文章编号：1001－9014(2016)02－0166－06

DOI:10.11972/j.issn.1001－9014.2016.02.008

Novel and efficient near-infrared quantum anti-jamming detection scheme based on statistical theory against malicious attack

ZHAO Nan[1,2*], ZHU Chang-Hua[1], PEI Chang-Xing[1], ZHONG Shao-Chen[2]

(1. State Key Laboratory of Service Networks, Xidian University, Xi'an 710071, China;
2. Department of Electrical & Computer Engineering, Michigan State University, MI 48824, USA)

Abstract: A novel and efficient quantum detection scheme based on statistical theories was proposed. The feasibility was verified by simulation. The simulation results show that the scheme is efficient and secure. Considering the integrity of the scheme, we constructed a complete model of links to obtain the threshold of the scheme.

Key words: efficiency, quantum key distribution, statistical theory, threshold
PACS: 03.67.Dd, 42.50.Dv

一种新颖和高效的基于统计理论的抗恶意攻击的近红外场量子检测方案

赵 楠[1,2*], 朱畅华[1], 裴昌幸[1], 钟邵晨[2]

(1. 西安电子科技大学 综合业务网理论与关键技术国家重点实验室,陕西 西安 710071;
2. 密歇根州立大学 电子与计算机系,美国 密歇根州 东兰辛 48824)

摘要:提出了一种基于统计理论的新颖和高效的量子检测技术,并通过仿真验证方案的可行性.仿真结果表明,该方案较现有方案更高效,更安全.考虑到方案的完整性,文中建立了链路模型以获得方案的阈值.

关 键 词:效率;量子密钥分发;统计理论;阈值

中图分类号:TN918.91,TN219 **文献标识码**:A

Introduction

Quantum Key Distribution (QKD), invented by Bennett and Brassard[1], can be considered the first application of quantum information science, and commercial products have already become available[2]. On the theory side, the security of several variants of QKD protocols against general attacks has been proved[3-7]. Meanwhile, experimental techniques have reached a state of development that enables key distribution over distances of 300 km[8]. However, there are always imperfections in security and efficiency[9-11], due to the non-ideal experimental environment in real implement.

In ideal QKD protocols we are required to employ particular states. However, we tend to adopt substitutes to transmit quantum information within our present experiment ability. This unperfected quantum source provides probabilities for eavesdrop, usually referred to as Eve. The combination of multi-photon signals of source and loss in the transmission line derives some powerful eavesdropping attack[12-13]. The photon number splitting (PNS) attack that was first mentioned by Huttner and Imoto[13], and usually replaces the noisy and lossy transmission line by a superior one. In the process, the loss in legitimate quantum channel can be divided into two portions including accessible and non-accessible losses. The non-accessible loss may contain minimum transmission losses and detector inefficiencies. Accessible loss is lead into by illegitimate participator. When the proportion of accessible loss is large enough, transmission becomes insecure. Due to the threshold of cryptography about the loss has been consulted, Eve can replace the legitimate quantum channel with an ideal one, intercept all

Received date: 2015-04-28, **revised date**: 2015-12-24 **收稿日期**:2015-04-28, **修回日期**:2015-12-24

Foundation items: Supported by National Nature Science Foundation of China(613001171,61372076), the Fundamental Research Funds for the Central Universities, China(K5051301018)

Biography: ZHAO Nan(1980-), male, Shaanxi Xi'an, Ph. D. associateprofessor. Research areas are optical communication, quantum communication and quantum information

* **Corresponding author**: E-mail: zhaonan@xidian.edu.cn

single-photon signals and satisfy the expectation of Bob with multiple photons only. If the loss is not heavy enough for Eve to conceal her behavior, Eve can intercept a portion of single-photon signals and gather the details from the remaining single-photon by other optimal eavesdropping attacks. The optical attacks include blinding attack[14]. Moreover, even with linear optics alone powerful attacks in this thread can be launched. The proportion of photons in Eve's hand will reveal the polarization after she masters the polarization bases during the pubic consultation according to the BB84 protocol[14-19].

