Conference materials
UDC 004.056.55
DOI: https://doi.org/10.18721/JPM.163.138

Detection-efficiency mismatch in a satellite-to-ground quantum communication

E.I. Ivchenko [1, 2, 3, 4] ✉, A.V. Khmelev [1, 2, 3], V.L. Kurochkin [1, 2, 3, 4]

[1] Russian Quantum Center, Moscow, Russia;
[2] Moscow Institute of Physics and Technology, Dolgoprudny, Russia;
[3] QSpace Technologies, Moscow, Russia;
[4] MISIS, Moscow, Russia
✉ ivchenko.ei@phystech.edu

Abstract. The detection efficiency mismatch is one of the issues with practical quantum key distribution. The challenge is also inherent in satellite quantum communication due to the detectors and optical elements imperfections in the different quantum channels. Here, we generalize the theory developed for optical fiber QKD to satellite-to-ground QKD with four unbalanced polarization channels to estimate the secret key length. We simulate satellite quantum communication for the measured parameters of the realistic receiving ground station and calculate bounds for the secret key rate and length using two approaches: the first one when you separate the data on bases and the second when calculate the key from the full amount of data. We discuss the advantages and disadvantages of each approach and describe ways to operate with them. For our ground station, the secret key rate turned out to be 20% less when the detection-efficiency mismatch was at 1:2 and we used the optimal way to calculate the key.

Keywords: quantum key distribution, satellite-to-ground channel, modeling, detection-efficiency mismatch

Funding: This work was supported by the Ministry of Education and Science of the Russian Federation in the framework of the Program of Strategic Academic Leadership "Priority 2030" (Strategic Project "Quantum Internet").

Citation: Ivchenko E.I., Khmelev A.V., Kurochkin V.L., Detection-efficiency mismatch in a satellite-to-ground quantum communication, St. Petersburg State Polytechnical University Journal. Physics and Mathematics. 16 (3.1) (2023) 216–220. DOI: https://doi.org/10.18721/JPM.163.138

Материалы конференции
УДК 004.056.55
DOI: https://doi.org/10.18721/JPM.163.138

Разная эффективность детектирования состояний в квантовом канале спутник-земля

Е.И. Ивченко [1, 2, 3, 4] ✉, А.В. Хмелев [1, 2, 3], В.Л. Курочкин [1, 2, 3, 4]

[1] Российский квантовый центр, Москва, Россия;
[2] Московский физико-технический институт, г. Долгопрудный, Россия;
[3] КуСпэйс Технологии, Москва, Россия;
[4] Университет науки и технологий МИСИС, Москва, Россия
✉ ivchenko.ei@phystech.edu

Аннотация. Разная эффективность детектирования является одной из проблем практического квантового распределения ключа (КРК). Эта проблема в большей сильнее влияет на канал спутник-земля из-за несовершенства детектора и различного влияния атмосферы на разные квантовые состояния. В этой статье мы расширяем теорию,

разработанную для волоконных систем КРК, на канал «спутник-земля» с четырьмя несбалансированными детекторами. Мы моделируем квантовое распределение ключа от спутника к наземной станции с учетом разной эффективности детекторов, описываем различные способы работы с необработанными данными, обсуждаем преимущества и недостатки каждого подхода и вычисляем ограничения для скорости и длины секретного ключа. Судя по измеренным характеристикам нашей наземной станции, при несоответствии эффективности обнаружения 1:2 генерация безопасного конечного ключа уменьшилась на 20%.

Ключевые слова: квантовое распределение ключа, канал спутник-земля, моделирование, несоответствие эффективностей детекторов

Финансирование: Работа выполнена при поддержке Министерства образования и науки Российской Федерации в рамках Программы стратегического академического лидерства «Приоритет 2030» (Стратегический проект «Квантовый Интернет»).

Ссылка при цитировании: Ивченко Е.И., Хмелев А.В., Курочкин В.Л., Разная эффективность детектирования состояний в квантовом канале спутник-земля // Научно-технические ведомости СПбГПУ. Физико-математические науки. 2023. Т. 16. № 3.1. С. 216–220. DOI: https://doi.org/10.18721/JPM.163.138

Introduction

Satellite-based quantum key distribution over long distances has made significant progress [1, 2], but its practical schemes have drawbacks. One of the practical challenges in satellite-to-ground QKD is the detection-efficiency mismatching of polarization photon states received by the ground station. This discrepancy includes the unequal optical efficiency of the polarization channels and the imbalance of the detectors. For fiber-optic systems with two detectors, the effect of efficiency mismatch on the secret key rate was studied [3, 4, 5]. Using satellite-to-ground QKD model, we investigate the influence of this mismatching on the final key rate for the system with four detectors.

