Blind quantum computation with a heralded single-photon source

Kurumiko Nagao, Tomoyuki Horikiri, and Toshihiko Sasaki

Phys. Rev. A **99**, 042324 — Published 16 April 2019

DOI: 10.1103/PhysRevA.99.042324

Blind quantum computation with a heralded single photon source

Kurumiko Nagao
Yokohama National University, 79-5 Tokiwadai, Hodogaya, Yokohama 240-8501, Japan

Tomoyuki Horikiri
Yokohama National University, 79-5 Tokiwadai, Hodogaya, Yokohama 240-8501, Japan and
JST PRESTO, Kawaguchi, Saitama 332-0012, Japan

Toshihiko Sasaki
The Univesity of Tokyo, 7-3-1 Hongo, Bunkyo 113-8654, Tokyo, Japan

Blind quantum computation is a scheme that adds unconditional security to cloud quantum computation. In the protocol proposed by Broadbent, Fitzsimons, and Kashefi, the ability to prepare and transmit a single qubit is required for a user (client) who uses a quantum computer remotely. In case a weak coherent pulse is used as a pseudo single photon source, however, we must introduce decoy states, owing to the inherent risk of transmitting multiple photon. In this study, we demonstrate that by using a heralded single photon source and a probabilistic photon number resolving detector, we can gain a higher blind state generation efficiency and longer access distance, owing to noise reduction on account of the heralding signal.

I. INTRODUCTION

Universal quantum computing has been developed rapidly in recent years. Indeed, it is thought that it is only a matter of time until it can be used practically. However, it is expected that powerful quantum computers will be very large and expensive. There are still a number of challenges that remain to develop such computers for personal or commercial use. Therefore, it is indispensable to develop techniques for individual users (clients) to use quantum computers securely when they are owned by large companies or institutions. Blind quantum computation is a method of using quantum computers remotely without leaking information to third parties, including its owner.

Various approaches exist for universal blind quantum computation. Among them, the BKF protocol—named after Broadbent, Fitzsimons, and Kashefi [1]—is regarded as practical because it does not require quantum memory nor quantum operations on the client side. In accordance with their protocol, we consider measurement-based quantum computing [2], which is a method of performing quantum computations with many qubit entanglements measured on the server side. In the BKF protocol, the server performs quantum computations by creating and measuring multipartite entanglements using qubits transmitted by the client. By giving randomness to the quantum state to be transmitted, the client can perform calculations with both the content and results of the calculations concealed on the server side.

Ideally, the BKF protocol guarantees unconditional security. However, in order to achieve this, the client must transmit a single photon for each qubit. Although photons are generally used for signal transmission, it is extremely difficult to prepare an ideal single photon source. Weak laser light (weak coherent pulse, WCP) is thus used as a pseudo single photon source in practice. However, with WCP, the number of photons follows Poissonian statistics, so the probability of transmitting multiple photons can never be zero. As such, information risks being stolen by the server exist. Given the existence of such imperfections, a protocol to prepare qubits (remote blind state preparation, RBSP) securely at remote locations is proposed by Dunjko et al. [3]. With this protocol, it is possible to create a single secure qubit from multiple signals. In addition, "ε - blindness" guarantees that the probability information leaked to the server is less than ε despite following the protocol correctly.

In the RBSP protocol, the client must send many pulses to prepare a single qubit. In order to estimate the number of pulses accurately and prove the security with fewer pulses, the decoy state method [4–6] used in the quantum key distribution (QKD) was brought into RBSP [7, 8]. The decoy state method more precisely estimates the transmittance for each photon number by sending “decoy” states of different intensities. By adopting this method in RBSP, it is possible to estimate the lower limit of the number of pulses N that the client needs to send. In particular, in the original RBSP protocol [3], $N = O(1/T^4)$ for the transmittance T. N increases considerably with the communication distance. With the decoy state method and an improved estimation method, by contrast, $N = O(1/T)$, which offers a significant improvement.

In QKD, a heralded single photon source (HSPS) has been shown to have an advantage over WCP regarding the communication distance [9, 10]. A single photon is thus heralded by the detection of the counterpart of two photons generated by spontaneous parametric down-conversion (SPDC). As a result, it is possible to reduce the dark count and extend the communication distance. In addition, the multi-photon probability can be decreased by measuring the photon number for the heralding signal, increasing the secure key generation rate.

In this study, we analyze the required number of pulses N when using HSPS rather than WCP in universal blind quantum computation (UBQC) and compare the results to the case of WCP. In Sec. II, we briefly review UBQC based on WCP. In Sec. III, we introduce HSPS in UBQC in an asymptotic case, and Sec. IV describes RBSP by using a HSPS. Sec. V compares the two cases followed by discussion in Sec. VI.

II. UNIVERSAL BLIND QUANTUM COMPUTATION WITH WEAK COHERENT PULSES

With the BKF protocol, all information except for the calculated size is completely concealed. However, since there are necessarily imperfections in the real world, complete concealment is difficult. Specifically, it is difficult to prepare an ideal single-photon source, and WCP utilization is generally assumed. However, insofar as the number of photons follows a Poisson distribution, pulses containing multiple photons can exist. If there are multi-photon signals, information leaks to the server (Bob). The RBSP protocol [3] has been proposed to increase security despite multi-photon signals. Further, "ε - blindness B serves as an index for the degree of security.

