Digital Object Identifier:10.11989/JEST.1674-862X.90416014

Elimination of Spatial Side-Channel Information for Compact Quantum Key Distribution Senders

Wei-Shao Huang | Wei Zhang* | Yi-Dong Huang

***Abstract*—For a compact quantum key distribution (QKD) sender for the polarization encoding BB84 protocol, an eavesdropper could take a side-channel attack by measuring the spatial information of photons to infer their polarizations. The possibility of this attack can be reduced by introducing an aperture in the QKD sender, however, the effect of the aperture on the QKD security lacks of quantitative analysis. In this paper, we analyze the mutual information between the actual keys encoded at this QKD sender and the inferred keys at the eavesdropper (Eve), demonstrating the effect of the aperture to eliminate the spatial side-channel information quantitatively. It shows that Eve's potential on eavesdropping spatial side-channel information is totally dependent on the optical design of the QKD sender, including the source arrangement and the aperture. The height of compact QKD senders with integrated light-emitting diode (LED) arrays could be controlled under several millimeters, showing great potential on applications in portable equipment.**

***Index Terms*—Diffraction-limited imaging system, mutual information, quantum key distribution, spatial side-channel information.**

1. Introduction

Quantum key distribution (QKD) is an technique for generating and sharing secret keys between two parties[1],[2], which is important in future security communications networks. Many efforts have been made to push QKD to real applications since the first QKD protocol (BB84[3]) was proposed thirty years ago. On one hand, the transmission distance of QKD is extending continuously by new developments on QKD protocols and techniques[4]-[9]. Using free space as quantum channels, the experimental demonstration of satellite-to-ground QKD has been realized, supporting a transmission distance over 1000 km[10]. The transmission distance of fiber based QKD has been over

*Corresponding author

Manuscript received 2019-04-15; revised 2019-05-31.

This work was supported by the National Key Research and Development Program of China under Grant No. 2017YFA0303704, National Natural Science Foundation of China under Grants No. 61575102, No. 61671438, No. 61875101, and No. 61621064, Beijing Natural Science Foundation under Grant No. Z180012, and Beijing Academy of Quantum Information Sciences under Grant No. Y18G26.

W.-S. Huang is with the Department of Electronic Engineering, Tsinghua University, Beijing 100084 (e-mail: hws16@mails.tsinghua.edu.cn).

W. Zhang and Y.-D. Huang are with the Beijing National Research Center for Information Science and Technology, the Beijing Innovation Center for Future Chips, and also the Department of Electronic Engineering, Tsinghua University, Beijing 100084; with Frontier Science Center for Quantum Information, Beijing 100084; also with Beijing Academy of Quantum Information Sciences, Beijing 100193 (e-mail: zwei@tsinghua.edu.cn; yidonghuang@tsinghua.edu.cn).

Color versions of one or more of the figures in this paper are available online at http://www.journal.uestc.edu.cn.

Publishing editor: Xuan Xie

400 km[11],[12] and several companies have provided commercial fiber based QKD equipment. On the other hand, short-distance free space QKD also attracts much attention, but is still under laboratory research[13]. One of difficulties on short-distance free space QKD is the portability and mobility of QKD senders and receivers. Since single photon detectors are still difficult to be miniaturized based on current technologies, the efforts on this direction are focused on how to reduce the size of the QKD sender, which emits photons with different quantum states. In 2006, Duligall *et al*.[14] proposed and realized a miniature QKD sender for the polarization-encoding BB84 protocol. Four commercial light emitting diodes (LEDs) were used as the light sources for photons with different polarizations, which were combined by a diffraction grating component. However, based on discrete optical components, its size was quite large for portable equipment. In 2015, Vest *et al*.[15] proposed another scheme of a miniature QKD sender. They used vertical cavity surface emitting lasers (VCSELs) as the light sources and combined the photons by a photonic integrated chip, which has a length of 2.5 cm. Recently, a hand hold QKD sender based on resonant-cavity light emitting diodes (RCLEDs) and miniature discrete optical components was reported, which supported the auto-alignment function for short-distance free space applications[16]. However, its length was over 5 cm including the alignment system. In these works, photons with different quantum states (usually encoding on polarization) are generated by different light sources. Without spatial filtering, the photons with different quantum states may have different spatial distributions. An eavesdropper (usually named as Eve) may estimate the state of a photon by the spatial location at which it is detected. Hence, the QKD security requires that photons with different states should be spatially indistinguishable. It is why the way to combine these photons is important and a spatial filter is required in the compact QKD sender to guarantee the QKD security. In [16], an aperture was introduced to reduce the spatial side-channel information introduced by the imperfect photon combination, however, its effect on the QKD security lacks of quantitative analysis.

