HOKKAIDO UNIVERSITY

Title	Evaluation of the phase randomness of a light source in quantum-key-distribution systems with an attenuated laser
Author(s)	Kobayashi, Toshiya; Tomita, Akihisa; Okamoto, Atsushi
Citation	Physical Review A, 90(3), 32320 https://doi.org/10.1103/PhysRevA.90.032320
Issue Date	2014-09-18
Doc URL	https://hdl.handle.net/2115/57548
Rights	©2014 American Physical Society
Type	journal article
File Information	PhysRevA.90.032320.pdf

Hokkaido University Collection of Scholarly and Academic Papers : HUSCAP

Evaluation of the phase randomness of a light source in quantum-key-distribution systems with an attenuated laser

Toshiya Kobayashi,* Akihisa Tomita, and Atsushi Okamoto
Graduate School of Information Science and Technology, Hokkaido University Kita 14, Nishi 9, Sapporo 060-0814, Japan
(Received 7 July 2014; published 18 September 2014)

Phase-randomized light is one of the key assumptions in the security proof of the Bennett-Brassard 1984 (BB84) quantum-key-distribution (QKD) protocol using an attenuated laser. Though the assumption has been believed to be satisfied for conventional systems, it should be reexamined for current high-speed QKD systems. The phase correlation may be induced by the overlap of the optical pulses, the interval of which decreases as the clock frequency increases. The phase randomness was investigated experimentally by measuring the visibility of interference. An asymmetric Mach-Zehnder interferometer was used to observe the interference between adjacent pulses from a gain-switched distributed feedback laser diode driven at 10 GHz. Low visibility was observed when the minimum drive current was set far below the threshold, while interference emerged when the minimum drive current was close to the threshold. The theoretical evaluation on the impact of the imperfect phase randomization provides target values for the visibility to guarantee the phase randomness. The experimental and theoretical results show that secure implementation of decoy BB84 protocol is achievable even for the 10-GHz clock frequency by using the laser diode under proper operating conditions.

DOI: 10.1103/PhysRevA.90.032320 PACS number(s): 03.67.Dd, 03.67.Hk, 42.50.Ex, 42.55.Px

I. INTRODUCTION

Quantum key distribution (QKD) offers an unconditionally secure method to share a cryptographic key between remote parties. The Bennett-Brassard 1984 (BB84) protocol [1] is one of the most developed QKD protocols, the security proof of which has been well established [2–5]. Recent research on the security proof focused on more practical aspects, such as imperfections in a QKD apparatus. In the actual QKD equipment, the device characteristics deviate from the ideal ones. Keeping the secure key rate with imperfect devices is an important issue [6,7]. Since a practical single-photon source, assumed in the original BB84 protocol, is still unavailable, most QKD experiments have utilized light pulses from a laser diode (LD) after strong attenuation. The attenuated laser pulses contain two photons or more with a finite probability. The multiple photon states opened the way to an efficient eavesdropping method called a photon number splitting (PNS) attack [8]. Gottesman, Lo, Lütkenhaus, and Preskill (GLLP [9]) analyzed the security against this imperfection. An improved protocol called decoy-BB84 [10–12] was proposed to yield a better secure key rate than GLLP. The decoy-BB84 protocol provides not only unconditional security with the attenuated laser light, but also the universal composability [13–16].

The strongly attenuated laser light is often called weak coherent light. This term is misleading because the security analysis in the GLLP and decoy-BB84 articles assumes that the light source emits photons in a phase-randomized Poissonian state, which is a mixture of coherent states with uniformly distributed phases

$$\rho = \frac{1}{2\pi}\int_{-\pi}^{\pi} d\phi |\alpha e^{i\phi}\rangle\langle\alpha e^{i\phi}| = e^{-|\alpha|^2}\sum_{n=0}^{\infty}\frac{\alpha^{2n}}{n!}|n\rangle\langle n|. \quad (1)$$

The state is represented by a diagonal density matrix with respect to photon-number basis. Lo and Preskill [17] showed that, if the photon states were really weak coherent, discrimination of the bases used in the BB84 protocol would be easier. Recently, Tang *et al.* [18] showed that the phase information also increases distinguishability between decoy and signal pulses used in the decoy-BB84 protocol. Those reports have issued a warning about the phase correlation among the laser pulses; the phase correlation will increase the information leakage and thus reduce the secure key rate. Active phase randomization was proposed and implemented by Zhao *et al.* [19]. The effect of the partially randomized phase was also examined for a plug-and-play system [20].

Nevertheless, most experimentalists have not taken this warning seriously with a few exceptions [18–21]. Their common belief is that pulses from a gain-switched LD have no phase relationship to other pulses. Therefore, the phase of the light source is automatically randomized, as long as the one-way QKD architecture is employed. The mechanism of the phase randomization is as follows. In the gain-switched mode, each current pulse excites the semiconductor medium from loss to gain. A laser pulse is generated from seed photons originating from spontaneous emission because the photons from the previous lasing have vanished during the pulse interval. The phase of the spontaneous emission is random, so that the phase of the laser pulses should vary from one pulse to another. This is true when the previously lased photons disappear completely in the interval. However, if the photons survive until the next excitation, the lasing can be seeded by the remaining photons. Then, the phase of the laser pulse may relate to the previous one because the stimulated emission conserves the phase. The effect of the residual photons will emerge significantly by increasing the pulse repetition rate and narrowing the pulse interval. The state-of-the-art QKD systems operate at high clock frequencies over 1 GHz, along with the improvement of the photon detectors [22–24]. The clock frequency would further increase to meet demands for

*Present address: Seiko Epson Corporation.

 ©2014 American Physical Society

high bit-rate secure communication. The interval time thus decreases down to hundreds of picoseconds or even shorter. Furthermore, the drive current may not return to zero to improve the modulation response of the laser. It is unclear whether the assumption of the phase-randomized source still holds in QKD systems operated at several GHz-clock frequencies.

In this article, we examine the phase randomness of the light source at 10-GHz clock frequency. Section II A introduces an asymmetric interferometer setup to measure the phase correlation between the adjacent optical pulses. We recall the relation of the phase correlation to the visibility of the interference fringe. Section II B considers the effects of the partial coherence in state discrimination, which were analyzed by Lo-Preskill [17] and Tang *et al.* [18] for perfectly coherent states. We provide target values of the visibility, under which we can regard the light source as phase randomized. Section III shows the measured visibility of the interference fringe of the adjacent pulses from a LD. We controlled dc bias current to the LD, which determines the effective pulse interval and the minimum drive current to the LD. We examined the accuracy of the estimated values of visibility, and applied corrections to the estimation. Section IV considers the relation between the observed phase correlation and the operating conditions. We also investigate the phase correlation between the pulses in terms of the effective photon lifetime of the LDs.

