Research Article | Vol. 25, No. 10 | 15 May 2017 | OPTICS EXPRESS 11894

Optics EXPRESS

Security analysis of quantum key distribution on passive optical networks

KYONGCHUN LIM, HEASIN KO, CHANGHO SUH, AND JUNE-KOO KEVIN RHEE*

School of Electrical Engineering, Korea Advanced Institute of Science and Technology (KAIST), 291 Daehak-ro, Yuseong-gu, Daejeon 34141, South Korea
**jk.rhee@kaist.ac.kr*

Abstract: Needs for providing security to end users have brought installation of quantum key distribution (QKD) in one-to-many access networks such as passive optical networks. In the networks, a presence of optical power splitters makes issues for secure key rate more important. However, researches for QKD in access networks have mainly focused on implementation issues rather than protocol development for key rate enhancement. Since secure key rate is theoretically limited by a protocol, researches without protocol development cannot overcome the limit of secure key rate given by a protocol. This brings need of researches for protocol development. In this paper, we provide a new approach which provides secure key rate enhancement over the conventional protocol. Specifically, we propose the secure key rate formula in a passive optical network by extending the secure key rate formula based on the decoy-state BB84 protocol. For a passive optical network, we provide a way that incorporates cooperation across end users. Then, we show that the way can mitigate a photon number splitting (PNS) attack which is crucial in an well known decoy BB84 protocol. Especially, the proposed scheme enables multi-photon states to serve as secure keys unlike the conventional decoy BB84 protocol. Numerical simulations demonstrate that our proposed scheme outperforms the decoy BB84 protocol in secure key rate.

OCIS codes: (270.5565) Quantum communications; (270.5568) Quantum cryptography; (270.5585) Quantum information and processing.

References and links

1. W.-Y. Hwang, "Quantum key distribution with high loss: Toward global secure communication," Phys. Rev. Lett. **91**, 057901 (2003).
2. H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," Phys. Rev. Lett. **108**, 130503 (2012).
3. K. Lim, H. Ko, K. Kim, C. Suh, and J.-K. Rhee, "The error tolerance bound for secure multi-qubit QKD against incoherent attack," IEEE J. Sel. Topics Quantum Electron. **21**, 1–9 (2015).
4. K. Patel, J. Dynes, M. Lucamarini, I. Choi, A. Sharpe, Z. Yuan, R. Penty, and A. Shields, "Quantum key distribution for 10 Gb/s dense wavelength division multiplexing networks," Appl. Phys. Lett. **104**, 051123 (2014).
5. Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, and H.-K. Lo, "Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution," Phys. Rev. Lett. **112**, 190503 (2014).
6. F. Xu, K. Wei, S. Sajeed, S. Kaiser, S. Sun, Z. Tang, L. Qian, V. Makarov, and H.-K. Lo, "Experimental quantum key distribution with source flaws," Phys. Rev. A **92**, 032305 (2015).
7. J.-P. Bourgoin, N. Gigov, B. L. Higgins, Z. Yan, E. Meyer-Scott, A. K. Khandani, N. Lütkenhaus, and T. Jennewein, "Experimental quantum key distribution with simulated ground-to-satellite photon losses and processing limitations," Phys. Rev. A **92**, 052339 (2015).
8. W.-Y. Liang, M. Li, Z.-Q. Yin, W. Chen, S. Wang, X.-B. An, G.-C. Guo, and Z.-F. Han, "Simple implementation of quantum key distribution based on single-photon Bell-state measurement," Phys. Rev. A **92**, 012319 (2015).
9. M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. Dynes, S. Fasel, S. Fossier, M. Fürst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J.-B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden, and A. Zeilinger, "The SECOQC quantum key distribution network in Vienna," New J. Phys. **11**, 075001 (2009).

#281430 https://doi.org/10.1364/OE.25.011894
Journal © 2017 Received 23 Nov 2016; revised 22 Apr 2017; accepted 25 Apr 2017; published 12 May 2017

Optics EXPRESS

10. M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger, "Field test of quantum key distribution in the Tokyo QKD Network," Opt. Express **19**, 10387–10409 (2011).
11. S. Wang, W. Chen, Z.-Q. Yin, Y. Zhang, T. Zhang, H.-W. Li, F.-X. Xu, Z. Zhou, Y. Yang, D.-J. Huang, L.-J. Zhang, F.-Y. Li, D. Liu, Y.-G. Wang, G.-C. Guo, and Z.-F. Han, "Field test of wavelength-saving quantum key distribution network," Opt. Lett. **35**, 2454–2456 (2010).
12. Y. Zhao, "Quantum secure communication networks: Products and solutions," http://2014.qcrypt.net/wp-content/uploads/Zhao.pdf .
13. V. Fernandez, R. J. Collins, K. J. Gordon, P. D. Townsend, and G. S. Buller, "Passive optical network approach to gigahertz-clocked multiuser quantum key distribution," IEEE J. Quantum Electron. **43**, 130–138 (2007).
14. I. Choi, R. J. Young, and P. D. Townsend, "Quantum key distribution on a 10Gb/s WDM-PON," Opt. Express **18**, 9600–9612 (2010).
15. A. Ciurana, J. Martínez-Mateo, M. Peev, A. Poppe, N. Walenta, H. Zbinden, and V. Martin, "Quantum metropolitan optical network based on wavelength division multiplexing," Opt. Express **22**, 1576–1593 (2014).
16. B. Fröhlich, J. F. Dynes, M. Lucamarini, A. W. Sharpe, Z. Yuan, and A. J. Shields, "A quantum access network," Nature **501**, 69–72 (2013).
17. H. Shim, K. Cho, Y. Takushima, and Y. Chung, "Correlation-based OTDR for in-service monitoring of 64-split TDM PON," Opt. Express **20**, 4921–4926 (2012).
18. Q. Feng, W. Li, Q. Zheng, J. Han, J. Xiao, Z. He, M. Luo, Q. Yang, and S. Yu, "Impacts of backscattering noises on upstream signals in full-duplex bidirectional PONs," Opt. Express **23**, 15575–15586 (2015).
19. X. Zhang, F. Lu, S. Chen, X. Zhao, M. Zhu, and X. Sun, "Remote coding scheme based on waveguide Bragg grating in PLC splitter chip for PON monitoring," Opt. Express **24**, 4351–4364 (2016).
20. X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," Phys. Rev. A **72**, 012326 (2005).
21. P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, and G. J. Milburn, "Linear optical quantum computing with photonic qubits," Rev. Mod. Phys. **79**, 135 (2007).
22. D. Hrg, A. Poppe, A. Fedrizzi, B. Blauensteiner, H. Hübel, and A. Zeilinger, "Security aspects and simulations of practical QKD platforms," Quantum physics of nature Theory, experiment and interpretation in collaboration with 6th European QIPC workshop, Austria (2005).
23. F. Mattioli, Z. Zhou, A. Gaggero, R. Gaudio, R. Leoni, and A. Fiore, "Photon-counting and analog operation of a 24-pixel photon number resolving detector based on superconducting nanowires," Opt. Express **24**, 9067–9076 (2016).
24. T. Moroder, M. Curty, and N. Lütkenhaus, "Detector decoy quantum key distribution," New J. Phys. **11**, 045008 (2009).
25. H.-L. Yin, Y. Fu, Y. Mao, and Z.-B. Chen, "Detector-decoy quantum key distribution without monitoring signal disturbance," Phys. Rev. A **93**, 022330 (2016).
26. P. Curtacci, F. Garzia, R. Cusani, and E. Baccarelli, "Performance analysis of different multi-user optical passive networks for quantum cryptography applications," Proc. SPIE **6187**, 61870U (2006).
27. H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," Phys. Rev. Lett. **94**, 230504 (2005).
28. F. Benatti, M. Fannes, R. Floreanini, and D. Petritis, *Quantum Information, Computation and Cryptography: An Introductory Survey of Theory, Technology and Experiments*, vol. 808 (Springer, 2010).
29. R. Renner, "Security of quantum key distribution," Int. J. Quantum Inf. **6**, 1–127 (2008).
30. P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," Phys. Rev. Lett. **85**, 441 (2000).
31. M. Dušek, M. Jahma, and N. Lütkenhaus, "Unambiguous state discrimination in quantum cryptography with weak coherent states," Phys. Rev. A **62**, 022306 (2000).
32. D. Gottesman, H.-K. Lo, N. Lutkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," in "Information Theory, 2004. ISIT 2004. Proceedings. International Symposium on," (IEEE, 2004), p. 136.
33. S. Miki, T. Yamashita, H. Terai, and Z. Wang, "High performance fiber-coupled NbTiN superconducting nanowire single photon detectors with Gifford-McMahon cryocooler," Opt. Express **21**, 10208–10214 (2013).
34. K. Takemoto, Y. Nambu, T. Miyazawa, Y. Sakuma, T. Yamamoto, S. Yorozu, and Y. Arakawa, "Quantum key distribution over 120 km using ultrahigh purity single-photon source and superconducting single-photon detectors," Sci. Rep. **5** (2015).
35. A. S. Holevo, "Bounds for the quantity of information transmitted by a quantum communication channel," Probl. Peredachi Inf. **9**, 3–11 (1973).