In this paper, we analyze the mutual information between the actual keys encoded at this QKD sender and the inferred keys at Eve, demonstrating the effect of the aperture to eliminate the spatial side-channel information leakage quantitatively. It shows that Eve's potential on eavesdropping spatial side-channel information is totally dependent on the optical design of the QKD sender, including the source arrangement and the aperture. We proposed a compact QKD sender scheme based on an LED array fabricated on the same chip according to this theoretical analysis. Calculation results show that its height can be controlled under several millimeters with a proper design of the aperture.

2. Spatial Side-Channel Information Leakage in a Compact QKD Sender

Consider a free-space QKD sender for the BB84 protocol with polarization encoding. It has four light sources emitting photons with four different polarizations. The four sources are integrated in a substrate similar to [15] and the plane of their surfaces is defined as the source plane. The sketch of the light (photon) distribution on the source plane is shown in Fig. 1 (a). Regions represent light distributions with different polarizations, which are indicated by the arrows in them. The photons emitted from the source plane should be attenuated to the single photon level and filtered to make them indistinguishable in their frequencies, then output from the QKD sender through a collimator. For simplicity, in this work the four regions are presumed to be four incoherent surface-sources on the source plane, neglecting the phase relationship among photons emitted from different positions.

As shown in Fig. 1 (a), in the QKD sender, photons with different polarizations have different spatial distributions in the source plane. Hence, Eve could expect that she could get the information of photons' polarization encoding by measuring their spatial distribution. Therefore, she could take a side-channel attack on the polarization encoding QKD system. To measure the spatial distribution of photons, firstly Eve should image the photons' distribution in the source plane to an image plane in her eavesdropping apparatus. Then,

she should measure the positions of imaged photons by a single photon detector array which is placed in the image plane. The measurement could be treated as an imaging system shown in Fig. 1 (b). The leftmost plane represents the source plane in the QKD sender. The four circles in the source plane denote the four regions of photons with different polarizations. The middle box is an equivalent diffraction-limited imaging system for the imaging process, which includes the optical path between the source plane in the QKD sender and the image plane in Eve's apparatus. The gray circle on the right surface of the box is the exit pupil of the diffraction-limited imaging system whereas the entrance pupil is not explicitly shown. The rightmost plane represents the image plane where Eve places her detector array. The four larger circles in the image plane represent the images, i.e. the spatial distribution, of photons with different polarizations. Without loss of generality, in the following analysis we consider an ideal eavesdropping condition, in which the magnification of the diffraction-limited image system is 1 and the spatial resolution of the detector array is extremely high. In each pixel of the array, the efficiency of single photon detection is 1 and the dark count is 0. Under this assumption, it can be seen that the imaged distributions of photons with different polarizations on the image plane have little overlap in the case shown in Fig. 1 (b), and hence, Eve can infer the polarization of a detected photon from its position with high likelihood.

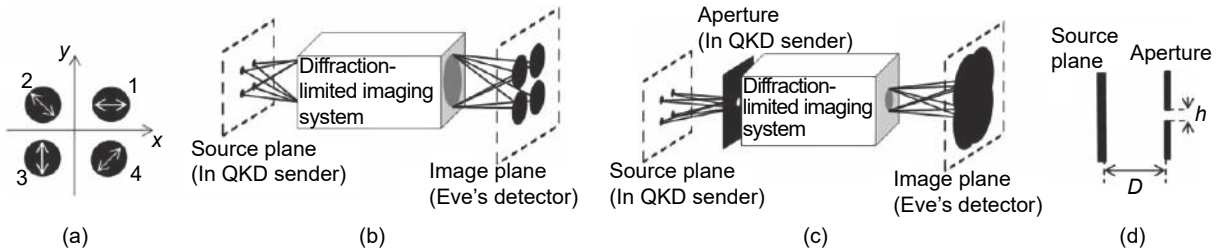

Fig. 1. Sketch of the attack by measuring the spatial side-channel information of photons and the effect of the aperture: (a) the sketch of the photon distribution on the source plane in the QKD sender, (b) Eve's measurement on photons' spatial distribution in the QKD sender, (c) the elimination of spatial side-channel information after introducing an aperture in the QKD sender, and (d) the arrangement of the aperture respect to the source plane in the QKD sender.

