Conference materials
UDC 53
DOI: https://doi.org/10.18721/JPM.173.246

Security of BB84-like protocol on coherent states with different intensities

E.A. Dedkov[1,2,3,4]✉, R.A. Shakhovoy[1,3]

[1] Limited Liability Company "QRate", Moscow, Russia;

[2] Russian Quantum Center, Moscow, Russia;

[3] National University of Science and Technology MISiS, Moscow, Russia;

[4] Moscow Institute of Physics and Technology, Dolgoprudniy, Russia

✉ dedkov.ea@phystech.edu

Abstract. There are a large variety of quantum key distribution (QKD) protocols, which can provide unconditional security even with practically possible coherent states instead single-photon ones. Most of them require equal intensities of states emitted, which can be achieved only with some precision. However, in some state preparation schemes, for example, in those based on optical injection, equal intensities cannot be achieved without additional elements, which increases the cost and complexity of QKD setup. In this work we analyze the influence of different state intensities on achievable secret key rate in classical BB84 scheme.

Keywords: quantum key distribution, BB84, coherent pulses with random phases, decoy state

Citation: Dedkov E.A., Shakhovoy R.A., Security of BB84-like protocol on coherent states with different intensities, St. Petersburg State Polytechnical University Journal. Physics and Mathematics. 17 (3.2) (2024) 230–235. DOI: https://doi.org/10.18721/JPM.173.246

Материалы конференции
УДК 53
DOI: https://doi.org/10.18721/JPM.173.246

Секретность протокола BB84 на когерентных состояниях различной интенсивности

Е.А. Дедков[1,2,3,4]✉, Р.А. Шаховой[1,3]

[1] ООО «КуРэйт», Москва, Россия;

[2] Российский квантовый центр, Москва, Россия;

[3] Национальный исследовательский технологический университет «МИСиС», Москва, Россия;

[4] Московский физико-технический институт (национальный исследовательский университет), г. Долгопрудный, Россия

✉ dedkov.ea@phystech.edu

Аннотация. Существует большое количество протоколов квантового распределения ключа (КРК), которые способны гарантировать безусловную секретность даже с использованием когерентных состояний вместо однофотонных. Большинство из этих протоколов требуют одинаковой интенсивности посылаемых состояний. Однако, в некоторых схемах приготовления состояний, например, на основе оптической инжекции, состояния равных интенсивностей не могут быть получены без дополнительных элементов, что увеличивает стоимость и сложность установки КРК. В данной работе мы анализируем влияние различия интенсивностей приготавливаемых состояний на достижимую скорость генерации ключа в классическом протоколе BB84.

Ключевые слова: квантовое распределение ключа, BB84, когерентные импульсы со случайной фазой, состояния-приманки

Ссылка при цитировании: Дедков Е.А., Шаховой Р.А. Секретность протокола BB84 на когерентных состояниях различной интенсивности // Научно-технические ведомости СПбГПУ. Физико-математические науки. 2024. Т. 17. № 3.2. С. 230–235. DOI: https://doi.org/10.18721/JPM.173.246

Introduction

Quantum key distribution (QKD) protocols allow two distant users, often referred to as Alice and Bob, to distribute a secret key, which privacy is guaranteed by the laws of quantum mechanics. They can be divided into two main families: discrete variable (DV) and continuous variable (CV) QKD. The DV QKD protocols are those, which encodes secrecy in finite set of optical modes. Basically, it is essential for such protocols to use single-photon states, however, since there are no reliable single-photon sources, in practice coherent states are generally employed. Fortunately, with slight modification, DV QKD protocols based on attenuated laser pulses may be reduced to single-photon protocols. This reduction often relies on the implicit assumption, that the intensities of coherent states are the same for different bases and bit choices. In this work we perform a careful analysis of consequences, to which the violation of this assumption brings to the most common QKD protocol — BB84.