In actual application, because of the imperfections from experiments and channels that may introduce some side channel information, Eve may utilize them to deploy an attack. Moreover, for the active decoy-state experiments[20], it is difficult to avoid eavesdrop from attacks with much more excellent performance based on the existing technologies.

Statistical techniques are employed in many research and industrial areas, and they play important roles in practical situations especially. Some researches of quantum field are performed about probability statistics characteristics of the number of photons in the last ten years[21-22]. The distribution characteristics of quanta are obtained and become an essential foundation in the field of quantum communication and cryptography.

In this paper, we adapted mathematical statistics method to solve issues focusing on the security in quantum cryptography incurred by non-ideal equipment and imperfect experimental condition.

1 Analyzing on mathematical statistics characteristics of quanta

These practical approaches differentiate in many essential aspects from the initial theoretical proposal, due to the present experimental capability that is unable to satisfy the demands technologies. In practice quantum states emitted by laser source, instead of single-photon, are weak coherent pulses with a low probability of containing photons in one pulse. All these modifications between the ideal BB84 protocol and real implementations may jeopardize the security of the protocol, and result in limitations including the efficiency and distance.

In quantum cryptography protocols, some thresholds are estimated according to the influences from quantum channel disturbance and malicious attack. The attenuation caused by the non-ideal channel can affect the result of threshold. This means that, the legitimate participators may misunderstand some errors introduced by non-ideal channel as those from attacks. Unfortunately legitimate participators may not gather any useful information if channel attenuation is always high without any attacks. As a result, the efficiency of quantum communication is declined severely.

We attempted to distinguish the errors introduced by non-ideal channel and attacks.

1.1 The proof of probability distribution of stochastic process

The first step is to determine the probability distribution about the number of photons in pulses. The number of photons at each pulse satisfies Poisson distribution with parameter λ, that is

$$P\{X = k\} = \frac{\lambda^k e^{-\lambda}}{k!}, k = 0,1,2,\cdots \quad , \quad (1)$$

where the number of photons is k.

Supposing that X_1 and X_2 are randomly variables that satisfy Poisson distribution with parameters λ_1 and λ_2, respectively, we let the denotations $\varphi_{X_1}(\mu)$ and $\varphi_{X_2}(\mu)$ are the eigenfunctions of X_1 and X_2, then we have

$$\varphi_{X_1}(\mu) = \sum_{k=0}^{\infty} P(X_1 = k) e^{i\mu k} = e^{\lambda_1(e^{i\mu}-1)} \quad , \quad (2)$$

$$\varphi_{X_2}(\mu) = \sum_{k=0}^{\infty} P(X_2 = k) e^{i\mu k} = e^{\lambda_2(e^{i\mu}-1)} \quad . \quad (3)$$

In the weak laser pulse beam, X_1 and X_2 are independent of each other, so

$$\varphi_X(\mu) = \varphi_{X_1+X_2}(\mu) = e^{(\lambda_1+\lambda_2)(e^{i\mu}-1)} \quad . \quad (4)$$

The eigenfunctions correspond uniquely to distribution functions respectively. The randomly variable $X = X_1 + X_2$ satisfies Poisson distribution with parameter $\lambda_1 + \lambda_2$. If $X(t)$, the number of occurrences of event during an arbitrary length of the time interval $t(t>0)$, satisfies Poisson distribution with parameter λ_t, $\{X(t), t>0\}$ is termed the homogeneous Poisson process or the Poisson process for short.

Let X_1 and X_2 represent Poisson process with λ_1 and λ_2, respectively, then we have

$$X(0) = X_1(0) + X_2(0) = 0 \quad . \quad (5)$$

$\{X_1(t), t\geqslant 0\}$ and $\{X_2(t), t\geqslant 0\}$ are independent incremental processes of each other, so the superposition of these two independent incremental processes can be expressed as $\{X(t) = X_1(t) + X_2(t), t\geqslant 0\}$. For any $t_1 < t_2$, from characteristics of additive Poisson distribution, it can be conclude that $X_1(t_2) - X_1(t_1) + X_2(t_2) - X_2(t_1)$ satisfies Poisson distribution with parameter $(\lambda_1 + \lambda_2)(t_2 - t_1)$, it means that $X(t_2) - X(t_1)$ satisfies Poisson distribution.