An effective way to reduce the successful rate of this side-channel attack is introducing an aperture after the source plane in the QKD sender, which is shown in Fig. 1 (c). The intention of the aperture is to reduce the entrance pupil of the equivalent diffraction-limited imaging system. As a result, the spatial distributions of photons with different polarizations in the image plane would be diffused according to diffraction and overlap with each other. It reduces the possibility for Eve to infer a photon's polarization correctly according to its position. Theoretically, for the incoherent surface-sources in the source plane, when a photon is emitted from a point at (x_0, y_0), the probability function of its detection around (x, y) in the image plane can be calculated by[17]

$$P((x,y)|(x_0,y_0)) = \frac{1}{\pi r^2}\left[J_1\left(\frac{\pi D r}{\lambda h}\right)\right]^2 \tag{1}$$

where J_1(x) denotes the first-order Bessel function and $r = \sqrt{(x-x_0)^2 + (y-y_0)^2}$. λ is the wavelength of the photon. D is the diameter of the aperture, and h is the distance between the aperture and the source plane, which are shown in Fig. 1 (d). Traditionally, the resolution of this diffraction-limited imaging system is indicated by the Rayleigh criterion

$$\text{Resolution} = \frac{1.22\lambda h}{D} \tag{2}$$

which is equal to the radius of the first dark fringe of the Airy pattern in the image plane. Hence, it can be expected that a small aperture is desired to eliminate this spatial side-channel information. However, the spatial side-channel information leakage should be quantitatively analyzed from the view of QKD security analysis based on the information theory, which may provide a clear direction to design the QKD sender with the aperture.

3. Theoretical Analysis of Mutual Information between QKD Sender and Eve

Mutual information can be used to quantitatively measure the percentage of information transmission between two parties when they choose specific ensembles to encode or decode the information, respectively[18],[19]. Fig. 2 shows the information transmission process when Eve takes the eavesdropping by the spatial side-channel information leakage. Four symbol sequences are used to carry the information in the process. The transformation between them could be modeled by three memoryless channels between the QKD sender and Eve. In the QKD sender, the symbol sequence (A) is the random bits that form the secret key, and the symbol sequence (B) is formed by the labels for the regions that emit photons with specific polarizations (defined in Fig. 1 (a)). These two sequences are formed by ensembles $B_1 = \{0, 1\}$ and $S = \{1, 2, 3, 4\}$, respectively. In Eve's apparatus, the symbol sequence (C) sequentially records the spatial coordinate of detected photons and is formed by the ensemble $C = \{(x, y) \in \mathbb{R}^2\}$. The symbol sequence ($D$) is the inferred version of the symbol sequence (A) and formed by ensemble $B_2 = \{0, 1\}$. The ratio of information eavesdropped by Eve is described by the mutual information between ensembles B_1 and B_2, which is denoted by $I(B_1; B_2)$.

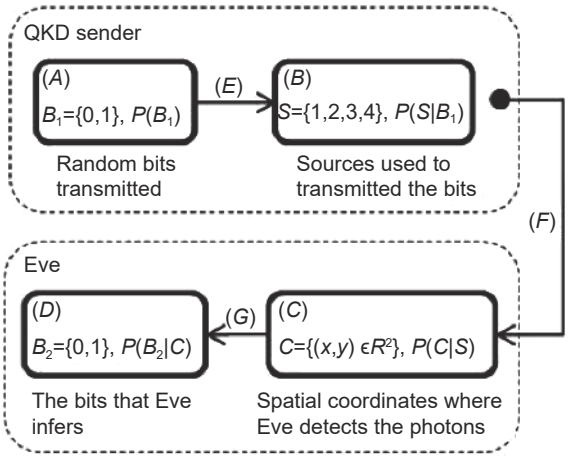

Fig. 2. Information transmission process when Eve takes the eavesdropping on the spatial side-channel information, including four symbol sequences (A) to (D) and three memoryless channels (E) to (G). The solid circle denotes the photons emitted by the QKD sender.

