# Revealing of photon-number splitting attack on quantum key distribution system by photon-number resolving devices

**A A Gaidash [1], V I Egorov [1], A V Gleim [1,2]**

[1] ITMO University, Kronverkskiy pr. 49, St.Petersburg 197101, Russian Federation
[2] Kazan National Research Technical University, K.Marx st. 10, Kazan 420111, Russian Federation

E-mail: andrewdgk@gmail.com

**Abstract**. Quantum cryptography allows distributing secure keys between two users so that any performed eavesdropping attempt would be immediately discovered. However, in practice an eavesdropper can obtain key information from multi-photon states when attenuated laser radiation is used as a source of quantum states. In order to prevent actions of an eavesdropper, it is generally suggested to implement special cryptographic protocols, like decoy states or SARG04. In this paper, we describe an alternative method based on monitoring photon number statistics after detection. We provide a useful rule of thumb to estimate approximate order of difference of expected distribution and distribution in case of attack. Formula for calculating a minimum value of total pulses or time-gaps to resolve attack is shown. Also formulas for actual fraction of raw key known to Eve were derived. This method can therefore be used with any system and even combining with mentioned special protocols.

## 1. Introduction

To share a private message communicating sides must have a secure method to share a key first, what might be not obvious task. Quantum cryptography systems (QKD) [1] allow performing secure quantum key distribution between two or more users. The use of single photons in transmission technology provides the legitimate users (Alice and Bob) an ability to detect an eavesdropper (Eve) by monitoring quantum bit error level (QBER) on receiver side. QKD protocols are based on general principles of quantum physics, so unconditional security can be achieved. In this case protocols might guarantee security without any restrictions on the technological level of the eavesdropper.

Security of QKD imposes restriction on the source of light, which must be true single-photon. There are several types of heralded true single-photon sources [2-4], even some most promising that function at room temperatures [5-8]. However this technology is immature and does not provide high photon emission rates. An obvious and easy (and also low-cost) solution to this problem is to use attenuated laser light with average energy per pulse or time-gap (in case of continuing distribution) less than energy of one photon [9]. Probability of particular number $n$ of photon per pulse or time-gap emitted by source of coherent states can be described by Poisson distribution:

$$P_{\mathrm{A}}(\bar{n}, n) = \frac{\bar{n}^n}{n!}\exp(-\bar{n}), \quad (1)$$

where $\bar{n}$ is average number of photons per pulse or time-gap and it can be chosen on purpose to make fraction of multi-photon states small. Since that attenuated coherent states source can be compatible with QKD system. Moreover several outstanding records were established by systems with weak laser source [10-12].

Nevertheless, security of these systems can in principle be compromised. Eavesdropper can exploit presence of multi-photon states and carry out photon-number splitting (PNS) attack [13]. She performs quantum non-demolition measurement (QND) on each of the quantum systems going from Alice to Bob; this technique claims to measure number of photons without disturbing quantum states [14 - 16]. If the number of photons is more than one, then Eve can divide photons (for example by using an adjustable beamsplitter) in two parts - one of them follows to Bob, and the rest Eve stores in her quantum memory. She can control the fraction of photons but set apart at least one photon. Since this attack introduces no errors, it cannot be detected by authorized partners if it is assumed that Bob has access only to the average detection rate, and not to the statistics of the photons he receives; this type of attacks is one of the most inconvenient.

PNS attack has been previously studied, and two counteractive methods were developed. The first is SARG04 protocol [17], which adds extra non-orthogonal bases and strong reference beam. The second commonly used technique is called decoy states [18] – PNS attack is detected with help of additional set of states with mean number of photons not equal to mean number $\bar{n}$ as for a signal state.

These methods do not rely on full analysis of photon number distribution although this might be another efficient way to detect PNS attack. The reason is that counter-PNS researches have been done before any of photon-number resolving (PNR) devices were demonstrated experimentally. There are two main methods to achieve photon-number resolving. One direct approach to reach photon-number-resolving capability is to simply break the detector active area into many distinct areas or pixels, so that each can register a photon independently of the others [19]. The second is to find proper material; there are devices whose output is inherently proportional to the number of photons, even if their detection efficiency might be low and their proportional response ultimately saturates at high input photons levels, for example [20]. Thus PNR devices provide information about number of photons in pulse or time-gap with high fidelity. One of the most promising devices is superconducting nanowire single-photon detector (SNSPD) [21]. It was shown that it can resolve up to 12 photons (depends on number of pixels). Detection efficiency for these devices is up to 60 % (using cavity) and repetition rate is up to 1 GHz [22]. We chose this type of detector for further simulations.