From mentioned above, the superposition of two independent Poisson processes with λ_1 and λ_2 is the Poisson process with parameter $\lambda_1 + \lambda_2$, so a sample comprised of the number of photons in the weak laser pulse is Poisson process.

Let $X(t)$ denote the number of photons which have arrived at the receiving terminals until the instant t, $\{X(t), t\geqslant 0\}$ be Poisson process with parameter λ, and τ_1, τ_2, $\cdots$ τ_n, $\cdots$represent the arrival time of every single photon in turn. We can let $T_n = \tau_n - \tau_{n-1}$ ($\tau_0 = 0, n = 1, 2, \cdots$) as the interval of the time that Poisson processes arrived at. According to the random process theory, $\{T_n, n = 1,2,\cdots\}$ satisfies the exponential distribution with parameter λ.

1.2 Analysis and simulation about probability distribution with malicious eavesdrop

When Eve intercepts single photons from the quantum channel, she must resend substitutes in time in order to avoid being detected. The operation of resending may affect the integrate distribution of photons when Eve blocks a fraction b of the photons. We found a resulting

photon number distribution that is different from Poissonian.

Firstly we redefined the Poissonian photon number distribution with mean photon number $\mu\eta$, that is

$$P_{\text{loss}}[k] = \frac{(\mu\eta)^k}{k!}\mathrm{e}^{-\mu\eta} \quad . \quad (6)$$

Malicious attack will introduce additional loss. Supposing that Eve blocks a fraction of the whole photons, we get a resulting photon number distribution, namely

$$P_{\text{attack}}[k] = \begin{cases} (1+a\mu)\mathrm{e}^{-\mu} & k=0 \\ ((1-a)\mu+\mu^2/2)\mathrm{e}^{-\mu} & k=1 \\ \frac{\mu^{k+1}}{(k+1)!}\mathrm{e}^{-\mu} & k>1 \end{cases} . \quad (7)$$

In fact according to the traditional strategies, Eve can adjust a to match the number of vacuum signals of attack to that of quantum channel for remaining undetected, $P_{\text{attack}}[0]=P_{\text{loss}}[0]$. We get

$$a_{\text{match}} = \frac{1}{\mu}(\mathrm{e}^{\mu(1-\eta)}-1) \quad . \quad (8)$$

Obviously the formula holds for the case that $a_{\text{match}} \in [0,1]$, especially, $a_{\text{match}}=0$ when $\eta=1$, which means that for a lossless channel Eve cannot gather information undetected by blocking photons.

It is an especial situation when $k=1$, because only one photon exists in each pulse that is the real single photon signal. It is difficult for Eve to block these photons without being detected because the probability of malicious gathering information from the single-photon is extremely remote. Certainly Eve can attack the quantum channel by blind attack that utilizes the large pulse to interrupt and manipulate the detector at the legitimate terminals, however it is difficult to achieve.

Under the two situations above it is not difficult for legitimate participators traditionally named Alice and Bob to detect the attack.

Considering the situation when $k>1$, Eve must guarantee that the quantity of gathered photons is below that of transmitted photons generated by legitimate participator, $P_{\text{attack}}[K]<P_{\text{loss}}[k]$, when $k>1$. On the premise we analyze the statistical distribution of photons in the quantum single at the existing of attack.

Many efforts devoted by Eve as an eavesdropper to intercepting more photons in the course of attack. As mentioned before it is not difficult to detect the attack with the first two types. Therefore we analyzed principally the attack on multiply photons pulses existing in the quantum signal.

We supposed that the resent photons from Eve satisfy some type of distribution.

1.2.1 Poisson distribution

Supposing that Eve resends the false photons satisfied Poisson distribution advisedly or not, we analyzed the final probability distribution of photons.

Faint incoherent light has excellent properties like single-photon. However, the specific location of single-photon is indefinable. When eavesdrop occurs, Eve adapts some strategy to gather information from multiple photons, and resends the false photons pulse to the legitimate initial pulse sequence. The operation will damage the probability distribution of the number of whole photons, because the distribution of single-photon pulse is not continuous.