According to the BB84 protocol, a channel (E) can be treated as a noiseless channel and the related possibilities can be presumed to be

$$P(b_1|b_1 \in B_1) = 0.5,$$

$$P(s|s \in S) = 0.25,$$

$$P(s = i|b_1 = 0, i \in \{1, 2\}) = 0.5,$$

$$P(s = j|b_1 = 1, j \in \{3, 4\}) = 0.5.$$

Here, b_1 and s represent the elements of the ensembles B_1 and S, respectively.

The channel (F) describes the behavior of photons travelling from the source plane in the QKD sender to the image plane in Eve's apparatus, which is shown in Fig. 1. The related conditional probability $P(C|S)$ can be

calculated by (1) and the distributions of photons with different polarizations in the source plane. Then, the mutual information $I(B_1;C)$ can be calculated by the following expression[20]:

$$I(B_1;C)=\sum_{b_1\in B_1}\sum_{c\in C}P(c,b_1)\log_2\frac{P(c,b_1)}{P(c)P(b_1)}=\sum_{b_1\in B_1}\sum_{c\in C}\sum_{s\in S}P(c|s)P(s|b_1)P(b_1)\log_2\frac{\sum_{s'\in S}P(c|s')P(s'|b_1)}{\sum_{s''\in S}P(c|s'')P(s'')} \tag{3}$$

here, c represents the element of the ensemble C.

The property of channel (G) and the conditional probability $P(B_2|C)$ depend on how Eve infers the keys based on her detection results. Hence, different data processing algorithms at Eve would lead to different mutual information between the ensembles B_1 and B_2 ($I(B_1;B_2)$). However the upper limit of $I(B_1;B_2)$ is $I(B_1;C)$, since $I(B_1;B_2)\le I(B_1;C)$ according to the property of mutual information[20]. Hence, the mutual information $I(B_1;C)$ can be used to evaluate the potential of Eve's eavesdropping on the spatial side-channel information.

4. Optical Design of Compact QKD Sender to Eliminate Spatial Side-Channel Information

Let us consider a simple compact QKD sender design that four incoherent surface light sources are placed at the source plane as a sources array, which emit photons with different polarizations. It is instructive to consider a simple case where all sources are point sources, shown by the four solid points in Fig. 3 (a). They locate in the source plane with coordinates of $(\pm a,\pm a)$, respectively. Here, we define a characteristic length to indicate the size of the array of the four sources, which is the maximum distance between any two points of these sources. In this case, the characteristic length is equal to $2\sqrt{2}a$. The mutual information $I(B_1;C)$ can be calculated by (1) and (3). And we find that in this case $I(B_1;C)$ only depends on the characteristic-length-to-resolution (CLR) ratio η

$$\eta=\frac{\text{Characteristic}-\text{length}}{\text{Resolution}}=\frac{2.32Da}{\lambda h}. \tag{4}$$

The resolution of the diffraction-limited imaging system is determined by (2). It can be seen that the information obtained by Eve is completely dependent on the design of the QKD sender. The square data (upper curve) in

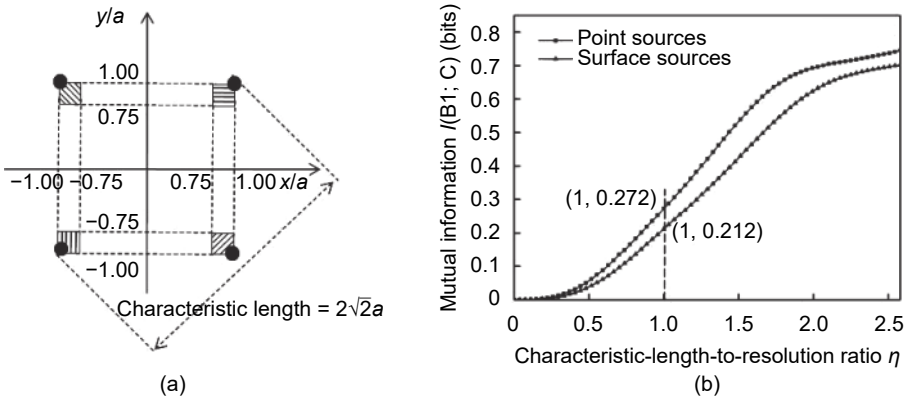

Fig. 3. Arrangement of photon sources and mutual information with different CLR ratios: (a) The arrangement of photon sources used for calculations of mutual information $I(B_1;C)$. The four solid circles represent the point-source case and the four striped squares represent the surface-source case. (b) Mutual information $I(B_1;C)$ under different CLR ratios η in both cases. The upper curve represents the point-source case and the lower curve represents the surface-source case. The dash straight line points out the Rayleigh criterion.