A. Interlaced 1-D Cluster computation

In the RBSP protocol, interlaced 1-D Cluster computation (I1DC) is used to create a single qubit from several pulses to increase security even in the case that a multi-photon pulse is included in the signal pulse sequence [3]. The client (Alice) sends several random-phased states to Bob. Bob then generates a single qubit using them. The phase of the generated qubit is the sum (or difference) of all the phases of the states used to create this qubit. Therefore, Bob cannot obtain information about the phase if any one of the states sent from Alice is unknown. That is, in the case of sending multiple pulses, no information leaks to Bob if there is at least one pulse in which just a single photon exists. The procedure is as follows.

1. Input
   Alice randomly assigns $\sigma_l = 0, \frac{\pi}{4}, \frac{2\pi}{4}, ..., \frac{7\pi}{4}$. Send states $|+_{\sigma_l}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\sigma_l}|1\rangle)$ $(l = 1, ..., k)$ to Bob.

2. Operation with Bob

   (a) Apply $CZ(H \otimes I)$ to i and the $i+1$-th qubit.

   (b) Measure the i-th qubit with Pauli X and output the measured value as s_i.

   (c) Repeat (a) and (b) from $i = 1$ to $k-1$.

   (d) Bob receives an unmeasured qubit of state $|+_\theta\rangle$ and tells Alice $s = (s_1, s_2, ..., s_k)$.

3. Output Alice calculates θ from $s = (s_1, s_2, ..., s_k)$ and σ_l.

$$\theta = \sum_{l=1}^{k} (-1)^{t_l} \sigma_l \tag{1}$$

$$t_i = \begin{cases} \sum_{j=1}^{k-1} s_i \quad mod\ 2 & (i > k) \\ 0 & (i = k) \end{cases} \tag{2}$$

In order for Bob to receive θ, it is necessary to know all σ_l. That is, Bob cannot know θ if there is at least one single photon signal σ_l unknown to Bob. From the no-cloning theorem, Bob cannot derive information on σ_l for pulses that contain only a single photon, and as such it suffices for there to be at least one pulse with only a single photon. Provided that this condition is satisfied, Alice can create a qubit where the phase is unknown to the server.

B. Remote blind qubit state preparation

RBSP proceeds according to the following procedure.

1. Preparation by Alice

   (a) Prepare N WCPs with an average photon number of $\mu = T$, where T denotes channel transmittance. Each pulse has a phase randomly selected from the set $\sigma_l = 0, \frac{\pi}{4}, \frac{2\pi}{4}, ..., \frac{7\pi}{4} (l = 1, ..., N)$. The state is described as follows:

$$\rho^{\sigma_l} = e^{-\mu} \sum_{k=0}^{\infty} \frac{\mu^k}{k!} |k\rangle \langle k|_{\sigma_l} \tag{3}$$

   (b) Send $\{\rho^{\sigma_l}\}_l$ to Bob.

2. Preparation by Bob

(a) Perform a quantum non-demolition measurement of the photon number on each received state. Keep signals with a nonzero photon number, and discard the others.

(b) Bob tells Alice the number of photons $(n_1, ..., n_N)$ in each state.

3. Calculation and operation by Alice and Bob

   (a) Alice makes sure that the number of reported vacuum states is not too large. Specifically, if it is larger than $N(e^{-T^2} + T^2/6)$, the protocol is aborted.

   (b) Bob transfers each state to a single qubit. Let the qubit number be M.

   (c) Use the above qubits to do I1DC. Obtain $t = (t_1, ..., t_M)$ and state $|+_\theta\rangle$.

   (d) Bob tells Alice t.

   (e) Alice calculates θ using σ_l and t.

At this time, the probability p_{fail} that information is leaked to Bob even though the protocol was executed correctly, and the probability p_{abort} that the protocol will be aborted even if Bob is not cheating, satisfy the following expression:

$$p_{fail}, p_{abort} \leq \exp\left(-\frac{NT^4}{18}\right), \tag{4}$$

where T is the channel transmittance [3].

C. Remote blind state preparation with weak coherent pulses: decoy state method

In Ref. [3], it was demonstrated that the RBSP rate using WCP decreases in proportion to the fourth power of channel transmittance. This is a major obstacle to attaining long-distance RBSP. Therefore, a method for improving the RBSP has been introduced using the decoy state method originally proposed in the field of QKD [7]. The procedure is as follows.

1. Preparation by Alice

   (a) Prepare N WCPs including the signal state and two kinds of decoy states with average photon numbers of μ, v_1, v_2, respectively. Each pulse has a phase randomly defined by $\sigma_l = 0, \frac{\pi}{4}, \frac{2\pi}{4}, ..., \frac{7\pi}{4}$ $(l = 1, ..., N)$. The signal state is described as follows:

$$\rho_\mu^{\sigma_l} = e^{-\mu} \sum_{k=0}^{\infty} \frac{\mu^k}{k!} |k\rangle \langle k|_{\sigma_l} \tag{5}$$

   Two decoy states $\rho_{v_1}^{\sigma_l}, \rho_{v_2}^{\sigma_l}$ are defined as well.