II. THEORY

A. Relation between visibility and phase correlation

The phase relation of laser light can be characterized with an interferometer. Figure 1 illustrates a schematic of an asymmetric interferometer to observe interference between the adjacent optical pulses. We focus on measuring the interference between the adjacent pulses because the phases between the adjacent pulses are more correlated than those between more temporally separated pulses. Light pulses generated in the source enter the asymmetric interferometer, where the delay time is adjusted to the pulse period. The adjacent optical pulses are combined at the output. A phase modulator is placed in one arm of the interferometer to provide a phase difference φ between the paths. The signals are detected by a high-speed photodetector and accumulated by an averager. If a fixed phase relation between the adjacent pulses exists, the amplitude of the signal takes a definite value according to the phase difference between the optical paths. A clear interference fringe will be observed as φ varies. If the phase between the pulses is

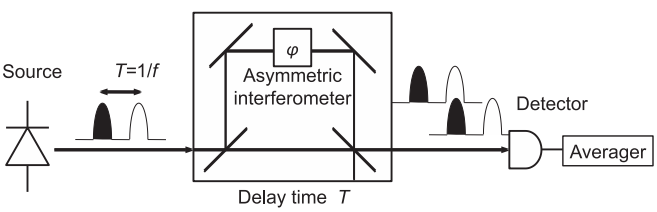

FIG. 1. A schematic illustration of a measurement apparatus for the phase correlation between the adjacent pulses. The delay time of the asymmetric interferometer is adjusted to the pulse period. The phase difference φ between the paths can be modulated.

random, the interference signal differs from pulse to pulse. Then the interference fringe will disappear after accumulation. The visibility of interference Θ, which represents the degree of the phase correlation, is defined by

$$0 \leqslant \Theta := \frac{I_{\max} - I_{\min}}{I_{\max} + I_{\min}} \leqslant 1, \tag{2}$$

where $I_{\max}$ stands for the peak (maximum), and $I_{\min}$ the valley (minimum) of the interference fringe. As the phase correlation becomes stronger, the visibility gets closer to 1.

In the following, we recall a relation between the visibility and the phase correlation [25]. The output intensity of the interferometer is given by

$$I(\varphi) \propto \mathcal{E}^2\{|a_A|^2 + |a_B|^2 + |a_A a_B| \exp[i(\theta + \varphi)] + \text{c.c.}\}, \tag{3}$$

where the coefficient $\mathcal{E} = \sqrt{\hbar\omega/2\epsilon_0 V}$ carries the dimension of the electric field. The complex amplitudes a_A and a_B represent the fields provided from paths A and B, respectively. In the asymmetric interferometer, the fields a_A and a_B correspond to those of the adjacent pulses. The relative phase between the pulses is given by θ. The third and fourth terms of Eq. (3) are responsible for the interference. Taking an average over an ensemble, we obtain the interference terms as

$$\langle a_A a_B \rangle \langle e^{i\theta} \rangle e^{i\varphi} + \text{c.c.}, \tag{4}$$

where we assume the phase difference φ varies slowly, while the relative phase θ is a probabilistic variable. Equation (4) shows that the interference visibility is governed by the expectation value of the relative phase $\langle \exp[i\theta] \rangle$. If the distribution of the phase obeys a Gaussian probability density function with the central value θ_0 and the standard deviation σ

$$g(\theta, \theta_0) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left[-\frac{(\theta - \theta_0)^2}{2\sigma^2}\right], \tag{5}$$

the expectation value is given by

$$\langle e^{i\theta} \rangle = \int_{-\infty}^{\infty} e^{i\theta} g(\theta, \theta_0) d(\theta) = \exp\left[-\frac{\sigma^2}{2}\right] e^{i\theta_0}. \tag{6}$$

The Gaussian probability distribution holds for LDs because the light field vector in the phase space is kicked by a number of photons generated by spontaneous emission [26]. Since the spontaneous emission occurs independently, the kicks force the field vector to walk randomly around the original position. Using Eqs. (3) and (6), we relate the visibility to the standard deviation of the phase distribution as

$$\begin{aligned} \Theta &= \frac{\langle |a_A a_B| \rangle (\langle e^{i\theta} \rangle e^{i\varphi_{\max}} - \langle e^{i\theta} \rangle e^{i\varphi_{\min}} + \text{c.c.})}{2\langle |a_A|^2 + |a_B|^2 \rangle} \\ &= \frac{4|a_A a_B| \exp\left[-\frac{\sigma^2}{2}\right]}{2(|a_A|^2 + |a_B|^2)} = \exp\left[-\frac{\sigma^2}{2}\right]. \end{aligned} \tag{7}$$

The interference signal takes the maximum value at $\theta_0 + \varphi_{\max} = 0$ and the minimum value at $\theta_0 + \varphi_{\min} = \pi$. We assume $|a_A| = |a_B|$ for simplicity in deriving the last equation of Eq. (7). As expected, the visibility decreases rapidly with increasing phase fluctuation σ. The analysis given above uses the classical complex amplitude of the electric field because the laser field can be well approximated with a classical

field. The wave properties of the field will not be altered by attenuation. Furthermore, the analysis using quantum operators will provide a similar description.

B. Impact of phase correlation

In the following, we consider the impact of phase correlation to provide criteria to guarantee the security of decoy-BB84 with a LD light source. As stated in the Introduction, the phase correlation enhances the distinguishability of the states, which are expected to be indistinguishable in the ideal situation [17,18]. The following calculation will treat two issues on the state discrimination: one is between the states of different bases and the other is between the signal and decoy pulses.

Most security proofs of BB84 rely on the assumption that the density matrix of one basis is indistinguishable to another. The distinguishability of two density matrices, sometimes called the imbalance of the quantum coin [9], helps the eavesdropper (Eve) to distinguish the state encoding. GLLP [9] described the imbalance in terms of the fidelity between the density matrices, and analyzed its effects on the security. Though the imbalance of the quantum coin often refers to the state preparation flaws, Lo and Preskill [17] showed that phase correlation also enhances the distinguishability. The imbalance of the quantum coin Δ is given by

$$\Delta = \frac{1 - F(\rho_X, \rho_Z)}{2}, \tag{8}$$

where the fidelity of the density matrices in X coding and Z coding is defined by

$$F(\rho_X, \rho_Z) = \mathrm{Tr}\left(\rho_Z^{1/2} \rho_X \rho_Z^{1/2}\right)^{1/2}. \tag{9}$$

Further, since Eve may exploit the channel loss, we should recalculate the imbalance to keep security as

$$\Delta' = \frac{\Delta}{\eta\mu} \tag{10}$$

for a given transmittance of the channel η and the average photon number μ of the source. Recently, Tamaki *et al.* [27] show that GLLP analysis is too conservative, and propose a loss-tolerant proof even with state preparation flaws. We here calculate Δ because it still provides a comprehensive measure of the state distinguishability. We can obtain Δ' from Δ based on the channel conditions, if we follow the GLLP analysis. The density matrices of the partially phase-randomized coherent states are expressed by

$$\begin{aligned}
\rho_Z &= \frac{1}{2}\int \left(|\sqrt{\mu}e^{i\theta}\rangle_F\langle\sqrt{\mu}e^{i\theta}| \otimes |0\rangle_S\langle 0| + |0\rangle_F\langle 0| \otimes |\sqrt{\mu}e^{i\theta}\rangle_S\langle\sqrt{\mu}e^{i\theta}|\right) g(\theta,\theta_0)\,d\theta \\
&= \frac{1}{2}e^{-\mu}\left(\sum_{M,N} \frac{\mu^{(M+N)/2} e^{-(M-N)^2\sigma^2/2} e^{i(M-N)\theta_0}}{\sqrt{M!N!}} |M\rangle_F\langle N| \otimes |0\rangle_S\langle 0| \right. \\
&\quad \left. + |0\rangle_F\langle 0| \otimes \sum_{M,N} \frac{\mu^{(M+N)/2} e^{-(M-N)^2\sigma^2/2} e^{i(M-N)\theta_0}}{\sqrt{M!N!}} |M\rangle_S\langle N|\right),
\end{aligned} \tag{11}$$

