Detection of beamsplitting attack in a quantum cryptographic channel based on photon number statistics monitoring

A A Gaidash, V I Egorov, A V Gleim
St.Petersburg National Research University of Information Technologies, Mechanics and Optics, Kronverkskiy pr. 49, St.Petersburg 197101, Russian Federation
E-mail: andrewdgk@gmail.com

Abstract. Quantum cryptography in theory 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. In order to overcome this possibility, it is generally suggested to implement special cryptographic protocols, like decoy states or SARG04. We present an alternative method based on monitoring photon number statistics after detection. This method can therefore be used with any existing protocol.

1. Introduction
Quantum cryptography systems [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) with an ability to detect eavesdropper (Eve) by monitoring quantum bit error level (QBER) on receiver side. However, in practice full security can only be guaranteed when a «true» single photon source is used [2-6], e.g. based on spontaneous parametric down-conversion [7]. Unfortunately, today these devices do not provide necessary key generation rate and stability; also they are available only in laboratory conditions. For this reason, most quantum cryptography experimental setups [1] and commercial products [8] use attenuated laser light as a source of quantum states with average probability of single photon emission per timeframe (“mean photon number”) about \( \mu \approx 0.1 \). In this case the security condition is no longer strict due to Poisson distribution of photons of coherent light: some pulses may contain more than one photon. Probability of \( n \)-photon state emission is described as follows:

\[
P(\mu, n) = \frac{\mu^n}{n!} \exp(-\mu),
\]

where \( \mu \) – average probability of single photon emission per timeframe, \( n \) – photon number.

This fact can be easily used by Eve to successfully perform undetectable beam-splitting or photon-number splitting (PNS) attack [9] without changing QBER, and receive a part of the key which can be significant at higher \( \mu \).

In this work, we present a new method of revealing PNS attacks by monitoring the statistics of multi-photon states on receiver side. We suggest using detectors which distinguish multi-photon states and can accumulate statistics. In case of PNS attack there will be different distribution of number of multi-photon states unlike it is expected.
2. PNS attack

In our research we use an analytical model of Eve which consists of three main elements: a device which can determine multi-photon pulses without measuring [9]; a single-photon detector with high quantum efficiency (up to 100%) and a controlled beam splitter. Eve performs the PNS attack by splitting and measuring the phonons from multi-photon pulses.

For preliminary calculations if we take into account losses, there only will be higher probability of detecting multi-photon states. Emitted n-photon state has a probability to be detected:

\[
\eta(n) = 1 - (1 - \eta)^n,
\]

where \( \eta \) is total loss.

And Poisson distribution on Bob’s side should be completed as:

\[
P^*(\mu, n) = \frac{\mu^n}{n!} \cdot \exp(\mu) \cdot \eta(n)
\]

But in this paper losses are not taken into consideration for better clarity because of theoretical priority of work. So we assume that probability of n-photon state emission equals to an appropriate probability of detection.

We estimated the impact of attack on key security by calculating the percentage of multi-photon states for different \( \mu \) and the resulting fraction of key information for several widely-used two-state and four-state protocols, the most common of which are B92 and BB84. Percentage of multi-photon states \( Q(\mu) \) is represented as a relation of multi-photon states detection probability and detection probability of any photon number states:

\[
Q_{EVE}(\mu) = \frac{(1 - P(\mu,0) - P(\mu,1)) \cdot N}{1 - P(\mu,0)} = \frac{1 - P(\mu,0) - P(\mu,1)}{1 - P(\mu,0)}
\]

where \( P(\mu,0) \) – detection probability of timeframe with no photons, \( P(\mu,1) \) – detection probability of timeframe with one photon, \( N \) – total amount of timeframes.

In particular, in case of most common \( \mu = 0.1 \) Eve can easily obtain photons from 4.9% of all timeframes. If Eve has at least one photon from current timeframe, she will know the bit in case of two-state protocol: if eavesdropper chose wrong basis, she can change it to opposite. This means that obtained photons from 4.9% of all timeframes represent equal amount 4.9% of key.

In case of four-state protocols Eve has a 50% chance to chose wrong basis, so there is in two times less 2.5% of the key used respectively.

![Figure 1. Percentage of multi-photon timeframes \( Q(\mu) \) depends on \( \mu \). For higher \( \mu \) there is a huge part of multi-photon states.](image-url)
Table 1. Table represents that Eve can obtain percentage $K_{B92}(\mu)$ and $K_{BB84}(\mu)$ of the key used for two-state and four-state protocols respectively.

| $\mu$  | 0.1 | 0.2 | 0.3 | 0.4 | 0.5 | 0.6 | 0.7 | 0.8 | 0.9 |
|--------|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| $K_{B92}$ (%) | 4.9 | 9.7 | 14.3 | 18.7 | 22.9 | 27.0 | 30.9 | 34.7 | 38.3 |
| $K_{BB84}$ (%) | 2.5 | 4.8 | 7.1 | 9.3 | 11.5 | 13.5 | 15.5 | 17.4 | 19.2 |

Today, two methods are known to overcome the PNS attack: Decoy States [10] and SARG04 [11] protocol. Although both of them were shown to be effective, they have certain drawbacks, increasing the complexity of cryptographic protocol and at the same time lowering key generation rate. Moreover, they cannot be directly applied to some setups [12].