   (b) Send the prepared states $\{\rho_\mu^{\sigma_l}\}_l, \{\rho_{v_1}^{\sigma_l}\}_l, \{\rho_{v_2}^{\sigma_l}\}_l$ to Bob.

2. Preparation by Bob

   (a) Bob tells Alice which pulses he has received.

3. Calculation and manipulation by Alice and Bob

   (a) Alice confirms that the yield of the signal and the two decoy states $(Q_\mu, Q_{v_1}, Q_{v_2})$ reported by Bob is not below a predetermined threshold. If it is, the protocol is aborted.

   (b) Alice tells Bob the position of the decoy and the computation size S.

   (c) Bob throws out the decoy states. The remaining qubits (the number is given by M_μ) are divided randomly into S groups and Bob performs I1DC for each group. Bob obtains $|+_\theta\rangle$ and sends the measurement result to Alice.

   (d) Alice calculates θ in accordance with the procedure of I1DC.

In this decoy scheme, as in the original RBSP [3], the failure probability p_{fail} is estimated and a condition that it becomes less than ε is found [7, 8]. Here, S is the computation size, which corresponds to the number of qubits ultimately created by Bob. Let the rate of the single photon pulse by Bob left after the decoy pulses are discarded be p_1. The number of signal states for each group is given by $m = M_\mu/S$, and the group fails unless there is at least one single photon pulse in it. The probability that a group fails is given by the following expression:

$$p_{fail} = \frac{\begin{pmatrix} m \\ M_\mu - M_1 \end{pmatrix}}{\begin{pmatrix} m \\ M_\mu \end{pmatrix}} \leq \left(\frac{M_\mu - M_1}{M_\mu}\right)^m = (1 - p_1)^m. \tag{6}$$

Here, M_1 is a single photon count number at Bob. If there is even one failed group among S groups, RBSP fails. Therefore, the overall failure probability P_{fail} is given by

$$P_{fail} \leq S p_{fail} = S(1 - p_1)^m. \tag{7}$$

The condition that this is less than ε is given by

$$m \geq \frac{\ln(\varepsilon/S)}{\ln(1 - p_1)}. \tag{8}$$

In finite-length analysis, we ensure that P_{fail} is less than the given security parameter ε. Below, we discuss the efficiency S/N and its asymptotic nature. For the asymptotic limit, we fix the security rate ε/S instead of the security parameter ε because the overall failure probability increases as the protocol repeats.

By using the relation (8), the lower limit of N is given by the following expression, under the assumption that the ratio of the signal in N pulses is p_μ:

$$N = \frac{M_\mu}{p_\mu Q_\mu} = \frac{mS}{p_\mu Q_\mu} \geq \frac{S}{p_\mu Q_\mu} \frac{\ln(\varepsilon/S)}{\ln(1-p_1)}. \tag{9}$$

Here, $p_\mu, \varepsilon/S$ are the default values predetermined and followed by the necessary computation and security level. Further, Q_μ is a characteristic value of a photon source and channel transmittance, while p_1 needs to be estimated. From the expression of Y_1^{L,v_1,v_2} in [7], the minimum of p_1 is given as follows:

$$\begin{aligned} p_1 = \frac{Q_1}{Q_\mu} &\geq \frac{Y_1^{L,v_1,v_2} \mu e^{-\mu}}{Q_\mu} \\ &= \frac{\mu^2 e^{-\mu}}{\mu v_1 - \mu v_2 - v_1^2 + v_2^2} \times \\ &\left[\frac{Q_{v_1}}{Q_\mu} e^{v_1} - \frac{Q_{v_2}}{Q_\mu} e^{v_2} - \frac{v_1^2 - v_2^2}{\mu^2 Q_\mu} \left(Q_\mu e^{\mu} - Y_0^L \right) \right]. \end{aligned} \tag{10}$$

It enables us to make μ almost independent to T whereas we have to make μ proportional to T without decoy-state method. Here, Y_i is a channel transmittance including the detection efficiency for the signal of photon number i. In the case of a zero photon number Y_0, it is given by the dark count probability of detectors.

III. HERALDED SINGLE PHOTON SOURCE

In QKD, an alternative photon source has been proposed, called a heralded single photon source (HSPS), which utilizes spontaneous parametric down-conversion (SPDC) [9, 10]. SPDC is a nonlinear optical process that generates a two-photon pair (or pairs) called a signal and idler. In this method, after the signal and idler are separated spatially by a polarizing beam splitter or a dichroic mirror, the photon number for the idler is measured using a practical photon number resolving detector [10], and signal pulses that include multi-photons are removed from the key generation process. Since the number of photons can only be measured stochastically, multiple photon pulses cannot be completely eliminated, yet the probability that a nonzero signal pulse consists of a single photon can be increased. In addition, by utilizing heralding with the idler detection, it is possible to reduce the detector dark count, insofar as Bob accepts signal pulses only when the corresponding idler photon is detected as a single photon. This enables longer distance communication. The photon (pair) number distribution of SPDC is thermal when single mode approximation is valid:

