Vol 16 No 11, November 2007
1009-1963/2007/16(11)/3402-05

Chinese Physics

© 2007 Chin. Phys. Soc.
and IOP Publishing Ltd

Influence of multi-photon pulses on practical differential-phase-shift quantum key distribution

Zhao Feng(赵 峰)[a)b)], Fu Ming-Xing(傅明星)[b)],
Lu Yi-Qun(路轶群)[a)†], and Liu Song-Hao(刘颂豪)[a)]

[a)] *Laboratory of Photonic Information Technology, School for Information and Optoelectronic Science and Engineering, South China Normal University, Guangzhou* 510006, *China*
[b)] *Department of Electronic and Information Engineering, Shaanxi University of Technology, Hanzhong* 723003, *China*

(Received 3 February 2007; revised manuscript received 21 June 2007)

The influence of multi-photon pulses on practical differential-phase-shift quantum key distribution (DPS-QKD) is analysed. We have estimated the information which Eve obtained by PNS (photon-number splitting) attack and BS (beam splitting) attack. The result indicates that the PNS attack and BS attack will not limit the transmission distance as long as we select an appropriate mean photon number. Also, the maximum mean photon number under BS attack in practical DPS-QKD system and the set of practical assumptions about Eve's capabilities are presented.

Keywords: multi-photon pulses, differential-phase-shift quantum key distribution, PNS attack, BS attack
PACC: 4250, 4230Q, 4210J, 0367

1. Introduction

Quantum key distribution offers secure key exchanges between remote parties.[1] In principle, single photon is an ideal information carrier whose quantum states represent the classical bits information. While at present, single photons cannot be applied in practice, especially in long distance transmission, and are often mimicked by faint laser pulses containing on average much less than one photon per pulse.[2−4] However, multiple photon pulses occur and open the door to efficient eavesdropping which is called photon-number splitting attack (PNS). PNS attacks threaten the security of quantum key distribution. Differential-phase-shift quantum key distribution (DPS-QKD) based on weak coherent pulses appears to have several important advantages which make it extremely promising for practical systems.[5,6] For example, it can be easily implemented in optical fibres by using readily available optical telecommunication tools and devices, and is insensitive to multi-photon pulses. These merits of DPS-QKD lead to higher communication rates and longer transmission distance. In experiments, most practitioners of quantum cryptography have converged upon a mean photon number of 0.1 as a good benchmark value. While Gisin *et al*[1] have noted that 'multi-photon pulses do not necessarily constitute a threat to key security, but they limit the key creation rate because they imply that more bits must be discarded during key distillation.' In this paper, we explore the influence of the multi-photon pulses on a practical DPS-QKD system and deduce a maximum mean photon number for a DPS-QKD system, based on weak coherent pulses.

2. PNS attack

The principle of DPS-QKD based on weak coherent pulses is described as follows:[7] Alice randomly phase-modulates a pulse train in weak coherent states by $\{0, \pi\}$ for each pulse and sends it to Bob with an average photon number less than one per pulse. Bob divides each incoming pulse into two paths and recombines them by 50:50 beam splitters, where the path-length difference is set equal to the time interval of the sequential pulses. Photon detectors are placed at the two outputs of the recombining beam splitter. At the detectors, the partial wave functions of the two sequential pulses interfere with each other, with an appropriate phase in the interferometer, detector 1 clicks when the phase difference between the two consecutive

†Corresponding author. E-mail: qkdscnu@126.com

pulses is 0 and detector 2 clicks when the phase difference is π. Alice and Bob create a secret key by the following protocol. After raw transmission, Bob tells Alice the time instances at which a photon is counted. From this time information and her modulation data, Alice knows which detector clicks in Bob's site. Under the agreement that the click by detector 1 denotes '0' and the click by detector 2 denotes '1', for example, Alice and Bob obtain an identical bit string.