We remind, that basic BB84 protocol consist of the following steps:

1. Alice prepares and sends to Bob one of four qubit states, which are typically: $|0_Z\rangle$, $|1_Z\rangle$, $|0_X\rangle \equiv (|0_Z\rangle + |1_Z\rangle)/\sqrt{2}$, $|1_X\rangle \equiv (|0_Z\rangle - |1_Z\rangle)/\sqrt{2}$ with respective probabilities $p_{\alpha j}$, $\alpha \in \{Z, X\}$, $j \in \{0,1\}$ that are commonly equal. However, in practice Alice's source may be non-ideal both in the sense of preparing states and in the sense of the probability distribution.
2. Bob chooses measurement basis between X and Z randomly with probabilities p_X^B, p_Z^B respectively.
3. Alice and Bob announces bases in which each state was prepared and detected. Mismatched events are dropped out.
4. Alice and Bob estimate bit error rate and correct errors.
5. Alice and Bob estimate phase error rate and perform privacy amplification.

This protocol implies, that Alice has single-photon source, and Bob receives and measures all photons sent. In practice this is not the case. First, Alice use laser, which is the source of coherent states. Second, only a small fraction of states can be detected because of losses in fiber and finite quantum single-photon efficiency. Thus in realistic scenario one need to develop another security proof, which takes into account these difficulties.

In the following section we extend a common approach to security proof of DV QKD in realistic scenario to the case of BB84 with different state intensities. Next we present the results of our approach, namely, the achievable secret key rate and draw a conclusion whether protocols with this imperfection type can be employed or not.

Materials and Methods

When establishing security proof for a QKD protocol based on the coherent states, the following framework is commonly used [1]. Alice is allowed to prepare her coherent states on a Hilbert space of two photonic modes. We will stick to the case, when each state has some fixed intensity μ_j and perfectly random phase:

$$\begin{gathered} \left|\psi_j\right\rangle = \left|\beta_j^E e^{i\varphi}\right\rangle_E \otimes \left|\beta_j^L e^{i\varphi}\right\rangle_L, \\ \left|\beta_j^L\right|^2 + \left|\beta_j^E\right|^2 = \mu_j. \end{gathered} \tag{1}$$

Here E and L denote two photonic modes, early and late here, however, they can be two arbitrary orthogonal modes, for example, horizontal and vertical polarization. Let $\hat{a}_{E,L}$, $\hat{a}^{\dagger}_{E,L}$ be annihilation/creation operators for E and L mode respectively. Then for each state type j we may introduce new pair of creation operators, defined as:

$$\begin{aligned}\hat{a}^{\dagger}_{j1} &= \frac{\beta^{E}_{j}}{\sqrt{\mu_j}}\hat{a}^{\dagger}_{E} + \frac{\beta^{L}_{j}}{\sqrt{\mu_j}}\hat{a}^{\dagger}_{L},\\ \hat{a}^{\dagger}_{j2} &= \frac{\beta^{L}_{j}}{\sqrt{\mu_j}}\hat{a}^{\dagger}_{E} - \frac{\beta^{E}_{j}}{\sqrt{\mu_j}}\hat{a}^{\dagger}_{L}.\end{aligned} \tag{2}$$

and corresponding annihilation operators. They obviously obey bosonic commutation relation, and thus induce another Fock basis on the space of two photonic modes. If we now rewrite state (1) in this basis, we will obtain:

$$\left|\psi_j\right\rangle = \left|\sqrt{\mu}_j e^{i\varphi}\right\rangle_{j1} \otimes \left|0\right\rangle_{j2}. \tag{3}$$

It can be shown, that in case Alice each time produces states with random phase φ, the averaged states are Poisson mixture of n-photon states:

$$\rho_j = \frac{1}{2\pi}\int_0^{2\pi}\left|\psi_j\right\rangle\left\langle\psi_j\right| d\varphi = e^{-\mu_j}\sum_{n=0}^{\infty}\frac{\mu_j^n}{n!}\left|n\right\rangle_{j1}\left\langle n\right|\otimes\left|0\right\rangle_{j2}\left\langle 0\right|. \tag{4}$$

Note that now the measurement of photon number does not have any impact on states sent in the sense that the probabilistic mixture of this measurement resulted states is the same as (4). This means, that theoretically Alice can have a photon number measuring device installed on her output, and thus she will know the number of photons in each pulse. We then may split the initial protocol into several subprotocols which generate secret key only on vacuum states, single-photon states, and multiphoton ones. However, we are still allowed to perform only the steps of the initial protocol. The multiphoton subprotocol generates no secret because of the photon number splitting (PNS) attack, in which Eve steal one photon from pulse, stores it in her quantum memory and measures it in the right basis after basis announcement step. The vacuum subprotocol is also pretty useless to run, since all detection events in it is due to dark counts and thus bit error rate is close to 50%, which gives zero key.

