Quantum key distribution using optical coherent states via amplitude damping

Abderrahim El Allati and Yassine Hassouni

abdou.allati@gmail.com, y-hassou@fsr.ac.ma

Abstract

A quantum key distribution protocol using an optical states based on nonorthogonal entangled pairs is investigated. It consists of sharing a similar key between the sender and the receiver by exchanging the quantum correlation of coherent states. These states are used as the support of the encoding information where affected by an amplitude damping channel. The security of the present protocol against beam splitter attack is studied as function of the information gain.

Q.C. using coherent states

A coherent state of one mode of the electromagnetic field can be expressed as

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

where $|n\rangle$ denotes the state with photon number n, $\langle n\rangle = |\alpha|^2$. For us, we use the coherent states as a carrying of information by the different manner:

$$\begin{aligned} |\alpha\rangle &\to |0_L\rangle, \quad |-\alpha\rangle \to |1_L\rangle \\ |\iota\alpha\rangle &\to |0_L\rangle, \quad |-\iota\alpha\rangle \to |1_L\rangle. \end{aligned} \tag{2}$$

Alice prepares the Bell states of coherent states,

$$\begin{aligned} |\psi^{\pm}\rangle &= N^{\pm}_{\alpha,\alpha}(|\alpha\rangle|\alpha\rangle \pm |-\alpha\rangle|-\alpha\rangle) \\ |\phi^{\pm}\rangle &= N^{\pm}_{\alpha,\alpha}(|\iota\alpha\rangle|\iota\alpha\rangle \pm |-\iota\alpha\rangle|-\iota\alpha\rangle), \end{aligned} \tag{3}$$

Amplitude damping

We consider the following non-Markovian master equation

$$\frac{\partial\rho^{\pm}}{\partial t} = \sum_{i=1}^{2} \gamma(t)[a_i\rho^{\pm}a_i^{\dagger} - \frac{1}{2}(a_i^{\dagger}a_i\rho^{\pm} + \rho^{\pm}a_i^{\dagger}a_i)], \tag{4}$$

In a non-Markovian channel an initial coherent state evolves as

$$|\pm\alpha\rangle \to |\pm\alpha e^{-\frac{1}{2}\Gamma(t)}\rangle, \tag{5}$$

the transmissivity of the channel is

$$\Gamma(t) = 2\int_0^t \gamma(s)ds. \tag{6}$$

The decay rate evaluated for an Ohmic reservoir with Lorentz-Drude cutoff,

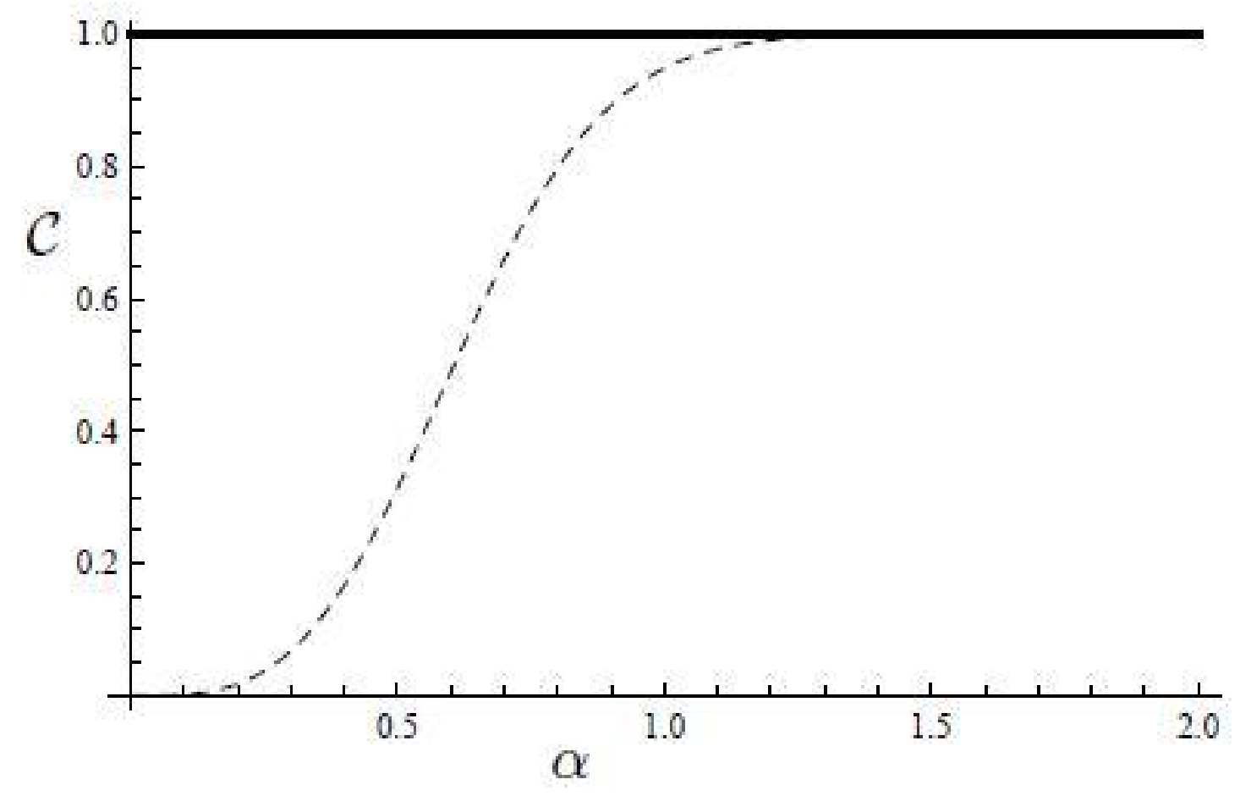
$$\Gamma(t) = \gamma_M[1 - e^{w_c}\cos w_0 t - \frac{w_c}{w_0}e^{-w_c t}\sin w_0 t] \tag{7}$$