$$\begin{aligned}
\rho_X &= \frac{1}{2}\int \left(\left|\sqrt{\frac{\mu}{2}}e^{i\theta}\right\rangle_F\left\langle\sqrt{\frac{\mu}{2}}e^{i\theta}\right| \otimes \left|\sqrt{\frac{\mu}{2}}e^{i\theta}\right\rangle_S\left\langle\sqrt{\frac{\mu}{2}}e^{i\theta}\right| + \left|\sqrt{\frac{\mu}{2}}e^{i\theta}\right\rangle_F\left\langle\sqrt{\frac{\mu}{2}}e^{i\theta}\right| \otimes \left|-\sqrt{\frac{\mu}{2}}e^{i\theta}\right\rangle_S\left\langle-\sqrt{\frac{\mu}{2}}e^{i\theta}\right|\right) g(\theta,0)\,d\theta \\
&= \frac{1}{2}e^{-\mu}\sum_{M,N}\left(\frac{\mu}{2}\right)^{(M+N)/2} e^{-(M-N)^2\sigma^2/2} \sum_{m,n} \frac{1+(-1)^{m-n}}{\sqrt{(M-m)!m!(N-n)!n!}} |M-m\rangle_F\langle N-n| \otimes |m\rangle_S\langle n|,
\end{aligned} \tag{12}$$

where the subscripts F and S denote fast and slow components of the time-bin qubits. A finite value of θ_0 is assumed for Z coding, while it is set to zero for X coding. Since only the relative phase between the two coding affects the distinguishability, this setting will not lose generality. The factor $\exp[-(M-N)^2\sigma^2/2]$ decreases rapidly for large σ, and only the $M = N$ terms survive. In this phase-randomized limit, the density matrices (11) and (12) coincide with those of the mixture of M-photon number states after the state preparation.

The imbalance of the quantum coin Δ can be calculated with Eq. (8) and the density matrices (11) and (12). The two states ρ_Z and ρ_X are most distinguishable when the central value of the phase $\theta_0 = \pi$, and least distinguishable when $\theta_0 = 0$. We calculated the fidelity numerically with the density matrices in the photon-number-state basis truncated to a finite photon number $N_{\max}$. We changed the number of bases to check the accuracy of the calculation. Since the average photon number is small, the results converged rapidly at $N_{\max} = 8$. We thus set $N_{\max} = 16$ in the following calculation. Figure 2 shows the calculated values of Δ as a function of the standard deviation of the phase distribution σ for the average photon numbers μ of 0.09 and 0.01. The imbalance of the quantum coin decreases as the standard deviation increases. For small standard deviation, that is, less phase randomized, the imbalance of the quantum coin for $\theta_0 = \pi$ is larger than that for $\theta_0 = 0$. The effect of the initial phase offset vanishes for large standard deviation, as the phases of the states become randomized. As seen in Fig. 2, Δ converges to finite values for large standard deviation. The relative errors from the asymptotic values fall below 10^{-2}, when the standard deviation exceeds the following values: 2.9 for $\mu = 0.01$ and $\theta_0 = 0$, 2.6 for $\mu = 0.01$ and $\theta_0 = \pi$, 3.2 for $\mu = 0.09$ and $\theta_0 = 0$, and 2.9 for $\mu = 0.09$ and $\theta_0 = \pi$. The values of standard deviation, 2.6, 2.9, and 3.2, correspond to the visibility of 0.034, 0.015, and 0.006, respectively, which are estimated with Eq. (7). Therefore, target visibility values would be 0.015 for

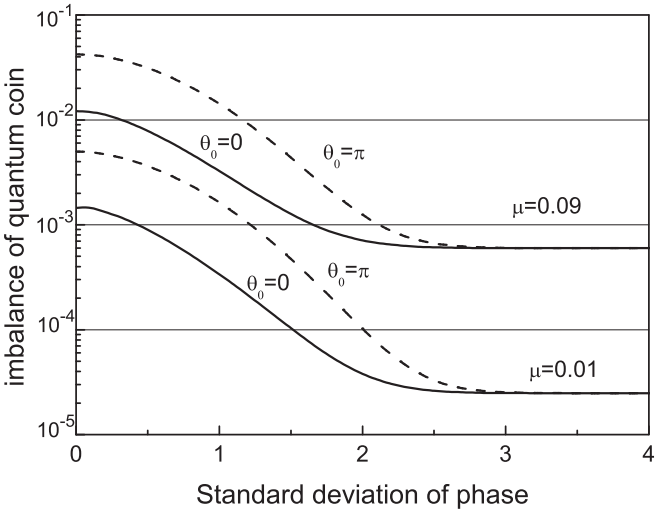

FIG. 2. The imbalance of the quantum coin, defined by $\Delta = [1 - F(\rho_Z, \rho_X)]/2$, as a function of standard deviation of phase distribution. Solid lines represent Δ for the difference of central phase value $\theta_0 = 0$, broken lines for $\theta_0 = \pi$.

$\mu = 0.01$ and 0.006 for $\mu = 0.09$ in terms of the imbalance of the quantum coin.

The imbalance of the quantum coin does not reach zero in the completely phase-randomized limit. The asymptotic value for $\mu = 0.09$ is larger than that for $\mu = 0.01$ due to the multiple photon contributions, which increase the distinguishability between the two states. It would be instructive to write the density matrices (11) and (12) in the completely phase-randomized limit as a sum of n-photon contributions; $\rho_Z = \rho_Z^{(0)} + \rho_Z^{(1)} + \rho_Z^{(2)} + \cdots$ and $\rho_X = \rho_X^{(0)} + \rho_X^{(1)} + \rho_X^{(2)} + \cdots$. The single- and two-photon contributions are given by

$$\rho_Z^{(1)} = \frac{1}{2} e^{-\mu} \mu (|1\rangle_F\langle 1| \otimes |0\rangle_S\langle 0| + |0\rangle_F\langle 0| \otimes |1\rangle_S\langle 1|), \quad (13)$$

$$\rho_Z^{(2)} = \frac{1}{2} e^{-\mu} \frac{\mu^2}{2} (|2\rangle_F\langle 2| \otimes |0\rangle_S\langle 0| + |0\rangle_F\langle 0| \otimes |2\rangle_S\langle 2|), \quad (14)$$

$$\rho_X^{(1)} = \frac{1}{2} e^{-\mu} \mu (|1\rangle_F\langle 1| \otimes |0\rangle_S\langle 0| + |0\rangle_F\langle 0| \otimes |1\rangle_S\langle 1|), \quad (15)$$

$$\rho_X^{(2)} = \frac{1}{2} e^{-\mu} \frac{\mu^2}{2} \left(\frac{1}{2} |2\rangle_F\langle 2| \otimes |0\rangle_S\langle 0| + \frac{1}{2} |2\rangle_F\langle 0| \otimes |0\rangle_S\langle 2| + \frac{1}{2} |0\rangle_F\langle 2| \otimes |2\rangle_S\langle 0| + \frac{1}{2} |0\rangle_F\langle 0| \otimes |2\rangle_S\langle 2| + |1\rangle_F\langle 1| \otimes |1\rangle_S\langle 1| \right). \quad (16)$$