$$P(n) = \frac{\mu^n}{(1+\mu)^{n+1}}. \tag{11}$$

We assume that the photon number of the idler for generating heralding signals on Alice's side is measured by using a fiber beam splitter and single photon detectors, which do not themselves have a photon number resolution [11–13]. The so-called time-multiplexed detector works well if the detectors' quantum efficiencies are good. In practice, currently available superconducting single photon detectors typically offer detection efficiencies higher than 0.85. Assuming that the number of couplers is x, the mode number X after the fiber beamsplitter output ports is $X = 2^x$. The probability of measuring m photon pulse as l photon $P(l|m)$ with the detection probability at each detector as η_A is given as follows [11]:

$$P(l|m) = \begin{pmatrix} X \\ l \end{pmatrix} \sum_{j=0}^{l} (-1)^j \begin{pmatrix} l \\ j \end{pmatrix} \left[(1-\eta_A) + \frac{(l-j)\eta_A}{X} \right]^m. \tag{12}$$

After discarding multi-photon pulses and leaving only single photon pulses, the yield Q_μ and error rate E_μ are given by Eqs. (13) and (14), respectively. Here, we set the dark count rate of the detectors on Alice's side (heralding detector) as d_A:

$$Q_\mu = Y_0 X d_A \frac{1}{1+\mu} + \sum_{i=1}^{\infty} Y_i P(1|i) \frac{\mu^i}{(1+\mu)^{i+1}}, \tag{13}$$

$$E_\mu Q_\mu = e_0 Y_0 X d_A \frac{1}{1+\mu} + \sum_{i=1}^{\infty} e_i Y_i P(1|i) \frac{\mu^i}{(1+\mu)^{i+1}}. \tag{14}$$

IV. REMOTE BLIND STATE PREPARATION WITH DECOY HSPS

We now turn to the case of HSPS. In this case, the mean photon number for the signal and two decoy states is defined in the same manner as the WCP case (μ, v_1, v_2):

$$0 \leq v_2 < v_1, \tag{15}$$

$$v_1 + v_2 < \mu. \tag{16}$$

The yield for decoy states Q_{v_1}, Q_{v_2} is expressed as well.

Then, the following can be derived:

$$\begin{aligned}
&v_1 Q_{v_2}(1+v_2)^2 - v_2 Q_{v_1}(1+v_1)^2 \\
&= [v_1(1+v_2) - v_2(1+v_1)]\times \\
&Y_0 X d_A - v_1 v_2 \Bigg\{ \left[\frac{v_1}{1+v_1} - \frac{v_2}{1+v_2} \right] Y_2 P(1|2) \\
&\qquad + \left[\frac{v_1^2}{(1+v_1)^2} - \frac{v_2^2}{(1+v_2)^2} \right] Y_3 P(1|3) + \cdots \Bigg\} \\
&\le [v_1(1+v_2) - v_2(1+v_1)] Y_0 X d_A \qquad (17)
\end{aligned}$$

and

$$\begin{aligned}
&Y_0 X d_A \ge Y_0^L X d_A \\
&= max \left\{ \frac{v_1 Q_{v_2}(1+v_2)^2 - v_2 Q_{v_1}(1+v_1)^2}{v_1(1+v_2) - v_2(1+v_1)}, 0 \right\}. \qquad (18)
\end{aligned}$$

The lower bound of Y_0 is obtained as Y_0^L. Here, a relation $\frac{v_1}{1+v_1} > \frac{v_2}{1+v_2}$, from $v_1 > v_2$, is utilized. Equation (18) holds for $v_2 = 0$. Hence, the best lower bound is obtained in the condition. Furthermore, Eq. (19) is derived from Eq. (17), and Eq. (20) is derived from Eq. (16):

$$\sum_{i=2}^{\infty} Y_i P(1|i) \frac{\mu^i}{(1+\mu)^i} = Q_\mu (1+\mu) - Y_0 X d_A - Y_1 \eta_A \frac{\mu}{1+\mu}, \qquad (19)$$

$$\frac{\left(\frac{v_1}{1+v_1}\right)^2 - \left(\frac{v_2}{1+v_2}\right)^2}{\left(\frac{\mu}{1+\mu}\right)^2} \ge \frac{\left(\frac{v_1}{1+v_1}\right)^i - \left(\frac{v_2}{1+v_2}\right)^i}{\left(\frac{\mu}{1+\mu}\right)^i}. \qquad (20)$$

By removing Y_0 from Q_{v_1} and Q_{v_2}, the minimum of Y_1 is estimated (Y_1^{L,v_1,v_2}) in Eq. (21).

$$\begin{aligned}
&Y_1 \eta_A \ge Y_1^{L,v_1,v_2} \eta_A \\
&= \frac{\frac{\mu}{1+\mu}}{\frac{v_1}{1+v_1}\frac{\mu}{1+\mu} - \frac{v_2}{1+v_2}\frac{\mu}{1+\mu} - \left(\frac{v_1}{1+v_1}\right)^2 + \left(\frac{v_2}{1+v_2}\right)^2} \times \\
&\Bigg[Q_{v_1}(1+v_1) - Q_{v_2}(1+v_2) - \frac{\left(\frac{v_1}{1+v_1}\right)^2 - \left(\frac{v_2}{1+v_2}\right)^2}{\left(\frac{\mu}{1+\mu}\right)^2} \\
&\times \{Q_\mu - Y_0^L X d_A\} \Bigg] \qquad (21)
\end{aligned}$$

Inequalities (18) and (21) represent the minimum of Y_0 and Y_1, respectively. The expressions of the lower limits allow us to estimate the lower limit of p_1:

$$p_1 = \frac{Q_1}{Q_\mu} \ge \frac{Y_1^{L,v_1,v_2} \eta_A \frac{\mu}{(1+\mu)^2}}{Q_\mu}, \qquad (22)$$

where Q_1 is the yield for single photon pulses. The lower limit of N to attain "ε - blindness B by using an HSPS is obtained by substituting Eq. (22) with Eq. (9).