Now, an eavesdropper (Eve) can perform so-called photon-number splitting (PNS) attack on the multi-photon pulses.[8] Since the bit information is embedded over two sequential pulses, a photon positioned over two neighbouring pulses is needed for Eve to extract the bit information. Thus, she probes the transmitted signal and judges whether or not there are more than two photons positioned over two pulses. From pulses that contain more than two photons, she takes out one photon, stores it, and lets the two pulses go to Bob through a lossless transmission line.[6] For other pulses, she blocks them. Then after the signal transmission, Eve measures the stored photons based on time information disclosed by Bob. This is called PNS attack.[8] We assume that Eve attacks each photon individually. The assumption of individual attacks implies that Eve cannot use the measurement results of one photon to refine her measurement on the rest of the photons. Eve can measure the photon number using a state preserving quantum non-demolition measurement. Based on the assumption and Ref.[6], Eve's split photons are in a linear superposition of all the bits of the secret key, plus the irrelevant time slots where no photon has been detected. Because Eve does not know the phases, her state is in fact a mixture of the different values of the phases. It can be described as follows:[6]

$$\rho_{\mathrm{e}} = \frac{1}{M}\left[2\sum_{k\in B}|x_k\rangle\langle x_k| + \sum_{j\in\bar{B}}|j\rangle\langle j|\right], \qquad (1)$$

where M is the number of coherent pulses transmitted by Alice, B is the set of all time slots in which a detection event is observed by Bob, and $\bar{B}$ is the set of all other time slots in which Bob observes nothing. From Eq.(1), we see that Eve's state is, in fact, a random mixture of orthogonal states. This turns the problem into one of classical probability theories instead of quantum measurement. That is, if Bob records y detection events, each split photon will reveal a bit of Eve's key with probability $2y/M$, and will reveal no information with the probability 1–$2y/M$. While the probability that one finds n photons in a coherent state follows the Poissonian photon number distribution, expressed as

$$p(n,\mu) = \frac{\mu^n}{n!}\mathrm{e}^{-\mu}, \qquad (2)$$

where μ is the mean photon number per pulse. After the pulses pass through the quantum channel, the probability that at least one photon arrives at Bob is

$$\begin{aligned} p_{n\geq 1} &= \sum_{k=1}^{n}\binom{n}{k}(T\eta)^k(1-T\eta)^{n-k} \\ &= 1-(1-T\eta)^n, \end{aligned} \qquad (3)$$

where T is the fibre transmission efficiency, and η is Bob's detection efficiency. Hence, the quantum bit transmission efficiency is

$$p = \sum_{n=1}^{\infty} p(n,\mu)p_{n\geq 1} = 1-\exp(-\mu T\eta). \qquad (4)$$

When Alice sends M sequential weak coherent pulses to Bob who will observe on average $M[1-\exp(-\mu T\eta)]$ detection events, and Eve can then split off $M[1-\exp(-\mu T\eta)]$ of the photons, so the probability that Eve can gain information about the key is $2[1-\exp(-\mu T\eta)]$. She sends them to Bob and stores $M[1-\exp(-\mu(1-T\eta))]$ photons coherently to be measured after Alice and Bob have revealed all classical information. The information obtained by Eve is $2M[1-\exp(-\mu T\eta)]\{1-\exp[-\mu(1-T\eta)]\}$. Hence, the fraction of the total information Eve acquires on the sifted key is

$$I_{\mathrm{E}} = 2\{1-\exp[-\mu(1-T\eta)]\}, \qquad (5)$$

where $T = 10^{-\alpha l/10}$, l is the distance of the transmission fibre from Alice to Bob. Usually, we assume that $\alpha = 0.25\,\mathrm{dB/km}$ and $\eta = 0.3$. From Eq.(5), the information of sifted key which Eve acquires with PNS attack is shown in Fig.1.

Figure 1 illustrates the fractions of the information Eve acquires on the sifted key with PNS attack when the transmission distances are 1km and 150 km, respectively. It is shown that the transmission distance of DPS-QKD system is hardly influenced by PNS attacks. It mainly depends on the mean photon number μ.

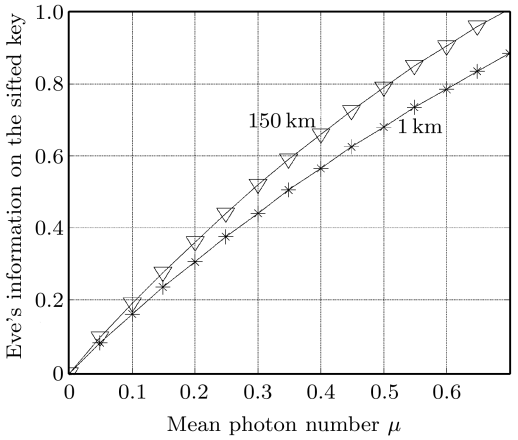


Fig.1. The fraction of information Eve gains on the sifted key with PNS attack.

Furthermore, the PNS attack will change the transmitted signal from a state that every pulse has a photon with a finite probability into the state that some two sequential pulses definitely have one photon and other pulses have no photons. When the pulse with a probability of having a photon interferes with a vacant (the photon was stolen by Eve), the bit errors can be introduced. So we can easily detect the existence of eavesdropper by estimating the error rate.