As seen in Eqs. (13) to (16), the single-photon contributions $\rho_Z^{(1)}$ and $\rho_X^{(1)}$ are identical. The two-photon contribution $\rho_Z^{(2)}$ is given by diagonal elements describing that either the fast or slow pulse component contains two photons. On the other hand, $\rho_X^{(2)}$ contains off-diagonal elements and a diagonal element describing that each fast and slow pulse component contains one photon in addition to the diagonal elements identical to $\rho_Z^{(2)}$. Multiple photon contributions make the density matrices ρ_Z and ρ_X distinguishable by those additional elements in $\rho_X^{(k)}$, $(k \geqslant 2)$.

The decoy method uses the states with different average photon number, called signal and decoy. A key assumption of the decoy method is that Eve cannot distinguish the signal pulses from the decoy. In other words, Eve can measure the photon number contained in a pulse, but cannot measure the average photon number of an individual pulse. Then Eve's strategy is limited to the one that depends only on the photon number of the pulse. The security proof of the decoy method should consider such a limited eavesdropping strategy. Tang *et al.* [18] pointed out that phase correlation between the signal and decoy states enable an unambiguous-state-discrimination (USD) measurement. The final key generated by the non-phase-randomized system can be compromised by combing the USD measurement and the PNS attack. When the phase is partially randomized, the USD measurement is no longer possible. However, if Eve allows finite probability to obtain inconclusive results P_{inc}, she can still increase the probability of the correct decision P_C [28]. In the Appendix, we derive the optimum positive-operator-valued measure (POVM) to discriminate the signal state from the decoy state for partially coherent states. The results of the POVM enable to extend the analysis presented by Tang *et al.* [18].

We here investigate the fidelity between the signal and decoy states described by

$$\rho_1 = e^{-a_1^2} \sum_{m,n} \frac{a_1^{m+n} e^{-(m-n)^2\sigma^2/2} e^{i(m-n)\theta_0}}{\sqrt{m!n!}} |m\rangle\langle n|, \quad (17)$$

$$\rho_2 = e^{-a_2^2} \sum_{m,n} \frac{a_2^{m+n} e^{-(m-n)^2\sigma^2/2}}{\sqrt{m!n!}} |m\rangle\langle n|. \quad (18)$$

Following Tang *et al.* [18], we consider only the fast component of the time-bin qubits, which carries no information on the key-bit value. The density matrices ρ_1 and ρ_2 describe partially phase-randomized coherent states with the average photon numbers $\mu = 2a_1^2$ and $\nu = 2a_2^2$, respectively. We calculated the fidelity numerically by truncating the number of a basis to a finite photon number $N_{\max} = 16$, as in the imbalance of the quantum coin. Figure 3 shows the distinguishability defined as $[1 - F(\rho_1, \rho_2)]/2$ with the fidelity of ρ_1 and ρ_2. The distinguishability decreases as the phase randomization, and asymptotically reaches the value for the completely phase-randomized states. The relative discrepancy between the two became less than 10^{-2} for $\sigma > 2.5$, which corresponds to the visibility of 0.044. This value would be a target visibility in terms of the signal-decoy discrimination.

The fidelity was calculated for $\theta_0 = \pi$ because the coherent states with the initial phase $\theta_0 = 0$ yield the same fidelity as the completely phase-randomized states. However, the coherent states still provide an advantage to the eavesdropper to perform an individual attack as seen in the Appendix.

In this section, we have derived criteria of the phase randomness and thus the interference visibility. The target values depend on the average photon numbers. Moreover, the eavesdropping methods are not exhausted with those considered above, so that the target values may be further lowered. Nevertheless, we believe that the present analysis

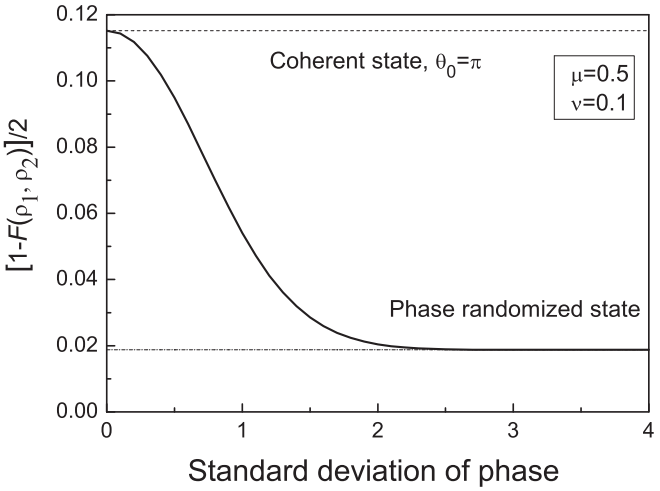

FIG. 3. Distinguishability $[1 - F(\rho_1,\rho_2)]/2$ between the signal and decoy states as a function of the standard deviation of phase. Calculation was done for the partially phase randomized states of average photon number 0.5 (signal) and 0.1 (decoy). Solid line represents the calculated fidelity for $\theta_0 = \pi$. Dashed-dot line stands for the distinguishability between the completely phase randomized states, and dashed line between coherent states with $\theta_0 = \pi$.

covers a wide range of eavesdropping, and the values estimated here should be good indications.

We observe that the initial phase offset $\theta_0 = \pi$ increases the distinguishability between the bases and between signal and decoy. A finite initial phase may appear in some implementations. First, we show an example using the Mach-Zehnder interferometer for state preparation and pulse intensity modulation. In a conventional two-electrode Mach-Zehnder modulator, the output field is determined by the phases ϕ_1 and ϕ_2 applied to the arms [29] as

$$E_{\text{out}} \propto \exp\left[i\frac{\phi_1+\phi_2}{2}\right]\cos\left(\frac{\phi_1-\phi_2}{2}\right). \tag{19}$$

Therefore, the initial phase is given by the difference of $(\phi_1 + \phi_2)/2$. Suppose the intensity of the decoy state is half of that of the signal. Setting $(\phi_1,\phi_2) = (-\pi/2, -\pi/2)$ for the signal and $(\phi_1,\phi_2) = (3\pi/4,\pi/4)$ for the decoy will provide $\theta_0 = \pi$. Similarly, the initial phase offset can be also finite in state preparation, depending on the setting of ϕ_1 and ϕ_2. For the second example, consider an absorption-type intensity modulator, which can be used in the decoy method. It also provides an initial phase offset because the refractive index changes with the absorption coefficient, following the Kramers-Kronig relationship. In this case, however, the initial phase offset would be smaller than π. For the third example, the path length can be different to provide an arbitrary initial phase, if we employ an independent light source for each state or each intensity. The last example may be applied in decoy method; the intensities of the signal and decoy states are determined with independent fixed attenuators to obtain accurate intensities, which are important for channel estimation. These examples show careless implementations would increase the risk of eavesdropping.