1.2.2 Normal distribution

Normal distribution is an appropriate function to describe the natural and social sciences for real-valued random variables. When Eve resends the regenerated photons, ordinarily the optical pulses are independent and the number of photons is random. We adapted normal distribution to express probability distribution of this event, namely

$$f(x) = \frac{1}{\sigma\sqrt{2\pi}}\mathrm{e}^{\frac{(x-\mu)^2}{2\sigma^2}} \quad , \quad (9)$$

where μ means mean or expectation of the distribution, σ is its standard deviation, so its variance is σ^2. For convenience, letting $\mu=0$, $\sigma=1$, we get

$$f(x) = \frac{1}{\sqrt{2\pi}}\mathrm{e}^{-\frac{x^2}{2}} \quad . \quad (10)$$

As an independent identical distribution random variable, the number of photons in pulses is discrete. We changed the traditional normal distribution form to describe discrete variable. According the value of the number of photons in Poisson distribution, we proposed the discrete probability distribution, namely

$$P_{\text{regular}}[k] = \begin{cases} \int_{-\infty}^{0.1}\frac{1}{\sqrt{2\pi}}\mathrm{e}^{-\frac{x^2}{2}}\mathrm{d}x & k=0.1 \\ \int_{0.1}^{x}\frac{1}{\sqrt{2\pi}}\mathrm{e}^{-\frac{x^2}{2}}\mathrm{d}x & k\geqslant 0.1 \end{cases} . \quad (11)$$

We took the value of k in 0.1, 0.2, 0.3, …, because they are the reasonable values about the number of photons in pulse. We used this function to convert continuous probability distribution to the discrete probability in order to compare the distribution with the Poisson distribution.

According to the different weights of photons from Eve and legitimate participators, the final probability distribution can be expressed as

$$f(k) = \frac{1}{\sqrt{2\pi}}\mathrm{e}^{-\frac{(\alpha k)^2}{2}} - \int_{-\infty}^{k}\frac{\mu^{\beta m+1}}{\beta m!}\mathrm{e}^{-\mu}\mathrm{d}m \quad , \quad (12)$$

where α,β are the proportions of the number of photons from legitimate participators and Eve, respectively, and $\alpha+\beta=1(\alpha,\beta\geqslant 0)$. From Eq. 6, $\mu\eta$ is the mean value of the Poisson distribution, and transmission efficiency $\eta \leqslant 1$. Ordinarily the number of single-photon from each pulse in faint incoherent light is near the 0.1, so here we can suppose $\mu\geqslant 0.01$.

We let $\mu=0.01$, and simulate the probability distributions of the number of photons from legitimate participator and eavesdropper with different proportions. The result is shown is figure 1. For convenient observation, we adopted a continuous form of curves.

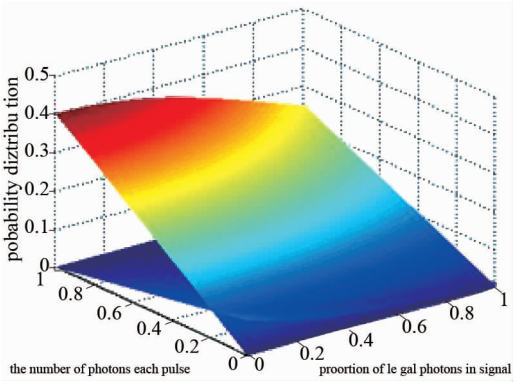

Fig. 1　Probability distributions of the number of legitimate and false photons in signal
图 1　信号中合法与伪造光子的数目概率分布图

From Fig. 1, with the increase of the number of photons or the proportion of false photons, the values of probability distribution raise. We need to guarantee that the value of probability distribution $f(k)$ satisfies $f(k) \geqslant 0$. Specially, when $f(k) = 0$, it is impossible to distinguish legitimate and false photons with probability distribution. Eve cannot attack quantum channel with a fixed probability distribution of the number of photons continuously and without being detected.

Here remains a problem about proportions of legitimate and false photons. We may adopt methods from information theory obtain the exact value about affect from proportion of false photons. Here we only analyzed this problem by the simulation results briefly.