Goal of this paper is to consider possibilities of detecting PNS attack using photon-number resolving (PNR) detectors by Bob [23]. Compared to previous mentioned methods, using PNR detectors is efficient way to prevent eavesdropper actions with neither changes in protocol nor decreasing of key rate, which also can be implemented with any kind of QKD system, even combing with two existing methods.

## 2. Considered model

In this paper we expand previous research [24], where first attempts to describe advantages of PNR detectors were shown, by taking into account losses in fibers and detection efficiency of real devices. As a model for simulations we use ideal laser sources with $\bar{n} = 1$, 100 km of optical fiber SMF-28 with 0.2 dB/km losses and a detector with 60% quantum efficiency. All splicing and other small fractions of losses are supposed to be negligible. Eavesdropper is considered to operate at the beginning of quantum channel and to not know basis of each obtained photon; this kind of assumptions is to estimate upper bound of known-to-Eve part of key. Also we use approximation of infinitely long keys.

It is well-known that losses introduce changes in Poisson distribution as additional attenuation as follows:

$$P_{\mathrm{B}}(\bar{n},n)=\frac{(\gamma\cdot\bar{n})^{n}}{n!}\exp(-\gamma\cdot\bar{n}), \tag{2}$$

where $\gamma$ is transmission efficiency of optical fiber line. However this way of representation is inconvenient because it provides not much information about interconnection of initial distribution $P_A(\bar{n},n)$ and final one $P_B(\bar{n},n)$, thus there is another one:

$$P_{\mathrm{B}}(\bar{n},n)=\sum_{k=n}^{\infty}\left[P_{\mathrm{A}}(\bar{n},k)\cdot\frac{k!}{n!\cdot(k-n)!}\cdot\eta^{k-n}\cdot\gamma^{n}\right], \tag{3}$$

where $\eta=1-\gamma$ is total loss. We should expect transform with the same kernel for detector as follows:

$$P_{\mathrm{D}}(\bar{n},n)=\sum_{k=n}^{\infty}\left[P_{\mathrm{B}}(\bar{n},k)\cdot\frac{k!}{n!\cdot(k-n)!}\cdot(1-QE)^{k-n}\cdot(QE)^{n}\right], \tag{4}$$

where QE is quantum efficiency of the detector.

In case of PNS attack, when Eve split one photon from each pulse or time-gap at the beginning of quantum channel where is no losses, distribution of multi-photon states can be shown as follows:

$$P_{\mathrm{E}}(\bar{n},n)=\begin{cases}P_{\mathrm{A}}(\bar{n},0),\text{for } n=0;\\ P_{\mathrm{A}}(\bar{n},1)+P_{A}(\bar{n},2),\text{for } n=1;\\ P_{\mathrm{A}}(\bar{n},n+1),\text{for } n\geq 2.\end{cases} \tag{5}$$

This distribution can be put into transformations (3) and (5) instead of $P_A(\bar{n},n)$ to obtain final distribution $P_{D-PNS}(\bar{n},n)$ in case of PNS attack, so the goal is to distinguish two final distributions.

## 3. Method description

If Bob has access to information of multi-photon distribution, he can discover PNS attack. In this case it modifies distribution of number of photons arrived to Bob; to estimate an order of the deviation one can apply rule of thumb as follows:

$$\frac{P_D(\bar{n},n)}{P_{D-PNS}(\bar{n},n)}\approx\frac{n+1}{\bar{n}},\text{for } n\geq 2. \tag{6}$$

However, difference in multi-photon distribution can be resolved within limits of appropriate confidence only for small number of photons. Actually there is a trade-off between increasing maximal number of photons which Bob should consider and increasing of total number of pulses or time-gaps per session as following:

$$N(n_{\max})>\left(z\cdot\frac{\sqrt{P_D(n_{\max})}+\sqrt{P_{D-PNS}(n_{\max})}}{P_D(n_{\max})-P_{D-PNS}(n_{\max})}\right)^{2}, \tag{7}$$

where *z* is chosen according to "68–95–99.7" rule (also known as "3σ rule"): for z = 1 random number of pulses of time-gaps will be within limit of confidence with 68% probability, for z = 2 with 95% probability, for z = 3 with 99.7% probability and so on. Thus for chosen $n_{\max}$ there is minimum value of total pulses or time-gaps $N(n_{\max})$ to resolve PNS attack. For instance, $N(3)=3.1\cdot10^{9}$ for z = 5 and $\bar{n}$ = 1.