Fig. 3 (b) show the mutual information $I(B_1;C)$ under different CLR ratios η in this case. It can be seen that $I(B_1;C)$ increases monotonically against η. It is natural since a small η means that it is difficult for the imaging system to distinguish the photons emitted from different sources, even they are emitted from two points with the maximum distance. Hence, it is difficult for Eve to get the spatial side-channel information by the imaging system. However, traditionally the resolution of the imaging system is defined by the Rayleigh criterion. For the photons from two point sources, their distributions at the image plane are airy disks. The Rayleigh criterion means they only overlap partially (one's maximum is on the first dark fringe of the other). Hence, it can be expected that $\eta = 1$ is not adequate for eliminating the spatial side-channel information. The calculation result for $\eta = 1$ is marked in Fig. 3 (b). It shows that the mutual information $I(B_1;C)$ is 0.272 bits under the Rayleigh criterion, which implies that Eve can get 27.2% of the spatial side-channel information.

Another case closer to the real application is consider here, in which all the four photon sources are incoherent surface-sources. As shown in Fig. 3 (a), the four striped squares represent the photon emission of the surface-sources with different polarizations. They locate at the four corners of the square defined by the coordinate of $(\pm a, \pm a)$, respectively. All the square regions have the same side length of $0.25a$. The characteristic length of this surface-source array is also defined by the maximum distance between any two points in these sources, which is $2\sqrt{2}a$ again. The incoherent surface-sources mean that the photons emitting from the same source are incoherent if they are from different locations. In this case, the expression of conditional probability $P(c|s)$ can be calculated by

$$P(c|s) = \iint\limits_{(x_s,y_s)\in\sigma_s} P(c|(x_s,y_s))\,P((x_s,y_s)|s)\,\mathrm{d}x_s\mathrm{d}y_s. \tag{5}$$

where σ_s denotes the area of the source labeled by $s \in S$. The expression of $P(c|(x_s,y_s))$ is similar to (1). $P((x_s,y_s)|s)$ is the normalized photon-emitting probability distribution of source s in the source plane, which is assumed to be uniform inside the surface-source region and 0, otherwise.

The CLR ratio η also can be defined by using (4). However, the mutual information $I(B_1;C)$ depends not only on the CLR ratio η but also on the size and the normalized photon emitting probability distribution of each source. The calculation result of $I(B_1;C)$ under different CLR ratios η in this case is shown by the triangle data (lower curve) in Fig. 3 (b). It can be seen that it is similar to the case of point-sources and $I(B_1;C)$ also increases monotonically against η. Besides, the curve is always lower than the one in the previous case, showing that $I(B_1;C)$ is smaller in this case if the CLR ratios η are the same. The mutual information is also marked under the Rayleigh criterion and indicates that Eve can obtain 21.2% of the spatial side-channel information. Hence, the Rayleigh criterion is also not adequate for eliminating the spatial side-channel information in this case.

It is worth noting that in the calculation we do not consider the coherence between the photons emitted from different points. It is a reasonable assumption for incoherent surface-sources, such as LEDs. For coherent surface-sources, such as VCSELs, the coherence between the photons emitted from different points should be considered by modifying (1) and (5) to include the phase distribution function of sub-point sources in a surface-source.

According to above analysis, a small CLR ratio η is preferred to eliminate the spatial side-channel information in a compact QKD sender. The relation between $I(B_1;C)$ and the CLR ratio η can be calculated under a given surface-source array by (1) to (3). On the other hand, the upper bound of $I(B_1;C)$ required for the elimination of the spatial side-channel information could be determined by the requirement of QKD security (which depends on its private amplification algorithm[21]). Then, the CLR ratio η of the QKD sender could be determined for the specific surface-source array. Since the characteristic length is known for a given source array, the parameters to be optimized are the diameter D of the aperture and the distance h between the aperture and the source plane.