3. Method description

It is known that some types of single photon detectors are able to distinguish multi-photon states upon detection [13, 14], thus gathering information not only about the fact of photon existence in a certain timeframe, but also about the mean number of photons arriving at the detector. In particular, superconducting nanowire single photon detectors [15] can be easily adjusted so that they would detect only the states with the number of photons exceeding the defined minimum. These detectors are also characterized by low noise (about 10 Hz) and high quantum efficiency (up to 57% at 1550 nm [14]), which makes them perfect for quantum cryptography applications.

In this work, we suggest an alternative method of monitoring the received photon number statistics by detectors which distinguish multi-photon states.

In order to uncover this attack, Alice and Bob first define input $\mu$ as well as total loss in the communication line, which allows them to calculate modified Poisson distribution at Bob’s side taking losses into account. In this work we assume that input Poisson distribution does not modify in case of lossless setup. Then, using known equations for Poisson statistics, probabilities of detecting of $n$ photons ($n > 1$) are derived. At some point of quantum key distribution process Bob adjusts the detector in order to gather statistics of multi-photon pulse arrival probability. For example, in case of a superconducting nanowire detector this can be done by changing the critical current. The received results are compared to calculated expectations and detector noise level. PNS attack is detected when certain deviations are discovered.

![Figure 2](image1.png)  
**Figure 2.** Number of timeframes on Bob’s side as function of photons number for $\mu = 0.1$ compared to modified distribution in case of attack, where Eve obtains all photons except one from each timeframe, which amount is $10^6$.

![Figure 3](image2.png)  
**Figure 3.** Number of timeframes on Bob’s side as function of photons number for $\mu = 0.1$ compared to modified distribution in case of attack, where Eve obtains only one photon from each timeframe, which amount is $10^6$. 

So there are two extreme cases. In first one Eve obtain all photons except one, and in second case conversely obtains only one photon and leaves the rest.

In first case there will not be any timeframes with more than one photon. These changes greatly modify expected distribution and allows detect such PNS attack.

For second case the calculations show than if Eve splits only one photon from each multi-photon pulse, the number of pulses with \( n > 1 \) decreases more than one order of magnitude, while there appears to be a slight increase in single-photon states. These changes may be discovered when raw key rate is high enough to mask the detector noise.

If we take into account noise level on our detector about 10 Hz and necessary relation of signal to noise at least 100:1, so bitrates is to be at least 1000 bit/s. But if we want to discern the lost photons from about 5% (for \( \mu = 0.1 \)) of all timeframes, we should rise bitrates up to 20 Kbit/s. Our estimations show that the technique can be used in systems with bitrates higher than 20 Kbit/s for two-state protocols, and 40Kbit/s for four-state protocols. Systems with those bitrates can be constructed for sure, because there are systems with bitrates up to 1Mbit/s [16].

In order to implement this method, taking into account losses, Alice and Bob must control the length of optical channel in order to make sure that Eve has not introduced a segment with lower losses.

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 developed. The use of detectors which distinguish multi-photon states allows revealing such attacks by analyzing statistics on receiver’s side. In particular, we analysed the efficiency of PNS attack on quantum key distribution system with coherent light source and studied the ability of using these detectors to ensure security against PNS attack. The changes exceed the detector noise at bitrates higher than 20 Kbit/s and 40Kbit/s for two-state protocols and four-state protocols, respectively. Moreover, our method does not exclude possibility of combining with other known methods and can be used with any quantum cryptography setup.

Acknowledgements

This work was financially supported by Government of Russian Federation, Grant 074-U01.

References

[1] V. Scarani, H. Bechmann-Pasquinucci, N.J. Cerf et al 2009 Rev. Mod. Phys. 81, pp 1301–1350
[2] D.C. Unitt, A.J. Bennett, P. Atkinson et.al 2005 Journal of optics 7, pp 129
[3] Hartschuh, H. N. Pedrosa, J. Peterson, et al 2005 Chem. Phys. Chem. 6, № 1.
[4] A. Hogele, C. Galland, M. Winger et al 2008 Phys. Rev. Lett. 100, № 217401.
[5] T. B. Pittman, J. D. Franson, B. C. Jacobs 2007 New J. Phys. 9, № 195.
[6] B. C. Jacobs, T. B. Pittman, J. D. Franson. 2006 Phys. Rev. 74, № 217401.
[7] A. Kalachev, D. Kalashnikov, A. Kalinkin et al 2007 Laser Phys. Lett. 4, pp 722–725
[8] L. Lydersen, C. Wiechers, C. Wittmann et al 2010 Nature Photonics 4, pp 686–689
[9] N. Gisin, G. Ribordy, W. Tittel et al 2002 Reviews of modern physics 74, pp 181
[10] Hoi–Kwong Lo, Xiongfeng Ma, Kai Chen 2005 Physical Review Letters 94, № 230504
[11] Valerio Scarani, Antonio Acin, Nicolas Gisin et al 2004 Phys. Rev. Lett. 92, № 057901
[12] O. Guerreau, J.-M. Mérolla, A. Soujaeff et al 2003 IEEE J.Sel.Top.Quantum Electron. 9, pp 1533–1540
[13] M. D. Eisaman, J. Fan, A. Migdall et al 2011 Rev. Sci. Instrum. 82, № 071101
[14] Robert H. Hadfield 2009 Nature photonics 3
[15] G. N. Gol’tsman, O. Okunev, G. Chulkova et al 2001 Applied physics letters 79, № 6, pp 705
[16] Z. L. Yuan, A. R. Dixon, J. F. Dynes et al 2009 New Journal of Physics 11, № 045019