Unambiguous state discrimination and joint measurement attacks on passive side channel of the light source in BB84 decoy-state protocol

D Babukhin$^{1,3,4}$ and D Sych$^{2,3,4,5}$

$^1$QRate LLC, Moscow 121353, Russia
$^2$NTI Center for Quantum Communications, National University of Science and Technology MISiS, Leninsky prospekt 4, Moscow 119049, Russia
$^3$National University of Science and Technology MISiS, 119049, Moscow, Russia
$^4$Sirius University of Science and Technology, 1 Olympic Ave, 354340, Sochi, Russia
$^5$P.N. Lebedev Physical Institute, Russian Academy of Sciences, Moscow, 119991, Russia

Abstract. Quantum key distribution (QKD) has a promise of unconditionally secure communication between the remote sides. The real-world QKD implementations, however, have numerous loopholes, both of engineering and physical origin, and compromise the security promise. In this work, we investigate two attack strategies on the passive side channel of the light source along with the optimal cloning attack on the BB84 protocol with decoy-states. We calculate an upper bound of a secret key rate for these situations and show that the joint measurement attack on the signal and side channel degree of freedom is more effective to the adversary.

1. Introduction

Quantum communication is the most developed part of quantum technologies up to date. Quantum communication promises to create a secure sequence of bits between two parties (Alice and Bob) oblivious to the third party (Eve). It is possible if legitimate sides use single photons as carriers of secret bits. The quantum no-cloning theorem guarantees that one cannot copy a photon state without introducing disturbance. This change will result in errors in communication between legitimate parties, and thus eavesdropping will be revealed. When the QKD protocol is implemented in hardware, different loopholes and side channels arise in the protocol. These side channels allow the adversary to obtain more information about secret bits without alerting legitimate parties. This oblivious leakage makes it impossible to correct these errors during security amplification, and the promised security is compromised. For example, a sender-side can use several lasers as a source of photons for the protocol. Physical differences in lasers lead to differences in carrier photons. These discrepancies lead to additional distinguishability between photons, and thus, adversary can obtain more information about communication. Investigation of side channels arising from the difference between theory and real-world devices is a subject of practical security of QKD [1]. From a point when the security of theoretical BB84 protocol was established [2], many efforts were to incorporate different discrepancies between theoretical models and real-world devices [3-5].

Here we investigate two attack strategies, which the adversary can use to get additional information about the secret bit from physical differences of carrier photons. We estimate this information using
two-photon interference [1] for a phase-covariant optimal cloning attack on the decoy-state BB84 protocol. We provide an upper bound for the secret key rate for these cases and demonstrate, that it is more effective to make a joint measurement of both cloned signal and side channel states rather than make an unambiguous state measurement of the side channel followed by measurement of the cloned signal.

2. The individual unitary attack on the BB84 protocol
During the individual unitary attack, Eve brings a carrier photon into the unitary interaction with an ancillary quantum system to obtain two quantum systems with states which are optimal clones of the initial state. That means states of outgoing two systems have a close to unity fidelity with the initial system. This optimal cloning procedure is equivalent to the individual attack on the BB84 protocol [6]. If we consider photon states from X and Y bases, the following transform does the optimal cloning

\[ U|\Psi(\phi)\rangle_B|0\rangle_E = \frac{1}{\sqrt{2}} (|0\rangle_B|0\rangle_E + \cos \eta |1\rangle_B|0\rangle_E + \sin \eta |0\rangle_B|1\rangle_E) \] (1)

\[ |\Psi(\phi)\rangle_B = \frac{1}{\sqrt{2}} (|0\rangle_B + e^{-i\phi}|1\rangle_B) \] (2)

Here, B denotes the Hilbert space of Bob, E denotes the Hilbert space of Eve, \( \phi \) is a relative phase of quantum states from XY plane, and \( \eta \) is a control parameter of cloning. This operation creates two quantum states which have a high-fidelity overlap with the quantum state sent by Alice. It is instructive to see the extreme cases of this transform: for \( \eta = 0 \), this transform does nothing, and for \( \eta = \pi/2 \), it flips the state of Bob and the initial state of Eve.

3. Attack strategies on the passive side channel of the light source
As a model for photon distinguishability, we consider the augmentation of a side channel degree of freedom. Formally, we attached a side channel degree of freedom to the bases of the BB84 protocol:

\[ \rho_x = \frac{1}{2} (|0_x\rangle\langle 0_x| \otimes \rho^d_{x,0} + |1_x\rangle\langle 1_x| \otimes \rho^d_{x,1}) \] (3)

\[ \rho_y = \frac{1}{2} (|0_y\rangle\langle 0_y| \otimes \rho^d_{y,0} + |1_y\rangle\langle 1_y| \otimes \rho^d_{y,1}) \] (4)

where states \( \text{Tr}[\rho^d_{a,b} \rho^d_{a,b}^\dagger] = \delta_{aa} \delta_{bb} + (1 - \delta_{aa})(1 - \delta_{bb}) \) are nonorthogonal to each other in general case. We use this model to demonstrate two strategies of eavesdropping with the use of photon distinguishability.