V. RESULT

Thus far, we have considered an asymptotic case where the size S has an infinite length. However, when considering the generation of a finite-length graph state in practice, it is necessary to evaluate the deviation from the Poissonian, which should be attained in an infinite-length graph state. Here, it is necessary to evaluate the blind state generation efficiency, defined as S/N. Its maximization is considered a performance index of RBSP. For WCP blind quantum computations without decoy states [3], for Bob detection number $M_\mu = O(N\mu T)$, all signals that consist of more than two photons are assumed to be detected by Bob $M_{\ge 2} = O(N\mu^2)$. Then, $M_{\ge 2}/M_\mu = O(\mu/T)$. Therefore, if $\mu \le O(T)$ is not satisfied, $M_{\ge 2}/M_\mu \ge 1$. Even if m is increased, an inequality $(\frac{M_{\ge 2}}{M_\mu})^m < p_{fail}$ cannot be satisfied. As μ increases, M_μ becomes larger, so $\mu = O(T)$. As for p_{abort}, the difference $N\Delta$ between the number M_0 of states for which the server measured 0 and its expectation value is bounded $O(\sqrt{N})$ because it obeys Eq. (9) of the supplimentary material of [3], which is Hoeffding's bound, and they consider p_{abort} as a small constant. The signal detection number M_μ needs to be much higher than M_0, $O(N\mu T) > O(\sqrt{N})$. Then, $N > O((\mu T)^{-2})$ is necessary. Finally, the efficiency is $S/N = O(T^4)$.

Indeed, the bound of the statistical fluctuation $N\Delta$ in [3] is loose. Hoeffding's bound for independent random variables can be replaced with the Chernoff bound. It bounds the difference between the actual and expected values of M_μ to be $O(\sqrt{N\mu T})$. It makes this difference irrelevant to the efficiency of the protocol in the asymptotic regime. In this study, the total detection number M_μ is the same, whereas $M_{\ge 2} = O(N\mu^2 T)$, because the value is precisely estimated by decoy states. Therefore, $M_{\ge 2}/M_\mu = O(\mu)$, such that the qubit number m for obtaining a single qubit does need not increase as the distance increases ($m = O(1), \mu = O(1)$). As a result, the efficiency will be $S/N = M_\mu/(Nm) = O(T)$. For the finite-length RBSP, we can still take advantage of utilizing decoy states.

In the following, we will evaluate the efficiency S/N and the performance of HSPS. Parameters Q_μ, Q_{v_1}, Q_{v_2} needed to calculate S/N are obtained using the transmittance T, derived by Eq. (26), where α(dB/km) is the loss factor in an optical fiber, L is the fiber length (km), t_s is the transmittance inside the server, and η_s, is the detection rate on the server side. Here, μ is the average photon number, and in the case of WCP and HSPS, we use Eqs. (27) and (28), respectively. We also set the average photon numbers v_1 and v_2 for decoy states.

$$Q_\mu \simeq Y_0 + T\mu, \tag{23}$$
$$Q_{v_1} \simeq Y_0 + Tv_1, \tag{24}$$
$$Q_{v_2} \simeq Y_0 + Tv_2, \tag{25}$$

$$T = 10^{-\alpha L/10} t_s \eta_s, \tag{26}$$

$$\mu_{wcp} = \mu \tag{27}$$

$$\mu_{thermal} = \sum_{i=0}^{\infty} \frac{\mu^i}{(1+\mu)^{i+1}} P(1|i). \tag{28}$$

Here, $\alpha = 0.2$ dB/km, $L = 25$ km, $t_s = 0.45$, $\eta_s = 0.1$, and the server's dark count Y_0 is set to 6×10^{-6} [8]. Furthermore, v_2 is the optimum value 0, and $v_1 = 0.125$. We also set the signal proportion p_μ to 0.9. These values are adjusted to the values used in [8] for comparison. Furthermore, the detection efficiency η_A of the heralding detector on Alice included only in HSPS is set to 0.85, and the dark count rate d_A is set to 1.0×10^{-8}. This is a value sufficiently achievable with a commercially available superconducting single photon detector [14].

In Fig. 1, the dependence of S/N on μ is shown. In WCP (HSPS), the maximum is obtained with $\mu = 0.625, p_1 = 0.51$ ($\mu = 0.605$, $p_1 = 0.65$). Moreover, S/N for WCP is about 3/2 times higher. The reason S/N is inferior in HSPS is because the efficiency of the heralding detector is imperfect and because the multi-photon probability for HSPS (thermal) is higher than the Poisson distribution. When the efficiency of the heralding detector approaches unity, it approaches the WCP.