Protocol

The correlation of the coherent states allows to transmit the key between two parties securely. Alice prepares a sequence of coherent states by sending one of the states to Bob.

1. Alice chooses a subset of random positions within a sequence of data to be transmitted.
2. Alice transmits random bits encoded with a set of non-orthogonal states $|\alpha\rangle = |0_L\rangle$ and $|-\alpha\rangle = |1_L\rangle$ or $|\iota\alpha\rangle = |0_L\rangle$ and $|-\iota\alpha\rangle = |1_L\rangle$ from chosen subset which provides a raw key.
3. Bob randomly chooses a quadratures, either $\hat{x}$ or $\hat{p}$, to measure the traveling qubits. Then he sends via classical channel his choices of the measurements to Alice without giving the information about the results of measurement.
4. Alice measures the first state of mode-1 from the classical information which sent by Bob ($\hat{x}$ or $\hat{p}$).
5. Using the detectors, Bob can easily detect the presence of eavesdropping in the quantum channel. He warns Alice in the case where he detects any.
6. Alice deduces Bob results by using the results of home qubits. In the end, they get the secret key.

The evolution of the bipartite quantum entanglement $\mathcal{C}$ as function of α, where the solid curve presents ρ^-_{ϕ} and ρ^-_{ψ} and dashed curve presents ρ^+_{ϕ} and ρ^+_{ψ}.



Eavesdropping

Eve's task is to distinguish the four states. However, the four states are not orthogonal. In order to known how much she can learn and how much she disturbs the signal state, it is sufficient to calculate Eve's error rate QE_e on the sifted key for this particular scheme.

$$\begin{aligned} U_{BS}|\alpha\rangle_b|0\rangle_e &= |\sqrt{T}\alpha\rangle_b|-\sqrt{R}\alpha\rangle_e \\ U_{BS}|-\alpha\rangle_b|0\rangle_e &= |-\sqrt{T}\alpha\rangle_b|\sqrt{R}\alpha\rangle_e, \end{aligned} \tag{8}$$

After beam splitter attack, the resultant state is entangled with respect to the mode of Bob and Eve. The associated marginal density matrices for Bob are $\rho^B_{\pm\alpha(t)}$ and $\rho^B_{\pm\iota\alpha(t)}$ and for Eve are $\rho^E_{\pm\alpha(t)}$ and $\rho^E_{\pm\iota\alpha(t)}$ which, after the beam splitter, are calculated as

$$\begin{aligned} \rho^B_{\pm\alpha(t)} &= |\pm\sqrt{T}\alpha(t)\rangle\langle\pm\sqrt{T}\alpha(t)|, \\ \rho^B_{\pm\iota\alpha(t)} &= |\pm\iota\sqrt{T}\alpha(t)\rangle\langle\pm\iota\sqrt{T}\alpha(t)|, \\ \rho^E_{\pm\alpha(t)} &= |\mp\sqrt{R}\alpha(t)\rangle\langle\mp\sqrt{R}\alpha(t)|, \\ \rho^E_{\pm\iota\alpha(t)} &= |\mp\iota\sqrt{R}\alpha(t)\rangle\langle\mp\iota\sqrt{R}\alpha(t)|. \end{aligned} \tag{9}$$

Consider that Eve uses an optimum decision strategy that results in the smallest possible error when distinguishing two non-orthogonal coherent states $|\mp\sqrt{R}\alpha(t)\rangle$ and $|\mp\iota\sqrt{R}\alpha(t)\rangle$. Eve's error rate QE_E:

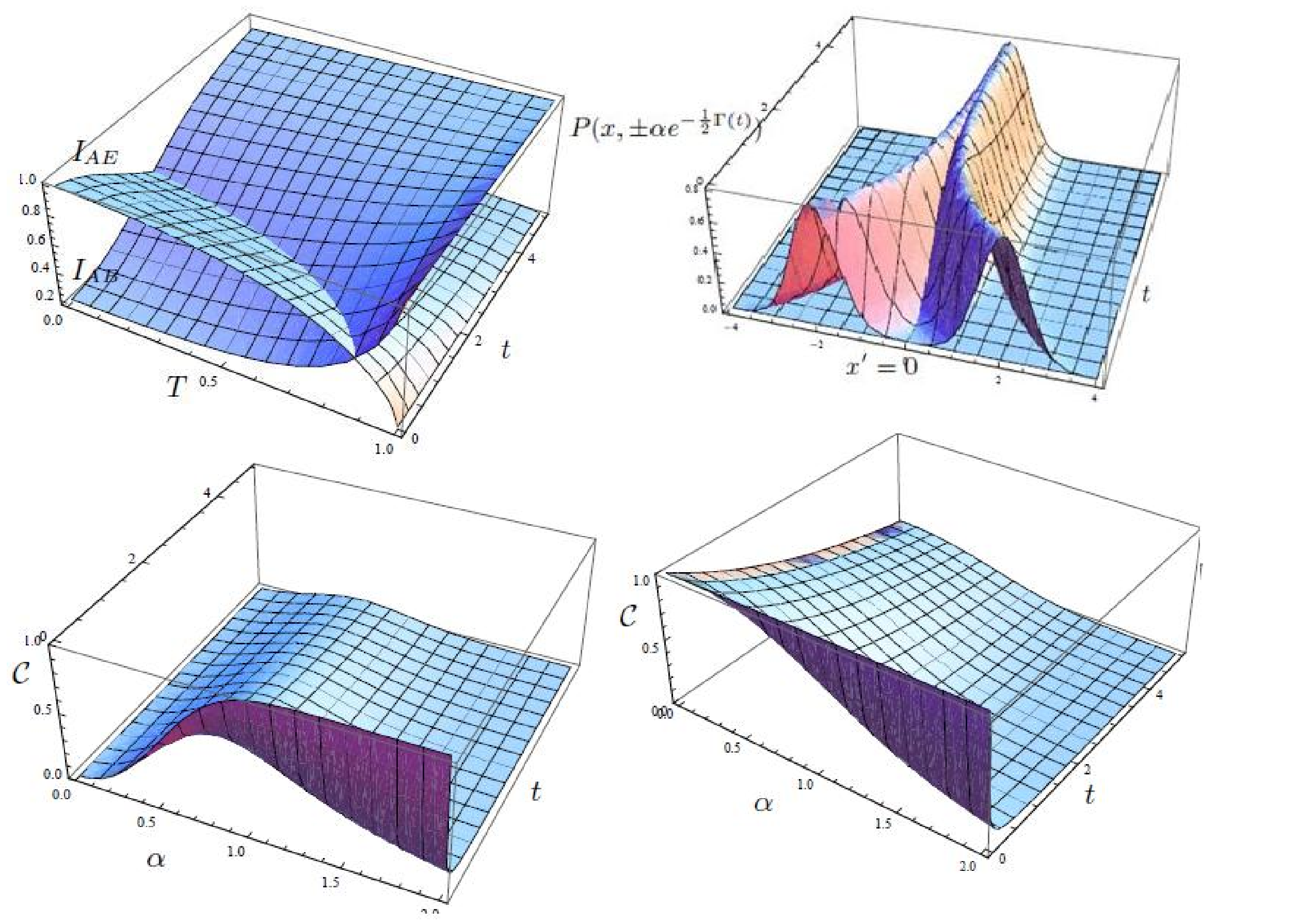
$$QE_E = \frac{1}{4}(1 - \sqrt{1 - e^{-2(1-T)|\alpha(t)|^2}}). \tag{10}$$

Now, Alice and Bob want to evaluate QE_E or Eve's average information gain $I_{AE} = 1 - H(QE_E)$,

$$H(QE_E) = -QE_E\log QE_E - (1 - QE_E)\log(1 - QE_E).$$

It is immediately confirmed that the sum of the squared measures of disturbance V_E and distinguishability $D_B = 1 - 2QE_E = \sqrt{1 - V_E^2}$ reaches its expected upper bound of unity; $D_B^2 + V_E^2 = 1$. On the other hand, Bob's information gain $I_{AB} = 1 - H(QB_B)$ is easily evaluated by publicly revealing a part of his sifted keys.

Results



After the transmission of a large number of states, Bob constructs his key by taking into account the following decision rule:

$$\begin{cases} 1, & \text{if } x > x' \\ 0, & \text{if } x < x' \end{cases} \tag{11}$$

Then the probability distribution of quadrature measured by Bob is written as

$$P(x, \alpha) = |\langle x|\alpha\rangle|^2 = \frac{\sqrt{2}}{\sqrt{\pi}}e^{-2(x-\alpha)^2}. \tag{12}$$

If Alice announces the states she sent, Bob can observe the quadrature distributions for the coherent states as presented in figures.

Conclusion

As a coherent state qubit travels along a fiber-optic cable it suffers from two forms of decoherence. Absorption causes both a decrease in the amplitude of the coherent state and a dephasing in the qubit basis. The amplitude can be restored through quantum key distribution using a specially prepared Bell-state.

References

[1] A. El Allati, M. El Baz and Y. Hassouni, Quantum Information Processing, **10**, 589 (2011).

[2] A. El Allati and M. El Baz, DOI : 10.1007/s11082-014-9959-2, Optical and Quantum Electronics (2014)