From Fig. 1, the probability distribution of the number of photons is disturbed obviously when the proportion of false photons exceeds 25%. Supposing that Eve sends false photon P_{false} that accounts for 25% of the total sifted photons to legitimate participator, the proportion is much less than 50% and is not enough for Eve to gather the useful information. So the performance of our scheme degrades when $P_{\text{false}} \leqslant 25\%$, and it could be secure because the deficiency of leaked information.

Under the traditional strategy, participators estimate the security of quantum cryptography through consulted threshold that is fixed before the transmitting of quantum information. The thresholds may be different in many papers because the supposed backgrounds are not identical. To compare easily, we employed the frequent one as the traditional threshold. Taking the data appeared above as the parameters of the model, we compared our strategy with the traditional one. Then we set 25% as a value of threshold, it means when the measurements from terminal show that false quantum bits account for 25% of total amounts, the process of cryptography will be regard as unsecure communication. The successful and secure cryptography under the traditional and new strategies are compared in the table below.

Table 1　secure and success of traditional and new strategies
表 1　传统与新策略的安全性与成功率

QBER/(%)	25	30	40	50
Secure/(td/new)	n/y	n/y	n/y	n/n
Success/(td/new)	n/y	n/y	n/y	n/n

In the Table 1, "td" and "new" represent traditional and new strategy, respectively. It is shown that under the background described above, the performances of traditional and new strategies change with the increasing of QBER. When the QBER is from 25% to 40%, and 25% of them are caused by channel noise, the process is determined as an unsecure cryptography by the traditional strategy. Therefore the efficiency of cryptography is extremely low with the traditional strategy when QBER is below 50%. With our strategy we can distinguish different error, and then the efficiency of the whole quantum cryptography is improved.

In summary, the probability distribution of the number of photons in pulses from legitimate participator will be changed after malicious attack exists. The change makes the arriving time of photons no longer satisfy exponential distribution. We can observe the change about probability distribution of arriving time by detector located at the receiving terminals.

2　Model of the quantum binary symmetric channel under the BB84 protocol and its performance analysis

We established quantum channel model according to the success rate of transmitted quantum bits. Supposing that initial four quantum states are generated with same priori probability, β is defined as the number of photons from the sender, and α the number of photons with wrong distinguish. Supposing that the probability of successful measurement from the receiver is $1\text{-}\alpha/\beta$, then the channel model can be generalized by Fig. 3.

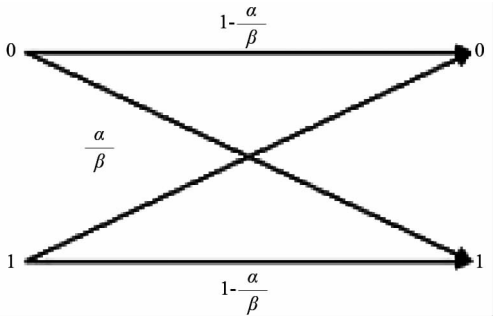

Fig. 2　Model of quantum binary symmetric channel without eavesdropping
图 2　无窃听的量子二元对称信道模型

Ordinarily we evaluated performance of quantum communication system with quantum bit error rate (QBER). When Eve attacks with intercept-resend strategy, the introduced error may change the cross error probability of quantum binary symmetric channel. Assuming that γ photons are intercepted and then the same amount of photons are resent by Eve, the probability of sending the code words successfully is $1\text{-}(\alpha\text{-}\gamma/2)/\beta$, and the crossover probability is $(\alpha—\gamma/2)/\beta$, with the channel model as shown in Fig. 4.

We adopted low-density parity check (LDPC) code possessed excellent performance to code the quantum information, considering that the long key can guarantee the security of the process of communication. Taking the

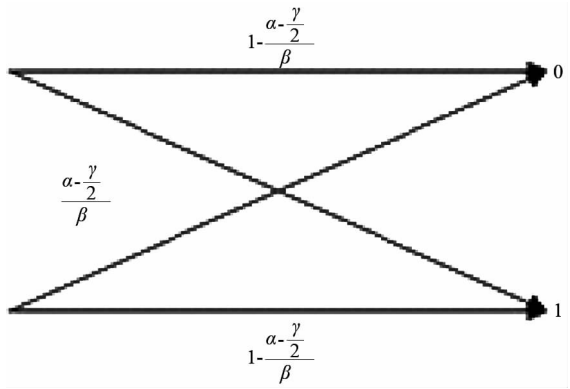

Fig. 3 Model of quantum binary symmetric channel with interception-retransmission eavesdropping
图3 截获重传窃听下的量子二元对称信道模型