In the above discussion, we suppose that Eve has such a lossless transmission line that the PNS attack will let the counting rate of Bob's detector unchanged and she has the abilities to discriminate the number of photons in each pulse. Even if Eve has these abilities, she cannot obtain the full information when the two legitimate users select an appropriate mean photon number. Moreover, they can apply privacy amplification technology to eliminate the Eve's information on the keys.

3. BS attack

In practice,[9] Eve has free access to Alice and Bob's quantum channel at any point outside their offices. She can install optical components (switches, couplers etc.) without being noticed. She has the real fibres with a pure silica core, which have lower losses[10] and a value of $a_{\rm e} = 0.171\,{\rm dB/km}$. Usually, the fibres between Alice and Bob have additional losses due to splices and connections in the centrals, and a value of $a_{\rm ab} = 0.25\,{\rm dB/km}$ is more realistic. Moreover, installed fibres rarely follow the bee-line, but they often follow roads or along with the mountains and go from one telecom central to another. Hence, the actual fibre transmission distance $l_{\rm ab}$ always longer than the bee-line distance $l_{\rm e}$, and usually we suppose that $l_{\rm ab} = 1.1 \times l_{\rm e}$. With these technologies, Eve can takes the strategies of BS attacks which insert a beam splitter on the transmission line just after Alice and partially split the transmitted signal.

Figure 2 shows the schematic of BS attack.[8] Eve uses an adaptive BS (beam splitter) to split photons in each pulse. The splitting ratio is α. At the BS output that causes the $1-\alpha$ part of photons go to Bob, Eve installs her low-loss fibre in order to compensate the signal loss due to beam splitting. The split pulses pass through an asymmetric interferometer and then are detected. After the signal transmission from Alice to Bob, Bob discloses time slots at which he detects photons. Eve listens in and obtains bit information from her detection events corresponding to Bob's detection time. BS attack does not destroy the coherent states, and the fraction of the photons split off is equal to the channel loss, hence, BS attack not only does not modify the communication rate but also does not introduce any errors.

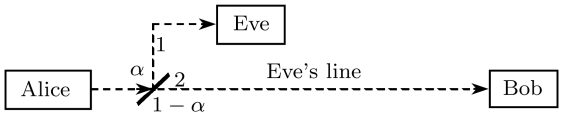


Fig.2. BS attack on DPS-QKD (taken from Ref.[8]).

Let us consider the information gained by Eve with BS attack. As Eve's action does not change the communication rate, the following condition can be obtained

$$P' = P, \tag{6}$$

where P' is Bob's counting rate under BS attack, and P is Bob's counting rate without BS attack. We assume that the beam splitter is lossless after the pulse passes through the beam-splitter, thus the probability of photons emitted from port 1 and port 2 (Fig.2) is

$$\sum_{n=0}^{\infty} \sqrt{P_n}|n> \otimes |0> \rightarrow \sum_{n=0}^{\infty} \sqrt{P_n} \sum_{i=0}^{n} c_i |i> \otimes |n-i>, \tag{7}$$

where P_n is the probability of finding n photons in a coherent state which follows the Poissonian photon number distribution when arriving at the beam splitter; c_i is the probability of i photons that emit from port 2 or port 1. If there are i photons emitted from port 2, then

$$c_i = C_n^i (1-\alpha)^i \alpha^{(n-i)}. \tag{8}$$

Hence, for each pulse, there are four outcomes at which photons will emit from port 1 and/or port 2: First, for the photons which emit from port 1 and port 2 simultaneously, the probability is

$$p_{\mathrm{BE}} = \sum_{n=2}^{\infty} P_n \sum_{i=1}^{n-1} c_i = 1 + \mathrm{e}^{-\mu} - \mathrm{e}^{-\alpha\mu} - \mathrm{e}^{-\mu(1-\alpha)}. \quad (9)$$

Second, for all photons emitted from port 1, the probability is

$$p_{\mathrm{E}} = \sum_{n=1}^{\infty} (P_n . c_0) = \mathrm{e}^{-(1-\alpha)\mu} - \mathrm{e}^{-\mu}. \quad (10)$$

Third, for all photons emitted from port 2, the probability is

$$p_{\mathrm{B}} = \sum_{n=1}^{\infty} (P_n . c_n) = \mathrm{e}^{-\alpha\mu} - \mathrm{e}^{-\mu}. \quad (11)$$

