Experimental comparison between one-decoy and two-decoy implementations of the Bennett-Brassard 1984 quantum cryptography protocol

Youn-Chang Jeong,[1,*] Yong-Su Kim,[1,2] and Yoon-Ho Kim[1,†]

[1] *Department of Physics, Pohang University of Science and Technology, Pohang, 790-784, Korea*
[2] *Center for Quantum Information, Korea Institute of Science and Technology, Seoul, 136-791, Korea*

(Received 4 June 2015; published 14 January 2016)

The decoy-state method allows the use of weak coherent pulses in quantum cryptography, and to date, various strategies for the decoy state have been proposed. Here, we experimentally compare the secret key generation rates between the one-decoy and two-decoy implementations of the Bennett-Brassard 1984 (BB84) quantum key distribution protocol through a 3.1-km optical fiber at 780 nm. Once the parameters of the experimental setup are optimized for the maximal secret key generation rate for each implementation, it is found that the two-decoy implementation outperforms the one-decoy implementation.

DOI: 10.1103/PhysRevA.93.012322

I. INTRODUCTION

Quantum key distribution (QKD) enables two communicating parties, Alice (transmitter) and Bob (receiver), to possess a secret string of random bits (0s and 1s) or cryptographic keys that are secure from an eavesdropper, Eve. To offer unconditional security, a single-photon source is an essential element for building a secure quantum cryptography system [1,2]. Since a high-efficiency single-photon source optimized for quantum cryptography is not yet available, QKD is often implemented with weak coherent pulses (WCPs) such that the average photon number per pulse $\mu = \bar{n} < 1$. Attenuated laser pulses or WCPs, however, follow the Poissonian photon statistics closely, so there is a nonzero probability of having two or more photons. An eavesdropper, Eve, could then implement the photon number splitting (PNS) attack on the quantum channel to extract some of the shared key bits without being detected [3–5].

To deal with the potential PNS attack, the Scarani-Acin-Ribordy-Gisin 2004 (SARG04) protocol [6] and the decoy-state method [7] have been proposed. SARG04 differs from the BB84 protocol [8] only in the classical sifting procedure. Although SARG04 can counter the PNS attack without extra efforts and cost, it has a lower secret-key generation rate than that of the Bennett-Brassard 1984 (BB84) protocol in the real world under the most general attack [9–11]. The decoy-state method, first proposed by Hwang [7] and further developed by others [12,13], counters the PNS attack differently. The basic idea of the decoy-state method is that Alice prepares and sends WCPs with several different μ, which consist of the signal and decoy states, to Bob. Due to the lack of knowledge of which WCP is the signal and which is the decoy, Eve is forced to carry out the PNS attack on all WCPs. As the signal and the decoy states have different μ, Eve's PNS attack will cause the signal and the decoy yields at Bob to differ [7,12,13]. This difference can then be used to test the presence of the PNS attack on the quantum channel. The decoy-state method is usually implemented using the BB84 protocol [8] and more than one-decoy states may be used [12,13]. Although the decoy-state method itself is not a QKD protocol, the one-decoy (two-decoy) state method is usually called one-decoy (two-decoy) state protocol [14].

The decoy-state method so far has been implemented for the free-space quantum channel [15,16] and for the fiber-optic quantum channel [17–19] for specific average photon numbers per pulse for the signal (μ) and the decoy (ν) states. Although the optimal values of μ and ν can be calculated [20,21], there has not been an experimental study which investigated whether the theoretical optimum conditions match well with those of the experimental ones. To be more specific, there has not been an experimental study to compare the performance of one-decoy and two-decoy-state protocols in a given experimental setting.