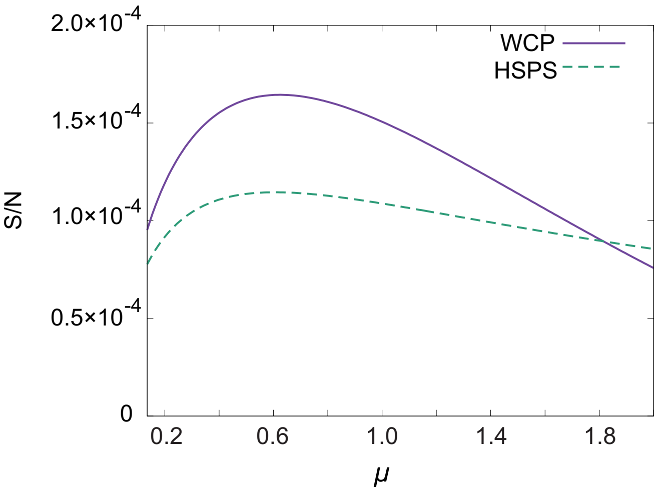

FIG. 1. Dependence of S/N on μ. ($\eta_A = 0.85, d_A = 1.0 \times 10^{-8}$)

We also calculated a case using the lowest dark count rate demonstrated so far [19]. Here, according to [19], the dark count rate per second is 0.01 cps, and d_A is 1.0×10^{-12} within the detection window width of 100 ps. The detection efficiency η_A is 0.04. The S/N dependence on μ is shown in Fig. 2. In this case, the upper limit of S/N was considerably low due to the influence of Alice's low detection efficiency η_A. It was about two orders of magnitude lower than in the case of WCP. From this result, we found that decreasing the photon detection efficiency by one order was more influential than improving the dark count rate by four orders of magnitude. Therefore, in the following calculation, we used the parameters $\eta_A = 0.85$ and $d_A = 1.0 \times 10^{-8}$.

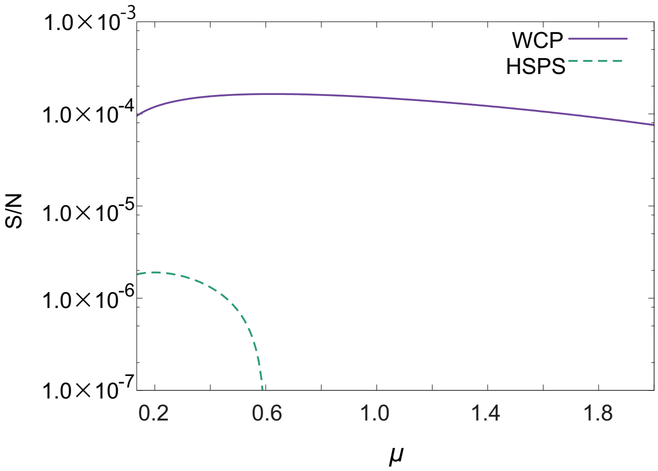

FIG. 2. S/N dependence on μ. ($\eta_A = 0.04, d_A = 1.0 \times 10^{-12}$)

Next, S/N dependence on the distance L is shown in Fig. 3. For each distance L, we numerically obtained the maximum S/N by varying μ. Up to 100 km, μ was constant at 0.625 for WCP and 0.605 for HSPS.

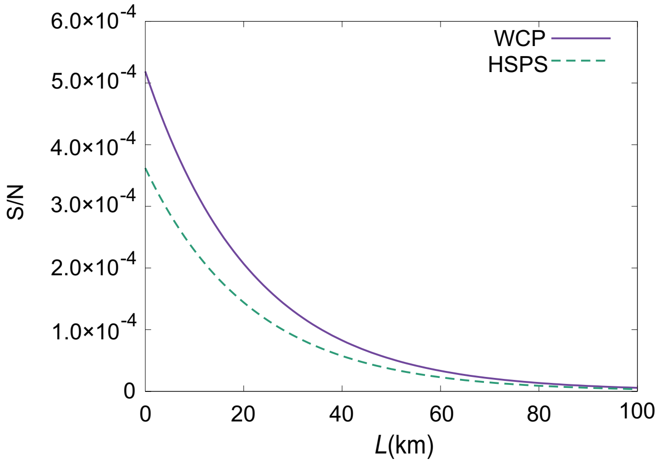

FIG. 3. S/N dependence on distance. $(\eta_A = 0.85, d_A = 1.0 \times 10^{-8})$

Furthermore, Fig. 4 shows the S/N up to L = 1000 km. In the long-distance regime, the S/N becomes constant. The signal from Alice rarely reaches Bob, owing to the decrease in transmittance T. The yields in Q_μ, Q_{v_1}, Q_{v_2} are all derived from dark counts and become constant regardless of the distance. So the flat area is removed from the plot to avoid confusion. Therefore, the distance that starts to become flat in Fig. 4 indicates the upper limit of the distance for RBSP. This was approximately 200 km by WCP and 500 km by HSPS. By reducing the probability of zero photon pulses with the use of the heralding detector, RBSP with HSPS extended the distance farther than with WCP.

