Quasi-unambiguous state discrimination for coherent states with phase fluctuation

A. Oka, K. Inoue

Osaka University, 2-1 Yamadaoka, Suita, Osaka 565-0871, Japan

ARTICLE INFO

Article history:
Received 19 July 2012
Received in revised form 17 February 2013
Accepted 21 April 2013
Available online 14 May 2013

Keywords:
Unambiguous state discrimination
Quantum key distribution
Differential-phase-shift QKD

ABSTRACT

This paper describes unambiguous state discrimination (USD) for a sequence of coherent states with fluctuating phase, while considering eavesdropping against differential-phase-shift quantum key distribution systems. A measurement system extracts a fraction of the incoming signal of coherent states, estimates the carrier phase from that fraction, and then conducts a USD measurement on the main signal based on the estimated carrier phase. In such a system, the estimated carrier phase can be different from a true value because of the phase fluctuation, and an error can occur in the USD measurement because of the error in the estimated phase. The USD performance in such a situation is formalized and simulated.

© 2013 Elsevier B.V. All rights reserved.

1. Introduction

Quantum state discrimination is a significant task in quantum information and communications. Generally, no measurement method can perfectly distinguish nonorthogonal signal states due to the law of quantum mechanics. Instead, there are measurement methods that give a conclusive answer with no error, but accompanied with a finite probability of no answer. That is called unambiguous state discrimination (USD). Many studies on USD have been conducted [1–8].

One application of USD is eavesdropping against quantum cryptography or quantum key distribution (QKD) systems that provide ultimately secured secret keys to legitimate parties [9]. Nonorthogonal quantum states are utilized to guarantee the ultimate security in those systems. An attack using a USD measurement against such nonorthogonal states (specifically, linearly independent nonorthogonal states such as weak coherent states used in practical QKD) gives a fraction of key information to an eavesdropper [10]. An example of eavesdropping using USD is a sequential attack against differential-phase-shift (DPS) QKD [11,12]. DPS-QKD is a type of QKD protocol [13] that uses a pulse train of two nonorthogonal coherent states, and features simplicity and robustness against photon number splitting attack [14]. Long-haul QKD transmission experiments have been reported using the DPS-QKD protocol [15,16]. While unconditional security proof has been completed for this protocol in general, a sequential attack with a USD measurement for two coherent states is known to be the most powerful eavesdropping scheme at the present [11]. The transmission distance of DPS-QKD systems is mostly restricted by this sequential attack.

Nonorthogonal states used in DPS-QKD systems are coherent states randomly phase-modulated by \([0, \pi]\), which are denoted as \(|\alpha e^{i\theta}\rangle >\) and \(|1-\alpha e^{i\theta}\rangle >\) where \(\alpha\) is a real number corresponding to the mean photon number \(\mu\) as \(\alpha = \sqrt{\mu}\) and \(\theta\) is a parameter representing the phase of the complex amplitude of light field. In the conventional sequential attacks [11,12], an eavesdropper (Eve) is assumed to know the phase \(\theta\) when conducting a USD measurement against those states. In order to make this attack less powerful, we previously proposed a countermeasure that imposes slow phase modulation onto DPS-QKD signals [17]. The slow phase modulation randomizes the phase \(\theta\) and prevents Eve from performing the optimum USD. DPS-QKD systems become more robust against the sequential attack as a result.

Here, it is noted that phase randomization can be unintentionally realized when a laser source with a finite spectral linewidth is used as a coherent source in DPS-QKD systems. The phase of the coherent state generated from such a laser randomly fluctuates and drifts, which is equivalent to phase randomization. Thus, the use of a laser source with a finite spectral linewidth in DPS-QKD systems may be effective to mitigate the sequential attack using USD.