We will stick to the case of ideally-prepared states, but with different intensities. Such states can be expressed as:

$$\begin{aligned}\rho_{z0} &= e^{-\mu_{z0}}\sum_{n=0}^{\infty}\frac{\mu_{z0}^n}{n!}\left|n\right\rangle_{Z1}\left\langle n\right|\otimes\left|0\right\rangle_{Z2}\left\langle 0\right|,\ \rho_{z1} = e^{-\mu_{z1}}\sum_{n=0}^{\infty}\frac{\mu_{z1}^n}{n!}\left|0\right\rangle_{Z1}\left\langle 0\right|\otimes\left|n\right\rangle_{Z2}\left\langle n\right|,\\ \rho_{x0} &= e^{-\mu_{x0}}\sum_{n=0}^{\infty}\frac{\mu_{x0}^n}{n!}\left|n\right\rangle_{X1}\left\langle n\right|\otimes\left|0\right\rangle_{X2}\left\langle 0\right|,\ \rho_{x1} = e^{-\mu_{x1}}\sum_{n=0}^{\infty}\frac{\mu_{x1}^n}{n!}\left|0\right\rangle_{X1}\left\langle 0\right|\otimes\left|n\right\rangle_{X2}\left\langle n\right|,\end{aligned} \tag{5}$$

where we use the following creation operators:

$$\begin{aligned}\hat{a}^{\dagger}_{Z1} &\equiv \hat{a}^{\dagger}_{E},\ \ \hat{a}^{\dagger}_{Z2} \equiv \hat{a}^{\dagger}_{L},\\ \hat{a}^{\dagger}_{X1} &\equiv \frac{1}{\sqrt{2}}\left(\hat{a}^{\dagger}_{E} + \hat{a}^{\dagger}_{L}\right),\ \ \hat{a}^{\dagger}_{Z2} \equiv \frac{1}{\sqrt{2}}\left(\hat{a}^{\dagger}_{E} - \hat{a}^{\dagger}_{L}\right).\end{aligned} \tag{6}$$

The single-photon subprotocol is then just basic BB84 protocol with ideal states, but different probabilities $\tilde{p}_{\alpha j} \propto p_{\alpha j}\mu_{\alpha j}e^{-\mu_{\alpha j}}$, $\sum_{\alpha,j}\tilde{p}_{\alpha j} = 1$. This result is simply the consequence of projecting (5)

onto the single-photon subspace. All we need then is to analyze the amount of secrecy N_{sec} in this slightly unideal BB84 protocol and run privacy amplification over single-photon states. The security analysis is straightforward and can be found in [2, 3]. It uses the concept of quantum coin and its imbalance, which can be calculated given distributed states expressions and probabilities $\tilde{p}_{\alpha,j}$. It worth noting, that we can always adjust initial state generation probabilities $p_{\alpha j}$ in such a way, that coin imbalance is zero. And thus we will have perfect BB84 single-photon protocol, which gives much higher key rate.

Alice, however, does not know the exact positions of the single-photon states sent. Fortunately, she can use proper privacy amplification technique to distill secrecy from the whole bunch of data originated from any states, not only single-photon ones. All she need to know is the amount of the secret key N_{sec} which can be obtained from these data in principle. Since this quantity is lower-bounded by the amount of secret key in single-photon states only, all Alice really needs is the lower bound on the amount of detected by Bob single-photon states, and the upper bound on bit error rates among them. She can obtain pretty tight bounds with the help of so-called *decoy-state technique* [1]. We will shortly review it here, since it is essential for our work.

We start with some definitions. The probability that Bob detects n-photon state of type j sent by Alice is called *yield*, and is denoted as Y_n^j, the fraction of n-photon states of type j, which produced the wrong click is called *error rate* and is denoted as e_n^j. Alice may choose from a set of different intensities for each state type $\mu_j \in \{\mu_j^{(1)}, \mu_j^{(2)},..., \mu_j^{(m)}\}$ and for each intensity and state type she has overall gain $Q_{\mu_j^{(i)}}^j$ which is the fraction of such states, that produced click on Bob's detector, and the overall error rate $E_{\mu_j^{(i)}}^j$ which is the fraction of wrong clicks among $Q_{\mu_j^{(i)}}^j$ detected states. If Alice can prepare and analyze arbitrary intensity, then she can find exact single-photon yield Y_1^j and error rate e_1^j. In [1] it was shown, that pretty tight bounds can be obtained also in case Alice has only three options for intensity.