3.1. Unambiguous discrimination of side channel states (USD)
A USD measurement is a type of optimal quantum measurement, which allows obtaining the full information about the state sent from an ensemble of possible states [7]. The trade-off is that this measurement can fail, and no information will be obtained about the measured state. For an ensemble of non-orthogonal and linearly independent states \( \{|\varphi_i\rangle, i = 1,2,3,4\} \), this measurement is formulated as follows:

\[ \sum M_k = I_n \] (5)

\[ \langle \varphi_i|M_k|\varphi_i\rangle = p_i \delta_{ik}, 1 \leq i,k \leq n \] (6)

where \( M_k \) are POVM operators, representing quantum measurement device and \( p_i \) are probabilities of states in the ensemble. The probability to fail measurement is defined as a probability to obtain an inconsistent result on a particular sent state, it is provided with a formula

\[ \langle \varphi_i|M_0|\varphi_i\rangle = 1 - p_i \] (7)

In this scenario of attack, Eve applies the USD measurement to the state of the side channel. If the measurement succeeds, Eve knows exactly what was the state of side channels. She waits until the basis exchange of legitimate sides and afterward knows exactly what was the state of the carrier.
photon on a corresponding position. However, if the measurement has failed, Eve attacks the signal photon state with the optimal cloning attack as in a usual scenario of the BB84 protocol eavesdropping. As a result, her information about the secret bit is

$$I_{AE} = P_{usd} + (1 - P_{usd})I_{AE}^{ind}$$  \hspace{1cm} (8)$$

where $I_{AE}^{ind}$ is the amount of information about the secret bit, which Eve obtains from a cloning attack on the signal photon state.

3.2. Joint measurement attack on side channel states

In this scenario of attack, Eve attacks a signal photon with an optical phase covariant cloner, thus obtaining a non-ideal copy of the signal photon state. Afterward, she jointly measures a copy of the signal photon with a side channel state with a minimum error measurement. After the cloning attack, Eve (after waiting for the basis exchange step) effectively has an ensemble, consisting of two states of the form:

$$|0_x\rangle\langle 0_x| \otimes \rho_{x,0}^d \text{ or } |1_x\rangle\langle 1_x| \otimes \rho_{x,1}^d$$  \hspace{1cm} (9)$$

To discriminate two states, Eve uses a Helstrom measurement. A probability to guess which state was sent from the ensemble of states $\rho_1$ and $\rho_2$ with minimal error is

$$P_{guess} = \frac{1}{2} \left( 1 + Tr \left[ \sqrt{ (\rho_1 - \rho_2)(\rho_1 - \rho_2)^T} \right] \right)$$  \hspace{1cm} (10)$$

4. Decoy state BB84

Although in theory the BB84 protocol is formulated for single photons, in a real experiment it is hard to incorporate a truly single-photon sources in a QKD setup. For QKD purposes, attenuated weak coherent pulses with randomized phases, which are easily generated with lasers, are usually used. These pulses have a form

$$\rho_x^\mu = \sum_{k=1}^{\infty} \frac{(\mu)^2}{k!} \left| k; x \right\rangle \left\langle k; x \right|,$$  \hspace{1cm} (11)$$

where $\mu$ is the intensity of the coherent signal and $x$ is a value of a secret bit. Signal states of this form have an incorporated vulnerability, which consists of two and more photon parts. This kind of state opens the door for another way of oblivious eavesdropping with a photon-number-splitting attack. Because the quantum phase of this state is random, Eve can make a non-demolishing photon number resolving the attack, and if there is more than one photon in the signal, she splits a single photon to herself. Because this photon has the same state, as other photons in the many-photon state, Eve has the same quantum state as Bob has at the end of the communication. After the basis exchange step, both Bob and Eve measure their photons in the proper basis and thus have the same value of a secret bit. Because there is no error in communication between Alice and Bob in this scenario, the QKD protocol is no longer secure.

The mentioned loophole is closed with the addition of decoy states to the conventional BB84 protocol [8,9,10]. Alice sometimes sends special phase-randomized weak coherent pulses with an intensity, different to informational signal pulses. Because Eve cannot discriminate between signals with different intensities, she applies the same attack sequence to every pulse in the channel. After the whole communication process, Alice and Bob reveal, which pulses were informational, and which pulses were decoy-states. They use decoy states statistics to estimate the single-photon component in the whole communication process, a component which Eve cannot attack without introducing disturbance. Thus, a security loophole of many-photon states from coherent pulses is closed.