Being motivated by the above considerations, this paper evaluates the performance of USD that discriminates between two coherent states with fluctuating and drifting phase due to a finite spectral linewidth of a light source. We assume that a train of coherent states with a fluctuating and drifting phase enters a measurement system. In order to discriminate each state in the train, the system has a means of tracking the carrier phase of the
incident lights, and performs a USD measurement based on the outcome from the phase tracking system. In such a situation, an error can occur in the phase tracking procedure, and therefore, an error can occur in the USD measurement as well, owing to the incorrect estimated phase reference. The probabilities of these errors are formalized and simulated in this work.

2. State discrimination system with phase tracking

The measurement system considered in this work is illustrated in Fig. 1. A train of \( \{0, \pi\} \) phase-modulated coherent states, \( |\alpha e^{i\phi}\rangle \) and \( |\pi e^{i\phi}\rangle \), enters the system, where \( \alpha \) and \( \phi \) correspond to the real amplitude and the phase of a coherent state carrying encoded phase information, respectively. The amplitude \( \alpha \) is given by the mean photon number \( \mu \) as \( \alpha = \sqrt{\mu} \), and the phase \( \theta \) is assumed to drift and fluctuate. A fraction of the incoming signal is split via an optical coupler and input to a phase tracking system, which outputs an outcome of \( \theta_o \). Here, \( \theta_o \) is not necessarily identical to \( \theta \) because of the phase fluctuation. Based on this outcome, a USD measurement is performed on the main signal sequence. A delay circuit is placed before the USD system in order to hold the main signal until the phase estimation is completed.

In the following, the performances of the phase tracking system and the USD measurement based on the erroneous phase are discussed in Sections 3 and 4, respectively, and then the performance of the total system is evaluated in Section 5.

3. Phase tracking system

The phase of the light field can be measured by phase-diversity homodyne detection, with the setup illustrated in Fig. 2. The system measures two quadratures \((x, y)\) of the light field – viz., the real and imaginary parts of its complex amplitude – with respect to local light. Then, the phase is obtained as \( \arctan(y/x) \) when \( x > 0 \), and \( \arctan(y/x) + \pi \) when \( x < 0 \).

However, the phase fluctuates and drifts due to quantum noise, phase noise of the light source, etc., particularly when the number of photons is quite small, which is the case in practical QKD systems. Thus, the phase tracking system averages the results of the homodyne detection to obtain an accurate value of the carrier phase. An issue here is that the measured states are \( \{0, \pi\} \) phase-modulated. The phases of each pulse state distribute around two values separated by \( \pi \), and thus simple averaging does not provide the carrier phase.

One possible scheme to extract the carrier phase from \( \{0, \pi\} \) phase-modulated light is squaring the complex amplitude, which is employed in digital coherent receivers in the latest optical communications [18]. The measurement system derives the complex amplitude from the results of the phase-diversity homodyne detection as \( x + iy \) \((= \alpha e^{i\phi})\), calculates its square as \( (x + iy)^2 \), and then obtains the carrier phase as \( \arctan(\text{Im}[x + iy^2]/\text{Re}[x + iy^2]) = \arctan(\text{Im}[\alpha e^{i\phi}]/\text{Re}[\alpha e^{i\phi}]) \) or \( \arctan(\text{Im}[\alpha^2 \sin(2\phi)/\alpha^2 \cos(2\phi)] = \arctan(\tan(2\phi)/(2 + \pi)/2 \pi) + \pi/2 \). This procedure outputs the carrier phase \( \theta \) regardless of \( \{0, \pi\} \) phase modulation. Employing this scheme with averaging, the phase tracking system can provide an averaged value of the carrier phase.

However, it is not obvious if the above scheme is the best way to track the carrier phase. There may be a more efficient scheme that we do not know. Therefore, in the present work, we employ an approach of evaluating the upper bound of the phase tracking performance. That is, we assume that a sequence of unmodulated coherent states is incident, from which the carrier phase is extracted. The accuracy of the obtained phase value would be better than that extracted from randomly phase-modulated states. In other words, the phase tracking system cannot achieve a better accuracy than this one. Since to clarify the upper bound of the eavesdropping performance is significant in QKD, to evaluate the upper bound of the phase tracking performance is significant as well in its application to QKD.

