THEORETICAL PHYSICS

Conference materials
UDC 535
DOI: https://doi.org/10.18721/JPM.163.277

Excess leakage of information in quantum key distribution with passive side channels

D.V. Babukhin[1]✉, D.V. Sych[2]

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

[2] P.N. Lebedev Physical Institute of the RAS, Moscow, Russia

✉ dv.babukhin@gmail.com

Abstract. Passive side channels of the photon source make quantum key distribution (QKD) protocols insecure. To restore security, we need to incorporate the leakage through the side channel into the secret key estimate, but there is no definitive way to do that. In this work, we compare several practical methods of secret key rate estimating in QKD protocols with photon distinguishability side channel. We calculate upper bounds on secret key generation rates, using two reinterpretations of eavesdropper excess information – the effective error method and the a-priori loss method. We demonstrate that the effective error method provides tighter upper bound on the secret key rate than a-priori loss. Our results refine the toolbox of estimating security of QKD protocols with passive source side channels.

Keywords: quantum key distribution, source side channels, BB84 with decoy states

Citation: Babukhin D.V., Sych D.V., Excess leakage of information in quantum key distribution with passive side channels, St. Petersburg State Polytechnical University Journal. Physics and Mathematics. 16 (3.2) (2023) 439–442. DOI: https://doi.org/10.18721/JPM.163.277

Материалы конференции
УДК 535
DOI: https://doi.org/10.18721/JPM.163.277

Избыточная утечка информации в системах квантового распределения ключей с пассивными побочными каналами

Д.В. Бабухин[1]✉, Д.В. Сыч[2]

[1] ООО «КуРэйт», Москва, Россия;

[2] Физический институт имени П. Н. Лебедева РАН, Москва, Россия

✉ dv.babukhin@gmail.com

Аннотация. Пассивные побочные каналы источника фотонов делают протоколы квантового распределения ключей (КРК) небезопасными. Чтобы восстановить безопасность, необходимо включить утечку через побочный канал в оценку секретного ключа, но не существует определенного способа сделать это. В этой работе мы сравниваем несколько практических методов оценки скорости секретного ключа в протоколах КРК с побочным каналом, возникающим от частичной различимости фотонов, и демонстрируем, что метод эффективной ошибки обеспечивает более жесткую верхнюю границу для скорости генерации секретных ключей, чем метод априорных потерь.

Ключевые слова: квантовое распределение ключей, побочные каналы источников информации, протокол ББ84 с состояниями-ловушками

Ссылка при цитировании: Бабухин Д.В., Сыч Д.В. Избыточная утечка информации в системах квантового распределения ключей с пассивными побочными каналами // Научно-технические ведомости СПбГПУ. Физико-математические науки. 2023. Т. 16. № 3.2. С. 439–442. DOI: https://doi.org/10.18721/JPM.163.277

Introduction

Theoretical QKD protocols, which promise unconditional security, are based on idealistic model of optical hardware. These models often differ from real devices performance. The gap between practice and theory leads to excess leakage of information about secret key towards an eavesdropper through side channels. There are many reasons why such leakage can occur, and the problem of estimating and/or eliminating unwanted leakages of information is an active research topic [1, 2].

Photon distinguishability side channel is one of such side channels, which provide the eavesdropper with additional information. This kind of such channel does not require any active interaction between the eavesdropper and hardware of legitimate users, so this side channel is passive. One of the prospective ways to solve the problem of passive source side channels is the development of methods to estimate information leakage. The standard method, used in the field, is a GLLP approach [3], which incorporates side channel eavesdropping from the general perspective. Although being general, this approach provides pessimistic rates of secret key generation, thus guaranteeing QKD systems to be secure only on very short distances. Taking into account specific structure and nature of a particular side channel, as well as considering explicit eavesdropping strategies on QKD systems with such a side channel can provide more optimistic security estimates [4].