In the last case that no photons emit from both port 1 and port 2, the probability is

$$p_{\mathrm{o}} = \mathrm{e}^{-\mu}. \quad (12)$$

So, after Eve's intervention with BS attack, the counting rate of Bob's detector will become

$$P' = (p_{\mathrm{BE}} + p_{\mathrm{B}})\, T_{\mathrm{e}}, \quad (13)$$

where T_{e} is the quantum transmission efficiency from Alice to Bob (low-loss transmission line), and $T_{\mathrm{e}} = t_{\mathrm{e}}\eta_{\mathrm{b}}$, $t_{\mathrm{e}} = 10^{-a_{\mathrm{e}} l_{\mathrm{e}}/10}$ is the fibre transmission efficiency with low losses, and η_{b} is the Bob's detection efficiency.

Whereas, without Eve's intervention Bob's counting rate is

$$P = \left(1 - \mathrm{e}^{-\mu}\right) t_{\mathrm{ab}} \eta_{\mathrm{b}}, \quad (14)$$

where $t_{\mathrm{ab}} = 10^{-a_{\mathrm{ab}} l_{\mathrm{ab}}/10}$ is the efficiency of transmission line between Alice and Bob. From Eq.(6), we know that BS attack must leave P unchanged such that Eve could not be revealed, that is,

$$\left(1 - \mathrm{e}^{-(1-\alpha)\mu}\right) \times 10^{-a_{\mathrm{e}} l_{\mathrm{e}}/10} = \left(1 - \mathrm{e}^{-\mu}\right) \times 10^{-a_{\mathrm{ab}} l_{\mathrm{ab}}/10}. \quad (15)$$

Equation (15) indicates that for a given distance and mean photon number, Eve can adjust the splitting ratio α to maintain the counting rate unchanged. By this way, the ratio of information acquired by Eve on the sifted key is

$$I'_{\mathrm{E}} = \frac{p_{\mathrm{BE}}}{p_{\mathrm{B}} + p_{\mathrm{BE}}} = \frac{1 + \mathrm{e}^{-\mu} - \mathrm{e}^{-\alpha\mu} - \mathrm{e}^{-(1-\alpha)\mu}}{1 - \mathrm{e}^{-(1-\alpha)\mu}}. \quad (16)$$

Thus, for a given distance, from Eqs.(15) and (16) we can calculate the relationship between I'_{E} and the mean photon number μ. Figure 3 shows the probability for Eve to gain information on the sifted key, which increases with the mean photon number. Also, we can see that the probability for Eve to gain information is hardly limited by transmission distances, it is mainly dependent on the mean photon number μ. For example, Eve obtains information on the 150 km fibre almost the same as that on the 50 km fibre. This indicates that the transmission distance in a practical DPS-QKD system is also not limited by BS attack when μ is less than 1.

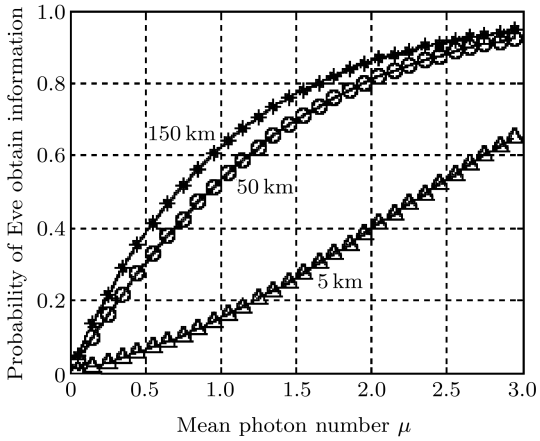


Fig.3. The probability for Eve to gain information with BS attack.

4. Key generation rate under BS attack

The aim of QKD is to produce a secure key in the sense that Eve has gained no information on that key. In practice, Eve's intervention will obtain partially the information about the key, so we can use the generalized private amplification to eliminate Eve's information on that key.[11−13] In this section we will consider the maximum key generation under BS attack in a practical DPS-QKD system. Under the BS attack, the collision probability between bits owned by Bob and Eve is expressed as follows[4,11]

$$p_{\mathrm{c}} = 2^{-n_{\mathrm{sif}}(1-P_{\mathrm{E}})}, \quad (17)$$

where n_{sif} is the sifted key. The compression factor of the privacy amplification τ_1 is expressed by[11]

$$\tau_1 = 1 + \frac{1}{n_{\mathrm{nsif}}} \log_2 p_{\mathrm{c}}. \quad (18)$$

Then, under BS attack the secure key generation rate per pulse is[4]