With the above considerations, we evaluate the performance of the phase tracking system that measures two quadratures \((x, y)\) of the unmodulated light and takes averages of them to extract the carrier phase. In the ideal situation, where signal fluctuation is only caused by quantum noise, the averaging approaches a true value as the averaging time increases. However, for a signal fluctuating due to other classical noises, the phase can drift and averaging does not necessarily lead to a true value. There may be an optimal averaging time, and there may be an error in the outcome even when such an optimal time is employed. In the following, we evaluate the probability of such an error.

We assume quantum noise and phase noise of a coherent source as causes of phase drift and fluctuation. The probability density functions (PDFs) of the two quadratures of the light field, \( x \) and \( y \), are written as

\[
P_d(x) = \frac{1}{\sqrt{2\pi}\sigma_q} \exp\left[\frac{-(x - \mu_p/2\cos\theta)^2}{2\sigma_q^2}\right],
\]

and

\[
P_d(y) = \frac{1}{\sqrt{2\pi}\sigma_q} \exp\left[\frac{-(y - \mu_p/2\sin\theta)^2}{2\sigma_q^2}\right],
\]

where \( \mu_p \) is the mean photon number of a state entering the phase tracking system, and \( \sigma_q = 1/2 \) due to quantum noise. Because of the phase noise of the coherent source, the phase \( \theta \) in the above PDFs fluctuates as

\[
\theta[n + 1] = \theta[n] + \Delta\phi,
\]

where \( \theta[n] \) is the phase of the \( n \)th state and \( \Delta\phi \) is a phase difference between adjacent states. Here, the fluctuation speed is assumed to be sufficiently slow for \( \theta \) to be regarded as a constant in each state. When the phase noise of the coherent source is the cause of the fluctuation, \( \Delta\phi \) follows a PDF written as

\[
g(\Delta\phi) = \frac{1}{\sqrt{2\pi}\sigma_\phi} \exp\left[-\frac{(\Delta\phi)^2}{2\sigma_\phi^2}\right].
\]
with

\[ \sigma_\phi = \sqrt{2\Delta f T}, \]

where \( \Delta f \) is the spectral linewidth (FWHM) of the coherent source and \( T \) is the time interval between adjacent states [19].

Using the above PDFs, we simulated the phase values estimated from fluctuating coherent states as follows: values of the quadratures \( x \) and \( y \) were randomly created for from the \((-M/2, M/2, \ldots, M/2, -M/2)\)-th state to the \((M/2, -M/2, \ldots, -M/2, M/2)\)-th state using Eqs. (1)-(3), where \( M+1 \) is the averaging time, their averages \( \bar{x} \) and \( \bar{y} \) were calculated, and the phase was estimated from the averaged values as \( \theta = \arctan(y/x) \) when \( x > 0 \) and \( \theta = \arctan(y/x) + \pi \) when \( x < 0 \). This calculation was carried out a number of times, and a normalized histogram (i.e., probability density) of the estimated phase values was plotted. The result is displayed in Fig. 3, where the horizontal axis is the estimated phase relative to the center value, the circles are the simulation results, and the solid line is a fitting curve that assumes a Gaussian distribution. The distribution of phase values displayed in the figure indicates that the phase obtained by averaging the results of the phase-diversity homodyne detection is erroneous. We note that we also carried out similar calculations using the squaring method described above for phase-modulated states, the result of which indicates a larger phase variance than that for unmodulated states though it is not presented here.

Fig. 3 is one example of the simulation employing an averaging time of 101. As described above, there may be an optimum number for averaging that would minimize the probability of error. To confirm this, the above simulation was carried out for various averaging numbers. The results are shown in Fig. 4, where the standard deviation of the estimated phases is plotted against the averaging number. An optimum number associated with the smallest standard deviation was observed. This result indicates that there is an optimum averaging time, and that an estimated phase value can be erroneous even when the optimum number is employed.

4. USD based on erroneous estimated phase

Based on the outcome \( \theta \), from the phase tracking system, a USD measurement is performed on a coherent state, \( |\alpha e^{i\theta}| > \) or \( |1-\alpha e^{i\theta}| > \).

