A phase-randomized coherent state by cross-Kerr nonlinearity for quantum key distribution

Seung-Woo Lee
Quantum Universe Center, Korea Institute for Advanced Study, Seoul 02455, Korea

Jaewan Kim
School of Computational Sciences, Korea Institute for Advanced Study, Seoul 02455, Korea

For the realization of quantum key distribution(QKD), a perfect single photon source is necessary but is not feasible within current technologies. In practical realizations, a weak laser has been instead widely used for the QKD source, which can be written as a coherent state

$$|\alpha e^{i\theta}\rangle = e^{-|\alpha|^2/2}\sum_{n=0}^{\infty}\frac{(\alpha e^{i\theta})^n}{\sqrt{n!}}|n\rangle, \tag{1}$$

where $e^{i\theta}$ is the phase of the coherent state and $|n\rangle$ is the photon number state. A necessary assumption for its security proof is that the phase of the coherent state is uniformly random [1, 2]. Thus, to an eavesdropper without a priori knowledge on the phase, the QKD signal with random phase source is indistinguishable with

$$\frac{1}{2\pi}\int_0^{2\pi}|\alpha e^{i\theta}\rangle\langle\alpha e^{i\theta}|d\theta = e^{-|\alpha|^2}\sum_{n=0}^{\infty}\frac{|\alpha|^{2n}}{n!}|n\rangle\langle n|, \tag{2}$$

a Poisson distributed mixed state in photon number basis.

However, it is challenging to realize continuous random phase from the source. It has been shown that if the phase is not fully randomized, the security of QKD is significantly reduced [1]. A phase modulator can be used to randomly modulate the phase from the source, but requires a perfect random number generator. Many efforts have been devoted to realize a random phase source in experiments and also to prove the security without perfect phase randomization. A direct phase modulation using gain-switched laser diodes has been developed, naturally providing phase-randomized coherent state pulse [3]. A security of QKD with non-random phase was analyzed in Ref. [1]. Recently, the security of QKD with discrete-phase-randomized coherent state was studied [2], and it was shown that the performance of QKD with discrete random phase (e.g. 10) is close to continuous randomization. However, it uses an active phase modulation by a phase modulator with random number generator.

We here propose a scheme to generate phase-randomized coherent states as an alternative source for QKD. It naturally provides a perfect discrete random phase without active phase modulation using random number generator. Our scheme employs a cross-Kerr nonlinearity with the interaction Hamiltonian $-\hbar\chi\hat{n}_1\hat{n}_2$ (here $\hat{n}_i$ is the number operator in ith mode). If it is applied to two-mode coherent state input $|\alpha\rangle_1|\beta\rangle_2$ for time $t = 2\pi/d\chi$, the output state becomes

$$\frac{1}{d}\sum_{j=0}^{d-1}\Big(\sum_{q=0}^{d-1}\omega^{-jq}|\alpha\omega^q\rangle\Big)_1|\beta\omega^j\rangle_2, \tag{3}$$

where $\omega^k = e^{2\pi ik/d}$ denotes the d number of discrete phases $k \in \{0, ..., d-1\}$. If a measurement is performed on mode 2 yielding equally probable outcomes j (e.g. by homodyne detection after 50:50 beam splitter), the output of 1st mode is determined as a discrete superposition of coherent states $\{|\alpha\rangle, |\alpha\omega\rangle, ..., |\alpha\omega^{d-1}\rangle\}$ on a circle in phase space [4, 5]

$$e^{-|\alpha|^2/2}\sum_{n\equiv j(\mathrm{mod}\ d)}^{\infty}\frac{\alpha^n}{\sqrt{n!}}|n\rangle. \tag{4}$$

By employing the state for QKD, we study the security of BB84 protocol with different interaction time and nonlinearity. The effect of noise and basis dependence of the source is investigated. We will discuss the possibility to enhance the key rate by formulating a high-dimensional QKD protocol based on our scheme.

[1] H.-K. Lo and J. Preskill, Quantum Inf. Comput. **7**, 0431 (2007).
[2] Z. Cao, Z. Zhang, H.-K. Lo, and X. Ma, New J. Phys. **17**, 053014 (2015).
[3] Z. L. Yuan *et al.*, Phys. Rev. X **6**, 031044 (2016).
[4] J. Kim *et al.*, Optics Communication **337**, 79-82 (2015).
[5] Y. W. Cheong and J. Lee, J. Kor. Phys. Soc. **51**, 1513 (2007).