Simultaneous classical communication and quantum key distribution based on Gaussian modulated coherent states

Youngjun Kim and Young-Chai Ko
School of Electrical Engineering, Korea University, Anam-dong 5 ga, Seongbuk gu, Seoul, Korea
a) koyc@korea.ac.kr

Abstract: We propose a new quantum communication scheme using quantum coherent states. In our scheme, classical information and the secret key are transmitted simultaneously without any loss of secret key rate performance, while only the secret key is transmitted in the conventional protocol. In our protocol, classical information is first modulated by pulse amplitude modulation (PAM). The secret key is then mapped by random Gaussian modulation and is added to the PAM symbol. The receiver decodes the classical information, treating the Gaussian signal as additive noise. The classical symbol is discarded from the received state after successive decoding of the classical information, and the secret key is then distilled by conventional protocol. We demonstrate that after the classical symbol is discarded, the remaining system is identical to the conventional quantum key distribution system. Our proposed scheme provides the same secret key rate as that of the conventional quantum key distribution system and provides an additional data rate of classical information.

Keywords: continuous variable quantum key distribution (CV-QKD), coherent states, homodyne detector

Classification: Optical systems

References

[1] P. Carruthers and M. M. Nieto: “Phase and angle variables in quantum mechanics,” Rev. Mod. Phys. 40 (1968) 411 (DOI: 10.1103/RevModPhys.40.411).
[2] D. Mayers: “Unconditional security in quantum cryptography,” J. ACM 48 (2001) 351 (DOI: 10.1145/382780.382781).
[3] M. Osaki, et al.: “Derivation and physical interpretation of the optimum detection operators for coherent-state signals,” Phys. Rev. A 54 (1996) 1691 (DOI: 10.1103/PhysRevA.54.1691).
[4] K. Kato, et al.: “Quantum detection and mutual information for qam and psk signals,” IEEE Trans. Commun. 47 (1999) 248 (DOI: 10.1109/26.752130).
[5] A. Peres and W. K. Wootters: “Optimal detection of quantum information,”
1 Introduction

Coherent states [1] are eigen states of the annihilation operator of the quantum harmonic oscillator. The detecting precision of the position and the momentum of the coherent state is limited according to the Heisenberg’s uncertainty principle. Because of this quantum mechanical property, the coherent states are widely used in quantum optics and quantum key distribution [2]. Osaki et al. suggested a detection operator to distinguish a set of coherent states which are constructed by phase shift keying (PSK) modulation [3]. Kato et al. developed a quantum communication scheme using quantum PSK and quadrature amplitude modulation (QAM) [4] for modulation and square root measurement [5] for demodulation.

Continuous variable quantum key distribution (CV-QKD) which uses quantum coherent states and homodyne detectors is an alternative scheme used to implement QKD. QKD protocol using Gaussian-modulated coherent states, also called GG02 (name derived from Grosshans and Grangier) [6], is an implementation-friendly scheme used to perform BB84 type QKD protocol [7]. Many studies have been carried out based on GG02 [6] for long distance communication [8] and for Gaussian noise added source [9].

In this paper, we focus on the fact that at the receiver’s side, the Gaussian distributed random values sent in the GG02 protocol can be regarded as an additive Gaussian noise. We also assume that ordinary classical communication with a channel code gives error free transmission, even in a high loss channel. Based on this background, we propose a new scheme in which, compared to GG02, the classical information and secret key are conveyed by coherent states without loss of secret key rate.

This paper is structured as follows. We first describe our proposed protocol which sends classical information using the coherent state selection strategy. We then explain how to add the secret key information to the selected state and describe how the receiver distills the classical information from the received state. Finally, we extract the secret key by discarding the classical information successively and demonstrate that the achievable secret key rate is the same as that of GG02.
2 Classical communication using coherent states

We prepare a set of coherent states to send classical information. In this paper, we consider rectangular quadrature amplitude modulation (QAM). Note that QAM is a two-dimensional (2-D) modulation with in-phase and quadrature-phase. In classical communication, the rectangular QAM can be demodulated by projecting the received signal onto the in-phase and quadrature-phase axes. Similar to the rectangular QAM, coherent states are also represented in the 2-D space because a coherent state is characterized by the complex eigen value of the annihilation operator. Coherent states are detected by homodyne detectors and the detecting procedure can be seen as a projective measurement onto the position axis or the momentum axis.

In rectangular QAM, we can choose various modulation sizes, $M$, such as $M = 2^2 = 4$ or $M = 2^4 = 16$. The coherent states for rectangular QAM are constructed by arranging the eigen numbers of the annihilation operator as a form of rectangular QAM. Fig. 1(a) shows an example of coherent states for rectangular QAM for $M = 16$. The states $|\psi_m\rangle$ ($m = 1, \ldots, 16$) can be written as

$$|\psi_m\rangle = \left\{5 - 2(m \mod 4)\right\} \frac{n_S}{10} + i \left\{5 - 2\left\lfloor\frac{m}{4}\right\rfloor\right\} \frac{n_S}{10}$$

where $\lfloor \cdot \rfloor$ denotes the ceiling function and $n_S$ denotes the average number of photons, as will be explained later in detail.