III. EXPERIMENT

The phase-correlation measurement system consists of the interferometer and the pulsed light source to be tested. We employed the configuration similar to the one depicted in Fig. 1. The source was a distributed feedback (DFB) LD (NEL, NLK5C5EBKA,) which was designed for 10-GHz direct modulation to emit optical pulses in a single longitudinal and transversal mode. It lases around the wavelength of 1560 nm at the threshold current of 9.5 mA. The LD was driven by the combination of a 10-GHz sinusoidal current (I_{ac}) and a dc bias current (I_{dc}.) The sinusoidal current injected to the laser is expressed by

$$I_{\text{ac}} = \frac{I_{\text{pp}}}{2}\cos(2\pi f t + \phi_{\text{LD}}), \tag{20}$$

where I_{pp} stands for the peak-to-peak value of the sinusoidal current. The current changes periodically with the frequency $f = 10$ GHz and an initial phase ϕ_{LD}. The sinusoidal signal from a pulse-pattern-generator (PPG) was amplified to a fixed amplitude $V_{\text{pp}} = 4.615$ V. We estimated the peak-to-peak ac current to the LD as $I_{\text{pp}} = 92.3$ mA, considering the 50-Ω load resistance. However, in a high-frequency region such as 10 GHz, the emerging effects of parasitic impedances of the LD and the circuit may reduce the current injected into the LD active layer. To correct this effect, we measured the modulation response of the LD with a network analyzer and a 45-GHz bandwidth photodetector. The resonant-like frequency was about 12 GHz in this measurement, so that the intrinsic response of the LD has little affect on the modulation response up to 10 GHz. It was found that the optical power response of the LD decreased by about 1 dB at 10 GHz from that at 100 MHz. Since the optical power is proportional to the injected current, we regard the reduction of the response as the decrease of the current with the same proportion. Then the net current I_{net} is reduced from the nominal value I_{nom} by $10\log_{10}(I_{\text{net}}/I_{\text{nom}}) = -1$. The net ac current thus swung by $I_{\text{pp}} = 92.3 \times 0.794 = 73.3$ mA, where $10^{-1/10} \simeq 0.794$. The total current to the LD is expressed by $I_{\text{ac}} + I_{\text{dc}}$. The operating condition of the LD was controlled by changing the DC bias current I_{dc}. We define the minimum drive current defined by $I_{\text{min}} = -I_{\text{pp}}/2 + I_{\text{dc}}$, which refers to the drive current at the bottom of the ac current. In the following, we use normalized excitation to describe the operating condition. The normalized minimum excitation is defined by

$$\Lambda = \frac{I_{\text{min}} - I_{\text{th}}}{I_{\text{th}}}. \tag{21}$$

As mentioned, the laser threshold current was $I_{\text{th}} = 9.5$ mA. The LD was always turned on when $\Lambda > 0$. The LD was turned off during the pulse interval, when $\Lambda < 0$. The turn-off duration increases as the dc bias current decreases, which is obtained as a solution of $I_{\text{ac}} + I_{\text{dc}} = I_{\text{th}}$ with Eq. (20). The LD was reversely biased and no current was injected at the minimum, when $\Lambda < -1$. In the present experiment, $\Lambda = 0$ and $\Lambda = -1$ correspond to $I_{\text{dc}} = 46.15$ mA and $I_{\text{dc}} = 36.75$ mA, respectively.

We employed a commercially available asymmetric Mach-Zehnder interferometer (AMZI) module (Kylia, WT-MINT-M-L) to obtain interference between the adjacent pulses at

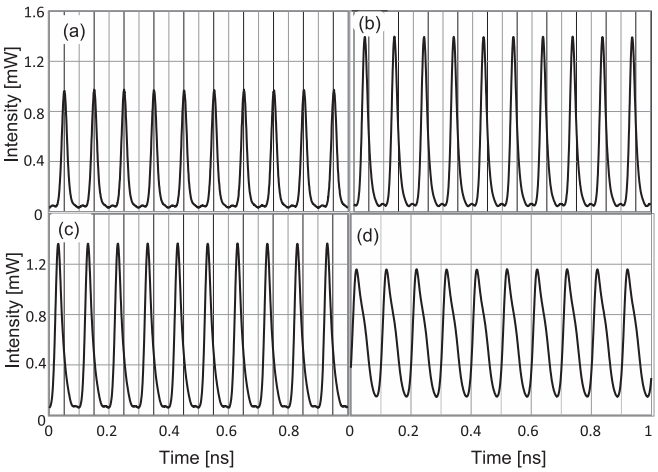

FIG. 4. Waveforms of the LD pulses. The values of the normalized minimum excitation are as follows: (a) $\Lambda = -1.6$, (b) $\Lambda = 0.074$, (c) $\Lambda = 0.49$, and (d) $\Lambda = 2.6$.

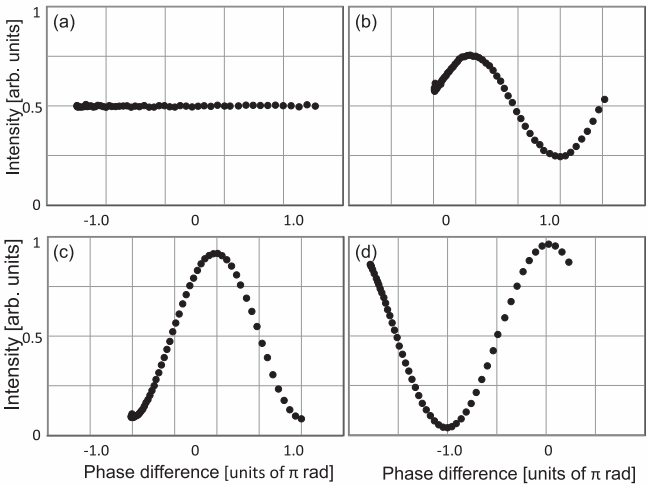

FIG. 5. Interference fringes for several values of the normalized minimum excitation: (a) $\Lambda = -1.6$, (b) $\Lambda = 0.074$, (c) $\Lambda = 0.49$, and (d) $\Lambda = 2.6$.

10 GHz, which was developed as a demodulator for 10-GHz differential phase shift keying (DPSK.) The phase difference between the optical paths was modulated with a phase shifter integrated in the AMZI module. The signal was accumulated for 256 samples and measured with a sampling oscilloscope of 40-GHz optical bandwidth to observe the interference fringe. The output of the AMZI was attenuated by an optical attenuator to avoid saturation of the photodetector. The peak and valley intensities of the accumulated interference fringes were measured.

Figure 4 shows the observed waveforms of light pulses for (a) $\Lambda = -1.6$, (b) $\Lambda = 0.074$, (c) $\Lambda = 0.49$, and (d) $\Lambda = 2.6$, where the minimum drive current $I_{\min}$ was (a) below the threshold, (b) near the threshold, (c) above the threshold, and (d) far above the threshold. By setting the $I_{\min}$ close to the threshold, sharp and intense pulses were obtained as shown in Figs. 4(b) and 4(c). When the $I_{\min}$ was far above the threshold, the laser output reflected the input current waveform as in Fig. 4(d). The LD was no longer operated in the gain-switched mode in this dc bias region.