In this paper, we will consider the BB84 protocol with passive basis choice. In that case, we have four detectors, each of which responds to some bit 0 or 1 in some basis X or Z. It is quite difficult to design detectors with the same quantum efficiency, and the influence of the atmosphere is added in the satellite-to-ground channel, so the mismatch in our case is a significant challenge.

The eavesdropper can get additional information about the sifted key due to the imbalance that can be used for simple key guessing, knowing that 0 is greater than 1, or for possible attacks on the QKD protocol. Thus, we must additionally compress the key during the secrecy amplification procedure.

Methods

We work in terms of density matrices with initial states $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$ that correspond to bases X, Z and bits 0, 1, respectively. To estimate the security of a practical implementation of the discrete variable QKD protocol with four detectors, we use the following assumptions:

1. The mismatch t_{xz} between two bases is present;
2. The imbalance η between accepting 0 and 1 in various bases is equal.

We assume that the detector with the highest number of clicks has one hundred percent efficiency, and all additional losses occur in channel. As a result, other detector efficiencies are normalized on the mentioned one, and the mismatches in receiving bits η and bases t_{xz} are defined.

A positive operator-valued measure (POVM) with measurement probabilities p_x and p_z for the X and Z Bob's bases can be described in the following form:

$$\begin{gathered} P^B_{z,0} = p_z\,|0\rangle\langle 0|, \quad P^B_{z,1} = p_z\eta\,|1\rangle\langle 1|, \\ P^B_{x,0} = p_x t_{xz}\,|+\rangle\langle +|, \quad P^B_{x,1} = p_x t_{xz}\eta\,|-\rangle\langle -|, \\ P^B_{\varnothing} = I_3 - P^B_{z,0} - P^B_{z,1} - P^B_{x,0} - P^B_{x,1}. \end{gathered} \tag{1}$$

The POVM for Alice has the same form with the values $t_{xz} = 1$, $\eta = 1$.

The final density matrix after the quantum states transmitting over the channel, bases choice, and error correction has the same form as in the article [4], but with the measurement operators in Eqs. (1). So, we can use final equality for the key rate:

$$K = \min_{\rho_{AB} \in S} D\left(G_{ch}(\rho_{AB}) \| Z\left(G_{ch}(\rho_{AB})\right)\right) - p_{pass} h(Q_s), \tag{2}$$

where $S = \{ \rho \geq 0 \text{ on } H_A \otimes H_B \| \ Tr\, \Gamma_{ij} \rho = \gamma_{ij}, \forall i,j \}$.

The conditions for the density matrix S can be found from measurements of the observables, which corresponds to operators $\Gamma_{ij} = P_i^A \otimes P_j^B$. However, these restrictions are dependent, and we should use a set of demands that define the number of received pulses, detection mismatch, and quantum bit error rate (QBER). It has the following restrictions:

$$\begin{gathered}
\Gamma_1 = I_2 \otimes \left(\eta P_{z,0}^B + P_{z,1}^B + t_{xz}\left(\eta P_{x,0}^B + P_{x,1}^B\right)\right) = \eta\left(p_z + t_{xz} p_x\right) I_2 \otimes I_2, \\
\Gamma_2 = \frac{t_{xz}}{p_x^2}\left(P_{x,0}^A \otimes P_{x,1}^B + \eta P_{x,1}^A \otimes P_{x,0}^B\right) + \frac{1}{p_x^2}\left(P_{z,0}^A \otimes P_{z,1}^B + \eta P_{z,1}^A \otimes P_{z,0}^B\right), \\
\Gamma_3 = I_2 \otimes \left(P_{z,0}^B + P_{z,1}^B + t_{xz}\left(P_{x,0}^B + P_{x,1}^B\right)\right).
\end{gathered} \tag{3}$$

The first and third operators are responsible for the probability of accepting impulses in the experiment with and without unbalance. They allow for expressing the imbalance of the detectors and the number of received pulses. The second operator expresses the probability of QBER in the received bits.