Here, \( \theta \) is not necessarily equal to \( \theta \), as indicated in the previous section. We analyze USD under such a condition.

First, we briefly review conventional USD, following the previous works [2,4,8], where states to be discriminated, \( |p> \) and \( |q> \), are exactly known in advance. A measurement system maps candidate states onto two orthogonal subspaces, called the conclusive subspace and the inconclusive subspace, by coupling them with an auxiliary state \( |u_0> \) through a joint unitary operation \( \hat{U} \) as

\[ \hat{U}|p> |u_0> = \alpha|p_1> |u_1> + \beta|p_2> |u_2> , \]
\[ \hat{U}|q> |u_0> = \gamma|q_1> |u_1> + \delta|q_2> |u_2> . \]

In the above equations, \( |u_1> , |u_2> > \) is an orthogonal basis of the auxiliary system, \( \{ |p_1>, |q_1> \} \) is an orthogonal basis of the unambiguous subspace of the concerned system, and \( |p_2> , |q_2> > \) are unit states lying on the ambiguous subspace of the concerned system (i.e., \( \langle p_2|q_2> = 0 \)). After the unitary operation, a measurement is performed on the auxiliary state, the result of which is \( |u_1> > \) or \( |u_2> > \). When the former is obtained, another measurement between \( |p_1> > \) and \( |q_1> > \) concludes that the primary state is \( |p> \) or \( |q> \). When the latter is obtained, no conclusive answer is given. Provided that the primary state is \( |p> \) or \( |q> \), with an equal probability of 1/2, the probability of obtaining a conclusive answer is \( (\mu^2+\nu^2)/2 = 1-(\mu^2+\nu^2)/2 \). This probability is maximized to be \( 1-\langle p_1|q_2> = |p_2> |q_1> \) and \( \mu^2 = \nu^2 = 0 \). For \( \{ 0, \pi \} \)-modulated coherent states, this maximized probability is \( 1-\exp(-2\mu) \) with \( \mu \) being the mean photon number, which is assumed in the conventional sequential attacks against DPS-QKD [11,12].

We assume that the present USD system also employs the same scheme as above. Based on the outcome from the phase tracking system, the USD system supposes that a measured state is \( |\alpha e^{i\theta}| > \) or \( |1-\alpha e^{i\theta}| > \), and prepares an auxiliary state \( |u_0> > \) and conducts a unitary operation, by which the primary state is evolved as

\[ \hat{U}|\alpha e^{i\theta}| > |u_0> = \sqrt{1-|\beta|^2}|s_1> |u_1> + |\beta|s_3> |u_2> , \]
\[ \hat{U}|1-\alpha e^{i\theta}| > |u_0> = \sqrt{1-|\beta|^2}|s_2> |u_1> + |\beta|s_3> |u_2> , \]

where all states are normalized, and \( |\beta|^2 = |\langle p|\alpha e^{i\theta}| > -\alpha e^{i\theta}| > | \rangle = e^{-2\mu} \) with \( \mu = |\alpha|^2 \) being the mean photon number. After the evolution, a
measurement is performed on the auxiliary state, and another measurement between \(|s_1\rangle > \) and \(|s_2\rangle > \) is conducted when the outcome of the measurement on the auxiliary state is \(|u_1\rangle > \). Then, the system concludes that the state is \(|\alpha \theta \rangle > \) when the outcome is \(|s_1\rangle > \) (\(|s_2\rangle > \)). For \(\theta = 0\), this procedure gives an error-free answer with a probability of \(1-|\beta|^2 - 1-e^{-2\Delta^2}\).