Taking the surface-source case shown in Fig. 3 (a) as an example, η should be 0.147 if the requirement of $I(B_1; C)$ is 1×10^{-3} bits according to the calculated relation between $I(B_1; C)$ and η shown in Fig. 3 (b). If the requirement of $I(B_1; C)$ is enhanced to 1×10^{-4} bits, η should reduce to 0.073. Assuming that the surface-source array is realized by red LEDs fabricated in the same chip, with a central wavelength of 630 nm and a characteristic length of $2\sqrt{2} \times 25$ μm (≈71 μm), the values of D and h satisfying the requirement of $I(B_1; C)$ are shown in Fig. 4. It can be seen that this compact QKD sender design has potential to be realized in a small package with a height of several millimeters, which is preferred to the applications of portable equipment.

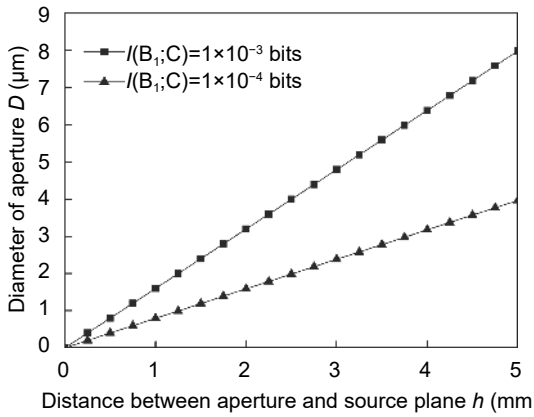

Fig. 4. Design of aperture at different requirements of $I(B_1; C)$.

5. Conclusions

In this paper, we develop a method to analyze the spatial side-channel information in a compact QKD sender for the polarization encoding BB84 protocol, in which photons with different polarizations are emitted from different incoherent surface-sources at the source plane. The effect of the aperture for eliminating the spatial side-channel information is demonstrated theoretically. By the analysis of the mutual information between the actual keys encoded at the QKD sender and the inferred keys at Eve, it shows that Eve's potential on eavesdropping the spatial side-channel information is totally dependent on the optical design of the QKD sender, including the source arrangement and the aperture. For a given source arrangement, the Rayleigh criterion is not a good direction to design the aperture. It should be designed according to the requirement of QKD security, which provides a limit of the mutual information between the sender and Eve. Theoretical analysis shows that the height of the compact QKD sender could be controlled under several millimeters with an aperture to eliminate the spatial side-channel information leakage, if an integrated LED array is used with a characteristic length of 71 μm.

References

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Reviews of Modern Physics*, vol. 74, no. 1, pp. 145-195, Jan. 2002.

[2] D. J. Rogers, *Broadband Quantum Cryptography*, San Rafael: Morgan & Claypool Publishers, 2010.

[3] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. of IEEE Intl. Conf. on Computers, Systems and Signal Processing*, Bangalore, 1984, pp. 175-179.

[4] H. K. Lo, X.-F. Ma, and K. Chen, "Decoy state quantum key distribution," *Physical Review Letters*, vol. 94, no. 23, pp. 230504:1-4, Jun. 2005.

[5] X.-B. Wang, "Beating the photon-number-splitting attack in practical quantum cryptography," *Physical Review Letters*, vol. 94, no. 23, pp. 230503:1-4, Jun. 2005.

[6] M. Lucamarini, Z.-L. Yuan, J. F. Dynes, and A. J. Shields, "Overcoming the rate-distance limit of quantum key distribution without quantum repeaters," *Nature*, vol. 557, no. 7705, pp. 400-403, May 2018.

[7] X.-F. Ma, P. Zeng, and H.-Y. Zhou, "Phase-matching quantum key distribution," *Physical Review X*, vol. 8, no. 3, pp. 031043:1-26, Aug. 2018.

[8] G. N. Gol'tsman, O. Okunev, G. Chulkova, *et al*., "Picosecond superconducting single-photon optical detector," *Applied Physics Letters*, vol. 79, no. 6, pp. 705-707, Aug. 2001.

[9] L.-X. You, H. Li, W.-J. Zhang, *et al*., "Superconducting nanowire single-photon detector on dielectric optical films for visible and near infrared wavelengths," *Superconductor Science and Technology*, vol. 30, no. 8, pp. 084008:1-7, Jul. 2017.

[10] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, *et al*., "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, no. 7670, pp. 43-47, Sept. 2017.

[11] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, *et al*., "Measurement-device-independent quantum key distribution over a 404 km optical fiber," *Physical Review Letters*, vol. 117, no. 19, pp. 190501:1-5, Nov. 2016.