In this work, we report an experimental comparison between one-decoy and two-decoy implementations of the BB84 quantum cryptography protocol. By using a 3.1 km optical fiber spool as the quantum channel and using 780 nm WCP, we have investigated the optimal conditions (i.e., maximum secure key generation rates) for the one-decoy and the two-decoy implementations of the BB84 protocols. Our experimental results show clearly that, given the same experimental conditions, the two-decoy (i.e., vacuum and WCP) state protocol outperforms the one-decoy (i.e., WCP only) state protocol.

II. SECRET KEY GENERATION RATE

Alice and Bob can generate the secret key from the sifted key by classical postprocessing that consists of error correction and privacy amplification [22,23]. The sifted keys contain errors, so Alice and Bob reconcile the sifted key via the error correction process. Some of the widely used error correction methods in QKD experiments are the cascaded method, winnow, and the low-density parity check (LDPC) [24–27]. Choosing a proper error correction code is important since each code requires different computing power and has a different efficiency. In theory, however, once the efficiency of the error correction is given, one can estimate the maximum secret key generation rate regardless of the actual QKD implementation. In the following, we set the error correction efficiency $f(x) = 1$ as widely assumed [14,21]. After the

[*] w31400@gmail.com
[†] yoonho72@gmail.com

error correction process, Alice and Bob possess identical keys, but the key may not be completely private. The privacy amplification process is then applied to extract secure keys.

The secret key generation rate after the classical postprocessing can be determined by the overall gain G_μ and the overall quantum bit error rate (QBER) Q_μ. The overall gain G_μ denotes the probability that Bob can obtain a detection event when Alice sends a WCP with average photon number μ. For a QKD system based on WCP, the overall gain can be represented as $G_\mu = \sum_{i=0}^{\infty} G_i = \sum_{i=0}^{\infty} Y_i \frac{\mu^i}{i!} e^{-\mu}$, where G_i and Y_i denote the gain and the yield of the i-photon state. The $\frac{\mu^i}{i!} e^{-\mu}$ factor represents the Poissonian photon number distribution of the WCP. The QBER Q_μ represents the probability that Bob will receive an incorrect bit value when Alice sends a bit value encoded in WCP with μ [14,21]. The secret key generation rate per pulse sent by Alice is then given as

$$r \geqslant r^L = -qG_\mu H_2(Q_\mu) + qG_1^L - qG_1^L H_2\big(Q_1^U\big), \qquad (1)$$

where q is the basis reconciliation factor (1/2 for the BB84 protocol), $H_2(x)$ is the binary Shannon entropy, and $G_1^L = Y_1 e^{-\mu}\mu$ and Q_1^U are the lower bound of the gain and the upper bound of QBER for the single-photon state, respectively. The first and third terms in Eq. (1) represent the error correction and the privacy amplification processes, respectively. Note that Eq. (1) includes the lower and upper bounds for the single-photon gain and QBER rather than the exact values. Therefore, G_1^L and Q_1^U need to be accurately estimated in an experiment to achieve the maximum secret key generation rate.

A. Two-decoy-state method

The BB84 protocol applied with the decoy-state method yields a larger number of secret keys than the BB84 protocol without the decoy. This is due to the fact that the BB84 with decoy allows us to more accurately estimate the values of G_1^L and Q_1^U than the BB84 without decoy. In the two-decoy-state method, two decoy states with average photon numbers ν_1 and ν_2 are transmitted. Usually, one of the decoy states is set to the vacuum state, $\nu_1 = 0$, and the other is usually weaker than the signal state, $\nu_2 = \nu < \mu$.