Optics EXPRESS

1. Introduction

Quantum key distribution (QKD) has been received much attention as it provides a new paradigm of secure communications. An application to point-to-point (P2P) links in a backbone network is a good example for the quantum secure networks. To achieve this, many research groups have conducted and reported theoretical and experimental results of QKD for P2P networks [1–8]. By being accelerated, nationwide QKD field trials have been conducted in leading countries [9–11]. Recently, QKD systems based on decoy BB84 protocol are commercialized [12]. However, due to different network structures between core and access networks, these results are not enough to characterize the security of multi-user networks. In order to provide services for end users, researches for multi-user networks have been carried out [13–16].

An objective of the point-to-multi-point networks is to provide higher secure key rate to end users. To achieve this, we aim to develop the way that all users collaborate to lower power of eavesdropping. We propose a way to combat against a photon number splitting (PNS) attack with the help of information on coincidence detection among end users at multi-points. By the proposed scheme, we show that some of pulses having multiple photons can be used as secret keys unlike in the conventional decoy BB84 protocol.

Nevertheless, most works for multi-user networks mainly focus on implementing QKD access networks with decoy BB84 protocol because a QKD system with decoy BB84 protocol is easy to implement and was theoretically proven to be unconditionally secure. Implementation issues such as wavelength assignment and consolidation between conventional and quantum channels are considered in [13–15]. The authors in [16] considered configuration issues by comparing downstream and upstream quantum access networks. They asserted it is beneficial in terms of cost and feasibility of the systems to configure the downstream quantum access networks in which transmitters are located in end users. However, secure key rate of the researches can be eventually limited without development of protocols. In the decoy BB84 protocol, a critical limiting factor in secure key rate is caused by a PNS attack. By the attack, pulses having multiple photons referred to as multi-photon states cannot generate secure keys [1]. Therefore, only pulses having a single photon referred to as single-photon states can generate secure keys in the decoy BB84 protocol. Since the researches did not consider the protocol development to mitigate a PNS attack, their performance cannot overcome the limitation regardless of system configurations such as a transmission direction. The insufficiency of researches to overcome the limitation has brought necessity for the research about protocol development.

In this work, we investigate access networks in which there is a splitter which makes the network structure of one-to-many type. One such example is passive optical network (PON). Based on the network, we show that the aforementioned limitation can be overcome by a simple way using the characteristics of a PON: coincidence detections among end users can lower the amount of secret keys taken by a PNS attack. Consequently, multi-photon states can be used to generate secret keys, which has been perceived unusable states for secure keys. Since a standard PON can be typically deployed with the maximum of 1 to 64 split ratio [17–19], we incorporate coincidence detection into the GLLP model [20] and performed numerical evaluations about a PON with 64 end users.

The remaining parts of this paper are structured as follows. In Section 2, a system model for QKD on PON is described. Section 3 introduces general decoy BB84 QKD protocol for PON. The proposed method is explained in Section 4. Corresponding secure key rate is discussed in Section 5. A numerical analysis of secret key rate of QKD protocol for PON with the proposed method is discussed in Section 6. Finally, we conclude our paper in Section 7 with some concluding remarks.

Optics EXPRESS

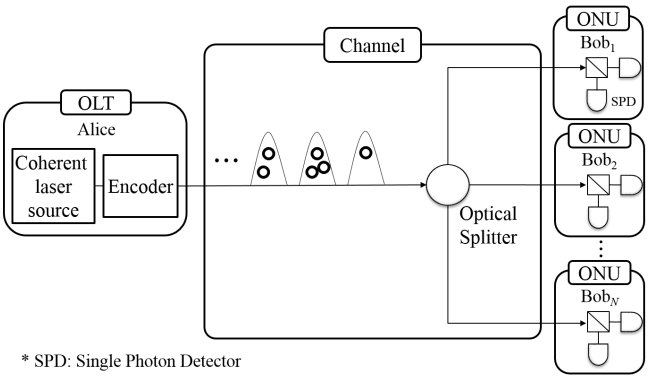


Fig. 1. System model for a general down-stream PON system.

2. System model

A QKD system with decoy BB84 protocol on PON consists of one optical line terminal (OLT), one optical fiber channel and multiple optical network units (ONUs) as in Fig. 1. To describe the structure, specific characteristics of a laser source, a channel, and a detector such as a distribution of photons generated from a laser source, channel loss, and photon detection probabilities are modeled with a typical way as in [20].

Alice in an OLT possesses a phase randomized coherent laser source and an encoder to generate the quantum states for QKD session. By the characteristics of the source, the number of photons follows the Poisson distribution as follows:

$$\Pr(\text{the number of photons} = i) = \frac{\mu^i}{i!} e^{-\mu}, \tag{1}$$

where μ is a mean photon number of the source.

A channel considered in this paper can be called as quantum channel because a quantum state can be delivered through this channel. This quantum channel can be characterized by its internal transmittance. Let T_{ch} denote the transmittance of a quantum channel. Then, T_{ch} can be decomposed into two parts which are the transmittance of fiber itself, T_{fiber}, and transmittance of a splitter, T_{splitter}.

$$T_{\text{ch}} = T_{\text{fiber}} T_{\text{splitter}} = 10^{-\frac{\alpha l}{10}} 10^{-\frac{L_{\text{splitter}}}{10}}, \tag{2}$$

where α, l, and L_{splitter} represent channel loss coefficient in dB/km, distance of optical fiber in km, and splitting loss in dB, respectively.

A quantum state arrived at an ONU, Bob, suffers additionally from internal transmittance of the ONU. Internal transmittance of an ONU, T_{ONU}, can be expressed as follows:

$$T_{\text{ONU}} = 10^{-\frac{L_{\text{ONU}}}{10}}, \tag{3}$$

where L_{ONU} represents internal loss of an ONU in dB.