[12] A. Boaron, G. Boso, D. Rusca, *et al*., "Secure quantum key distribution over 421 km of optical fiber," *Physical Review Letters*, vol. 121, no. 19, pp. 190502:1-4, Nov. 2018.

[13] O. Elmabrok and M. Razavi, "Wireless quantum key distribution in indoor environments," *Journal of the Optical Society of America B*, vol. 35, no. 2, pp. 197-207, Feb. 2018.

[14] J. L. Duligall, M. S. Godfrey, K. A. Harrison, W. J. Munro, and J. R. Rarity, "Low cost and compact quantum key distribution," *New Journal of Physics*, vol. 8, no. 10, pp. 249:1-16, Oct. 2006.

[15] G. Vest, M. Rau, L. Fuchs, *et al*., "Design and evaluation of a handheld quantum key distribution sender module," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 21, no. 3, pp. 6600607:1-7, May-Jun. 2015.

[16] H. Chun, I. Choi, G. Faulkner, *et al*., "Handheld free space quantum key distribution with dynamic motion compensation," *Optics Express*, vol. 25, no. 6, pp. 6784-6795, Mar. 2017.

[17] J. W. Goodman, *Introduction to Fourier Optics*, 3rd ed. Greenwood Village: Roberts and Company Publishers, 2005, ch. 6.

[18] S. Nauerth, M. Fürst, T. Schmitt-Manderbach, H. Weier, and H. Weinfurter, "Information leakage via side channels in freespace BB84 quantum cryptography," *New Journal of Physics*, vol. 11, no. 6, pp. 065001:1-8, Jun. 2009.

[19] A. Lamas-Linares and C. Kurtsiefer, "Breaking a quantum key distribution system through a timing side channel," *Optics Express*, vol. 15, no. 15, pp. 9388-9393, Jul. 2007.

[20] D. J. C. MacKay, *Information Theory*, *Inference*, *and Learning Algorithms*, Cambridge: Cambridge University Press, 2003, ch. 8.

[21] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Trans. on Information Theory*, vol. 41, no. 6, pp. 1915-1923, Nov. 1995.

Wei-Shao Huang was born in 1993. He received the B.S. degree in physics from Tsinghua University, Beijing in 2016. He is currently pursuing the M.S. degree with the Department of Electronic Engineering, Tsinghua University. His research interest is quantum cryptography.

Wei Zhang was born in 1974. He received his B.S. degree from Tsinghua University in 1998 and received his Ph.D. degree in physical electronics from the Institute of Information Optoelectronics, Department of Electronic Engineering, Tsinghua University in 2003. Then, he joined the Institute of Information Optoelectronics, Department of Electronic Engineering, Tsinghua University. At present, he is the tenured associate professor with the Department of Electronic Engineering, Tsinghua University. At the same time, he works with the Beijing National Research Center for Information Science and Technology, Tsinghua University and the Beijing Innovation Center for Future Chips, Tsinghua University; with Frontier Science Center for Quantum Information, Beijing; also with Beijing

Academy of Quantum Information Sciences, Beijing. His research interests include micro/nano photonic quantum devices and their applications.

Yi-Dong Huang was born in Beijing. She received the B.S. and Ph.D. degrees in optoelectronics from Tsinghua University in 1988 and 1994, respectively. From 1991 to 1993, she was with Arai Laboratories, Tokyo Institute of Technology, Tokyo, on leave from Tsinghua University. Her Ph.D. dissertation was mainly concerned with strained semiconductor quantum well lasers and laser amplifiers. In 1994, she joined the Photonic and Wireless Devices Research Laboratories, NEC Corporation, Tokyo, where she was engaged in the research on semiconductor laser diodes for optical-fiber communications and became an assistant manager in 1998. She received “Merit Award” and “Contribution Award” from NEC Corporation in 1997 and 2003, respectively. She joined the Department of Electronic Engineering, Tsinghua University in 2003, as a professor, and was appointed as the Changjiang Distinguished Professor and the National Talents Engineering in 2005 and 2007, respectively. She was the Vice Chairman of the Department of Electronic Engineering, Tsinghua University from 2007 to 2012 and has been the Chairman of the department since 2013. At the same time, she works with the Beijing National Research Center for Information Science and Technology, Tsinghua University and the Beijing Innovation Center for Future Chips, Tsinghua University; with Frontier Science Center for Quantum Information; also with Beijing Academy of Quantum Information Sciences. She is presently engaged in the research on nano-structure optoelectronics.