For the two-decoy scheme, the lower bound G_1^L of the signal photon gain and the upper bound Q_1^U of the single-photon QBER are given by [14,17]

$$G_1 \geqslant G_1^L = \frac{\mu^2 e^{-\mu}}{\mu\nu - \nu^2}\left(G_\nu^L e^{\nu} - G_\mu e^{\mu}\frac{\nu^2}{\mu^2} - Y_0^U \frac{\mu^2 - \nu^2}{\mu^2}\right), \qquad (2)$$

$$Q_1 \leqslant Q_1^U = \frac{G_\mu Q_\mu - e_0 Y_0 e^{-\mu}}{G_1^L}, \qquad (3)$$

respectively. Here, G_ν^L is the lower bound of the decoy gain $G_\nu^L = G_\nu\big(1 - \frac{10}{\sqrt{N_\nu G_\nu}}\big)$, where N_ν is the number of decoy pulses sent by Alice. Y_0^U and $e_0 = 0.5$ denote the upper bounds of the dark count probability and the error probability due to a dark count, respectively. Note that Y_0^U can be obtained directly from the vacuum decoy state. From Eqs. (1)–(3), we can calculate the lower bound of the secret key generation rate for the two-decoy-state method with BB84.

B. One-decoy-state method

The one-decoy-state method does not use the vacuum state, relying only on a single decoy state with photon number ν. Since the vacuum state is not used, the upper bound Y_0^U of the dark counts probability cannot be obtained from the experimental data but must be estimated as $Y_0 \leqslant Y_0^U = \frac{G_\mu Q_\mu \exp(\mu)}{e_0}$. Applying the estimated Y_0^U to Eqs. (2) and (3), one can get the lower bound G_1^L of the single-photon gain and the upper bound e_1^U of the single-photon QBER [14].

III. EXPERIMENT

Before we describe our experimental setup, it would be beneficial to briefly introduce the BB84 QKD protocol [8]. In the original BB84 protocol, Alice sends a single-photon pulse encoded randomly in one of the four polarization states that form two nonorthogonal bases to Bob. The polarization bases widely used in BB84 are the Z basis $\{|H\rangle, |V\rangle\}$ and the X basis $\{|45^\circ\rangle, |-45^\circ\rangle\}$. Here, $|H\rangle$ and $|V\rangle$ denote horizontal and vertical polarizations, respectively, and $|45^\circ\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$ and $|-45^\circ\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle)$. Bob then randomly selects the measurement basis and records the detection events. Later, Alice and Bob compare their bases via a classical communication channel and generate sifted keys only when their bases are the same. Secret keys can then be generated by classical postprocessing.

In our QKD system to implement one-decoy- and two-decoy-state protocols (Fig. 1), Alice's setup consists of two diode lasers (780 nm; one for the signal and the other for the decoy), a variable attenuator, two Pockels cells, a fiber polarization controller (FPC), and a field-programmable gate array (FPGA) controller. The signal and decoy laser pulses are combined by a single-mode fiber to clean up the spatial mode (not shown in Fig. 1). The average photon numbers of the signal and decoy can be changed by using a variable attenuator and a neutral density (ND) filter.

Alice first generates three random bit sequences: one for selecting the encoding basis, another for the raw key, and the third for choosing to launch the signal or decoy. The signal and decoy pulses are randomly encoded to one of four polarization

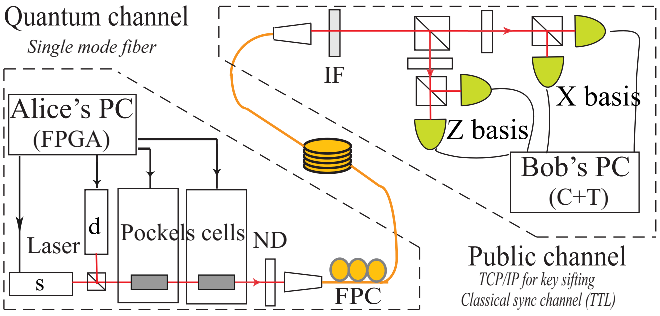

FIG. 1. Schematic of experimental setup. Alice: The signal laser (s) pulses and the decoy laser (d) pulses are strongly attenuated and polarization encoded with two Pockels cells (PC1, PC2). The signal laser, decoy laser, and Pockels cells are controlled by a field-programmable gate array module (FPGA). Bob: Bob's detection events are recorded using a PC-based counter and timer (C + T).

states ($|V\rangle,|H\rangle,|45^\circ\rangle,|-45^\circ\rangle$) by two Pockels cells. They are split into two paths; one is connected to a single-photon detector that checks the average photon number; the other is linked to Bob through the quantum channel, which is a 3.1-km-long single-mode fiber spool. The attenuation coefficient of the fiber at 780 nm is $\alpha = 3$ dB/km.