After internal optical circuits of an ONU, a quantum state is detected by one out of two single photon detectors (SPD) in an ONU. Detection efficiency of a SPD can be referred to as γ_{det}. With γ_{det} and Eqs. (2) and (3), we can calculate the overall detection quantum efficiency, γ_{all}, of a quantum state sent from Alice:

$$\gamma_{\text{all}} = \gamma_{\text{det}} T_{\text{ONU}} T_{\text{ch}}. \tag{4}$$

Optics EXPRESS

The aforementioned γ_{all} is related to transmittance of a single photon. In a real situation, however, multiple photons can be transmitted by characteristics of a laser source in Eq. (1). Unfortunately, most conventional SPDs can only resolve either zero or non-zero photons [21]. Thereby, we cannot identify the number of photons in an incoming quantum state from a detection event. Due to this reason, detection efficiency of i-photon states, γ_i, can be expressed as follows:

$$\gamma_i = 1 - (1 - \gamma_{\text{all}})^i. \tag{5}$$

There is another factor causing detection of a SPD, which is the dark count of a SPD. Due to the dark count, detection can occur in Bob's side even for zero photon states. Accordingly, to calculate conditional probability that a quantum state is detected given a quantum state, we need to take into account γ_i and dark count. The conditional probability previously specified is also called $yield$ as in [20]. We define Y_i as the conditional probability that a quantum state is detected given an i-photon state generated by a laser source in Alice:

$$Y_i = \Pr(\text{detection occurs} \mid i\text{-photon state}). \tag{6}$$

By assuming detection events from two different sources, which are a transmitted quantum state and dark count are independent, Y_i can be comprised as follows:

$$Y_i = \gamma_i + Y_0 - \gamma_i Y_0, \tag{7}$$

where Y_0 the false alarm probability caused by dark count. That is, Y_0 corresponds to a dark count probability per unit time, p_{dark}. As in [22], p_{dark} is defined as probability that at least one dark count occurs among two detectors in Bob's side.

Let Q_i denote the probability of detection of an i-photon state, which is called as $gain$ of an i-photon state as in [20]. With Y_i and the Poisson distribution of a laser source, Q_i can be calculated as follows:

$$\begin{aligned} Q_i &= \Pr(i\text{-photon state, detection occurs}) \\ &= Y_i \frac{\mu^i}{i!} e^{-\mu}. \end{aligned} \tag{8}$$

Through detections, received states are converted to information having errors. This can be modeled as quantum bit error rate (QBER). To model QBER, define e_i as QBER of an i-photon state. QBER is affected by two major factors which are dark count and system imperfection. In case of dark count, it causes errors with a probability of e_0. Since dark counts of two detectors in Bob's side are independent, e_0 is 1/2 in this system. For a received quantum state, an error can occur with probability modeled as e_{d} characterizing system imperfection. Based on the aforementioned features,

$$\begin{aligned} e_i &= \frac{\Pr(\text{erroneous detection occurs}|i\text{-photon state})}{\Pr(\text{detection occurs}|i\text{-photon state})} \\ &= \frac{e_0 Y_0(1-\gamma_i) + e_{\text{d}}\gamma_i(1-Y_0) + e_0 e_{\text{d}}\gamma_i Y_0}{Y_i}. \end{aligned} \tag{9}$$

Based on Eqs. (8) and (9), we can calculate the overall gain and QBER. First, the overall gain, Q_μ, represents detection probability given a laser source with mean photon number μ.

$$\begin{aligned} Q_\mu &= \Pr(\text{detection occurs}) \\ &= \sum_{i=0}^{\infty} Q_i \\ &= 1 - (1 - Y_0)e^{-\gamma_{\text{all}}\mu}. \end{aligned} \tag{10}$$

Optics EXPRESS

Second, the overall QBER, E_μ, represents error probability given a laser source with mean photon number μ. This can be calculated as follows:

$$\begin{aligned} E_\mu &= \frac{\Pr(\text{erroneous detection occurs})}{\Pr(\text{detection occurs})} \\ &= \frac{\sum_{i=0}^{\infty} e_i Q_i}{\sum_{i=0}^{\infty} Q_i} \\ &= \frac{e_0 Y_0 e^{-\gamma_{\text{all}}\mu} + e_{\text{d}}(1-Y_0)(1-e^{-\gamma_{\text{all}}\mu})}{1-(1-Y_0)e^{-\gamma_{\text{all}}\mu}}. \end{aligned} \tag{11}$$

3. General QKD protocol for PON

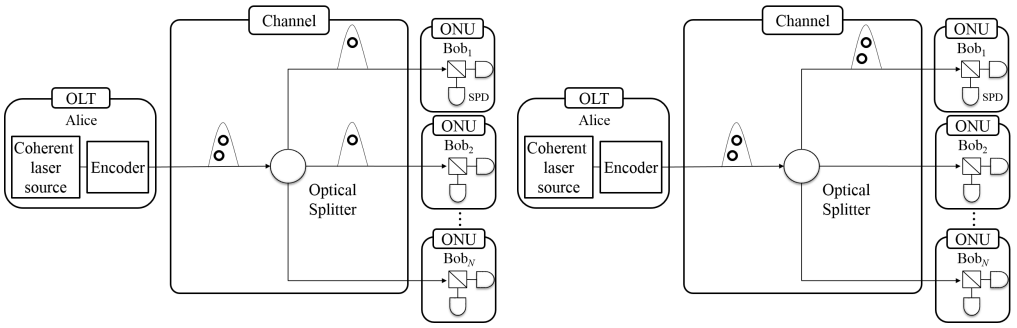
In this paper, we consider a decoy BB84 based QKD protocol for a down-stream PON with our proposed method which is an estimation step for photon number distribution utilizing characteristics of a PON. For understanding of the proposed method, we briefly introduce a decoy BB84 QKD protocol [20] on PON. As in most cases, assume that a QKD session is generated between a pair of an OLT and an ONU. That is, there exist N QKD sessions generated if a PON is installed with N ONUs. Due to the aforementioned assumption, the protocol is symmetric for each pair of an OLT and an ONU. Since transmitter and receiver are generally called as Alice and Bob in quantum cryptography, from now on, Alice and Bob substitute for OLT and ONU, respectively. The typical protocol is as follows:

- Alice randomly chooses mean photon number of laser source to select either a decoy or a signal state. Then, Alice randomly generates weak coherent pulses and modulate them among four states using either phase or polarization modulation. Four states are selected from two bases which are $\mathrm{Z} = \{|0\rangle, |1\rangle\}$ or $\mathrm{X} = \{|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}, |-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}\}$ bases. Then, modulated pulses are sent to Bob.
- To detect the received quantum state, Bob generates a random bit sequence to choose a basis between is Z and X bases.
- After a session of transmission, Alice and Bob announce detection time and basis information through a public channel. Additionally, Alice announces whether decoy or signal states each pulse belonged to. Here, by investigating detection ratios of decoy and signal states, it is blocked that an eavesdropper, Eve, intentionally transmits more multi-photon states than single-photon states for a PNS attack. Then, detected outcomes are sifted out to discard the photon measurements at Bob that have used different bases from those of Alice. The remained bit sequence is called the $sifted\ key$.
- Alice and Bob compare some of the sifted key to estimate QBER. Based on the estimated QBER, Alice and Bob calculate the corresponding secure key rate.
- To generate a final secure key, Alice and Bob perform post-processing consisting of error correction and privacy amplification by sending additional information through a pubic channel.