In recent paper [5], there was introduced a practical method to estimate excess leakage of information through the photon distinguishability side channel in a BB84 decoy state protocol. This method uses reinterpretation of additional information of the eavesdropper to calculate a so-called effective error, a cumulative parameter, which incorporates both eavesdropping on the protocol and on the passive side channel. This method is aimed to be a convenient practical tool to estimate security of QKD. Here we further refine the idea of this method. In particular, we consider another possible reinterpretation of additional information, dubbed a-priori loss method, and investigate the security of the QKD protocol, estimated using both of described methods. We show that the effective error method provides more tight security estimate than the a-priori loss method.

Materials and Methods

When the eavesdropper (Eve) attacks the QKD protocol without side channels, she obtains information about secret key bit at the cost of introducing errors in legitimate sides communication, Alice (sender) and Bob(receiver), of the value Q. If a side channel is available, Eve obtains excess information Δh about the secret key without introducing communication error. This excess information formally incorporated to the loss of mutual information between legitimate sides and interpreted as an information leaked to the eavesdropper. The secret key rate of the QKD protocol then is calculated from information relations between three main actors:

$$R^{\Delta} = 1 - h(Q) - (h(Q) + \Delta h), \tag{1}$$

Formally, the excess information term can be moved across the secret key rate, and the meaning of this term changes. In particular, the secret key rate (1) contains three terms. The first term (the a-priori term) corresponds to initial entropy of the Alice source and bounds the amount of information to be send through a communication channel (it is 1 bit in most QKD protocols with discrete variables). The second term (the a-posteriori term) is the conditional entropy of the Bob after measurement of the physical carrier (a photon or another light pulse) at the end of the communication channel. Finally, the third term corresponds to information leakage towards Eve as a result of her eavesdropping actions. Moving the excess information from side channels to one

of the two first terms, we reinterpret excess information of the eavesdropper such that this amount of information influences legitimate sides instead of the adversary. This transforms the equation for the secret key rate to the following:

$$R^{\Delta} = 1 - h(Q) - (h(Q) + \Delta h) = 1 - h(Q^{\Delta}) - h(Q) = 1 - \Delta h - 2h(Q). \quad (2)$$

Moving excess information to the a-priori term corresponds to Bob knowledge about Alice before measurement or, alternatively, to the randomness of Alice source; this interpretation constitutes the *a-priori loss method* of estimating QKD security. Contrary, moving excess information to the a-posteriori term corresponds to information gain about Alice photon state after Bob's measurement; this interpretation constitutes *the effective error method.*

The proposed two methods provide novel points of view on the effect of the source side channel on the communication process. The first point is the decrease of the randomness of the Alice source, and the other point is the reduced quality of Bobs measurement devices, leading to equivalent theoretic information relations between communication sides. It is interesting to compare these interpretations in application to a particular QKD protocol. To do so, we calculate secret key rates in the BB84 protocols with decoy states in two ways: using the effective error method

$$R_1^{\Delta} = Q_1\left(1 - h\left(e_1^{\Delta}\right)\right) - fQ_{\mu}h\left(E_{\mu}^{\Delta}\right), \quad (3)$$

and using the a-priori loss method

$$R_2^{\Delta} = Q_1\left(1 - \Delta h - h\left(e_1\right)\right) - fQ_{\mu}h\left(E_{\mu}\right). \quad (4)$$

To model the eavesdropping on the signal degree of freedom – the photon physical quantity, used to distribute a secret key bit – we use a phase-covariant cloning attack, which is the most powerful attack on the ideal BB84 protocol (without side channels and with single photons as a bit carrier) [6]. This operation then is followed by a collective attack on the signal and side channel system: Eve measures the state of composite system with a collective measurement, which gives her the Holevo value amount of information [7] about secret bits. The main purpose of this work is to compare these two methods and to define which one provides a tighter upper bound on the secret key rate for the BB84 decoy state protocol with a passive source side channel.