Bob receives the signal and decoy pulses through a 3-nm interference filter (IF) in order to reduce the background noise. The measurement basis is randomly chosen by the beam splitter in the X basis ($|45^\circ\rangle,|-45^\circ\rangle$) or the Z basis ($|V\rangle,|H\rangle$) by polarization analyzers and four single-photon detectors. To reduce background noise, the single-photon detectors are gated on at the expected arrival time of the incoming photon within 100-ns time windows. The detection efficiency is $\eta_{\text{Bob}} \approx 0.4$, and the detector dark count probability $p_d = (3.3 \pm 0.6) \times 10^{-5}$. The detection events are stored at Bob's computer in two counter and timer (C + T) peripheral component interconnect (PCI) boards.

The one- and two- (vacuum + weak) decoy-state methods with the BB84 protocol were implemented in the same QKD system under a fixed quantum channel. We experimentally investigated the lower bound of the secret key generation rate in one- and two-decoy-state methods under the most general eavesdropping attack. The numbers of raw keys were 109 Mbits in the one-decoy-state method for 109 s and 99 Mbits in the two-decoy-state method for 99 s.

IV. RESULTS AND DISCUSSION

Before the experiment, the numerical calculation was performed to determine the theoretical optimal conditions to maximize the number of secret keys using Eq. (1). For the one-decoy-state method, the optimal average photon numbers of the signal and decoy were calculated to be $\mu \approx 0.21$ and $\nu \approx 0.14$, respectively; the optimal signal-to-decoy-state ratio was found to be $\frac{N_\mu}{N_{\text{total}}} : \frac{N_\nu}{N_{\text{total}}} = 0.708 : 0.292$, where N_{total}, N_μ, and N_ν are the total numbers of raw, signal, and decoy bits sent by Alice. Note that the optimal value of the average photon numbers in our simulation is very different from the previous value ($\mu \approx 0.8$ and $\nu \approx 0.12$ in Ref. [17]) due to the large differences in the simulation parameters (Table I).

TABLE I. The key parameters for the optimal condition estimation are the detection error probability e_{det}, the dark count rate of the detector Y_0, the transmittance in Bob's side η_{Bob}, and the loss in the quantum channel ($10^{-\alpha l/10}$), where l is the length of the quantum channel and α is an attenuation coefficient. The detection error probability characterizes the stability and the alignment of the optical system and is usually independent of the length of the quantum channel. λ is the operating wavelength.

	λ (nm)	α (dB/km)	$e_{\text{det}}(\%)$	η_{Bob}	Y_0
Ref. [17]	1550	0.21	0.8269	0.0227	2.11×10^{-5}
This work	780	3	3.7	0.4	1.32×10^{-4}