For \(\theta \neq 0\), however, measured states are not transformed as in Eq. (5). In order to discuss how the states evolve through the above unitary operation, we first decompose a measured state to sates in the two dimensional space spanned by \(|\alpha \theta \rangle > , -|\alpha \theta \rangle > \) and its complementary orthogonal space as

\[
|\alpha \theta \rangle > = a_1|\alpha \theta \rangle > + b_1|-\alpha \theta \rangle > + c_1|s_1\rangle > ,
\]

\[
-|\alpha \theta \rangle > = a_2|\alpha \theta \rangle > + b_2|-\alpha \theta \rangle > + c_2|s_2\rangle > ,
\]

where \(|s_1\rangle > \) and \(|s_2\rangle > \) are unit states in the complementary space that are orthogonal to \(|\alpha \theta \rangle > \) and \(-|\alpha \theta \rangle > \).

The coefficients in Eq. (6) are analytically obtained as follows. First, we assume a unitary operation \(\hat{R}\), that rotates the phase of a coherent state by \(\pi\). This operation transforms the above states as

\[
\hat{R}|\alpha \theta \rangle > = (|\alpha \theta \rangle > , -|\alpha \theta \rangle > ) = (a|\alpha \theta \rangle > , b|\alpha \theta \rangle > ) \cdot e^{i\pi a|\alpha \theta \rangle > , b|\alpha \theta \rangle > > ,
\]

\[
\hat{R}|-\alpha \theta \rangle > = (|\alpha \theta \rangle > , -|\alpha \theta \rangle > ) = (a|\alpha \theta \rangle > , b|\alpha \theta \rangle > ) \cdot e^{i\pi a|\alpha \theta \rangle > , b|\alpha \theta \rangle > > ,
\]

\[
\hat{R}|\alpha \theta \rangle > = (|\alpha \theta \rangle > , -|\alpha \theta \rangle > ) = (a|\alpha \theta \rangle > , b|\alpha \theta \rangle > ) \cdot e^{i\pi a|\alpha \theta \rangle > , b|\alpha \theta \rangle > > ,
\]

\[
\hat{R}|-\alpha \theta \rangle > = (|\alpha \theta \rangle > , -|\alpha \theta \rangle > ) = (a|\alpha \theta \rangle > , b|\alpha \theta \rangle > ) \cdot e^{i\pi a|\alpha \theta \rangle > , b|\alpha \theta \rangle > > .
\]

By applying Eq. (7) to Eq. (6), we obtain the following relationship among the coefficients in Eq. (6)

\[
a_1 = b_2 \equiv a,
\]

\[
b_1 = a_2 \equiv b.
\]

Using these relationships, Eq. (6) is simplified as

\[
|\alpha \theta \rangle > = a|\alpha \theta \rangle > + b|-\alpha \theta \rangle > + c_1|s_1\rangle > ,
\]

\[
-|\alpha \theta \rangle > = b|\alpha \theta \rangle > + a|-\alpha \theta \rangle > + c_2|s_2\rangle > .
\]

Next, we multiply \(< \alpha \theta | \) or \(< -\alpha \theta | \) to Eq. (9a), and obtain the following equations

\[
< \alpha \theta | a|\alpha \theta \rangle > = a_1 + b_1|-\alpha \theta \rangle > ,
\]

\[
< -\alpha \theta | a\alpha \theta \rangle > = a_2 + b_2|-\alpha \theta \rangle > ,
\]

where the orthogonality between \(|s_1\rangle > \) and \(\{ |\alpha \theta \rangle > , -|\alpha \theta \rangle > \} \) is used. From Eq. (10), coefficients \(a\) and \(b\) are obtained as

\[
a = \frac{< \alpha \theta | a|\alpha \theta \rangle > - < -\alpha \theta | a\alpha \theta \rangle > < \alpha \theta | -|\alpha \theta \rangle > }{1 - < \alpha \theta | -|\alpha \theta \rangle > ^2},
\]

\[
b = \frac{< -\alpha \theta | a|\alpha \theta \rangle > - < \alpha \theta | a\alpha \theta \rangle > < -\alpha \theta | -|\alpha \theta \rangle > }{1 - < \alpha \theta | -|\alpha \theta \rangle > ^2}.
\]

In the above equations, each inner product is expressed as \(< \alpha \theta | a|\alpha \theta \rangle > = \exp\{\chi(1-e^{-2\Delta^2})\} \), \(< -\alpha \theta | a\alpha \theta \rangle > = \exp\{-\chi(1-e^{-2\Delta^2})\} \), and \(< \alpha \theta | -|\alpha \theta \rangle > = \exp\{\chi\} \), where \(\Delta^\theta = \theta_0 - \theta\). This consideration indicates that coefficients \(a\) and \(b\) are explicitly determined for a given \(\Delta^\theta\).