4. Estimation of a photon number distribution

A photon number distribution can be estimated with photon number resolving detectors [23] or photon number non-resolving detectors [24, 25]. Obviously, the former is expected to better estimate the distribution. In this work, we consider the worst-case scenario based on the latter setting to evaluate the minimal performance gain that can also be guaranteed for the former case. We also emphasize that the latter case is more realistic due to the high cost of using the photon number resolving detectors.

Optics EXPRESS



(a) The case where each Bob receives a single photon.

(b) The case where at least one Bob receives multiple photons.

Fig. 2. The possible cases when a pulse having multiple photons is generated.

As related works, the authors in [24, 25] estimate the distribution with a photon number non-resolving detector and a variable attenuator in point-to-point network. In our proposed method, we utilize the collaboration among ONUs with photon number non-resolving detection. In this way, the photon state distributed over a point-to-multi-point PON by an optical splitter, instead of using variable attenuators can be collectively exploited for more information on photon number distribution, as discussed with specific details below.

When photon number distribution can be estimated by a collaborative measurement of photon detections at multiple Bobs we can anticipate increase of secure key rate, as it can mitigate a PNS attack, which leads generating of secure keys from multi-photon states. This can be achieved by using characteristics of a PON which provides coincidence detection among Bobs.

In a PON, a multi-photon state can be randomly routed to Bobs in the particle-like behavior limit at an optical splitter due to the fact that a photon is indivisible by nature [26]. This characteristics generates coincidence detections. The coincidence detection provides information about photon number distribution in a pulse sent by an OLT, Alice. By collecting all detection information, Alice can estimate the distribution of detections, e.g., the number of detections in one Bob, the number of detections in two different Bobs by the same pulse, and so on. This prevents an eavesdropper, Eve, from a certain PNS attack because it makes estimated distribution of detections apart from theoretically calculated distribution of detections with given system parameters. Therefore, Eve can perform a PNS attack to limited portion of multi-photon states.

For easy understanding, here, we address how the estimation limits a PNS attack with an example. Assume eavesdropping happens after the splitter. Specifically, there are two cases whether Eve can perform a PNS attack or not. A safe case is about multi-photon states in which Eve cannot perform a PNS attack. Assume there are the number N of Bobs and an i-photon state in which $i \leq N$. Then, the safe case represents i Bobs detect at the same time slot. An example of a two-photon case, $i = 2$, is shown in Fig. 2(a). In this case, two Bobs detect a single photon. Unsafe cases that Eve can perform PNS attacks are all the cases that more than one photon can be routed to one Bob. An example for this is shown in Fig. 2(b). In this case, at least one Bob receives multiple photons.

For given system parameters such as detection channel loss, internal loss of Bob, and detection efficiency of a SPD, we can calculate the frequency of detection. After a session of transmission, Alice can estimate the frequency of detection by receiving detection information from Bobs. By comparing the calculated and estimated frequencies of detection, if Eve performs a PNS attack for all multi-photon states as if she does on a conventional decoy BB84 QKD system, it can be detected because the two values become different. Assume that Eve per-

Optics EXPRESS

Table 1. Secure key rates for different attacks.

Attack	Control of the splitter	Distribution of coincidence detections	Distributions of photon numbers	Secure key rate
Before the splitter	No	Changed	Changed	Eq. (16)
			Unchanged	Eq. (12)
		Unchanged	Changed	Eq. (16)
			Unchanged	Eq. (15)
	Yes	Changed	Changed	Eq. (16)
			Unchanged	Eq. (12)
		Unchanged	Changed	Eq. (16)
			Unchanged	Eq. (19)
After the splitter	No	Changed	Changed	Eq. (16)
			Unchanged	Eq. (12)
		Unchanged	Changed	Eq. (16)
			Unchanged	Eq. (19)
	Yes	Changed	Changed	Eq. (16)
			Unchanged	Eq. (12)
		Unchanged	Changed	Eq. (16)
			Unchanged	Eq. (19)

forms a PNS attack on the safe case. Then, coincidence detection among Bobs decreases. This manifests as difference between calculated and estimated frequency of detection.

Here we add a new behavior to the conventional protocol of Section 3:

- Coincidence Monitoring: To accumulate the statistics of i-Bob coincidence detections to monitor whether it is different from the theoretically calculated value with given system parameters or not.

Therefore, Eve should perform a PNS attack except for the safe case to hide her existence. That is, Alice and Bob can obtain additional secure key from some multi-photon states corresponding to the safe case.

5. Secure key rate

In this section, we explicitly provide secure key rates depending on possible attacks. The corresponding results are summarized in Table 1.

5.1. Attack before splitter

Assume the PNS attack performed before the splitter. First, consider that Eve cannot intentionally control the splitter. In this case, the PNS attack changes the distribution of coincidence detections because Eve cannot disambiguate the safe and unsafe cases. This leads to the following secure key rate based on the GLLP model of decoy-state BB84 protocol if the photon number distributions of signal and decoy states are invariant [27].

$$R \geq \frac{1}{2}\{-Q_\mu f(E_\mu)H_2(E_\mu) + Q_1[1 - H_2(e_1)]\}, \tag{12}$$

where $H_2(\cdot)$ and $f(\cdot)$ represent binary Shannon entropy and error correction efficiency, respectively. Other parameters are defined in Section 2. In Eq. (12), the first term represents the number

Optics EXPRESS

of required bits for error correction. When we consider leaked information to an eavesdropper, Eve, there are two cases that correspond to single photon and multi-photon states. In case of single-photon states, Eve cannot perform a PNS attack over single-photon states prevented by decoy states. Instead, Eve performs a coherent attack which is the most powerful attack constrained by only law of physics [28]. When a length of secret keys becomes infinity, the amount of information that can be extracted by a coherent attack becomes the same as that of collective attack [29]. In a collective attack, extracted information can be calculated based on Holevo information. Because Eve can obtain $H_2(e_1)$ bits for a single-photon state by the attack [30], these should be removed by privacy amplification. This is expressed in the second term in Eq. (12) representing the number of remained bits after privacy amplification for a single-photon state. For multi-photon states, as already mentioned that Eve can perform a PNS attack on them, secure key cannot be generated from them. For that reason, gain from multi-photon states is not included in Eq. (12).

On the other hand, Eve can maintain the distribution for coincidence detections. In order to maintain it, Eve cannot perform a PNS attack. Since eavesdropping happens before the splitter and Eve doesn't control the splitter in this case, the PNS attack maintaining the distribution is impossible. Instead, Eve can perform collective and unambiguous state discrimination (USD) attacks [31]. First, consider that a collective attack is performed without an USD attack. By the attack, the maximum mutual information between Alice and Eve, $I(A;E)_i$, is expressed as follows:

$$I(A;E)_i = H_2\left(\frac{1+\cos^i c}{2}\right), \tag{13}$$

where $\cos c = 1 - 2e_i$. See Appendix A for the detailed calculation. This leads to:

$$R \geq \frac{1}{2}\left\{-Q_\mu f(E_\mu)H_2(E_\mu) + Q_1[1-H_2(e_1)] + \sum_{i=2}^{\infty} Q_i\left(1 - I(A;E)_i\right)\right\}, \tag{14}$$

Assume Eve performs collective and USD attacks. An USD attack can succeed for more than two-photon states with a non-zero probability [31]. For more than two-photon states, if Eve transmits qubits only when the USD attack succeeds, she can do perfect eavesdropping without causing errors. On the other hand, for single and two-photon states, Eve can only perform the collective attack because the USD attack fails with certainty. Therefore, secure keys can be obtained from only single and two-photon states by performing privacy amplification on them. Based on this, we can calculate the secure key rate against the both attacks.

$$R \geq \frac{1}{2}\left\{-Q_\mu f(E_\mu)H_2(E_\mu) + Q_1[1-H_2(e_1)] + Q_2\left(1 - I(A;E)_2\right)\right\}. \tag{15}$$

If the distributions of photon numbers for signal and decoy states are altered, this indicates the distributions are controlled by Eve. This severely degrades a secure key rate regardless of the distribution for coincidence detections. In this case, the following secure key rate can be achieved as in [32].

$$R \geq \frac{1}{2}\left\{-Q_\mu f(E_\mu)H_2(E_\mu) + \left(Q_\mu - P_{\text{multi}}\right)\left[1 - H_2\left(\frac{E_\mu}{Q_\mu - P_{\text{multi}}}\right)\right]\right\}, \tag{16}$$

where P_{multi} represents the probability that Alice generates multi-photon states.