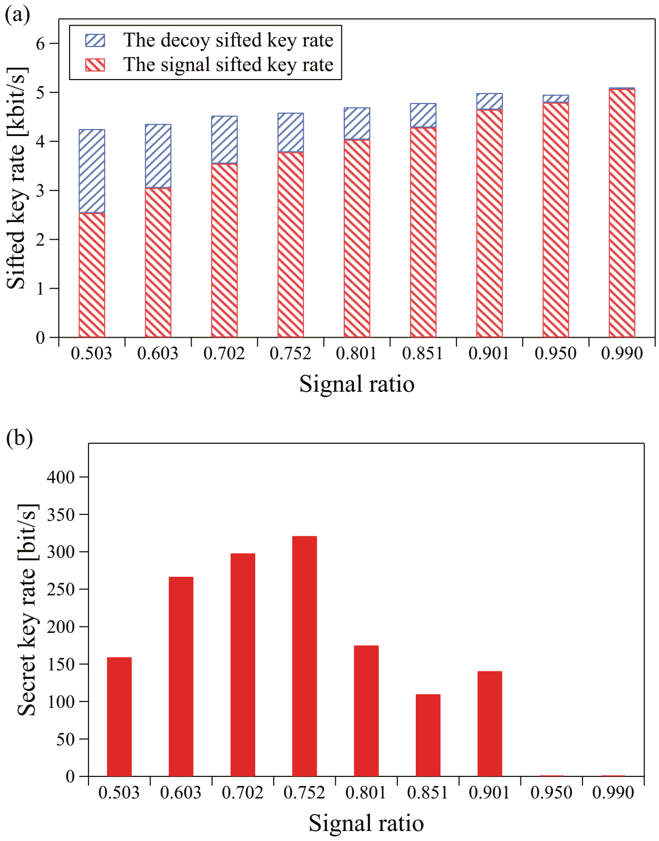

FIG. 2. (a) The sifted key rate and (b) the secret key rate for various signal ratios on BB84 with the one-decoy-state method. Experiments are done for $\mu \approx 0.211$ and $\nu \approx 0.135$.

A. The signal-to-decoy ratio in the one-decoy-state method

First, we experimentally investigated the optimal signal ratio at the fixed average photon numbers of the signal ($\mu \approx 0.211$) and of the decoy ($\nu \approx 0.139$) in the one-decoy-state protocol [Fig. 2(a)]. Because the signal has a larger average photon number than the decoy, the total sifted key rate slightly increases as the ratio of the signal increases. The QBERs were 4.2% ± 0.1% for the signal and 4.7% ± 0.2% for the decoy. The secret key rates [Fig. 2(b)] were estimated from the experimentally obtained QBER and the sifted key rate of the signal and decoy using Eq. (1). Although the sifted key rate increased as the signal ratio increased when $\mu > \nu$, the secret key rate cannot be increased with increasing signal ratio because we cannot obtain the tight bound of G_1^L as the sifted key rate of the decoy decreases. Hence, an optimal signal ratio which maximizes the secret key rate exists at a fixed average photon number of the signal and decoy. The secret key rate was highest when the signal ratio was 0.752 and was similar to the theoretical optimal signal ratio of 0.708.

We implemented the one-decoy-state protocol for several average photon numbers of the decoy. Although each result used the same average photon number ($\mu \approx 0.301$) for the signal, it had a different sifted key rate due to different optimal signal ratios [Fig. 3(a)]. The QBER of the decoy decreased from 5.6% to 4.0% as the average photon number of the decoy increased but did not change much if the dark count contributions were subtracted. Secret keys cannot be generated if the average photon number of the decoy is the same as that of the signal; this condition corresponds to the original BB84 protocol [11,28]. The secret key rate was highest at $\nu \approx 0.248$;