Unfortunately, if Alice is not permitted to use decoy states, the bounds are loose, mostly because we cannot reliably estimate the number of detected vacuum states (the first term in the right side):

$$Q_\mu = \sum_{n=0}^{\infty} \frac{\mu^n}{n!} e^{-\mu} Y_n^{(\mu)} \le e^{-\mu} Y_0^{(\mu)} + \mu e^{-\mu} Y_1^{(\mu)} + \left[1 - (1+\mu) e^{-\mu}\right]. \quad (7)$$

Fortunately, we may estimate the total number of vacuum and single-photon states, i.e. vacuum + single-photon gain and total errors number:

$$Q_{0,1}^{(\mu)} \ge Q_\mu - \left[1 - (1+\mu) e^{-\mu}\right], \; Q_{0,1}^{(\mu)} E_{0,1}^{(\mu)} \le E_\mu Q_\mu. \quad (8)$$

However, this leads to a problem: we need to analyze the security of BB84 protocol with qutrit states. Although Koashi's approach [2] based on quantum coin is applicable here, it gives extremely poor, if not always zero, key rate. This is the result of huge "losses" (recall, that theoretical coin imbalance should be divided on yield), which are present in the system since only a small fraction of vacuum states is detected by Bob. Therefore, in this case we need to either find better consideration instead of just normalizing quantum coin imbalance or use loss-tolerant approach, like in [4] is done for three-state protocol. Since the first approach is not developed yet, we use the second one. Moreover, the presence of the fourth state in BB84 protocol allows us to include vacuum states into the analysis naturally. It worth noting, that loss-tolerant approach requires a little bit more postprocessing, since it utilizes and counts events which failed sifting, i.e. where Alice's and Bob's bases differ.

The whole analysis is rather complicated, so we present here only the crucial ideas and address the reader to the original work [4] or our future article, where we will cover this question in detail. The first point is to observe, that the states (5), projected onto the zero and one photon subspace are in semi-diagonal form, i.e. their density matrix are block-diagonal, with single number characterizing vacuum component, and qubit submatrix characterizing single-photon component. Thus we will need only one extra transmission rate, which characterizes the transmission of vacuum states, additionally to the transmission rates of X, Z Pauli matrices and identity

matrix. This four transmission rates are perfectly obtainable via the solution of the system of four linear equations, one equation for each state type. The second point to highlight is that we need to know *exact* yields and gains in order to obtain phase error. This is not the case, but we are able to find reliable bounds they lie within. Fortunately, the expression for the phase error rate is almost linearly dependent on the observable quantities, thus with some analysis one may state, that upper bound on the phase error is achieved on the boundary of observables. This means, we may calculate phase error upper bound as maximum over a finite set.

Results and Discussion

Using the security proof, sketched here, we may characterize the influence of state intensities mismatch on the achievable secure key rate. We will stick to the case when the intensities are related as following: $2\mu_{0z} = 2\mu_{1z} = \mu_{0x} = \xi^{-1}\mu_{1x}$. Such choice is natural for state preparation scheme based on the optical injection. Fig. 1,*a* represents the key rate per state sent dependent on transmission channel length for various scenarios (modelling parameters are listed in Table and intensities were chosen to maximize key generation at 30 km). It worth noting that in decoy-states scenario the key rate of BB84 with different intensities and balanced probabilities almost follows the key rate of that with same intensities. All reasonable probability balancing scenarios for BB84 without decoys are with high precision the same and follows the key rate for BB84 with equiprobable states choice. The reasons for it is employing loss-tolerant approach and generation high part of key from dark counts.

