Explicit attacks on passive side channels of the light source in the BB84 decoy state protocol

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

1 QRate LLC, Novaya av. 100, Moscow 121353, Russia
2 NTI Center for Quantum Communications, National University of Science and Technology MISiS, Leninsky prospekt 4, Moscow 119049, Russia
3 Sirius University of Science and Technology, 1 Olympic Ave, 354340, Sochi, Russia
4 P.N.Lebedev Physical Institute, Russian Academy of Sciences, Moscow, 119991, Russia
E-mail: dv.babukhin@gmail.com

Abstract. Various imperfections of the hardware in quantum key distribution (QKD) lead to discrepancies between the theory and real-world devices. An eavesdropper can use these discrepancies to compromise the QKD security, thus legitimate sides need to estimate the influence of imperfections to prevent the loss of security. Here we investigate explicit eavesdropping attacks on passive side channels of the light source for a BB84 decoy states QKD protocol. We consider an optimal phase-covariant cloning attack, followed by unambiguous state discrimination and a joint measurement. Our calculations provide a hint that for state-of-the-art light sources the inherent presence of passive side channels still allows the protocol to be secure, albeit with the reduced secret key rates.

1. Introduction
Quantum cryptography promises an unconditionally secure distribution of a secret key between two parties due to the no-cloning theorem. However, experimental QKD realizations lead to various loopholes and side channels, and, consequently, to additional information leakage to an eavesdropper. This leakage does not increase errors on receiving side, so an intervention into the QKD remains unnoticed by legitimate parties. As a result, an eavesdropper has more information about distributed bits than the protocol allows him, and the resulting key is no longer secure. An example of such a side channel is a light source that generates signal photons with slightly varying spatial, spectral, and temporal modes. These physical differences allow the adversary to distinguish photons more effectively than just attacking a quantum state of the signal photon. Possible ways of proper side channels account were an object of many investigations in recent years [1-4].

We investigate explicit eavesdropping attacks on passive side channels of the light source. The optimal phase-covariant cloning attack on the BB84 QKD protocol with decoy states is considered along with explicit attacks on the passive side channel of the light source - the unambiguous state discrimination and the collective measurement attacks. We compare our results with side-channel-free theoretical secret key rates of this protocol. We use a Hong-Ou-Mandel visibility as an experimentally accessible value to apply our estimates to characterization of state-of-the-art light sources. Our calculations provide a hint that for state-of-the-art light
sources the inherent presence of passive side channels still allows the protocol to be secure, but with reduced secret key rates.

2. Optimal phase-covariant cloning attack

The optimal phase-covariant cloning attack is a unitary operator of a special form, which brings a signal state and an ancillary state to a specific entangled state. This entangled state has partial states with high fidelity for the initial state of the incoming photon. The optimal phase-covariant cloner implements an individual unitary attack on the BB84 protocol [5]. For signal states of the BB84 from the XY plane of the Bloch sphere, the action of the cloning unitary is

\[ U|\psi(\phi)\rangle_B|0\rangle_E = \frac{1}{\sqrt{2}}(|0\rangle_B|0\rangle_E + \cos \eta e^{i\phi}|1\rangle_B|0\rangle_E + \sin \eta e^{i\phi}|0\rangle_B|1\rangle_E), \]

where indices B and E correspond to state spaces of Bob and Eve, \( \phi \) is a rotation angle around the Z-axis and \( \eta \) is a cloning parameter. The final state doesn’t depend on the phase parameter, which is a property of phase covariance. The cloning unitary distributes information about the state, sent by Alice, between Bob and Eve states.

3. Explicit attacks on the side channel

We added an additional degree of freedom to states of two bases of the BB84 protocol:

\[ \rho_x = \frac{1}{2}|0_x\rangle\langle 0_x| \otimes \rho_{x,0}^\Delta + \frac{1}{2}|1_x\rangle\langle 1_x| \otimes \rho_{x,1}^\Delta \]

\[ \rho_y = \frac{1}{2}|0_y\rangle\langle 0_y| \otimes \rho_{y,0}^\Delta + \frac{1}{2}|1_y\rangle\langle 1_y| \otimes \rho_{y,1}^\Delta \]

where augmented states \( \rho_{basis,bit}^\Delta \) have fixed scalar products among each other. With use of this approach, we modeled two types of attack on the passive side channel.