The observed interference fringes are shown in Fig. 5. Clear interference fringe was observed for a large excitation ($\Lambda = 2.6$) with the visibility close to unity ($\Theta = 0.93$,) while no clear interference fringe was observed for a excitation ($\Lambda = -1.6$.) The results indicate that the phases of the pulses for a gain-switched LD are still random even at 10-GHz pulse frequency for small minimum drive currents. In Fig. 5, we show the normalized values of the output signal to set the averaged value to 0.5; (Intensity) = (Observed power)/(Averaged Power). Due to the limitation of the device, the range of phase modulation was only slightly larger than 2π. The phase difference of the interferometer was stable enough for the short time to obtain an interference fringe. It was not stable for days, so that the origin of the phase difference varied as shown in Figs. 5(a) to 5(d.)

IV. DISCUSSION

We consider origins of errors to examine the accuracy of the results obtained in the experiment. First, the imperfections in the interferometer, such as fluctuation of path length, imbalanced branch ratio of the beam splitters, polarization rotation, and depolarization will reduce the visibility. In fact, we obtained the visibility of only 0.95 with continuous wave (CW) light emitted from the LD excited solely by the dc current of 50 mA, which was far above the threshold. The LD linewidth implies that the phase of the CW light should be well conserved in the time scale of 100 ps. Therefore, we should consider the obtained visibility was affected mainly by the imperfections in the interferometer. Assuming the imperfections are the same throughout the experiment, we should correct the visibility by multiplying 1.05. Second, the system noise affects the visibility estimation. In the present experiment, we recorded the observed maximum and minimum values, which included noise. Thus, the estimated values of visibility should have been overestimated from the real ones. The effect of noise emerges significantly for small visibilities. From the conservative points of view for the security certification, this overestimation causes no harm. However, it is undesirable for the practical use because we may lose some amount of final key by unnecessary privacy amplification. To obtain a better estimation, we examined the results showing low visibilities by magnifying the scale of intensity, as shown in Fig. 6. The error bars originated mainly from the noise of the sampling oscilloscope. The observed signal-to-noise ration were about 17 dB, where the average intensity was normalized to 0.5. The r.m.s. value of the noise suggests that it would be hard to measure the visibility less than 0.02. Nevertheless, a periodic dependence on the phase difference is seen in Fig. 6(b). By taking the center values denoted by the squares in Fig. 6, we could fit the interference fringe with

$$I(\varphi) = A[1 + \Theta\cos(\varphi + \varphi_0)]. \tag{22}$$

The result of the fitting is depicted as a thick solid line in Fig. 6. For excitation of $\Lambda = -1.6$ [Fig. 6(a)], the best-fitting value for Θ was 0.004, which reflected very weak periodic dependence on the phase difference. The fitted visibility was much less than the one estimated from the maximum and

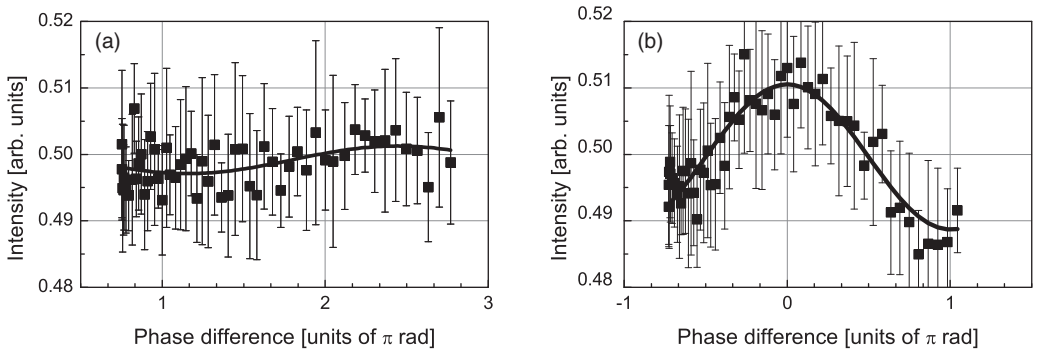

FIG. 6. Magnified view of the interference fringe. (a) $\Lambda = -1.6$ and (b) $\Lambda = -1.2$. Solid lines denote the fitted curve. The fitted values of the visibility were 0.004 and 0.02.

minimum intensities, 0.014. For Fig. 6(b), $\Lambda = -1.2$, the fitted value of the visibility was 0.022, while the estimated one was 0.030. The fit was done well, as we consider the 95% confidence interval of the fitting value [0.019, 0.025]. The discrepancy between the fitted and estimated visibility decreases as the visibility increases. On the basis of the above, we conclude that the present experimental setup can detect the visibility down to 0.02. The effect of the noise should be reduced by using low noise front-end and by increasing number of accumulation to obtain a lower measurement limit of the visibility.

We applied the corrections discussed above. The results are summarized in Fig. 7, where the visibility is plotted as a function of the normalized minimum excitation. Figure 7 shows the visibility increases as the minimum excitation increases. It raises steeply around $\Lambda = 0$, where the LD was always turned on. The interference fringe almost disappeared when $\Lambda < -1$, i.e., the LD was reversely biased at the bottom. In particular, for $\Lambda = -1.6$ ($I_{dc} = 30.95$ mA,) the visibility was fitted to 0.004, which satisfied the strictest criterion given in Sec. II B. Though the fitted value may not be accurate as

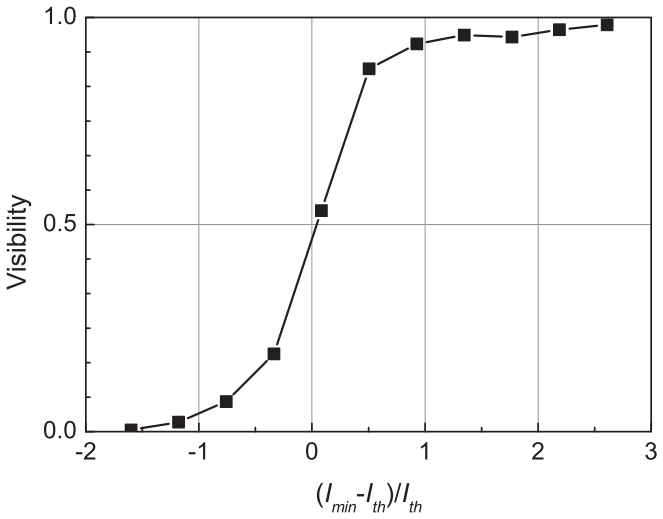

FIG. 7. Visibility of the interference as a function of the normalized minimum excitation Λ. For $\Lambda > 0$, the LD was always turned on. The LD was reversely biased at the bottom of the pulse, when $\Lambda < -1$.

described above, the visibility satisfied the target values 0.015 for the imbalanced coin at $\mu = 0.01$, and 0.044 for the decoy state discrimination. It should be noted that the interference fringe was observed even when the LD was turned off during the pulse interval. When the minimum drive current was set in the range $-1 < \Lambda < 0$, the light source can be no longer be regarded as phase randomized in terms of the imbalance of the quantum coin. For example, the visibility reached 0.08 for $\Lambda = -0.76$. If we care only about the laser waveform (as is common in most applications,) we may set the bias to the value where the minimum drive current is close to the LD threshold because it yields the best waveform as seen in Figs. 4(b) and 4(c). Unfortunately, the phases of the pulses are correlated under this operating condition. The observed visibility was 0.534 for the case (c), where $\Lambda = 0.074$. The corresponding standard deviation of the phase distribution is about $\sigma = 1.12$. We then need to sacrifice more bits to guarantee the security of final key in the privacy amplification.