Using introduced notation it is easy to estimate potential known-to-Eve part of raw-key with no losses:

$$E_{\text{lossless}}=C_{\mathrm{pr}}\cdot\frac{1-\exp(-\bar{n})-\bar{n}\cdot\exp(-\bar{n})}{1-\exp(-\bar{n})}, \tag{8}$$

where $C_{\mathrm{pr}} \leq 1$ is constant depending on particular protocol and information known by Eve about bases of photons. For estimations on upper bound here and later in text we assume $C_{\mathrm{pr}} = 1$. Also we provide a general formula including total losses in fiber and QE of detector as follows:

$$E = \frac{1 - P_{SNSPD-PNS}(\bar{n}, 0) - \bar{n} \cdot QE \cdot \gamma \cdot \exp(-\bar{n})}{1 - P_{SNSPD-PNS}(\bar{n}, 0)}. \quad (9)$$

Thus potential known-to-Eve fraction of key is 50% for mentioned parameters of system.

However Eve can resend the taken photon. Let us consider this case, where eavesdropper may not know right basis of photon, so she prepares state in random basis. In part of events she will be right and keep proper amount of photons in pulse or time-gaps, but in other part of events resent photon will not recover distribution. Hence there will be mixture of expected distribution and distribution in case of pure PNS, so PNR device can be useful even in case of PNS with resend, however it requires higher amount of total pulses or time gaps to resolve attack.

## 4. Results and conclusions

As a result of research, a method of defending against PNS attacks on quantum key distribution system with coherent light source was analyzed, including brief review of the problem. The use of detectors which resolve multi-photon states allows revealing PNS attack by analyzing statistics on receiver's side. The ability of using these detectors to ensure security against PNS attack was studied. There is always a trade-off between increasing maximal number of photons which Bob should consider to reveal most actions of eavesdropper and increasing of total number of pulses, what might greatly increase the time of single session. In particular, expressions of the efficiency of PNS attack on quantum key distribution system with coherent light source were derived to provide one's general estimations. Moreover, the method does not exclude possibility of combining with other known methods and can be used with any quantum cryptography setup without any hardware additions.

## References

[1] C Bennett and G Brassard 1984 *Proceedings IEEE International Conference on Computers, Systems and Signal Processing* **175**
[2] B Lounis and M Orrit 2005 *Rep. Prog. Phys.* **68** 1129
[3] M Eisaman, J Fan, A Migdall et al. 2011 *Rev. Sci. Instrum.* **82** 071101
[4] S Lukishova 2013 *Proceed. SPIE* **9056** 90650C
[5] S Lukishova, L Bissell, J Winkler, and C Stroud Jr 2012 *Optics Letters* **37** 7 1259
[6] I Aharonovich, A Greentree, S Prawler 2011 *Nature Photonics* **5** 397
[7] A Jechow, A Heuer, and R Menzel 2008 *Optics Express* **16** 17 13439
[8] M Fiorentino, S M Spillane, R G Beausoleil et al. 2007 *Opt. Express* **15** 7479
[9] ID3100/ID3110 Clavis Quantum Key Distribution System, (http://www.idquantique.com/photon-counting/clavis.html)
[10] H Takesue, Q Zhang, R H Hadfield et al. 2007 *Nature Photonics* **1** 343
[11] D Stucki, N Walenta, F Vannel et al. 2009 *New J. Phys.* **11** 075003
[12] B Korzh, C Ci Wen Lim, R Houlmann et al. 2015 *Nature Photonics* **9** 163-168
[13] M Dušek, O Haderka, M Hendrych 1999 *Optics Communications* **169** 103-108
[14] V Braginsky, Y Vorontsov, K Thorne 1980 *Science* **209** 4456
[15] B Johnson, M Reed, A Houck et al. 2010 *Nature Physics* **6** 663
[16] L Liang, G Lin, Y Hao 2014 *Physical Review* **A 90** 055801
[17] V Scarani, A Acin, N Gisin and G Ribordy 2004 *Phys. Rev. Lett.* **92** 057901

[18] H-K Lo, X Ma, K Chen 2005 *Physical Review Letters* **94** 230504
[19] D Kalashnikov, S Tan, M Chekhova 2011 *Opt. Express* **19(10)** 9352-63
[20] A Lita, A Miller, and S Nam 2008 *Opt. Express* **16** 3032
[21] Z Zhou, S Jahanmirinejad, F Mattioli et al. 2014 *Optics Express* **22** 3 3475
[22] D-K Liu, S-J Chen, L-X You et al. 2012 *Appl. Phys. Express* **5** 125202
[23] M Eisaman, J Fan, A Migdall et al. 2011 *Rev. Sci. Instrum.* **82** 071101
[24] A Gaidash, V Egorov, A Gleim 2014 *J. Phys.: Conf. Ser.* **541** 012062