Let us elaborate on the use of decoy states statistics. If Bob receives a signal with intensity $\mu$, a probability to have a click on the detector is

$$Q_\mu = \sum_{k=0}^{\infty} \frac{(-\mu)^2}{k!} \frac{1}{Y_k},$$  \hspace{1cm} (12)$$
where $Y_k$ is a k-photon yield:

$$Y_k = \sum \sum P_A(a)P_{AB}(b|A=a),$$

Using this statistics of counts, Bob can estimate the bit error rate

$$E_{\mu} = \frac{1}{Q_\mu} \sum e^{-\mu \frac{\mu^2}{k_1}} Y_k e_k,$$

These detection outcomes are further used to estimate the vacuum yield $Y_0$, the single-photon yield $Y_1$, and single-photon error rate $e_1$. These quantities are used to calculate the single-photon part of all communication process, which is a quantum-secure part. The secret key rate for this component is given by (see [11]):

$$R(e_1) = \frac{1}{2} \left( Q_1 I_{AB}(e_1) - f Q_\mu \max \left( I_{AE}(E_\mu), I_{BE}(E_\mu) \right) \right),$$

where $f$ is the efficiency of error correction and $e_1$ is a single-photon fraction error.

5. The Hong-Ou-Mandel visibility and side channel states

The Hong-Ou-Mandel (HOM) effect is a two photons interference effect when these photons are incident on a balanced beam splitter. When modes of these photons are perfectly matched (i.e., they have the same polarization, spectral and temporal distribution), they exit the beam splitter pairwise. But when the indistinguishability of these photons is not complete, they will sometimes exit different sides of the beam splitter. The degree of photons indistinguishability is the HOM interference visibility, which for phase randomized weak coherent pulses reads (see [1] for details)

$$V_{\rho_1,\rho_2} = \frac{1}{2} Tr[\rho_1 \rho_2]$$

6. Results and discussion

We have calculated secret key rates for the aforementioned attack strategies with different powers of informational leakage through a source side channel (which correspond to different values of the HOM visibility of the sources). We provide calculation results in figure 1. We used the following parameters for simulations: a postprocessing efficiency $f = 1.22$, a quantum channels attenuation values $\alpha = 0.2$ dB/km, efficiency of the Bob detector $\eta_{\text{Bob}} = 0.01$, background yield $Y_0 = 10^5$, background error rate $e_0$ is 0.5 and mean photon number in a pulse $\mu = 0.5$. The critical length of the transmission line is provided with the formula

$$L(e_1) = \frac{10}{\alpha} \log_{10} \left( \frac{Y_0(e_0-e_1)}{\eta_{\text{Bob}}(e_1-e_{\text{det}})} \right),$$

where $e_1$ is the error in the single-photon fraction and $e_{\text{det}}$ is the detection error.

From figure 1 we conclude, that the joint measurement of the signal state after phase-covariant cloner attack and the side channel state allows Eve to gain more information about the secret bits, than using the USD attack on the side channel alone and then proceeding with the attack on the signal degree of freedom if the USD attack fails. We also prove that using the physical distinguishability of photons does not give Eve much additional information about the secret key. For HOM visibility values in the range from 0.4 to 0.5 (which correspond to the state-of-the-art values of contemporary photon sources), we see only a slight decrease in the security of the protocol. We can conclude that physical differences between signal photons, which lead to additional distinguishability at the level of the state-of-the-art photon sources, do not lead to a severe drop in the BB84 protocol secrecy under the considered attacks.
Figure 1. Dependence of the secret key rate $R$ on the length of the transmission channel $L$ for several values of the two-photon interference visibility $V$. Different curves correspond to the USD measurement of side channel state (circles) and the joint measurement of cloned signal and side channel states (triangles).

Acknowledgements
Denis Sych acknowledges funding by RFBR, Sirius University of Science and Technology, JSC Russian Railways and Educational Fund “Talent and success”, project number 20-32-51004. Danila Babukhin acknowledges funding by FASIE.

References
[1] Duplinskiy A and Sych D V 2021 Phys. Rev. A 104 012601
[2] Shor P W and Preskill J 2000 Phys. Rev. Lett. 85 441-444
[3] Gottesman D, Lo H-K, Lutkenhaus N and Preskill J 2004 Quant. Inf. Comput. 5 325-360
[4] Koashi M and Preskill J 2003 Phys. Rev. Lett. 90 057902
[5] Koashi M 2009 New J. Phys. 11 045018
[6] Bruß D, Cinchetti M, D’Ariano G M and Macchiavello C 2000 Phys. Rev. A 62 012302
[7] Eldar Y C 2003 IEEE Trans. Inf Theor. 49 446-456
[8] Hwang W-Y 2003 Phys. Rev. Lett. 91 057901
[9] Lo H-K, Ma X and Chen K 2005 Phys. Rev. Lett. 94 230504
[10] Lo H-K 2004 Proc. IEEE ISIT (IEEE Press) p 137
[11] Ma X, Qi B, Zhao Y and Lo H-K 2005 Phys. Rev. A 72 012326