In the following, we consider the dependence of the phase correlation on the minimum excitation in terms of effective photon life time. As described before, if the photons survive during the pulse interval, the phase may correlate with the previous pulses. Typical photon life time τ_{ph} of a LD cavity is several picoseconds. The effective photon lifetime can be increased by stimulated emission, even when the excitation is insufficient for lasing. Photon density S in the cavity will decay approximately as

$$\frac{dS}{dt} = \left(\Gamma g(n) - \frac{1}{\tau_{ph}}\right)S + n_{sp}, \tag{23}$$

where $\Gamma g(n)$ denotes the modal gain for the lasing mode at the carrier density n. The term n_{sp} represents the contribution of the spontaneous emission to the lasing mode. The photon field is governed by the spontaneous emission, when the photon density decreased to satisfy $S \leqslant n_{sp}$. Then, the phase of the light field becomes random.

The details of the dynamics are described with involved nonlinear coupled equations on photon density and carrier density. Roughly speaking, though, the photon field loses the phase information after the effective photon life time given by $[\Gamma g(n) - 1/\tau_{ph}]^{-1}$, as seen in Eq. (23). Since $[\Gamma g(n) - 1/\tau_{ph}]\tau_{ph}$ equals approximately to $(I - I_{th})/I_{th}$, the effective photon lifetime scales with the normalized excitation. When the normalized minimum excitation Λ exceeds zero,

the effective photon life time becomes infinite. Then, the photons of previous pulses remain to contribute the phase correlation. Even when Λ is less than zero, the photons may survive during the interval and contribute to the next lasing. For example, at $I_{dc} = 42.95$ mA or $\Lambda = -0.33$, the effective photon the time life is about three times as large as the cavity life time at the bottom of the pulse. The turn-off duration is calculated as 13 ps from Eq. (20). If we take the cavity life time as $\tau_{ph} = 3$ ps, the effective photon lifetime increased to 10 ps, which is comparable to the turn-off duration. Therefore, we suppose that a nonnegligible number of photons may have remained under this condition. In fact, the observed visibility was 0.188, indicating some phase correlation. For small excitation satisfying $\Lambda < -1$, the LD is reversely biased, and the effective photon life time should be equal to the cavity life time at least in the bottom of excitation. The calculated turn-off duration is as long as 30 ps for $\Lambda = -1.6$. Under this condition, photons should have disappeared during the pulse interval, and the lasing phase became random, as was observed.

We see that the observed dependence of the visibility on the excitation can be explained with the relation between the effective photon life time and the turn-off duration. A guide to the operating condition is summarized that the effective photon lifetime should be less than the turn-off duration. As described above, this condition is satisfied with $\Lambda < -1$ for 10 GHz.

The clock frequency of current high-speed QKD experiments does not exceed 1–2 GHz, which corresponds to the pulse intervals of 0.5 to 1 ns. The operating condition of the laser is expected to be much relaxed for such long interval. It is enough to set the minimum excitation slightly below the threshold; $\Lambda < -0.006$ for 2 GHz and $\Lambda < -0.003$ for 1 GHz, respectively, from the above consideration. In fact, we observed phase randomization of a gain-switched LD operated at 1 GHz for a wide range of the dc bias current (preliminary results were reported in [30].) Yuan *et al.* [21] also obtained the phase-randomized laser oscillation with a fairly high bias current at 2 GHz to demonstrate a random number generator utilizing interference signals between the adjacent pulses.

V. CONCLUSION

In the BB84 protocol using an attenuated laser source, the secure key generation rate is lowered if the source emits non-phase-randomized optical pulses. We evaluated the effect of the phase correlation in terms of the imbalance of the quantum coin and the discrimination of the decoy from the signal pulses, for the partially coherent states. We obtained criteria for the source to be regarded as phase randomized. The target values for the visibilities were 0.006 and 0.015 in terms of the imbalance of the quantum coin at $\mu = 0.09$ and at $\mu = 0.01$, and 0.044 in terms of the discrimination of the decoy pulses ($\nu = 0.1$) from the signal ($\mu = 0.5$.)

We constructed a phase-correlation test system to measure visibility of the interference fringe between the adjacent pulses using an asymmetric Mach-Zehnder interferometer. It enables to evaluate the phase correlation between the laser pulses experimentally at a high clock frequency of 10 GHz. We found that the phase correlation of the pulses from a LD depends on the operating condition. The target values were satisfied with the gain-switched LD by setting dc bias current small. The condition is that the LD should be reversely biased at the bottom of the pulses, and the turn-off duration should be longer than the effective photon lifetime. The results indicate that QKD system clock can be increased to 10 GHz as far as the security issue on the laser light source is concerned. In practice, a number of technical problems remain. Among the remaining issues, the most important ones would be high-speed photon detection and postprocessing.

ACKNOWLEDGMENTS

The authors would like to thank Dr. Kiyoshi Tamaki and Dr. Yoshihiro Nambu for helpful discussions, and Takahisa Seki for his assistance in the experiment. This work has been conducted under the commissioned research of National Institute of Information and Communications Technology (NICT), Japan "Secure photonic network technology."

APPENDIX: OPTIMAL DISCRIMINATION OF TWO DENSITY MATRICES

We here drive the optimum discrimination of the decoy from the signal in partially coherent states, which were given in Eq. (18). We optimized the POVM for given values of P_{inc} to obtain the highest P_C in discriminating the two mixed states. All the density matrices here are real and symmetric. The POVMs Π_i, $i = 0,1,2$ satisfy

$$\Pi_0 + \Pi_1 + \Pi_2 = 1, \tag{A1}$$

where Π_1 and Π_2 correspond to the conclusive decision that the state is ρ_1 and ρ_2, respectively, while Π_0 represents the inconclusive results. The probability of inconclusive results is given by

$$P_{inc} = \mathrm{Tr}(\rho\Pi_0) = 1 - \mathrm{Tr}[\rho(\Pi_1 + \Pi_2)], \tag{A2}$$

and the probability to yield a correct decision is

$$\begin{aligned} P_C &= p\mathrm{Tr}(\rho_1\Pi_1) + (1-p)\mathrm{Tr}(\rho_2\Pi_2) \\ &= 1 - P_{inc} - p\mathrm{Tr}(\rho_1\Pi_2) - (1-p)\mathrm{Tr}(\rho_2\Pi_1), \end{aligned} \tag{A3}$$

where ρ is defined with the probability of ρ_1's occurrence p by

$$\rho = p\rho_1 + (1-p)\rho_2. \tag{A4}$$

We applied the iteration method developed by Fiurášek and Ježek [28] to maximize P_C (A3) under the constraint (A1) and (A2) for a given value of P_{inc} using Lagrange multipliers. The iteration was performed with symmetrized equations to keep the POVMs Hermite and positive semi-definite. We set average photon numbers for the signal and decoy state $\mu = 0.5$ and $\nu = 0.1$, respectively, and assumed the signal and decoy state appear with the same probability ($p = 1/2$) for simplicity. The optimization was done for two values of the probability of the inconclusive results: $P_{inc} = 0.983$, which refers to the probability of the inconclusive results in the USD measurement to weak coherent states of $\theta_0 = 0$, and $P_{inc} = 0.712$ of $\theta_0 = \pi$. No USD measurement for $\theta_0 = 0$ exists to satisfy $P_{inc} = 0.712$. Figure 8 shows the probability of correct decision as a function of the standard deviation of phase. Successful USD measurement ($P_C = 1$) is achieved for the coherent states ($\sigma = 0$.) The probabilities of correct