Results and Discussion

Fig. 1 shows secret key rates for two estimation approaches described above. We use standard parameters of QKD setups – optical fiber attenuation $\alpha = 0.2$, average photon number per pulse $\mu = 0.5$, optical error rate 1%, dark count probability $Y_0 = 10^{-5}$, and error correction efficiency $f = 1.1$.

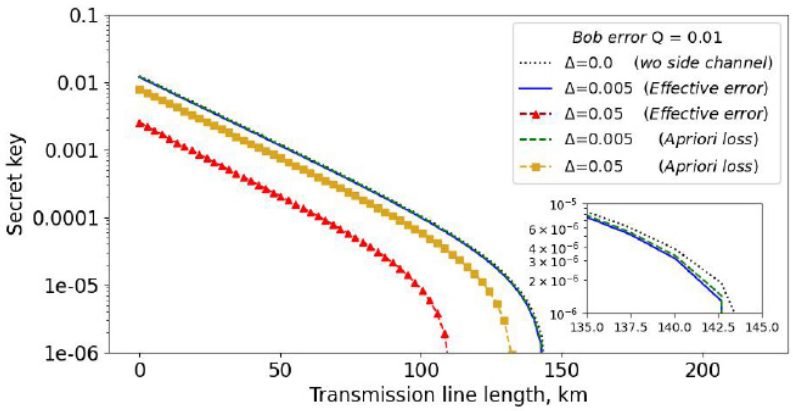

Fig. 1. Secret key rates, calculated with two methods, the effective error method and a-priori loss method, for different values of side channel leakage parameter Δ

From the figure we can see the difference between resulting secret key rates, calculated with two approaches. In particular, the effective error method provides tighter upper bound on the secret key generation rate than the a-priori loss method. This result illustrates imbalance in interpreting excess eavesdropper information as an information change of legitimate sides.

Conclusion

In this work we provided an extended analysis of the method to estimate QKD security with passive source side channels, proposed in [2]. We show that assigning the loss of excessive error to a-posteriori outcome of legitimate receiver, the basis of the effective error method, provides tighter estimate of the secret key upper bound than in the case of a-priori information loss. This finding allows us to definitely use the effective error method as a practical way to estimate security of QKD with passive side channels, compared to a-priori information loss interpretation. Development tools of estimating security in real-world QKD systems, which inevitably contain side channels, allow faster engagement of these systems into practice.

REFERENCES

1. **Scarani V., Kurtsiefer C.,** The black paper of quantum cryptography: real implementation problems, Rev. Mod. Phys. 1 (560) (2014) 27–32.

2. **Sych D.V., Duplinskiy A.V., Babukhin D.V.,** Practical security of quantum key distribution in the presence of side channels, J. Phys.: Conf. Ser. (1984) 012001.

3. **Gottesman D., Lo H.-K., Lütkenhaus N., Preskill J.,** Security of quantum key distribution with imperfect devices, Quant. Inf. Comput. 5 (2004) 325–360.

4. **Babukhin D., Kronberg D., Sych D.,** Explicit attacks on the Bennett-Brassard 1984 protocol with partially distinguishable photons, Phys. Rev. A 106, 042403 (2023).

5. **Babukhin D.V., Sych D.V.,** Joint eavesdropping on the BB84 decoy state protocol with an arbitrary passive light-source side channel, arXiv2211.13669.

6. **Bruß D., DiVincenzo D.P., Ekert A., Fuchs C.A., Macchiavello C., Smolin J.A.,** Optimal universal and state dependent quantum cloning, Phys. Rev. A 57, 2368 (1998).

7. **Holevo A.S.,** Bounds for the Quantity of Information Transmitted by a Quantum Communication Channel, Problems Inform. Transmission 9 (1973) 177–183.

THE AUTHORS

BABUKHIN Danila V.
dv.babukhin@gmail.com

SYCH Denis V.
denis.sych@gmail.com

Received 07.07.2023. Approved after reviewing 13.07.2023. Accepted 26.09.2023.