The USD measurement system applies the unitary operation \(\hat{U}\), that works as in Eq. (5), to the states expressed in Eq. (9) with \(|u_0\rangle > \), through which the states evolve as

\[
\hat{U}|\alpha \theta \rangle > |u_0\rangle > = \hat{U}(a|\alpha \theta \rangle > + b|-\alpha \theta \rangle > + c_1|s_1\rangle > \otimes |u_0\rangle > ,
\]

\[
\hat{U}|\alpha \theta \rangle > |u_0\rangle > = a\hat{U}|\alpha \theta \rangle > |u_0\rangle > + b\hat{U}|-\alpha \theta \rangle > |u_0\rangle > + c_1\hat{U}|s_1\rangle > |u_0\rangle > ,
\]

\[
\hat{U}|-\alpha \theta \rangle > |u_0\rangle > = \hat{U}(b|\alpha \theta \rangle > + a|-\alpha \theta \rangle > + c_2|s_2\rangle > \otimes |u_0\rangle > ,
\]

\[
\hat{U}|-\alpha \theta \rangle > |u_0\rangle > = a\hat{U}|\alpha \theta \rangle > |u_0\rangle > + b\hat{U}|-\alpha \theta \rangle > |u_0\rangle > + c_2\hat{U}|s_2\rangle > |u_0\rangle > .
\]

In the above equations, we do not know the states of \(\hat{U}|s_1\rangle > |u_0\rangle > \) and \(\hat{U}|s_2\rangle > |u_0\rangle > \) in explicit forms. However, they are orthogonal to the first two states, since \(\{s_1|\theta\rangle > , s_2|\theta\rangle > \} \) are orthogonal to \(\{ |\alpha \theta \rangle > , -|\alpha \theta \rangle > \} \). Thus, the first two states can be distinguished from \(\hat{U}|s_1\rangle > |u_0\rangle > \) and \(\hat{U}|s_2\rangle > |u_0\rangle > \) by mapping them to a space orthogonal to \(\hat{U}|s_1\rangle > |u_0\rangle > \) and \(\hat{U}|s_2\rangle > |u_0\rangle > \).

After the unitary operation expressed by Eq. (12), the first two states are extracted and then a measurement is performed on the auxiliary state. When the outcome is \(|u_0\rangle > , \) the probability of which is \((1-|\beta|^2)(|a|^2 + |b|^2))\), another measurement is conducted on the primary state, the outcome of which is \(|s_1\rangle > \) or \(|s_2\rangle > \). Then, the system judges that the measured state is \(|\alpha \theta \rangle > \) when the outcome is \(|s_1\rangle > \). In this discrimination procedure, the outcome \(|s_2\rangle > \) from \(|\alpha \theta \rangle > \) results in misjudgment. The probability that \(|\alpha \theta \rangle > \) is judged as \(|-\alpha \theta \rangle > \) is given by

\[
P_e = \frac{|b|^2}{|a|^2 + |b|^2},
\]

(13)

In addition, the probability of obtaining an answer is given by

\[
P_d = (1-|\beta|^2)(|a|^2 + |b|^2),
\]

(14)

which can differ from the ideal value of \((1-|\beta|^2)\).

Based on the above discussion, we calculate the probability of error \(P_e\) and the discrimination probability \(P_d\). The results are plotted in Figs. 5 and 6, respectively. Fig. 5 shows that notable errors indeed occur when the extracted phase \(\theta_0\) is different from the true value \(\theta\), and Fig. 6 shows that the discrimination probability becomes small when the error of the extracted phase increases.