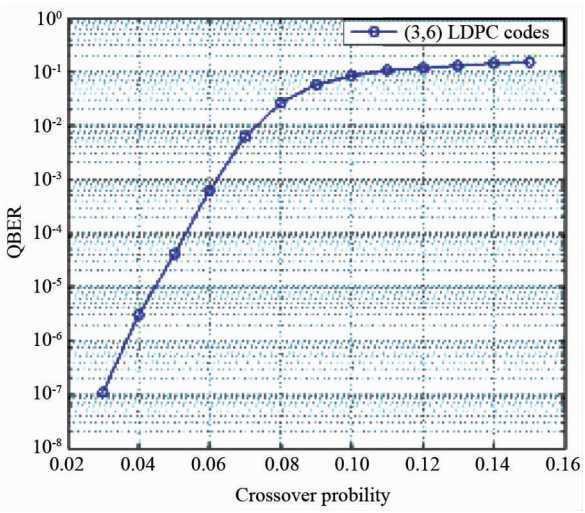

Fig. 4 Graph of quantum error rate against error transfer probability
图4 量子误码率与错误传输概率仿真图

(3,6) LDPC code with the code length of 1024 for example, the sum-product algorithm (SPA) was adopted as the decoding algorithm, and the maximum iterations are 50. The simulation results are shown in Fig. 5.

In Fig. 5, the abscissa represents the crossover probabilities of the quantum binary symmetric channel, and the ordinate represents QBER corresponding to different crossover probabilities. In real applications, usually we need to guarantee that QBER of a system is lower than the threshold set by the legitimate participators. The performance of codes deteriorates when QBER is below 10^{-5}, and keeps at 10^{-1} when crossover probability is above 0.1. However, quantum coding does not own a good correction performance when QBER is below10^{-5}. That means it is difficult to correct errors by coding when the circumstance of channel is deteriorated. Meanwhile, the threshold could be raised to enhance the ability of legitimate participators for detecting the attacks. The change of threshold caused by varied parameters of channel may reduce efficiency and security. In our scheme we adopted method of analyzing on mathematical statistics characteristics of quanta to distinguish the errors from affection of non-ideal channel or malicious eavesdropping, based on the observation of arriving time of photons. All these are based on the analysis in chapter 2 and the experiment results. Next we obtained a threshold of our scheme in real application according to simulation results above.

It can be seen in Fig. 5 that when the quantum bit error rate is 10^{-5}, the crossover probability $(\alpha-\gamma/2)/\beta = 0.045$. It follows from the graph of Fig. 4 that

$$\begin{cases} 1-\dfrac{\alpha}{\beta} = 0.03 \\ 1-\dfrac{\alpha}{\beta}+\dfrac{\gamma}{2\beta} = 0.045 \end{cases} . \quad (13)$$

Solving the above equations yields $\gamma/\beta = 3\%$ and $\alpha/\beta = 97\%$. Therefore, in the case of without considering code rate, when quantum bit error ratio caused by the channel itself is lower than 3%, the error may be corrected. When the eavesdropper adopts intercept-resend attacks with $\alpha/\beta > 0.7$, the coding/decoding performance will be seriously deteriorated.

Meanwhile, we can distinguish errors from non-ideal channel or attack by observing the change of arriving time of phones in pulses. We can adjust the code rate to satisfy the threshold mentioned in the last section, and make our scheme valid.

3 Conclusion

In this paper we proposed a scheme that utilizes mathematical statistics characteristics of quanta to distinguish errors introduced from eavesdrop. We obtained and verified the threshold of the scheme. We established the model of quantum channel and proved the feasibility of the scheme by simulation. One in particular is that intercept-resend eavesdrop is considered as the main attack strategy in our analysis and simulations. The following research will focus on improving the adaptability of our scheme to confront more malicious attacks.