We can get values for the observables for the matrix ρ_{AB}, by substituting operators, taking out the common factor in the first expression, and then simplifying the first and second ones.

$$\begin{gathered}
\mathrm{Tr}\,\Gamma_1 \rho_{AB} = t\eta\left(p_z + p_x t_{xz}\right), \\
\mathrm{Tr}\,\Gamma_2 \rho_{AB} = t\eta\left(p_z + p_x t_{xz}\right) Q, \\
\mathrm{Tr}\,\Gamma_3 \rho_{AB} = p_{pass}.
\end{gathered} \tag{4}$$

There are two different ways to post-processing data for this theory of obtaining a secret key. In the first method, we separate the initial bits into bases; in the second, we work with the full amount of data. Using the first approach, we can reduce our case to the discussed one in the article [4]. The final formula of the secret key rate for this approach has an analytical form:

$$K\left(Q_z, Q_x, \eta, t, p_{\text{pass}}\right) = p_{\text{pass}}^L \left[h\left(\frac{t^U (1+\delta^U)}{2 p_{\text{pass}}^L}\right) - h\left(\lambda\left(Q_x^U, \eta, t^L, p_{\text{pass}}^U\right)\right)\right] - p_{\text{pass}} h\left(Q_z\right), \tag{5}$$

where the values of t, p_{pass} and γ_2 are changed in accordance with Eq. (4) and superscripts L, U mean the lower and upper bounds of the values. That bounds appear from accounting for statistical fluctuations in clicks and errors, which we receive from restrictions Eq. (4). However, we estimate the generation rate twice on different bases and reduce the statistic, which is a problem for satellite-to-ground channels due to the limited time of data transmission.

For the second approach, we estimate the final key rate using full data with numerical methods, according to the Eqs. (2)-(4).

Results

We consider the real parameters of our ground station with telescope aperture of 600 mm [6] that gives as $\eta = 0.5$, $t_{xy} = 0.75$ and assume that p_x, $p_z = 0.5$. We use the results of the article [7] to calculate the transmission efficiency $\eta(t)$ of satellite-to-ground channels and the experimental parameters of the QKD to model the channels for different bases and bits, as follows:

$$Q_{\alpha,i,\varphi} = 1 - (1 - Y_0) * e^{-\eta_{\alpha,i,\varphi}(t)\delta_\varphi}, \tag{6}$$

$$e_{\alpha,i,\varphi} = e_0 Y_0 + e_{det}(1 - e^{-\eta_{\alpha,i,\varphi}(t)\delta_\varphi}). \tag{7}$$

These equations determine the gain and the probability of errors for the states of type φ, basis α and bit value i, where δ_φ – the average photon number for pulses of type φ. The results of

modeling are shown in the Fig. 1, *a*. Here, we simulate the satellite passage over the zenith, which does not reduce the generality of judgments but simplifies the calculations.

Table

Key parameters of the QKD experimental setup

μ	ν	p_x	p_z	p_s	p_d	p_v	f (Hz)	Y_0(/pulse)	e_{det}
0.8	0.1	0.5	0.5	0.5	0.25	0.25	10^8	5×10^{-6}	0.5%

Then, we use Equations (2)-(5) to estimate the key rate in different approaches. In order to present the feasible key rate at satellite passage, we evaluate such statistics as would be accumulated during the entire flight if the satellite were in one place. Fig. 1, *b* shows the dependence of the secret key rate on the time of satellite passage. As assumed, statistical fluctuations make a significant contribution when the calculations are performed for separated bases. Thus, the key rate is reduced by about half.

Then, we normalize the generation rate, which is calculated from full amount of data, to the one that is obtained with an efficiency of $(1+\eta+t_{xz}+\eta t_{xz})/4$ for all detectors. This curve is shown in Fig. 2 as a function of transmission efficiency for the general mismatching analysis. This transmission interval was chosen by taking into account the experimental data.