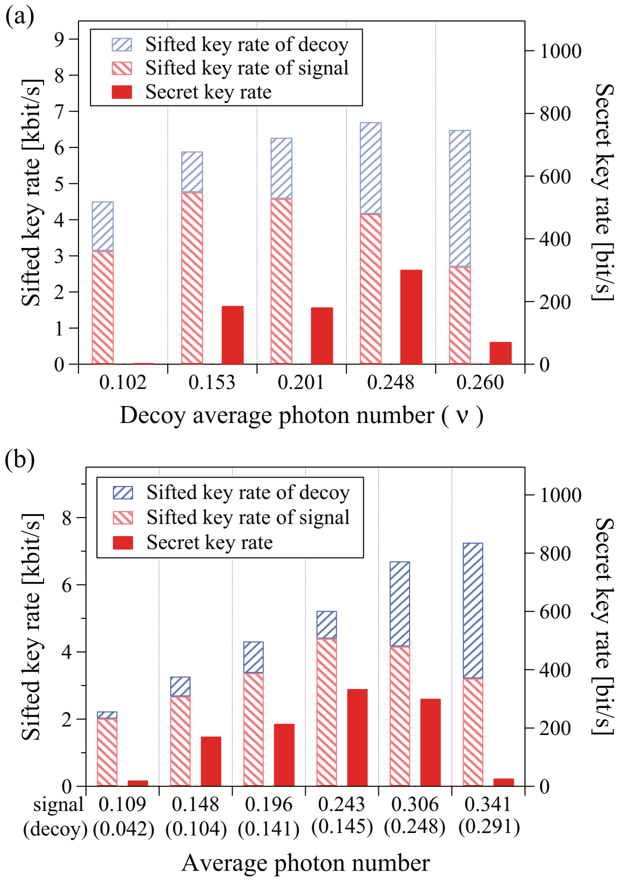

FIG. 3. (a) Key rates vs average photon number of the decoy for the one-decoy scheme. Each result uses the optimal signal ratio for a fixed average photon number of the signal ($\mu \approx 0.301$) and various average photon numbers of the decoy ($\nu \approx 0.102, 0.153, 0.201, 0.248,$ and 0.260). The QBERs of the signal were $\sim 4.1\%$. (b) Key rates for the various average photon numbers of the signal and decoy in the one-decoy scheme.

therefore the decoy average photon number has an optimal value when the average photon number of the signal is fixed at $\mu \approx 0.301$.

We repeated the sifted (secret) key rate vs decoy average photon number measurement for various values of the signal average photon number [Fig. 3(b)]; the total sifted key rate increased as the average photon number of the signal and the decoy increased; then the ratio of the decoy in the total sifted keys increased to generate many secret keys when the average photon number of the decoy was large. The QBER of the signal decreased from 4.6% to 3.7% as the average photon number of the signal increased, and the QBER of the decoy decreased from 5.9% to 3.9% as the average photon number of the decoy increased. However, the QBERs did not change much if the detector dark count contributions were subtracted; this result is similar to that obtained in a previous BB84 experiment [11,28]. The one-decoy-state method with BB84 has a maximum secret key rate of 334 bits/s at the optimal average photon number of the signal ($\mu \approx 0.243$) and the decoy ($\nu \approx 0.145$) in the 3.1-km quantum channel; these values are similar to the theoretical results ($\mu \approx 0.21$ and $\nu \approx 0.14$).