References

[1] Bennett C H, Brassard G. Quantum cryptography: Publish-keydistribution and coin tossing [C]. In Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, 1984, Bangalore, India, 175-179.

[2] GisinN, RibordyG, TittelW, *et al*. Quantum cryptography [J]. *Rev. Mod. Phys*, 2002, **74**:145-195.

[3] NamikiR, HiranoT. Security of quantum cryptography using balanced homodyne detection [J]. *Phys. Rev. A*,2003, **67**(2):2308.

[4] LeverrierA, GrangierP. Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation [J]. *Phys. Rev*,2009, **102**:180504.

[5] ScaraniV, B-PH, CerfN J, *et al*. The security of practical quantum key distribution [J]. *Rev. Mod. Phys*. 2009, **81**(10):1301-1350.

[6] ShorPW, PreskillJ. Simple proof of security of the BB84 quantum key distribution protocol[J]. *Phys. Rev. Lett*. 2000, **85**(2):441-444.

[7] Renner R, GisinN, KrausB. Distribution protocols [J]. *Phys. Rev. A*. 2005, **72**(1):573.

[8] PatelK A, DynesJ F, LucamariniM, *et al*. Quantum key distribution for 10 Gb/s dense wavelength division multiplexing networks [J]. *Appl. Phys. Lett*. 2014, **104**(5):051123-4.

[9] Hayashi M. Hypothesis testing for an entangled state produced by spontaneous parametric down conversion[J]. *Phys. Rev. A*. 2006, **74**(6):

154.
[10] Inamori H, Lütkenhaus N, Mayers D. Unconditional security of practical quantum key distribution[J]. *Europe. Phys. J. D*. 2007, **41**(3): 599 - 627.
[11] Hayashi M. Prior entanglement between senders enables perfect quantum network coding with modification[J]. *Phys. Rev. A*. 2007, **76**(4): 538.
[12] Scarani V, Renner R. Quantum cryptography with finite resources: unconditional security bound for discrete-variable protocols with one-way postprocessing[J]. *Phys. Rev. Lett*. 2008, **100**(20)1586 - 1594.
[13] Huttner B, Imoto N, GisinN, *et al*. Quantum cryptography with coherent states[J]. *Phys. Rev. A*. 1995, **51**(3): 1863 - 1869.
[14] Dunjko V, Kashefi E, Leverrier A. Blind quantum computing with weak coherent pulses[J]. *Phys. Rev. Lett*. 2012, -(20): 502.
[15] Wang X-B. Beating the PNS attack in practical quantum cryptography [J]. *Phys. Rev. Lett*. 2005, **94**(24): 6102.
[16] Acn A, Gisin N, Scarani V. Coherent-pulse implementations of quantum cryptography protocols resistant to photon-number-splitting attacks [J]. *Phys. Rev. A*. 2004, **69**(1): 2309.
[17] Qi B, Fung C-H F, Lo H-K. Time-shift attack in practical quantum cryptosystems[J]. *Quant. Inf. Comput*. 2007, **7**(1): 73 - 82.
[18] Lin S, Wen Q Y, Gao F, *et al*. Eavesdropping on secure deterministic communication with qubits through photon-number-splitting attacks [J]. *Phys. Rev. A*. 2009, **79**(5): 1744 - 1747.
[19] Ribordy G, Gisin N, Kraus B. Trojan-horse attacks on quantum-key-distribution systems[J]. *Phys. Rev. A*. 2006, **73**(24): 457 - 460.
[20] Lo H K, Ma X F, Chen K. Decoy state quantum key distribution: theory and practice[J]. *Phys. Rev. Lett*. 2004, **94**(23): 504.
[21] Yin Z Q, Fred Fung C H, Ma X F, *et al*. Mismatched-basis statistics enable quantum key distribution with uncharacterized qubitsources [J]. *Phys. Rev. A*. 2014, **90**(5): 319.
[22] Pastukhov V M, Vladimirova Y V, Zadkov V N. Photon-number statistics from resonance fluorescence of a two-level atom near a plasmonic nanoparticle[J]. *Phys. Rev. A*. 2014, **90**(6): 31.