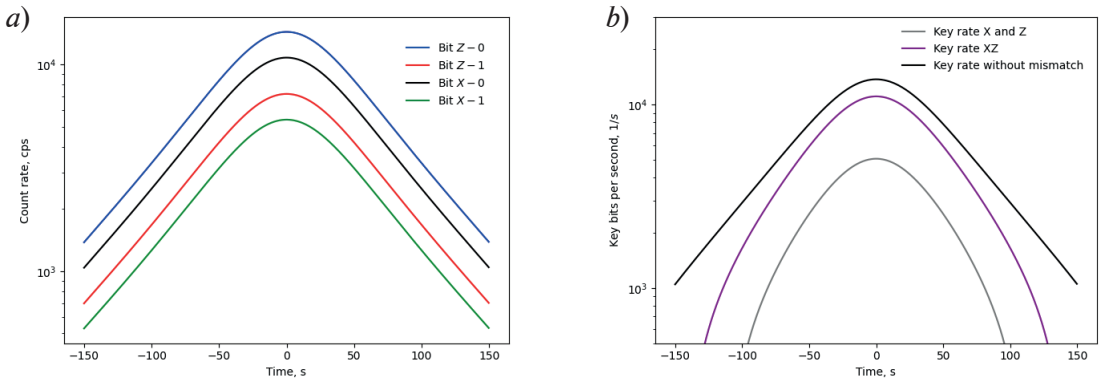

Fig. 1. Simulation results of (*a*) received model signals in the satellite-to-ground channel for different states depending on the passage time, and calculation results of (*b*) the secret key rate for the BB84 decoy-state protocol vs. the passage time. Purple line indicates a detector efficiency mismatch of 1:2 and calculation by full amount of data; gray line indicates a mismatch too, but calculation by different bases Eq. (5); black line indicates no detector efficiency mismatch, all detectors have an efficiency of $(1+\eta+t_{xz}+\eta t_{xz})/4$

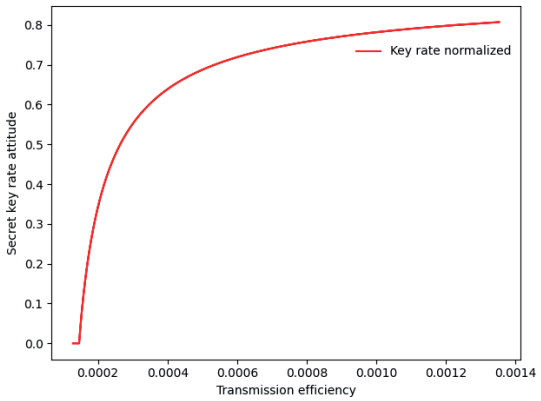

Fig. 2. Decrease of secret key rate in the detection efficiency-mismatch case with respect to the no-mismatch case as a function of transmission efficiency. The transmission bounds are taken from the real characteristic of our ground station [6]

Conclusion

To sum up, we have estimated the effect of the detection efficiency mismatch on the final key rate in the satellite-based QKD system and calculated its bounds. The analysis shows that the imbalance of the polarization channels in each measurement basis of 1:2 leads to a decrease of the key rate of less than 20%, if we make the calculation with all the data. However, the reduction will be 60% if we use Eq. (5) for two bases separately.

REFERENCES

1. **Lu C.Y., et al.,** Micius quantum experiments in space. Reviews of Modern Physics. 94 (2022) 3.
2. **Liao S.K., et al.,** Satellite-to-ground quantum key distribution. Nature. 549, 7670 (2017).
3. **Lo H.K., Ma X., Chen K.,** Decoy state quantum key distribution. Physical review letters. 94 (2005) 23.
4. **Bochkov M.K., Trushechkin A.S.,** Security of quantum key distribution with detection- efficiency mismatch in the single-photon case: Tight bounds. Physical Review A. 99 (2019) 3.
5. **Trushechkin A.,** Security of quantum key distribution with detection-efficiency mismatch in the multiphoton case. Quantum. 6 (2022) 771.
6. **Khmelev A.V., et al.,** Semi-Empirical Satellite-to-Ground Quantum Key Distribution Model for Realistic Receivers. Entropy. 25 (2023) 3.
7. **Khmelev A.V., et al.,** Recording of a single-photon signal from low-flying satellites for satellite quantum key distribution. Technical Physics Letters. 47 (2021) 858–861.

THE AUTHORS

IVCHENKO Egor I.
ivchenko.ei@phystech.edu
ORCID: 0000-0002-8163-4245

KUROCHKIN Vladimir L.
v.kurockin@goqrate.com
ORCID: 0000-0002-1599-9801

KHMELEV Aleksandr V.
a.khmelev@goqrate.com
ORCID: 0000-0003-1511-1128

Received 16.07.2023. Approved after reviewing 09.08.2023. Accepted 10.08.2023.