ and $|\mathrm{LE}\rangle$ with one of four relative phases (0, $\pi/2$, π, $3\pi/2$) 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. [8]. 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) [9].

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 a MZI on a single time-bin qubit is

$$\begin{aligned} |\mathrm{E}\rangle &\rightarrow i|a^-\rangle + ie^{i\phi}|b^-\rangle - e^{i\phi}|b^+\rangle + |a^+\rangle \\ |\mathrm{L}\rangle &\rightarrow i|b^-\rangle + ie^{i\phi}|c^-\rangle - e^{i\phi}|c^+\rangle + |b^+\rangle\,, \end{aligned} \tag{2}$$

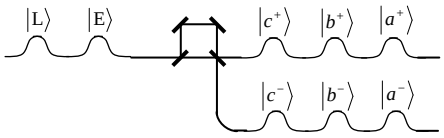

FIG. 1: The action of a Mach-Zehnder interferometer (MZI) on a single time-bin qubit. The two possible input states of the photon are mapped onto six possible output states according to Eq. (2).

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 of two time-bin qubits:

$$\begin{aligned} |\mathrm{EL}\rangle &\rightarrow |b^+b^+\rangle + |b^-b^-\rangle + i(|b^+b^-\rangle + |b^-b^+\rangle) \\ |\mathrm{LE}\rangle &\rightarrow |b^+b^+\rangle + |b^-b^-\rangle - i(|b^+b^-\rangle + |b^-b^+\rangle)\,, \end{aligned} \tag{3}$$

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

OWA and passive detection have been previously presented in separate proposals (Refs. [1] and [8], respectively). Here we present a new scheme that combines these two beneficial features in a single implementation. Let the states $|\mathrm{EL}\rangle$ and $|\mathrm{LE}\rangle$ in 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 ($|\mathrm{EL}\rangle \pm |\mathrm{LE}\rangle$) and the poles themselves to make up Alice's four signal states. As seen in Fig. 1, each time-bin qubit can lead to six different detection events. Thus, since the new protocol involves two photons, there are 36 possible detection events. By not postselecting his outcomes, Bob effectively performs a measurement in a larger Hilbert space. By exploiting

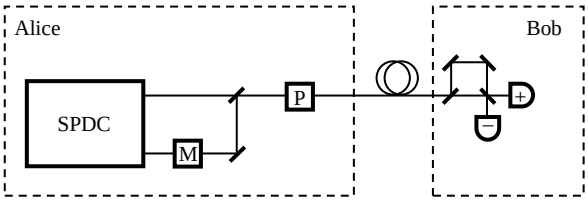

FIG. 2: A proposed implementation for the passive detection, autocompensating QKD scheme described in the text. "SPDC" is a nonlinear crystal pumped by a brief pulse to produce a noncollinear, polarization-entangled two-photon state via spontaneous parametric down-conversion. The action of elements "M"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

the additional information provided by measuring in this larger Hilbert space, Bob is no longer required to switch between noncommuting bases. Thus, enlargement of the Hilbert space imbues the scheme with autocompensation and passive detection.

We group possible detection patterns on Bob's side into three classes. Valid two-photon detections are those in which Bob registers one detection for each of the two photons sent by Alice, such that his joint detection pattern is consistent with one of Alice's four signal states. Valid one-photon detections are those in which the single detection corresponds to one of extremal time slots ($|a^{\pm}\rangle$ or $|c^{\pm}\rangle$ in Fig. 1). All other detection patterns (e.g. no detections, more than two detections, etc.) are considered invalid.

The protocol operates as follows. When Bob's detection pattern is invalid, he announces this and the corresponding run of the exchange is discarded. When Bob obtains a valid one-photon detection, he announces that he has measured in the time basis ($\{|\mathrm{EL}\rangle, |\mathrm{LE}\rangle\}$), as opposed to the phase basis ($\{|\mathrm{EL}\rangle \pm |\mathrm{LE}\rangle\}$). When Bob obtains a valid two-photon detection and both photons are detected in their respective middle time slots, he announces that he has measured in the phase basis. When Bob obtains a valid two-photon detection involving any temporal combination besides the two middle time slots, he announces that he has measured in the time basis. Alice then announces the basis from which the signal state was chosen. On the occasions when their bases match, Bob is able to infer the state that Alice sent, based on his detection pattern. 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).

A feasible implementation for this scheme is presented in Fig. 2. 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. 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 non-delayed portion.

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 that combines autocompensation and passive detection. Furthermore, we have proposed a practical implementation of the scheme (Fig. 2) that is feasible using existing technology.

[1] Z. Walton, A. F. Abouraddy, A. V. Sergienko, B. E. A. Saleh, and M. C. Teich, quant-ph/0207167 (2002).

[2] A. V. Belinsky and D. N. Klyshko, Laser Phys. (Moscow) **2**, 112 (1992).

[3] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, Appl. Phys. Lett. **70**, 793 (1997).

[4] D. S. Bethune and W. P. Risk, IQEC'98 Digest of Postdeadline Papers **12-2** (1998).

[5] M. A. Nielsen and I. L. Chuang, *Quantum Computing and Quantum Information* (Cambridge, New York, 2001).

[6] D. A. Lidar and K. B. Whaley, quant-ph/0301032 (2003).

[7] G. M. Palma, K.-A. Suominen, and A. K. Ekert, Proc. R. Soc. London A **452**, 567 (1996).

[8] J. Brendel, N. Gisin, W. Tittel, and H. Zbinden, Phys. Rev. Lett. **82**, 2594 (1999).

[9] C. H. Bennett and G. Brassard, Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, pp. 175–179 (1984).

[10] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).