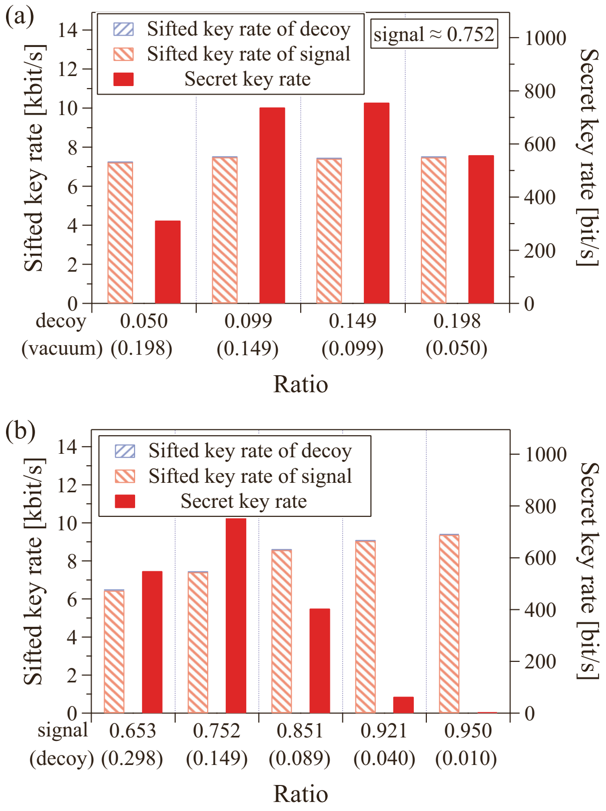

FIG. 4. (a) Key rate vs weak decoy ratio when the signal ratio was fixed 0.752 and (b) key rate vs ratio of signal and weak decoy at two (vacuum + weak) decoys. Experiments are done for $\mu \approx 0.416$, $\nu \approx 0.010$, and vacuum. The sifted key rate of the decoy is very small because the decoy has a smaller average photon number than does the signal.

B. Two-decoy-state method

We also implemented the two- (vacuum + weak) decoy-state method with the BB84 protocol for a fixed average photon number of the signal ($\mu \approx 0.416$) and the decoy ($\nu \approx 0.010$). Theoretically, the fixed average photon number of the signal and the decoy is not an optimal value to maximize the number of the secret key in the two-decoy scheme. First, the two-decoy-state method with BB84 was implemented at the variation of the weak decoy ratio under a fixed signal ratio ($\frac{N_\mu}{N_{\mathrm{total}}} \approx 0.752$); then the sum of the ratio of the vacuum and the weak decoy state was fixed at $\frac{N_\nu + N_{\mathrm{vacuum}}}{N_{\mathrm{total}}} \approx 0.248$. The total sifted key rate in the experimental results [Fig. 4(a)] was almost constant because the signal average photon number was larger than the decoy (i.e., $\mu \gg \nu$). QBERs of the signal and decoy were 3.6% and 10.5%, respectively. The decoy state has a higher QBER than the signal state because the average photon number of the decoy is small. But QBERs of the signal and the decoy were almost the same when the dark count contribution was subtracted. As shown in Fig. 4(a), the secret key rate estimated from the sifted key rate and QBER was highest at $\frac{N_\nu}{N_{\mathrm{total}}} \approx 0.149$; that is, the weak decoy ratio has an optimal value under the fixed average photon number and signal ratio.

We implemented the two-decoy-state protocol for various values of the signal ratio [Fig. 4(b)] in $\mu \approx 0.416$ and $\nu \approx$

TABLE II. Comparison of experimental results for one and two decoys. The secret key rate, $R = N_{\text{total}} r$, is estimated from the number of signal and decoy pulses (N_μ, N_ν) sent by Alice, G_μ, G_ν, E_μ, and E_ν, where G_x and E_x are the overall gain and the overall QBER, $x = \mu, \nu$. Note that r is the secret key rate per pulse sent by Alice, and N_{total} is the number of total pulses sent by Alice.

	One decoy	Two decoys
N_{total}	1.09×10^8	9.9×10^7
G_μ	1.14×10^{-2}	1.95×10^{-2}
G_ν	6.91×10^{-3}	4.81×10^{-4}
E_μ	4.04×10^{-2}	3.76×10^{-2}
E_ν	4.37×10^{-2}	1.17×10^{-1}
R (bits/s)	3.34×10^2	7.56×10^2

0.010. In the result, the total sifted key rate increased according to increasing signal ratio, but QBERs of the signal and the decoy were almost constant at 3.8% and 11.4%, respectively. Then the measured dark count rate in the vacuum state was about $Y_0 = 6.8 \times 10^{-5}$. We estimated the secret key rate from the sifted key rate, QBER, and average photon number. The maximum secret key rate of 756 bits/s was generated at $\frac{N_\mu}{N_{\text{total}}} \approx 0.752$ and $\frac{N_\nu}{N_{\text{total}}} \approx 0.149$.

Finally, we compare the experimental results of one- and two-decoy-state methods in Table II. With the one-decoy-state method, we could generate a secret key rate of 334 bits/s, while we achieved 756 bits/s with the two-decoy-state method. The results clearly show that the two-decoy method outperforms the one-decoy method for the same experimental conditions.