**Fig. 5.** Probability of error in USD as a function of phase difference between estimated and true values, \(\Delta^\theta = \theta_0 - \theta\). The mean photon number per state is \(\mu = 0.1, 0.5,\) or 1.0. The result for \(\mu = 0.01\) almost overlaps onto that for \(\mu = 0.1\).
5. USD with phase tracking

The previous sections individually discussed and simulated the phase tracking performance and the USD performance. In this section, we evaluate the total performance of the measurement system where a fraction of incident signals is split for the phase tracking and then the USD measurement is conducted for the main signal based on the estimated carrier phase.

The estimated phase includes an error $\Delta \theta$ that follows a probability distribution function (PDF) as shown in Fig. 3, and the error probability and discrimination probability for a given phase error $\Delta \theta$ are calculated by Eqs. (13) and (14), respectively. Then, the total probability of error is evaluated as

$$P_{e}^{\text{total}} = \int_{-\infty}^{\infty} P_{d}(\Delta \theta)P_{\text{error}} \times d(\Delta \theta),$$

and the total discrimination probability is evaluated as

$$P_{d}^{\text{total}} = \int_{-\infty}^{\infty} P_{d}(\Delta \theta)P_{\text{discrimination}} \times d(\Delta \theta),$$

where $P_{d}(\Delta \theta)$ and $P_{\text{error}}(\Delta \theta)$ are the error probability and the discrimination probability for a given $\Delta \theta$ as plotted in Figs. 5 and 6, respectively, and $P_{\text{error}}$ is a PDF for the estimated phase relative to the center value, as plotted in Fig. 3. In the following calculations, $P_{\text{error}}$ is assumed to be Gaussian with a variance fitted to the numerically obtained values; i.e., the distribution denoted by the solid line in Fig. 3 is used as $P_{\text{error}}$.

An issue here is the splitting ratio for the phase tracking: $P_{e}(\Delta \theta)$, $P_{d}(\Delta \theta)$, and $P_{\text{error}}$ in Eqs. (15) and (16) depend on the mean photon number of a measured state, and the mean photon numbers available for the phase tracking and the USD measurement are determined by the splitting ratio for a given mean photon number that has been incident to the measurement system. To obtain high performance in an individual USD measurement, a small splitting ratio is preferred, whereas a large splitting ratio is desired for a small phase estimation error. Thus, an optimum splitting ratio should exist that can achieve the best USD performance in total. In order to examine this dependence of USD performance on the splitting ratio, we calculated the error probability and the discrimination probability as functions of the splitting ratio. The example plot is shown in Fig. 7. As the splitting ratio increases from 0, the error probability first drastically decreases and then slowly decreases beyond $\sim 0.3$, while the discrimination probability monotonically decreases.

The above simulation shows that the behaviors of the error probability and the discrimination probability are different as functions of the splitting ratio. In such a situation, what is the optimum splitting ratio is dependent on systems to which the USD measurement is applied. In case of the sequential attack against DPS-QKD [11], a discrimination error induces a quantum bit error in the legitimate receiver and thus its probability should be small. On the other hand, a high discrimination probability is preferable for inducing a small amount of quantum bit errors, as discussed in the next section. Then, the optimum splitting ratio is determined by the total amount of attainable information taking these two effects into account.

Finally, the total USD performance as a function of the linewidth of the coherent source is evaluated. The result is plotted in Fig. 8, where the horizontal axis is the linewidth multiplied by the time interval of incoming states, $\Delta f \times T$, considering that the phase fluctuation is determined by this parameter, as indicated in Eq. (3). The splitting ratio for the phase extraction is 0.3. For a large phase fluctuation, the error probability is large and the
discrimination probability is small. Such properties are quantitatively shown in the figure.

6. Impact on practical DPS-QKD

As described in the introduction section, the present work is motivated by the considerations that the performance of USD measuring phase fluctuating coherent states could degrade from that measuring ideal coherent states and, as a result, the performance of eavesdropping (specifically, sequential attack) against practical DPS-QKD systems using a laser source with a finite spectral linewidth could degrade from that conventionally supposed. Thus, the next concern is how the results obtained in the previous sections affect the DPS-QKD system performance suffering from the sequential attack. In the last of this paper, we mention this issue.