Second, consider that Eve can intentionally control the splitter so that the distribution for coincidence detections is invariant. However, the PNS attack on the safe cases changes the photon number distributions of signal and decoy states because Eve cannot distinguish between signal and decoy states at each time instance. Therefore, the corresponding secure key rate can be calculated as in Eq. (16).

Optics EXPRESS

Instead, Eve can keep all the distributions under no PNS attack on the safe cases. In this case, Eve performs collective and USD attacks on the safe cases. First, consider the scenario of the collective attack without the USD attack.

For the secure key rate from the safe cases, we need to calculate the detection probability of the safe cases. For $i \geq 2$, let Q_{ii} denote the probability that i Bobs detect single photons when Alice generates an i-photon state. This can be calculated as follows:

$$Q_{ii} = \underbrace{\frac{\mu^i}{i!}e^{-\mu}}_{(1)} \underbrace{\binom{i}{i}\gamma_{\text{all}}^i}_{(2)} \underbrace{\frac{1}{n}\binom{n-1}{i-1}\frac{(i-1)!}{1!\cdots 1!}\left(\frac{1}{n}\right)^{i-1}}_{(3)} \underbrace{(1-Y_0)^{n-i}}_{(4)}. \tag{17}$$

In Eq. (17), the first factor (1) represents the probability that Alice generates an i-photon state. Since all i photons should be detected, it is reflected as in factor (2). Factor (3) refers to the probability that i photons are routed to i Bobs one by one. Since a secure key rate is calculated in terms of a given Bob, one single photon should be routed to that Bob. This is reflected as $1/n$ in factor (3). By using multinomial distribution, the other terms in factor (3) represent $(i-1)$ photons are routed to $(i-1)$ Bobs one by one. Simultaneously, no dark count should happen at any of $(n-i)$ Bobs that do not receive a photon.

Based on the number, N_{Bob}, of Bobs in a network, with Eqs. (13) and (17), we can formulate secure key rate R as follows:

$$\begin{aligned} R &\geq \frac{1}{2}\left\{-Q_\mu f(E_\mu)H_2(E_\mu) + Q_1[1-H_2(e_1)] + \sum_{i=2}^{N_{\text{Bob}}} Q_{ii}\left(1-I(A;E)_i\right)\right\} \\ &= \frac{1}{2}\left\{-Q_\mu f(E_\mu)H_2(E_\mu) + Q_\mu - \text{PA}_{\text{overall}}\right\}, \end{aligned} \tag{18}$$

where

$$\begin{aligned} \text{PA}_{\text{overall}} &= Q_0 + Q_1 H_2(e_1) + \sum_{i=2}^{N_{\text{Bob}}} Q_{ii} I(A;E)_i + \sum_{i=2}^{N_{\text{Bob}}}(Q_i - Q_{ii}) + \sum_{i=N_{\text{Bob}}+1}^{\infty} Q_i \\ &= Q_0 + Q_1 H_2(e_1) + \sum_{i=2}^{N_{\text{Bob}}} Q_{ii} I(A;E)_i + \sum_{i=2}^{N_{\text{Bob}}}(Q_i - Q_{ii}) + Q_\mu - \sum_{i=0}^{N_{\text{Bob}}} Q_i \\ &= Q_\mu + Q_1(H_2(e_1) - 1) + \sum_{i=2}^{N_{\text{Bob}}} Q_{ii}(I(A;E)_i - 1). \end{aligned}$$

As in Eq. (18), the overall secure key rate can be expressed by three terms, which infer how the proposed protocol works. In Eq. (18), the first, second, and third terms indicate required information for error correction, detected information, and required information for privacy amplification, respectively. This infers that a secure key can be obtained by removing the amount of information corresponding to $\text{PA}_{\text{overall}}$ from a detected signal without a procedure for distinguishing safe and unsafe cases.

Assume Eve performs collective and USD attacks. In this case, the USD attack for more than two-photon states and a PNS attack on the unsafe two-photon states guarantee perfect eavesdropping without causing errors. Therefore, only single and the safe two-photon states can generate secure keys through privacy amplification.

$$R \geq \frac{1}{2}\left\{-Q_\mu f(E_\mu)H_2(E_\mu) + Q_1[1-H_2(e_1)] + Q_{22}\left(1-I(A;E)_2\right)\right\} \tag{19}$$

Optics EXPRESS

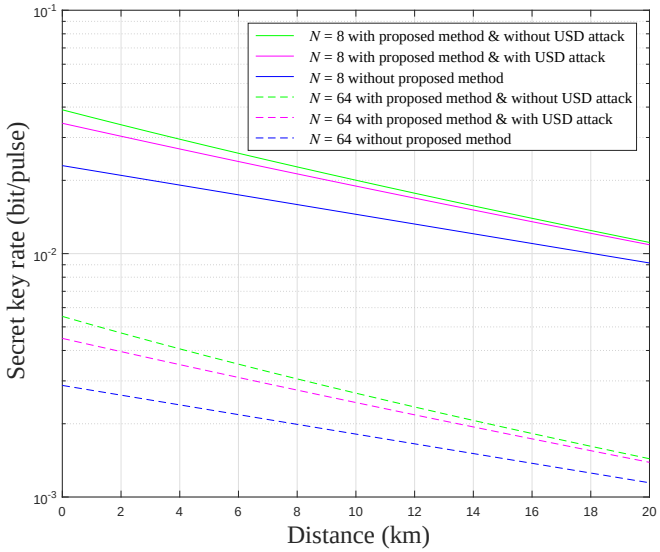


Fig. 3. Comparison of secure key rate between QKD system with and without the proposed method under an ideal setup.

5.2. *Attack after splitter*

Assume the PNS attack is performed after the splitter. First, consider that Eve cannot intentionally control the splitter. In this case, Eve can distinguish the safe and unsafe cases so that she can maintain the distribution for coincidence detections. Here, if Eve wants to maintain the photon number distributions of signal and decoy states, only the PNS attack on the unsafe cases is allowable. Therefore, Eve performs collective and USD attacks on the safe cases. The corresponding secure key rate can be calculated as in Eq. (19).

Second, assume Eve can control the splitter. Then, Eve can maintain all the distributions if she only performs the PNS attack on the unsafe cases. The corresponding secure key rate is the same as in Eq. (19).