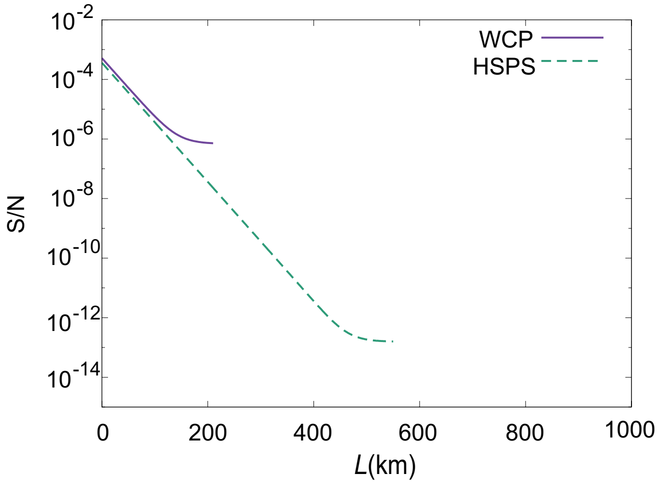

FIG. 4. S/N dependence on distance up to a 1000 km. $(\eta_A = 0.85, d_A = 1.0 \times 10^{-8})$

As discussed above, the S/N for HSPS is lower than in the case of WCP. This is because of the difference in the photon number distributions. Specifically, this is due to a lower single photon probability in SPDC compared to the Poisson distribution of WCP. When using HSPS with a broad spectral width, which corresponds to a case where the Poisson distribution is obtained [18], there is considerable dispersion in the optical fiber and this cannot be ignored. Consequently, it is unrealistic to consider this case.

Moreover, in order to consider the upper limit from using HSPS, calculations were also made when $\eta_A = 1.0$ and $d_A = 1.0 \times 10^{-8}$. The value of S/N with varying fiber length L is given in Fig. 5. For the purpose of comparison, the case of WCP is also shown.

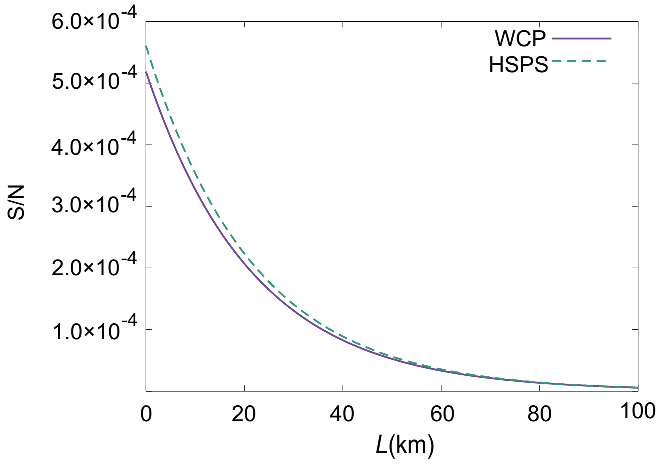

FIG. 5. S/N dependence on distance $(\eta_A = 1.0, d_A = 1.0 \times 10^{-8})$.

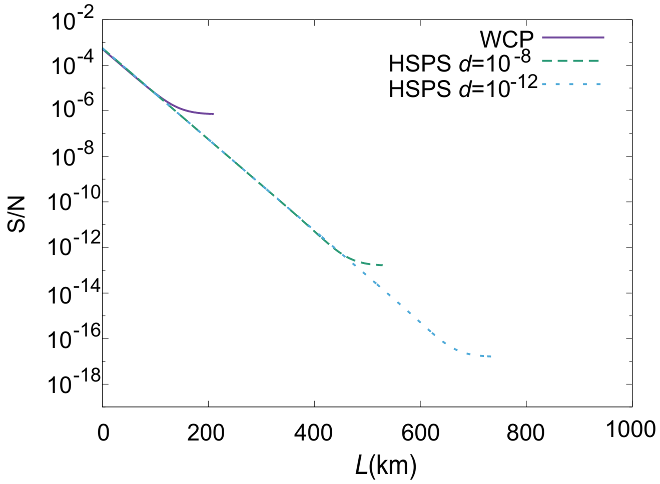

FIG. 6. S/N dependence on distance (Purple solid: WCP, green dashed: HSPS with $\eta_A = 1.0, d_A = 1.0 \times 10^{-8}$, blue dotted: HSPS with $\eta_A = 1.0, d_A = 1.0 \times 10^{-12}$).

It can be seen from this figure that HSPS exceeds WCP when the heralding detector's efficiency is at unity though the improvement is small (roughly around 8 %). Note that since we are utilizing a time-multiplexed detector to obtain the photon number resolution, there is still a probability of failure, in which a multi-photon is counted as a single photon.This is possible when a multi-photon exists and stays in the same mode after the final fiber coupler. To see the longest distance available by the state of the art technology, we assume the dark count rate of 10^{-12} with unit detection efficiency in Fig. 6. While S/N improvement is mild, the longest distance is close to 700 km which is more than three times of the distance achievable with WCP. Clearly, the improvement is due to the small dark count probability which enables the lower signal transmittance.