V. CONCLUSION

We have successfully performed an experimental implementation of one-decoy- and two-decoy-state (vacuum + weak) protocols via a 3.1-km quantum channel. We have checked the optimal value for the average photon number and signal-to-decoy ratio in the one-decoy-state protocol with both theory and experiment. We have also shown the optimal ratio of the signal and the decoy in the two-decoy protocol. With these results, we have experimentally shown that the two-decoy-state method can generate a larger number of secret keys than the one-decoy-state method at the same length of the quantum channel.

ACKNOWLEDGMENTS

This work was supported in part by the National Research Foundation of Korea (Grant No. 2013R1A2A1A01006029).

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).

[3] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A **51**, 1863 (1995).

[4] G. Brassard, N. Lutkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).

[5] N. Lutkenhaus, Phys. Rev. A **61**, 052304 (2000).

[6] V. Scarani, A. Acin, G. Ribordy, and N. Gisin, Phys. Rev. Lett. **92**, 057901 (2004).

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

[8] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, New York, 1984), pp. 175–179.

[9] B. Kraus, C. Branciard, and R. Renner, Phys. Rev. A **75**, 012316 (2007).

[10] Y.-C. Jeong, Y.-S. Kim, and Y.-H. Kim, Laser Phys. **21**, 1438 (2011).

[11] Y.-C. Jeong, Y.-S. Kim, and Y.-H. Kim, Laser Phys. Lett. **11**, 095201 (2014).

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

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

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

[15] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter, Phys. Rev. Lett. **98**, 010504 (2007).

[16] M. Jofre, A. Gardelein, G. Anzolin, W. Amaya, J. Capmany, R. Ursin, L. Penate, D. Lopez, J. L. San Juan, J. A. Carrasco, F. Garcia, F. J. Torcal-Milla, L. M. Sanchez-Brea, E. Bernabeu, J. M. Perdigues, T. Jennewein, J. P. Torres, M. W. Mitchell, and V. Pruneri, Opt. Express **19**, 3825 (2011).

[17] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, Phys. Rev. Lett. **96**, 070502 (2006).

[18] C.-Z. Peng, J. Zhang, D. Yang, W.-B. Gao, H.-X. Ma, H. Yin, H.-P. Zeng, T. Yang, X.-B. Wang, and J.-W. Pan, Phys. Rev. Lett. **98**, 010505 (2007).

[19] Y. Liu, T.-Y. Chen, J. Wang, W.-Q. Cai, X. Wan, L.-K. Chen, J.-H. Wang, S.-B. Liu, H. Liang, L. Yang, C.-Z. Peng, K. Chen, Z.-B. Chen, and J.-W. Pan, Opt. Express **18**, 8587 (2010).

[20] S. Ali and M. R. B. Wahiddin, Eur. Phys. J. D **60**, 405 (2010).

[21] X. Ma, Ph. D. thesis, University of Toronto, 2008.

[22] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).

[23] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **4**, 325 (2004).

[24] G. Brassard and L. Salvail, in *Advances in Cryptology—EUROCRYPT '93*, Lecture Notes in Computer Science Vol. 765 (Springer Verlag, Berlin, 1994), pp. 410–423.

[25] W. T. Buttler, S. K. Lamoreaux, J. R. Torgerson, G. H. Nickel, C. H. Donahue, and C. G. Peterson, Phys. Rev. A **67**, 052303 (2003).

[26] G. Van Assche, J. Cardinal, and N. J. Cerf, IEEE Trans. Inf. Theory **50**, 394 (2004).

[27] N. Benletaief, H. Rezig, and A. Bouallegue, J. Quantum Inf. Sci. **4**, 117 (2014).

[28] Y.-S. Kim, Y.-C. Jeong, and Y.-H. Kim, Laser Phys. **18**, 810 (2008).