Note that the receiver, Bob, can choose only one axis, $x$ or $p$, because of the Heisenberg-type uncertainty of the homodyne receiver. If Bob chooses $x$, then the uncertainty of momentum, $\Delta p$, is increased and Bob cannot obtain a non-negative information rate from momentum. Bob can measure only the coefficient of $x$ but not that of $p$. Hence, the actual degree of freedom (DOF) of classical modulation is one and we can use only one-dimensional (1-D) modulation, such as PAM.

We propose a constellation set which is reduced from 16-QAM to 4-PAM as shown as Fig. 1(b). The states $|\psi_m\rangle$, $m = 1, \ldots, 4$ can be written as

$$|\psi_m\rangle = \left(5 - 2m\right)\sqrt{n_S/10}(1 + i)$$

The minimum distance between signals seems to be increased by $\sqrt{2}$ times, but the actual distance is not increased because states are projected onto one basis axis and are measured.
An achievable classical information rate is given by a function of the signal-to-noise ratio (SNR), and SNR is given by a function of the signal power, line transmission, and receiver noise power. Given the line transmission and classical information rate constraint, we can choose average signal power. Let the average signal power be $V_C N_0$, where $N_0$ is the shot noise variance. The average number of photons, $N_S$, is the concept corresponding to the signal power in classical communication, which can be calculated as

$$N_S = \sum_{m=1}^{M} \frac{1}{M} \langle \psi_m | \hat{a}^\dagger \hat{a} | \psi_m \rangle = V_C N_0.$$  \hspace{1cm} (3)

We can also calculate $N_S$ by averaging the square of amplitude of coherent states illustrated on the phase space in Fig. 1(b). Now classical information is mapped into the coherent states described in (2).

3 Gaussian modulation on the QAM states

In this section, we add the Gaussian modulated signal which contains information for QKD to the selected coherent state. Similar to the case of GG02, the transmitter, Alice, draws two random values, $x_A$ and $p_A$, from $\mathcal{N}(0, V_A N_0)$. Instead of sending $|x_A + ip_A\rangle$ as in the case of GG02, Alice sends $|\psi_A\rangle$ constructed as

$$|\psi_A\rangle = |\psi_m + x_A + ip_A\rangle,$$  \hspace{1cm} (4)

where $|\psi_m\rangle$ is given in (2).

Fig. 2 shows the process used to make the coherent state that contains both the secret key and classical information. In Fig. 2(a), the Gaussian modulated random state used to transmit the secret key is illustrated as an arrow mark. The state constructed in Fig. 2(a) for the secret key is added to the state chosen in Fig. 1(b) for classical information. In Fig. 2(b), the coherent state transmitted by Alice is illustrated as a concentric circle.

We also assume the attack by the entangling cloner from Eve, the eavesdropper, as in the case of GG02 [6]. Let the input quadratures of cloner to be $(x_{in}, p_{in})$, the output of the cloner be $(x_E, p_E)$, and the received quadratures of Bob be $(x_B, p_B)$ given by

$$x_B = G_1^{-1/2}(x_{in} + B_x) + N_{rx, x},$$  \hspace{1cm} (5)
\[ p_B = G_p^{1/2}(p_{in} + B_p) + N_{rx,p}, \]  
(6)

with

\[ \langle x_{in}^2 \rangle = \langle p_{in}^2 \rangle = (1 + V_A + V_C)N_0, \]  
(7)

where \( G \) is the channel gain.

In (5) and (6), \( B_x \) and \( B_p \) are the equivalent input noises with variance of \( \chi_x N_0, \chi_p N_0 \) which are given, respectively, by [6]

\[ \langle B_x^2 \rangle = \chi_x N_0, \]  
(8)

\[ \langle B_p^2 \rangle = \chi_p N_0, \]  
(9)

\[ \langle x_{in} B_x \rangle = \langle p_{in} B_p \rangle = 0. \]  
(10)

Also, \( N_{rx,x} \) and \( N_{rx,p} \) in (5) and (6) are the receiver noise of the position and momentum axes, respectively, satisfying

\[ \text{Var}(N_{rx,x}) = \text{Var}(N_{rx,p}) = N_r N_0. \]  
(11)

### 4 Decoding classical information

Now Bob first distills the classical information from the received states. Let us assume that Bob chooses the axis of position, \( x \). The variance of the received signal on Bob, \( V_B \), is to be calculated as

\[ V_B = G(1 + V_A + V_C + \chi)N_0 + N_r N_0. \]  
(12)

Then the received SNR, \( \gamma \), can be written as

\[ \gamma = \frac{V_C}{1 + V_A + \chi + N_r / G}. \]  
(13)

For each pulse, if Alice transmits fewer bits than the Shannon capacity given as \( \frac{1}{2} \log_2(1 + \gamma) \), Bob can decode the transmitted information without error, in principle. Let the pulse rate in Hz be \( p \). For each pulse, we can transmit bits of \( \frac{1}{2} \log_2 M \).