6. Simulation results

Performance of the system with the proposed method in terms of secure key rate is numerically evaluated in this section. For performance comparison, the conventional BB84 protocol with decoy-state is used. Since attacks without the change of monitoring factors such as the distributions are mainly considered in QKD, we evaluate the secure key rates for the corresponding cases. Specifically, we simulate the secure key rates with Eqs. (12), (18) and (19). For fare performance comparisons, each simulation is conducted with an optimal mean photon number of each system. We conduct two numerical simulations depending on parameters of devices and the number of ONUs (Bobs) in a PON. The first simulation is conducted with almost ideal devices. The purpose of the first simulation is to provide an ideal upper bound in terms of secure key rate. Subsequently, we conduct the second simulation to identify an achievable secure key rate considering currently available devices to compare with the upper bound.

The simulation parameters used in the first case are as follow. Basically, the optical loss of fiber is $\alpha = 0.2$dB/km as a conventional optical fiber. Each Bob has ideal SPDs with 100% detection efficiency, $\gamma_{\mathrm{det}} = 1$, and 0 dark count probability, $Y_0 = 0$. Inside of each Bob, there is no optical loss, $L_{\mathrm{ONU}} = 0$ dB, and no system error, $e_{\mathrm{d}} = 0$. In post-processing, it is assumed that

Optics EXPRESS

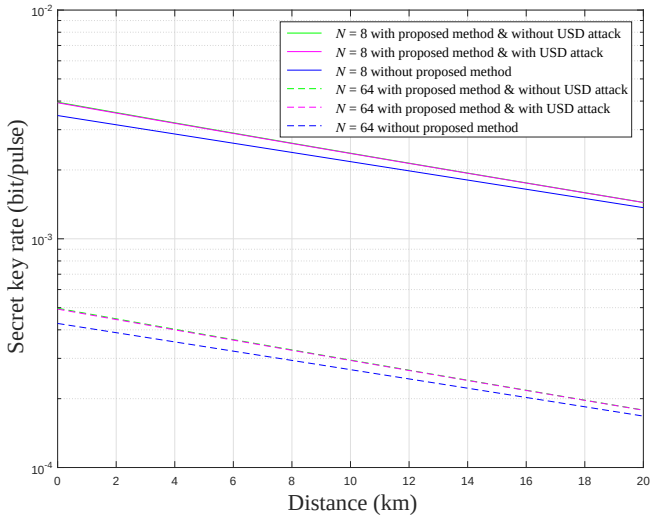


Fig. 4. Comparison of secure key rate between QKD system with and without the proposed method under an implementable setup.

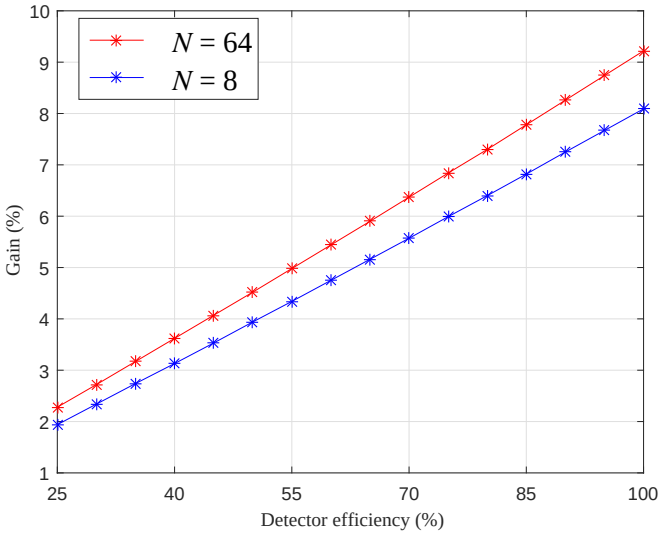


Fig. 5. Comparison of secure key rate gain depending on detector efficiency

Bob can perform ideal error correction, which means $f(E_\mu) = 1$. Results of the corresponding evaluations are shown in Fig. 3, where solid and dotted lines indicate QKD systems with and without the proposed method, respectively. Since distance between an OLT and an ONU is about 20km or less in a conventional PON, we plot results up to 20km. In case of a QKD system without the proposed method, for $N = 8$ and 64, optimal mean photon numbers to achieve the maximum secure key rate are 1.001 obtained by differentiating Eq. (12). For $N = 64$ (8), the optimal mean photon numbers of the proposed system are 1.270 (1.220) under no USD attack and 1.190 (1.170) under the USD attack. At a distance of 20 km, for $N = 64$ (8), the secure key

Optics EXPRESS

rates are enhanced by about 25.54% (21.44%) under no USD attack and 21.35% (18.82%) under the USD attack. The reason why we can obtain additional secure keys is utilizing multi-photon states as secret keys in the proposed method. By the same reason, the proposed method increases the usable mean photon number to generate additional secure keys because multi-photon states can be used to generate secure keys which is impossible without our proposed method.

In case of the second simulation, implementable parameters are considered. The same optical fiber loss is assumed as that of the previous simulation. As for the SPDs of Bobs, superconductor SPDs are assumed to be used, for which one can assume 67% detection efficiency, $\gamma_{\text{det}} = 0.67$, and 1.6×10^{-6} dark count probability, $Y_0 = 1.6 \times 10^{-6}$ [33]. L_{ONU}, e_{d}, and $f(E_\mu)$ are set to 3 dB, 2.3%, and 1.2, respectively, which are typical parameters in experimental results [34]. The corresponding simulation result is shown in Fig. 4. For $N = 64(8)$, the optimal mean photon number of the conventional system is 0.593 (0.592), while those of the proposed system are 0.630 (0.630) under no USD attack and 0.630 (0.630) under an USD attack, respectively. Here, for $N = 64(8)$, we demonstrate that our system provides 6.09 to 6.24% (5.33 to 5.43%) gain over the conventional system depending on the type of attacks at 20km. We see negligible performance degradation due to the USD attack.

Although superconductor SPDs show high detector efficiency, deployment of such SPDs in a PON can be a burden due to their cost. In order to consider a more realistic scenario in which we employ lower-cost SPDs which typically yield lower detector efficiency, we also conduct more simulations in which detector efficiency is varied over a wide range from 25% to 100%. Fig. 5 shows the gain due to our protocol as a function of detector efficiency when we assume a fiber distance of 20km and the USD attack. We see that a gain increases with detector efficiency, although the detector efficiency depends highly on the cost of SPDs that we can employ. For the larger N, we should use cheaper SPDs given the same budget, and this yields lower detector efficiency. On the other hand, the larger N provides a higher gain, as illustrated in Fig. 5. This implies that given the detector cost constraint (which may depend on implementation technology), there may be a sweet spot on N such that the gain is maximized. So our result sheds some lights into how to design such secured access networks in practice.

7. Conclusion

In this paper, we investigate how to improve secure key rate of QKD in a multi-user network such as PON. Specifically, to achieve that, we utilize characteristics of a PON which provides coincidence detection among ONUs, Bobs. Accordingly, we identify that secure keys can be exploited from multi-photon states unlike the conventional way which generates secure key only from single-photon states. For usable multi-photon states, we rigorously analyze the amount of information leaked to an eavesdropper, Eve. From this, we provide a mathematical model of secure key rate for QKD on a PON. Two different numerical simulations are conducted and presented for the cases of ideal and implementable setups. Our simulation results show that at 20km, the key rate improvement in the ideal setup is 21.35%. Even in the implementable setup, the gain is respectable: $\sim$ 6.09%. Furthermore, our results reveal that the effect of the USD attack is negligible. We believe that our work may pave a solid background for further researches on QKD in multi-user networks.