3.1. Unambiguous state discrimination (USD) of side channels states

Eve applies an unambiguous side state discrimination measurement to side-channel degree of freedom. This measurement either gives her a certain quantum state of quantum system or returns a maximally mixed state and gives no information about the side channel state [6]. The POVM for this kind of measurement can be constructed for an ensemble of non-orthogonal and linearly independent states \( |\phi_i\rangle \), \( i = 1, 2, 3, 4 \) in the following way:

\[ \sum_k M_k = I \]

\[ \langle \phi_i|M_k|\phi_i \rangle = p_i \delta_{ik}, 1 \leq i, k \leq n \]

where \( M_k \) are POVM operators and \( p_i \) are probabilities of measuring one of ensemble states. There is a POVM for inconsistent result, when no information about measured state is revealed:

\[ \langle \phi_i|M_0|\phi_i \rangle = 1 - p_i \]

If the USD measurement of the side channel state is successful, Eve obtains a secret bit without interacting with the signal state. If measurement gives an inconsistent result, she proceeds with the optimal phase-covariant cloning of the signal photon state. Her information with Alice reads

\[ I_{AE} = P_{usd} + (1 - P_{usd}) * I_{ind}^{ae} \]

where \( I_{ind}^{ae} \) is a mutual information between Alice and Eve after the phase-covariant cloning.
3.2. Joint measurement of side channel states and signal states

Eve makes a joint measurement of signal and side channel states after the phase-covariant cloning. In particular, after attack on carrier photons and basis exchange between Alice and Bob, Eve has one of two possible states in her quantum memory:

\[ |0_x⟩⟨0_x| \otimes \rho_{x,0}^\Delta \text{ or } |1_x⟩⟨1_x| \otimes \rho_{x,1}^\Delta \] (9)

Eve optimally discriminates between these states with a minimum error measurement. A probability to successfully discriminate the two states \( \rho_1 \) and \( \rho_2 \) is

\[ P_{\text{opt}} = \frac{1}{2} \left( 1 + \text{Tr} \left[ \sqrt{ (\rho_1 - \rho_2)(\rho_1 - \rho_2)^\dagger} \right] \right) \] (10)

4. Decoy state BB84 protocol

In practice, signal photons are generated by lasers with an unlocked initial phase, which leads to the randomization of the initial phases of signal photons. Furthermore, laser sources also generate many-photon states along with single-photon states. The resulting carrier quantum state has the following form

\[ \rho_x^\mu = \sum_{k=0}^{\infty} e^{-\mu} \frac{\mu^k}{k!} |k; x⟩⟨k; x|, \] (11)

where \( \mu \) is the mean photon number of the coherent state and \( x \) is the encoded secret bit. To decrease the influence of many-photon states on the communication the mean photon number is usually taken low (less than one photon per pulse), and the resulting state is called a phase-randomized weak coherent pulse (PRWCP).

Even though many-photon parts are attenuated, they continue to be a vulnerability in the BB84 protocol. These parts contain photons of the same single-photon states and thus open Eve a possibility to hold one photon with the same quantum state as photons sent towards Bob. In the end, Eve has a clone of the Bob state without introducing disturbance, and the security of the protocol is compromised.

This vulnerability can be closed with a so-called decoy-state method [7,8,9]. This method is based on an assumption, that Eve applies the same attack action to signals with different intensities. This assumption allows Alice and Bob to use photon signals with different intensities to estimate the single-photon component weight, which composes the secret fraction of the distributed bits. They can further proceed with security amplification, taking into account only the secret fraction of their bits.

In particular, receiving \( k \)-photon states, where \( k \) has values from 0 to infinity, the full probability of having a detection count on Bob side for a pulse with intensity is

\[ Q_\mu = \sum_{k=0}^{\infty} e^{-\mu} \frac{\mu^k}{k!} Y_k, \] (12)

where \( Y_k \) is a \( k \)-photon yield:

\[ Y_k = \sum_a \sum_{b=0}^1 P_A(a) P_{A|B}(b|A = a), \] (13)

where \( A \) is a value of Alice’s random bit, and \( B \) is a value of Bob’s bit, obtained from measurement. The probability of bit error on the Bob side is

\[ E_\mu = \frac{1}{Q_\mu} \sum_{k=0}^{\infty} e^{-\mu} \frac{\mu^k}{k!} Y_k e_k, \] (14)
where $k = 0$ corresponds to dark counts of photodetectors. Using these quantities allows Bob to calculate a vacuum yield $Y_0$, a single-photon yield $Y_1$, and a single-photon error rate $e_1$. These quantities are further used to estimate the secret fraction of distributed bits. The secret key rate then is calculated with the formula (see [10] for details):

$$R(e_1) = \frac{1}{2}(Q_1 I_{AB}(e_1) - fQ_{\mu} \max(I_{AE}(e_1), I_{BE}(e_1))),$$  \hspace{1cm} (15)

where $f$ is a post-processing efficiency factor and $e_1$ is a bit error in single-photon component outcomes.

5. Hong-Ou-Mandel interference

When two photons are incident on the two sides of a balanced beam splitter, their exit this beam splitter depending on their quantum states. If the two photons are completely indistinguishable, their exit the beam splitter only pairwise. This phenomenon is called the Hong-Ou-Mandel (HOM) effect. Breaking the indistinguishability of photon states leads to exiting the beam splitter from different sides, and thus to coincidences on the detectors which are measuring beam splitter exits. Experimentally, this effect is usually characterized by the visibility of the interference (the HOM visibility). For PRWCP this visibility can be calculated in the following way (see [1] for details)

$$V_{\rho_1,\rho_2} = \frac{1}{2} \text{Tr}[\rho_1 \rho_2]$$  \hspace{1cm} (16)

where $\rho_1$ and $\rho_2$ are states of the incoming photons.