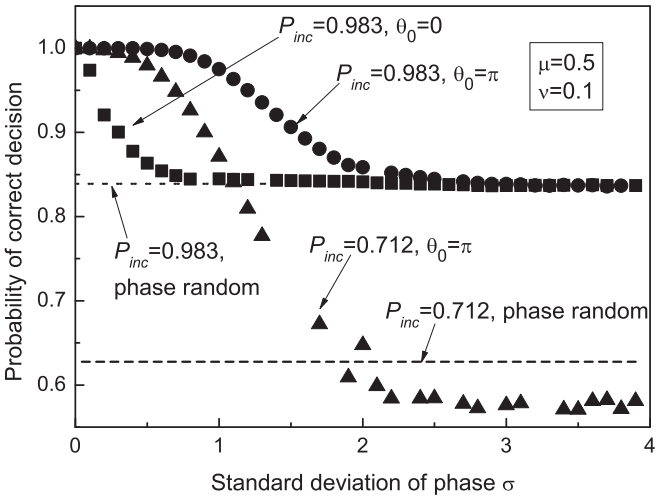

FIG. 8. Probability of correct decision in the optimal discrimination of the signal and decoy states as a function of the standard deviation of phase. The state discrimination was done for the partially phase-randomized states of average photon number 0.5 and 0.1. Inconclusive results are allowed in the state discrimination. Squares represent $P_{\rm inc} = 0.983$, $\theta_0 = 0$, circles $P_{\rm inc} = 0.983$, $\theta_0 = \pi$, and triangles $P_{\rm inc} = 0.712$, $\theta_0 = \pi$. Dotted line and dashed line refer to the probability of correct decision on the phase-randomized states under the conditions of $P_{\rm inc} = 0.983$ and $P_{\rm inc} = 0.712$, respectively.

decision decrease as the standard deviation of phase increasing. The probabilities converge to the values for completely phase-randomized states, when σ exceeds about 2.5, which corresponds to the visibility of 0.044.

We observed that the numerical optimization under the condition of $P_{\rm inc} = 0.712$ sometimes failed, in particular for large σ. It also returned the probability of correct decision lower than that for the phase-randomized states. Small errors in matrix operations may result in such suboptimal results. Nevertheless, we found the optimized POVMs for large σ states were almost the same as those for the phase randomized states.

The probability of correct decision is larger than 0.5 even for the completely phase-randomized case. The reason can be understood as follows. For the completely phase-randomized states, the POVM operators are diagonal in photon-number state basis. Then, the POVM provides the outcome "1" when the observed photon number is larger than a threshold, and the inconclusive result when it is smaller than the threshold. The given probability of the inconclusive results determines the threshold photon number. Suppose the probabilities that states ρ_1 and ρ_2 contain photons more than the threshold as $p_{\rm th}(1)$ and $p_{\rm th}(2)$, respectively. Since the average photon number of ρ_1 is larger than that of ρ_2, the probability $p_{\rm th}(1)$ exceeds $p_{\rm th}(2)$. The probability of correct decision (i.e., the state is ρ_1) conditioned by the outcome "1" is given by the Bayes rule as

$$P_C = \frac{p_{\rm th}(1)}{p_{\rm th}(1) + p_{\rm th}(2)} > \frac{1}{2}. \tag{A5}$$

The above inequality shows that it is more likely that the state is the one with a larger average photon number when a large photon number is observed.

[1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, New York, 1984) pp. 175–179.
[2] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[3] M. Koashi, arXiv:quant-ph/0505108v1.
[4] R. Renner, Int. J. Quantum Info. **6**, 1 (2008).
[5] M. Koashi, New J. Phys. **11**, 045018 (2009).
[6] M. Koashi and J. Preskill, Phys Rev Lett **90**, 057902 (2003).
[7] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[8] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).
[9] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Info. Comput. **4**, 325 (2004).
[10] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).
[11] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).
[12] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).
[13] M. Ben-Or, M. Horodecki, D. W. Leung, D. Mayers, and J. Oppenheim, in *Theory of Cryptography* (Springer, New York, 2005), pp. 386–406.
[14] J. Müller-Quade and R. Renner, New J. Phys. **11**, 085006 (2009).
[15] M. Hayashi and T. Tsurumaru, New J. Phys. **14**, 093014 (2012).
[16] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, Nat. Commun. **3**, 634 (2012).
[17] H.-K. Lo and J. Preskill, Quantum Info. Comput. **7**, 431 (2007).
[18] Y.-L. Tang, H.-L. Yin, X. Ma, C.-H. F. Fung, Y. Liu, H.-L. Yong, T.-Y. Chen, C.-Z. Peng, Z.-B. Chen, and J.-W. Pan, Phys. Rev. A **88**, 022308 (2013).
[19] Y. Zhao, B. Qi, and H.-K. Lo, Appl. Phys. Lett. **90**, 044106 (2007).
[20] S.-H. Sun, M. Gao, M.-S. Jiang, C.-Y. Li, and L.-M. Liang, Phys. Rev. A **85**, 032304 (2012).
[21] Z. L. Yuan, M. Lucamarini, J. F. Dynes, B. Frohlich, A. Plews, and A. J. Shields, Appl. Phys. Lett. **104**, 261112 (2014).
[22] A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, Opt. Express **16**, 18790 (2008).
[23] M. Sasaki *et al.* Opt. Express **19**, 10387 (2011).
[24] K.-I. Yoshino, M. Fujiwara, A. Tanaka, S. Takahashi, Y. Nambu, A. Tomita, S. Miki, T. Yamashita, Z. Wang, M. Sasaki, and A. Tajima, Opt. Lett. **37**, 223 (2012).
[25] A. Yariv and P. Yeh, *Photonics*, 6th ed., The Oxford Series in Electrical and Computer Engineering, (Oxford University Press, New York, 2006).
[26] C. H. Henry, IEEE J. Quantum Electron. **18**, 259 (1982).
[27] K. Tamaki, M. Curty, G. Kato, H.-K. Lo, and K. Azuma, arXiv:1312.3514.
[28] J. Fiurášek and M. Ježek, Phys. Rev. A **67**, 012321 (2003).
[29] Y. Nambu, K.-I. Yoshino, and A. Tomita, J. Mod. Opt. **55**, 1953 (2008).
[30] T. Kobayashi, A. Tomita, and A. Okamoto, in *SPIE OPTO* (SPIE, Bellingham, WA, 2014), pp. 899707–899707.