VI. DISCUSSION

The performance of the I1DC protocol with HSPS is worse than that with WCP from the viewpoint of S/N unless the efficiency of the heralding detector approaches 1. Now we focus on m as another performance index. The I1DC protocol creates a qubit using m pulses, such that a smaller m helps to reduce the tasks on the server. It is clear that m depends on p_1 from Eq. (8). In the protocol using WCP, the single photon probability p_1 is expressed as follows:

$$p_1 = \frac{Q_1}{Q_\mu} \geq \frac{Y_1^{L,v_1,v_2} \mu e^{-\mu}}{Q_\mu}, \tag{29}$$

where Y_1^{L,v_1,v_2} is the lower limit of single-photon transmittance, and $\mu e^{-\mu}$ is the probability of a single photon pulse by Poisson distribution. Since these values are fixed, it is impossible to raise the single photon probability further.

On the other hand, the single photon probability p_1 of HSPS includes the heralding detection probability η_A. This is a value that can be increased with the development of single photon detectors and other optical equipment. In addition, heralding maintains the value of Q_1 while decreasing Q_μ. Therefore, when HSPS is used, it is possible to reduce N and increase p_1—that is, reducing m. When a heralding detection efficiency η_A is 0.85, the dark count rate d_A is 1.0×10^{-8}, and the fiber length is $L = 25$ km, p_1 with HSPS is 0.65, exceeding that of WCP (0.51). In the case of $\eta_A = 1.0$, p_1 is 0.81. Therefore, the use of HSPS instead of WCP reduces the number of operations performed on the server.

VII. CONCLUSION

In this study, we investigated RBSP in blind quantum computation by using a heralded single photon source and decoy states. With the decoy-state method and the improved estimation, we show that the scaling of the required number N of pulses becomes $O(1/T)$. By lowering the multiphoton probability using HSPS and available photon number resolving detectors, the communication distance was extended to 500 km, which is more than twice that of WCP. We also showed that when the efficiency of the heralding detector approaches 1, RBSP-HSPS outperforms RBSP-WCP in terms of the efficiency S/N or the required number of pulses. Thus, the distance of secure cloud quantum computations can be greatly extended, facilitating the potential of future quantum computers.

ACKNOWLEDGEMENTS

We thank Keisuke Fujii and Yasunari Suzuki for their helpful discussion. TS was suppoerted by the ImPACT Program of the Council for Science, Technology and Innovation (Cabinet Office, Government of Japan), Photon Frontier Network Program (Ministry of Education, Culture, Sports, Science and Technology), CREST (Japan Science and Technology Agency), and JSPS KAKENHI Grant No. JP18K13469. TH was supported by the Toray Science foundation, SECOM foundation, Research Foundation for Opto-Science and Technology, JST PRESTO JPMJPR1769, and JST START ST292008BN.

[1] A. Broadbent, J. Fitzsimons and E. Kashefi, ”Universal blind quantum computation,” Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science, pp.517-526 (2009).

[2] R. Raussendorf and H. Briegel, ”A One-Way Quantum Computer,” *Phys. Rev. Lett.* **86**, pp.5188-5191 (2001).

[3] V. Dunjko, E. Kashefi and A. Leverrier, ”Blind quantum computing with weak coherent pulses,”*Phys. Rev. Lett.* **108**, 200502 (2012).

[4] W. -Y. Hwang, *Phys. Rev. Lett.* **91**, 057901 (2003).

[5] X. -B. Wang, *Phys. Rev. Lett.* **94**, 230503 (2005).

[6] H. -K. Lo, X. Ma and K. Chen, *Phys. Rev. Lett.* **94**, 230504 (2005).

[7] K. Xu and H.-K. Lo, ”Blind quantum computing with decoy states,”arXiv:quant-ph/ 1508.07910 (2015).

[8] Q. Zhao and Q. Li, ”Blind quantum computation with two decoy states,” *Advances in Intelligent Information Hiding and Multimedia Signal Processing*, pp.155-162

(2016).

[9] N. Lütkenhaus, *Phys. Rev. A* **61**, 052304 (2000).

[10] T. Horikiri and T. Kobayashi, *Phys. Rev. A* **73**, 032331 (2006).

[11] M. J. Fitch, B. C. Jacobs, T. B. Pittman, and J. D. Franson, *Phys. Rev. A* **68**, 043814 (2003).

[12] D. Achilles, C. Silberhorn, C. Sliwa, K. Banazek, and I. A. Walmsley, *Opt. Lett.* **28**, 2387 (2003).

[13] T. Horikiri, Y. Takeno, A. Yabushita, and T. Kobayashi, *Phys. Rev. A* **76**, 012306 (2007).

[14] http://www.scontel.ru/

[15] M. A. Nielsen, *Reports on mathematical physics* **57** , 147 (2006).

[16] R. Raussendorf, D. E. Browne and H. J. Briegel, *Phys. Rev. A* **68**, 022312 (2003).

[17] X. Ma, B. Qi, Y. Zhao and H.-K. Lo, *Phys. Rev. A* **72**, 012326 (2005).

[18] P. R. Tapster and J. G. Rarity, *Journal of Modern Optics* **45**, 595 (1998).

[19] H. Shibata, T. Honjo and K. Shimizu, *Optics Letters* **39**, 5078 (2014).