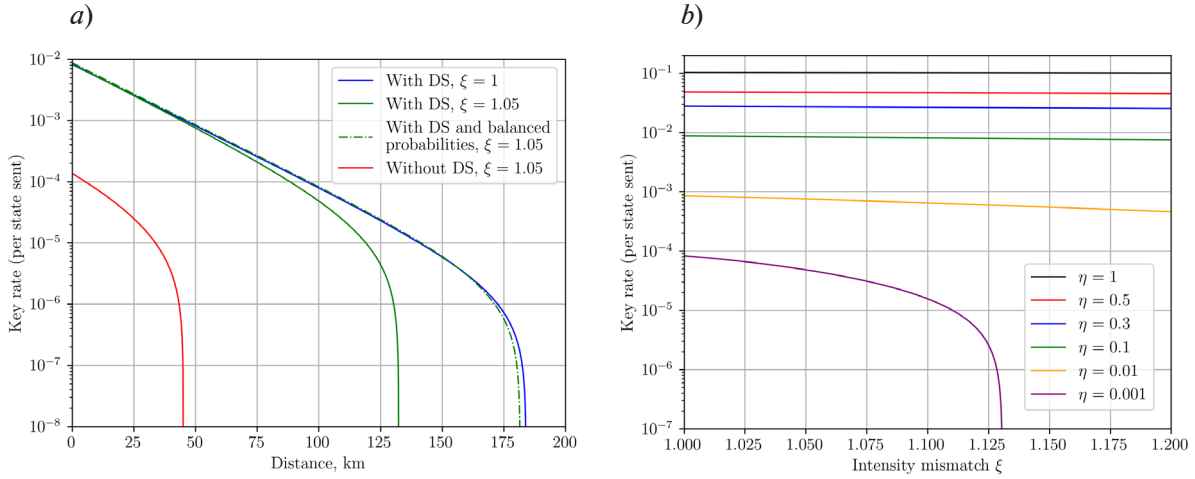

Fig. 1. Plot of key rate per state sent versus channel length (*a*). Plot of key rate per state sent at different channel transmission parameters η (including detector efficiency and transparency) versus intensity mismatch parameter (*b*)

Table

Parameters for key rates estimation

Fiber transparency	α=0.02 dB/km	Z-basis state intensity for decoy-state protocol	μ_{ds}=0.299
Detector efficiency	η=0.1	Z-basis state intensity for protocol without decoys	μ_{wods}=2.82·10^{-3}
Dark count probability	p_{dc}=10^{-6}	Decoy state attenuation coefficient	λ_1=0.5, λ_2=0.1
Probability of wrong click	p_{err}=0.01	Error correction efficiency	f_{ec}=1.22

Fig. 1, *b* shows the dependence of the key rate for various fixed transmission probabilities η, which incorporates both detector efficiency and channel opacity, on intensity mismatch parameter ξ in decoy-state scenario. Without decoys key rate barely depends on ξ, but slight grow can be observed. This is the consequence of the increase in the detection rate of one of the states sent due to its higher intensity.

Conclusion

We have analyzed the modified version of BB84 protocol on coherent states with different intensities of signal pulses. Despite our analysis is largely simplified and there potentially can exist better key rate formulas, we have shown that it is possible to distribute secret key without any correction of intensity. Moreover, such a protocol can be brought back to ideal BB84 just with adjustment of bit values distribution on the Alice's side, which may be done programmatically and requires no additional hardware changes.

The results obtained in this work are for asymptotic scenario only, i.e. when Alice and Bob gather infinitely much data and can estimate all statistics with arbitrary precision. In case of finite block size an additional complicated analysis is required, which will result in lower secret key rate.

REFERENCES

1. **Ma X., Qi B., Zhao Yi, Lo H.-K.,** Practical decoy state for quantum key distribution, Physical Review A. 72 (2005) 012326.

2. **Koashi M.,** Simple security proof of quantum key distribution based on complementarity, New Journal of Physics. 11 (2009) 045018.

3. **Gottesman D., Lo H.-K., Lütkenhaus N., Preskill J.,** Security of quantum key distribution with imperfect devices, Quantum Information & Computation. 4 (5) (2004) 325–360.

4. **Tamaki K., Curty M., Kato G., et al.,** Loss-tolerant quantum cryptography with imperfect sources, Phys. Rev. A. 90 (2014) 052314.

THE AUTHORS

DEDKOV Evgeniy A.
dedkov.ea@phystech.edu

SHAKHOVOY Roman A.
r.shakhovoy@goqrate.com
ORCID: 0000-0003-2750-0518

Received 29.07.2024. Approved after reviewing 12.08.2024. Accepted 15.08.2024.