Appendix A: Mutual Information leaked to an eavesdropper under photon number splitting attack on safe multi-photon states

As mentioned in Section 5, an eavesdropper, Eve, can performs a collective attack to a multi-photon state [3].

Since a photon has single-qubit information on a 2-dimensional Hilbert space $H^{\otimes 2}$, a general N-photon state can be modeled as multiple qubits on $2N$-dimensional Hilbert space $H^{\otimes 2N}$.

Optics EXPRESS

Here, since photons in a pulse are indistinguishable, we need to consider input state representation pertinent to indistinguishable photons when we analyze an Eve's attack for a N-photon state. For example, indistinguishable two photons are represented as four states such as $|00\rangle$, $(|01\rangle + |10\rangle)/\sqrt{2}$, $(|01\rangle - |10\rangle)/\sqrt{2}$, and $|11\rangle$. Based on this, for a given N-photon state $|\mathbf{Q}_N\rangle$ in which photons are indistinguishable, Eve's attack U can be formulated as follows:

$$U|\mathbf{Q}_N\rangle \otimes |\psi_0\rangle = \sum_{\mathbf{E}\subset\{1,2,\ldots,N\}} \sqrt{D_{\mathbf{E}}}\,|\mathbf{Q}_{\mathbf{E}}\rangle \otimes |\psi_{\mathbf{E}}^{\mathbf{Q}_N}\rangle\,, \tag{20}$$

where $|\psi_0\rangle$ represents ancilla qubit states prepared by Eve, $|\mathbf{Q}_{\mathbf{E}}\rangle$ and $|\psi_{\mathbf{E}}^{\mathbf{Q}_N}\rangle$ are qubit states after the attack. Specifically, compared to the input state $|\mathbf{Q}_N\rangle$, $|\mathbf{Q}_{\mathbf{E}}\rangle$ refers to qubits having errors on the i-th qubit where $i \in \mathbf{E}$. $|\psi_{\mathbf{E}}^{\mathbf{Q}_N}\rangle$ refers to Eve's ancilla qubits after the attack corresponding to $|\mathbf{Q}_{\mathbf{E}}\rangle$. The probability of each state is represented by $D_{\mathbf{E}}$. As in [3], by the Schmidt decomposition and characteristics of unitary transformation of Eq. (20), one can find a condition for $|\psi_{\mathbf{E}}^{\mathbf{Q}_N}\rangle$.

$$\langle\psi_{\mathbf{E}}^{\mathbf{Q}_N}|\psi_{\mathbf{E}'}^{\mathbf{Q}'_N}\rangle = 0 \quad \text{for } \mathbf{E} \neq \mathbf{E}'. \tag{21}$$

Before proceeding detailed calculation, for easy understanding, we show calculation of a two-photon state case first. By expanding the result of a two-photon state case, a general case can be easily calculated. To represent the bases and states of input qubits $|\mathbf{Q}_2\rangle$, we define

$$|\mathbf{Q}_2\rangle \equiv |q_{bs}q_{bs}\rangle\,, \tag{22}$$

where q_{bs} indicates a single qubit encoded with basis $b \in \{\mathrm{Z}, \mathrm{X}\}$ and state $s \in \{0, 1\}$. For example, $q_{\mathrm{Z}0}$ is a single qubit state encoded in state 0 with basis Z.

To analyze the information obtained by Eve, it is enough to consider a single basis case because Eve perform a symmetric attack regarding the bases. Unless Eve performs a symmetric attack, the attack can be easily detected because probability of error among bases are unbalanced. Therefore, we proceed calculation only for the ZZ basis, which means both qubits of Eve are encoded with Z basis. In this case, with Eq. (21) and a 16-dimensional Hilbert space to express all possible states of $|\psi_{\mathbf{E}}^{\mathbf{Q}_2}\rangle$, $|\psi_{\mathbf{E}}^{\mathbf{Q}_2}\rangle$ can be parametrized with four variables a_1, a_2, b_1, and b_2 as follows [3]:

$$|\psi^{q_{\mathrm{Z}0}q_{\mathrm{Z}0}}\rangle = |0\rangle|0\rangle|0\rangle|0\rangle\,, \tag{23}$$
$$|\psi_{\{1\}}^{q_{\mathrm{Z}0}q_{\mathrm{Z}0}}\rangle = |0\rangle|1\rangle|0\rangle|0\rangle\,, \tag{24}$$
$$|\psi_{\{2\}}^{q_{\mathrm{Z}0}q_{\mathrm{Z}0}}\rangle = |0\rangle|0\rangle|0\rangle|1\rangle\,, \tag{25}$$
$$|\psi_{\{1,2\}}^{q_{\mathrm{Z}0}q_{\mathrm{Z}0}}\rangle = |0\rangle|1\rangle|0\rangle|1\rangle\,, \tag{26}$$
$$|\psi^{q_{\mathrm{Z}1}q_{\mathrm{Z}0}}\rangle = |a_1\rangle|0\rangle|0\rangle|0\rangle\,, \tag{27}$$
$$|\psi_{\{1\}}^{q_{\mathrm{Z}1}q_{\mathrm{Z}0}}\rangle = |b_1\rangle|1\rangle|0\rangle|0\rangle\,, \tag{28}$$
$$|\psi_{\{2\}}^{q_{\mathrm{Z}1}q_{\mathrm{Z}0}}\rangle = |a_1\rangle|0\rangle|0\rangle|1\rangle\,, \tag{29}$$
$$|\psi_{\{1,2\}}^{q_{\mathrm{Z}1}q_{\mathrm{Z}0}}\rangle = |b_1\rangle|1\rangle|0\rangle|1\rangle\,, \tag{30}$$
$$|\psi^{q_{\mathrm{Z}0}q_{\mathrm{Z}1}}\rangle = |0\rangle|0\rangle|a_2\rangle|0\rangle\,, \tag{31}$$
$$|\psi_{\{1\}}^{q_{\mathrm{Z}0}q_{\mathrm{Z}1}}\rangle = |0\rangle|1\rangle|a_2\rangle|0\rangle\,, \tag{32}$$
$$|\psi_{\{2\}}^{q_{\mathrm{Z}0}q_{\mathrm{Z}1}}\rangle = |0\rangle|0\rangle|b_2\rangle|1\rangle\,, \tag{33}$$
$$|\psi_{\{1,2\}}^{q_{\mathrm{Z}0}q_{\mathrm{Z}1}}\rangle = |0\rangle|1\rangle|b_2\rangle|1\rangle\,, \tag{34}$$

Optics EXPRESS

$$|\psi^{q_{Z_1}q_{Z_1}}\rangle = |a_1\rangle|0\rangle|a_2\rangle|0\rangle, \tag{35}$$
$$|\psi^{q_{Z_1}q_{Z_1}}_{\{1\}}\rangle = |b_1\rangle|1\rangle|a_2\rangle|0\rangle, \tag{36}$$
$$|\psi^{q_{Z_1}q_{Z_1}}_{\{2\}}\rangle = |a_1\rangle|0\rangle|b_2\rangle|1\rangle, \tag{37}$$
$$|\psi^{q_{Z_1}q_{Z_1}}_{\{1,2\}}\rangle = |b_1\rangle|1\rangle|b_2\rangle|1\rangle, \tag{38}$$

where $|a_i\rangle = \cos a_i|0\rangle + \sin a_i|1\rangle$ and $|b_i\rangle = \cos b_i|0\rangle + \sin b_i|1\rangle$ for $i \in \{1,2\}$.