$$R = P_{\text{click}}\{1-\tau_1+f(e)\,[e\log_2 e + (1-e)\log_e(1-e)]\}, \tag{19}$$

where $f(e)$ characterizes the performance of the error correction algorithm, and the ideal error correction algorithm is characterized by $f(e)=1$. P_{click} is Bob's counting rate,

$$P_{\text{click}} = \left(1-\mathrm{e}^{-\mu}\right) t_{\text{ab}}\eta_{\text{b}} + d, \tag{20}$$

where d is the Bob's dark counts probability, which is typically about 10^{-5} per pulse. Usually, we suppose that the detector's quantum efficiency η_{b} is 0.11, so the total error rate is only caused by detector's dark counts which can be described as[6]

$$e = \frac{0.01P_{\text{click}} + d/2}{P_{\text{click}}}, \tag{21}$$

where 0.01 is assumed to be the baseline error rate. From Eqs.(14),(15),(18)–(21), we can calculate the maximum mean photon number under the practical BS attack. Figure 4 shows the secure key generation rate per pulse under BS attack for different transmission distances.

From Fig.4 we can see that under practical BS attack, the maximum mean photon number is limited by the transmission distance. When the transmission distance is 100 km the maximum mean photon number is 0.6; when the transmission distance extends to 150 km the maximum mean photon number drops to 0.3. Therefore, given a practical DPS-QKD system, we can choose an appropriate mean photon number by this way.

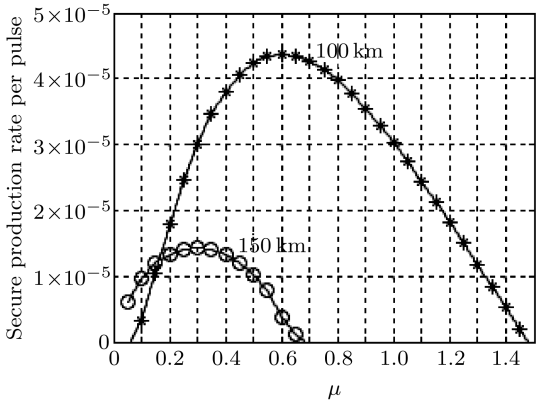


Fig.4. Secure key generation rate under BS attack.

5. Conclusions

We have discussed the influence of PNS attack and BS attack on multi-photon pulses in a DPS-QKD system based on weak coherent pulses. The result indicates that PNS attack and BS attack cannot limit the transmission distance as long as we select an appropriate mean photon number. The mean photon number is an important parameter when we design the practical QKD systems. Moreover, in order to guarantee the security of the final keys, Alice and Bob must survey the length of the fibre, its loss and the coincidence count rates at first, then adjust to an appropriate mean photon number. For the time being, DPS-QKD based on weak coherent pulse has no severe security problem due to multi-photon pulses. It is extremely promising for practical systems at present.

References

[1] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 1
[2] Li M M, Wang F Q, Lu Y Q, Zhao F, Chen X, Liang R S and Liu S H 2006 *Acta Phys. Sin.* **55** 4642 (in Chinese)
[3] Zhao F, Lu Y Q, Wang F Q, Chen X, Li M M, Guo B H, Liao C J and Liu S H 2007 *Acta Phys. Sin.* **56** 331 (in Chinese)
[4] Takesue H, Diamanti E, Honjo T, Langrock C, Fejer M M, Inoue K and Yamamoto Y 2005 *New J. Phys.* **7** 232
[5] Inoue K, Waks E and Yamamoto Y 2002 *Phys. Rev. Lett.* **89** 037902
[6] Waks E, Takesue H and Yamamoto Y 2006 *Phys. Rev.* A **73** 012344
[7] Inoue K, Waks E and Yamamoto Y 2003 *Phys. Rev.* A **68** 022317
[8] Inoue K and Honjo T 2005 *Phys. Rev.* A **71** 042305
[9] Felix S, Gisin N, Stefanov A and Zbinden H 2001 *J. Mod. Opt.* **48** 1
[10] Kato T, Hirano M, Onishi M and Nishimura M 1999 *Electron. Lett.* **35** 1615
[11] Lütkenhaus N 2000 *Phys. Rev.* A **61** 052304
[12] He G Q and Zeng G H 2005 *Chin. Phys.* **14** 541
[13] He G Q and Zeng G H 2006 *Chin. Phys.* **15** 1284