First, the DPS-QKD protocol and the sequential attack are briefly reviewed. Fig. 9 illustrates the system configuration, where a transmitter (Alice) sends a pulse train of weak coherent states phase-modulated by \{0, \pi\}, and a receiver (Bob) receives it with a one-pulse delay interferometer followed by two photon detectors. Which detector clicks is determined by the phase difference between adjacent pulses, from which a key bit is created. Against this QKD system, an eavesdropper (Eve) intercepts and measures the transmitted pulses with USD [11]. When she obtains a number of conclusive results in sequence, she resends a photon superpositioned over the same number of pulses via a lossless transmission line, which has the measured phase state for each pulse and the amplitudes with a Gaussian-shaped envelope. Otherwise, she resends nothing. During this eavesdropping, Bob occasionally receives a sequence of fake pulses. When he counts a photon from edges pulses of the sequence, a quantum bit error is introduced because of no interference at the edge pulses, from which the eavesdropping is revealed. This sequential attack is more effective than simple eavesdropping that resends a fake signal every time Eve obtains a conclusive measurement result (not in sequence), since the probability of the non-interfering detection at the edge pulses is lower and thus the eavesdropping-induced error probability is smaller, even though the unbalanced amplitudes slightly introduce quantum bit errors.

The effectiveness of the above sequential attack depends on the length of one sequence from Eve, such that a long sequence has a low probability of the non-interfering detection at the edge pulses and thus introduces a small quantum bit error rate (QBER). This length is determined by the discrimination probability of the USD employed by Eve, as described below. In the eavesdropping, Eve should not change Bob's photon counting rate \(P_{click}\) with this constraint, the probability of Eve's resending a pulse sequence \(P_{seq}\) should satisfy \(P_{seq} \geq P_{click}\), which is given by the probability of successive discrimination in the USD as \(P_{seq} = (P_d)^d\) where \(P_d\) is the discrimination probability for one pulse and \(d\) is the number of pulses from which conclusive results are sequentially obtained, i.e., the number of pulses in one sequence from Eve. The above consideration suggests that the length of one sequence is determined by the discrimination probability \(P_d\) such that a small \(P_d\) allows a small \(d\) and a small \(d\) causes a large QBER. Therefore, the degradation of the discrimination probability concluded in the previous sections reduces the effectiveness of the sequential attack.

In addition, the discrimination error in the USD also degrades the sequential attack. When the USD measurement gives a wrong answer to Eve, she resends a pulse sequence including a wrong phase state, which increases Bob's QBER.

Both the degradation of the discrimination probability and the discrimination error increase Bob's QBER, as described above. In such a situation, Eve attacks only a fraction of the transmitted signal so that the eavesdropping induced QBER does not exceed the original QBER in Alice–Bob system, and then the amount of information stolen by Eve is restricted. As a result, the amount of final key bits after privacy amplification increases, improving the DPS-QKD system performance. Unfortunately, quantitative evaluations of how the discrimination probability and the discrimination error rate reduces the amount of Eve's information and how the DPS-QKD system performance is improved will need further studies, which are outside the scope of the current paper.

7. Summary

Unambiguous state discrimination (USD) for a sequence of phase-modulated coherent states with a fluctuating and drifting carrier phase was described. A measurement system estimates the carrier phase from a fraction of incident states and then performs a USD measurement on the main signal states. The probability of error in the phase estimation and that in the USD measurement based on the erroneous estimated phase were formalized and simulated. The results obtained in this work will be useful in analyzing eavesdropping against practical DPS quantum key distribution systems where weak coherent light from a laser source with a finite spectral linewidth is phase-modulated by \{0, \pi\} and transmitted as an information carrier.

Acknowledgment

The authors would like to greatly thank to one of the reviewers of this paper, who gave them very fruitful comments and suggestions.

References