By the Shannon’s theorem, a channel code exists with code rate \( C \) which corrects all the errors if the following condition is satisfied [10]

\[ C \times \frac{p}{2} \log_2 M < \frac{1}{2} \log_2(1 + \gamma). \]  
(14)

Enlarging the length of the channel code, we can reduce the classical bit error rate to be an arbitrary small value and can achieve the classical information rate of \( \frac{1}{2} \log_2(1 + \gamma) \) in principle.

### 5 Secret key distribution

After distillation of the classical information, if the channel code is sufficiently powerful to correct all the errors, both Bob and Eve know the quantum state \( |\psi_m\rangle \) which is selected to transmit the classical information. By removing the quadrature of \( |\psi_m\rangle \) from \( x_{in} \) and \( p_{in} \), Bob and Eve can construct the system so it is equivalent to the case of GG02.

Let \( x'_{in} \) and \( p'_{in} \) to be the removed versions of \( x_{in} \) and \( p_{in} \), respectively. Eve can construct \( x'_{in} \) by subtracting the real part of \( \psi_m \) from \( x_{in} \) and \( p'_{in} \) by subtracting the imaginary part of \( \psi_m \) from \( p_{in} \) as
Bob can also remove the classical signal from the received state by subtracting the amplitude of $|ψ_m⟩$ from the received quadrature. Let $x'_B$ and $p'_B$ be the received quadrature of Bob after successive decoding of the classical information, which can be written as

\begin{align}
    x'_B &= G^{1/2}_x (x_{in} - \Re[ψ_m]) + B_x + N_{r,x}, \\
p'_B &= G^{1/2}_p (p_{in} - \Im[ψ_m]) + B_p + N_{r,p},
\end{align}

with

\begin{align}
    \langle x'^2 \rangle &= \langle p'^2 \rangle = (1 + V_A)N_0, \\
    \langle x'_B B_x \rangle &= \langle p'_B B_p \rangle = 0.
\end{align}

Note that we can calculate the variance of $x'_B$, denoted as $V'_B$ as

\begin{equation}
    V'_B = G(1 + V_A + \chi)N_0 + N_rN_0.
\end{equation}

We can also calculate the conditional variance of $x'_B$ in given Alice’s quadrature, denoted as $V'_{B|A}$ as

\begin{equation}
    V'_{B|A} = G(1 + \chi)N_0 + N_rN_0.
\end{equation}

From (21) and (22), the mutual information between Alice and Bob, $I_{AB'}$, can be written as

\begin{equation}
    I_{AB'} = \frac{1}{2} \log_2 \left[ \frac{V'_B}{V'_{B|A}} \right] = \frac{1}{2} \log_2 \left[ \frac{1 + V_A + \chi + N_r/G}{1 + \chi + N_r/G} \right].
\end{equation}

Eve’s minimum variance, limited by the Heisenberg-type uncertainty, $V(B'|E)$, can be written as

\begin{equation}
    V_{B'|E} = \frac{N_0}{G(\chi + (1 + V_A)^{-1})} + N_rN_0,
\end{equation}

and mutual information between Bob and Eve, $I_{BE}$ can be calculated as

\begin{equation}
    I_{BE} = \frac{1}{2} \log_2 [V'_B/V_{B'|E}] = \frac{1}{2} \log_2 \left[ \frac{G(V + \chi) + N_r}{1 + G(V + \chi)} + N_r \right] = \frac{1}{2} \log_2 \left[ \frac{G^2(V + \chi) + N_rG}{N_rG + 1} \right],
\end{equation}

where $V = V_A + 1$.

We can confirm that (23) and (25) are the same as (4a) and (4b) of [6], respectively, neglecting the receiver noise. The secret key rate after reverse reconciliation and privacy amplification can be calculated from (23) and (25) as...
\[ \Delta I_{RR} = I_{B^A} - I_{B^E} \approx -\frac{1}{2} \log_2[G^2(1 + \chi)(V^{-1} + \chi)]. \] (26)

Note that in (26), approximation is conducted by ignoring the receiver noise, \( N_r \). We can certify that (26) is the same as (5) in [6], which means that our proposed scheme provides the same rate of secret key in [6] and provides an additional rate of classical information.

### 6 Conclusion

We propose a new quantum communication scheme transmitting both the classical information and the secret key. The coherent states selected to convey the classical information is added to the Gaussian modulated signal to distribute the quantum secret key. In our scheme, we can achieve a quantum secret key rate of 

\[-\frac{1}{2} \log_2[G^2(1 + \chi)(V^{-1} + \chi)]\]

which is the same as that of the conventional protocol, and can simultaneously achieve an additional classical information rate of 

\[ \frac{1}{2} \log_2(1 + \gamma). \]

### Acknowledgments

This work was supported by the ICT R&D program of MSIP/IITP. [1711028311, Reliable crypto-system standards and core technology development for secure quantum key distribution network]