6. Results and conclusion

We calculated secret key rates for the BB84 protocol with two decoy states for the optimal phase-covariant cloning attack and two strategies of attacking the side-channel of the light source, described above. In our calculations we used typical parameters of the QKD setup: error correction coefficient $f = 1.22$, fiber attenuation $\alpha = 0.2$ dB/km, Bob detector efficiency $\eta_{Bob} = 0.01$, background yield $Y_0 = 10^5$, background error rate $e_0$ is 0.5 and the mean photon number in a pulse $\mu = 0.5$. A critical length of the transmission line is provided with a formula

$$L(e_1) = -\frac{10}{\alpha} \log_{10}\left[\frac{Y_0(e_0 - e_1)}{\eta_{Bob}(e_1 - e_{det})}\right]$$  \hspace{1cm} (17)

where $e_1$ is a single-photon component error rate and $e_{det}$ is a detector error rate.

We can see from Figure 1, that using different strategies of attacking the side channel degree of freedom does not lead to a significant decrease in the secret key generation rate. The state-of-the-art light sources have corresponding HOM visibilities in the range between 0.4 and 0.5, which we associate with a passive side channel. Thus, the presence of a physical mismatch between signal photon properties of the contemporary light sources does not completely compromise the security of the BB84 protocol with decoy states, provided that Eve uses the above-described attack strategies.

We conclude, that lower and upper bounds on the key rate leave a significant gap between the two. While the lower bound is very pessimistic in terms of the tolerable visibility values [1], the upper bounds given for the previously analyzed intercept-resend attack [11], and for presented here USD and joint measurement attacks allow visibility values to be much lower.

As a counter-measure against these attacks, we expect that protocols with complex alphabets [12-16] might be more resistant to side-channels due to the complexity of multiple state discrimination. Another possible solution is to use coherent states without phase randomization [17-20], which allows for higher information gain and a more accurate second-order visibility measurement.
Figure 1. Secret key rate $R$ as a function of fiber-optic communication distance $L$ for different values of Hong-Ou-Mandel interference visibility $V$, under the individual unitary attack on the BB84 decoy-state protocol for two attack strategies on the side channel degree of freedom (USD attack and joint measurement attack). We assume the standard single-mode optical fiber loss of 0.2 dB/km.

Acknowledgements
Denis Sych acknowledges support from Russian Foundation for Basic Research grant 20-32-51004, and Danila Babukhin acknowledges support from FASIE.

References
[1] Duplinskiy A and Sych D V Phys. Rev. A 104, 012601 (2021)
[2] Gottesman D, Lo H-K, Lutkenhaus N and Preskill J 2004 Quant. Inf. Comput. 5 325-60
[3] Koashi M and Preskill J 2003 Phys. Rev. Lett. 90 057902
[4] Koashi M 2009 New J. Phys. 11 045018
[5] D. Bruß, M. Cinchetti, G. Mauro D’Ariano, and C. Macchiavello 2000 Phys. Rev. A 62, 012302
[6] Eldar Y C, 2003 IEEE Trans. Inf Theor. 49 446-56
[7] Hwang W-Y 2003 Phys. Rev. Lett. 91 057901
[8] Lo H-K, Ma X and Chen K 2005 Phys. Rev. Lett. 94 230504
[9] Lo H-K 2004 Proc. IEEE ISIT (IEEE Press) p 137
[10] Ma X, Qi B, Zhao Y and Lo H-K 2005 Phys. Rev. A 72 012326
[11] Babukhin D and Sych D 2020 Journal of Physics: Conference Series 1695 012119
[12] Sych D V, Grishanin B A and Zadkov V N 2004 Phys. Rev. A 7 052331
[13] Sych D, Grishanin B and Zadkov V 2004 Laser Physics 14 1314–1321
[14] Sych D V, Grishanin B A and Zadkov V N 2005 Quantum Electronics 35 80–84
[15] Sych D, Averchenko V and Leuchs G 2017 Phys. Rev. A 96 053847
[16] Averchenko V, Sych D, Marquardt C and Leuchs G 2020 Phys. Rev. A 101 013808
[17] Sych D and Leuchs G 2010 New J. of Phys. 12 053019
[18] Sych D and Leuchs G 2010 Optics and Spectroscopy 108 326–330
[19] Sych D and Leuchs G 2016 Phys. Rev. Lett. 117 200501
[20] Shcherbatenko M L, Elezov M S, Goltsman G N and Sych D V 2020 Phys. Rev. A 101 032306