As in [3], with Eqs. (20), (23) to (38), and $\sum_{\mathbf{E}\subset\{1,2\}} D_{\mathbf{E}} = 1$, error probabilities can be expressed as follows:

$$D = \frac{f_1 f_2}{(1+f_1)(1+f_2)}, \tag{39}$$
$$D_{\{1\}} = \frac{f_2}{(1+f_1)(1+f_2)}, \tag{40}$$
$$D_{\{2\}} = \frac{f_1}{(1+f_1)(1+f_2)}, \tag{41}$$
$$D_{\{1,2\}} = \frac{1}{(1+f_1)(1+f_2)}. \tag{42}$$

where $f_1 = (1+\cos b_1)/(1-\cos a_1)$ and $f_2 = (1+\cos b_2)/(1-\cos a_2)$.

Note that, for multi photon states, multiple qubits are encoded with the same basis and state. That is, $\mathbf{Q}_2$ can be $|00\rangle$ or $|11\rangle$ in the ZZ basis. This reduces the number of possible outcomes from Eve's unitary operation working for arbitrary input states of $\mathbf{Q}_2$. As a result, this provides Eve has more information for a multi-qubit state than a single qubit state. To specifically calculate maximum mutual information between Alice and Eve for a two-qubit state $I(A;E)_2$, we use Holevo's theorem [35].

$$I(A;E)_2 \le S(\rho_E) - \sum_{s=0}^{1} Pr(q_{Z_s}q_{Z_s}) S(\rho_E^{q_{Z_s}q_{Z_s}}), \tag{43}$$

where $S(\cdot)$ indicates von Neumann entropy, ρ_E represents Eve's density matrix, $Pr(q_{Z_s}q_{Z_s})$ is the probability that Alice transmits qubit $|q_{Z_s}q_{Z_s}\rangle$, and $\rho_E^{q_{Z_s}q_{Z_s}}$ Eve's conditional density matrix given a qubit $|q_{Z_s}q_{Z_s}\rangle$ sent by Alice. Since, Alice transmits states with uniform distribution in this protocol, $Pr(q_{Z_s}q_{Z_s})$ in Eq. (43) becomes 1/2. Eve's density matrix is defined as $\rho_E = \sum_{s=0}^{1} Pr(q_{Z_s}q_{Z_s})\rho_E^{q_{Z_s}q_{Z_s}}$. Eve's conditional density matrix can be easily calculated by a partial trace of Eq. (20) with parameterization of $|\psi_{\mathbf{E}}^{\mathbf{Q}_2}\rangle$.

$$\rho_E^{q_{Z_s}q_{Z_s}} = \sum_{\mathbf{E}\subset\{1,2\}} D_{\mathbf{E}} |\psi_{\mathbf{E}}^{q_{Z_s}q_{Z_s}}\rangle\langle\psi_{\mathbf{E}}^{q_{Z_s}q_{Z_s}}|. \tag{44}$$

The remaining part of works are to calculate von Neumann entropies of ρ_E and $\rho_E^{q_{Z_s}q_{Z_s}}$. First, for $s = 0, 1$, eigenvalues of $\rho_E^{q_{Z_s}q_{Z_s}}$ are D, $D_{\{1\}}$, $D_{\{2\}}$, and $D_{\{1,2\}}$. Therefore,

$$\sum_{s=0}^{1} Pr(q_{Z_s}q_{Z_s}) S(\rho_E^{q_{Z_s}q_{Z_s}}) = S(\rho_E^{q_{Z_0}q_{Z_0}}) = -\sum_{\mathbf{E}\in\{1,2\}} D_{\mathbf{E}} \log_2 D_{\mathbf{E}}. \tag{45}$$

Second, eigenvalues of ρ_E are $D(1 \pm \cos a_1 \cos a_2)/2$, $D_{\{1\}}(1 \pm \cos b_1 \cos a_2)/2$, $D_{\{2\}}(1 \pm \cos a_1 \cos b_2)/2$, and $D_{\{1,2\}}(1 \pm \cos b_1 \cos b_2)/2$. With these eigenvalues, $S(\rho_E)$ is calculated as follows:

$$S(\rho_E) = Dg(c_+(a_1,a_2)) + D_{\{1\}}g(c_+(b_1,a_2)) + D_{\{2\}}g(c_+(a_1,b_2)) + D_{\{1,2\}}g(c_+(b_1,b_2))$$

Optics EXPRESS

$$
\begin{aligned}
&+ Dg\left(c_-(a_1,a_2)\right) + D_{\{1\}}g\left(c_-(b_1,a_2)\right) + D_{\{2\}}g\left(c_-(a_1,b_2)\right) + D_{\{1,2\}}g\left(c_-(b_1,b_2)\right) \\
&- \sum_{\mathbf{E}\in\{1,2\}} D_{\mathbf{E}} \log_2 D_{\mathbf{E}} \\
\leq\ & g\left(Dc_+(a_1,a_2) + D_{\{1\}}c_+(b_1,a_2) + D_{\{2\}}c_+(a_1,b_2) + D_{\{1,2\}}c_+(b_1,b_2)\right) \\
&+ g\left(Dc_-(a_1,a_2) + D_{\{1\}}c_-(b_1,a_2) + D_{\{2\}}c_-(a_1,b_2) + D_{\{1,2\}}c_-(b_1,b_2)\right) \\
&- \sum_{\mathbf{E}\in\{1,2\}} D_{\mathbf{E}} \log_2 D_{\mathbf{E}}, \qquad (46)
\end{aligned}
$$

where $g(x) = -x\log_2 x$ and $c_\pm(x,y) = (1 \pm \cos x \cos y)/2$. Inequality of Eq. (46) is derived from Jensen's inequality because $g(\cdot)$ is a concave function. The equality condition of Eq. (46) is satisfied when $a_1 = a_2 = b_1 = b_2 = c$ where c is constant. Then, we obtain

$$S(\rho_E) = g\left(\frac{1+\cos^2 c}{2}\right) + g\left(\frac{1-\cos^2 c}{2}\right) - \sum_{\mathbf{E}\in\{1,2\}} D_{\mathbf{E}} \log_2 D_{\mathbf{E}}, \qquad (47)$$

$$D = \left(\frac{1+\cos c}{2}\right)^2 = (1-D)^2, \qquad (48)$$

$$D_{\{1\}} = \left(\frac{1-\cos c}{2}\right)\left(\frac{1+\cos c}{2}\right) = D(1-D), \qquad (49)$$

$$D_{\{2\}} = \left(\frac{1+\cos c}{2}\right)\left(\frac{1-\cos c}{]}2\right) = (1-D)D, \qquad (50)$$

$$D_{\{1,2\}} = \left(\frac{1-\cos c}{2}\right)^2 = D^2, \qquad (51)$$

where D is error probability of a two-photon state. Since it is considered that errors by a channel are from eavesdropping, D is the same as error probability given two-photon state, e_2.

By substituting Eqs. (45) and (46) to Eq. (43), we find

$$I(A;E)_2 \leq g\left(\frac{1+\cos^2 c}{2}\right) + g\left(\frac{1-\cos^2 c}{2}\right). \qquad (52)$$

That is, Eq. (52) indicates leaked information to Eve from two-photon states. By expanding this result, the maximum mutual information between Alice and Eve for a general i-photon state can be obtained as follows:

$$I(A;E)_i \leq H_2\left(\frac{1+\cos^i c}{2}\right). \qquad (53)$$

Funding

ICT RD program of MSIP/IITP (1711028311, Reliable crypto-system standards and core technology development for secure quantum key distribution network); KAIST School of Electrical Engineering BK21 Program.