Practical security of quantum key distribution in the presence of side channels

D Sych\textsuperscript{1,2,3}, A Duplinskiy\textsuperscript{2} and D Babukhin\textsuperscript{2,3}

\textsuperscript{1} P.N.Lebedev Physical Institute, Russian Academy of Sciences, Moscow, 119991, Russia
\textsuperscript{2} NTI Center for Quantum Communications, National University of Science and Technology MISiS, Moscow, 119049, Russia
\textsuperscript{3} Sirius University of Science and Technology, 1 Olympic Ave, 354340, Sochi, Russia

E-mail: denis.sych@gmail.com

Abstract. Security of quantum key distribution (QKD) is based on fundamental laws of quantum physics. However, the security of QKD implementations is at risk due to various deviations, called side channels, of the real device from the theoretical model. In this work, we discuss the practical ways to avoid the threat of side channels in QKD. We use interference visibility measurement for estimation of distinguishability of quantum signals, and show how to integrate it into the security proof. Our results paves the way towards the development of novel robust QKD schemes.

1. Introduction
Quantum key distribution provides a way for communication with the security based on fundamental laws of quantum physics. The traditional security analysis of QKD takes into account various distortions of quantum signals, (e.g. attenuation, noise, errors, etc) as a signature of eavesdropping. However, the real-world QKD implementations can be attacked such that the quantum signal has no visible distortions, but the eavesdropper obtains a perfect copy of the key. Such quantum hacking exploits various deviations of the real QKD device from its idealized QKD model, and compromises the claim of security.

There are several countermeasures developed to date to prevent quantum hacking. For example, measurement-device-independent QKD closes most of the receiver loopholes. However, the transmitter part is still at risk. The basic idea of the light source side-channel attack is to exploit potential imperfections of the signal preparation part, for example, to measure differences in spectral or temporal properties of different quantum signals instead of trying to infer the operational degree of freedom.

In this work we discuss the practical ways to avoid the threat of such side channels in QKD. We use interference as the main method for estimating indistinguishability of different signals, and limit the unknown (but potentially existing) side channels by connecting the interference visibility with the QKD security. We consider second-order interference (interference of amplitudes) and fourth-order interference (interference of intensities, or Hong-Ou-Mandel interference), and show how to use these effects in the context of estimation of potential side channels in QKD. We explicitly consider discrete variable QKD protocols based on single photons, as well as modern continuous variable QKD protocols based on coherent states, and
show how to upgrade them to guarantee their practical security. Our security considerations allow to establish the upper and lower bounds for the secure key rate even when the side channels are unknown for legitimate sides.

2. Second-order interference

The second-order interference refers to the intensity measurement $I$ for the classical signals, or the measurement of number of photons $N$ for quantum signals (see Fig. 1 left). Depending on the relative phase $\varphi$ between the incoming pulses $x_1$ and $x_2 e^{i\varphi}$, we get $I = x_1^2 + x_2^2 + 2V x_1 x_2 \cos \varphi$, which results in interference fringes (shown in Fig. 1 right). To characterise identity of interfering pulses, the visibility $V = (I_{max} - I_{min})/(I_{max} + I_{min})$ is commonly used. A simple relation between the visibility $V$ and distinguishability $D$ can be obtained:

$$V + D \leq 1.$$  \hspace{1cm} (1)

If the pulses are absolutely identical to each other, then $D = 0$ and visibility can reach the maximum value $V = 1$, while if the pulses are perfectly distinguishable ($D = 1$), then visibility has the minimum value $V = 0$. Thus measurement of $V$ provides an upper bound on distinguishability of pulses ($D \leq 1 - V$), which can be directly integrated into the security proof.

![Figure 1](image_url)

**Figure 1.** Left: conceptual scheme for measuring the second-order interference visibility. Two pulses are matched on a beam splitter, and the result is measured with a photon detector (either SPD 1 or SPD 2). Right: photon number (counts) as a function of time delay between the pulses demonstrates interference fringes.

This type of visibility measurement can be used to verify indistinguishability of pure coherent states, and can be applied to the QKD protocols that utilise them \cite{1,2}. The photon counting is not required, since the same result can be obtained with strong classical fields and classical photodetectors. An alternative way to measure indistinguishability of pure coherent states is to perform homodyne measurements \cite{3,4} or estimate their modal fidelity \cite{5,6}.

3. Fourth-order interference

The fourth-order interference is a purely quantum effect which refers to the measurement of photon coincidences. Similarly to the second-order interference measurement, two pulses are matched on a beam splitter. Two photodetectors SPD 1 and SPD 2 measure the number of photons, and the number of coincidences $N$ is calculated (see Fig. 2 left). When the pulses are in a pure single photon state, the perfect modal overlap between them leads to the Hong-Ou-Mandel effect, i.e. disappearance of coincidences of photons on two detectors ($N = 0$). To characterise quality of fourth-order interference, visibility $V = (N_{max} - N_{min})/(N_{max} + N_{min})$...
is used. Two identical photons demonstrate “bunching”, and leave the beam splitter in pairs, which results in a pair of photon counts on one of the detectors, providing maximum visibility value $V = 1$. The measured number of coincidences demonstrates a dip that corresponds to the case of the best modal overlap (see Fig. 2 right). The similar effect takes place also for the phase-randomized weak coherent pulses. In contrast to the single-photon pulses, the maximum value of fourth-order interference visibility in this case is $V = 0.5$.

Figure 2. Left: conceptual scheme for measuring the fourth-order interference visibility. Right: photon detection coincidence counts as a function of time delay between the pulses.

This type of visibility measurement can be used to verify indistinguishability of single photon states and phase-randomised weak coherent states, and can be applied to the QKD protocols that utilise them [6–12]. Single photon counting is an essential ingredient in this case, which can be also extended for the multidimensional case [13,14].

4. Lower and upper bounds on the secret key rate
The measurement of interference visibility provides a convenient tool for estimation of states distinguishability without accessing different degrees of freedom. It gives an integral figure of merit, which takes the overall difference between the states. This difference can be exploited by an eavesdropper as a passive side channel attack on the light source. A crucial prerequisite for QKD—non-orthogonality of quantum states used for quantum communication, can fail after this attack [15, 16]. Clearly, visibility measurement implies matching of the operational degrees of freedom of quantum signals (e.g. polarization), thus the corresponding transformations should be applied during the entire QKD session (e.g. an additional combination of beam splitters and waveplates [17]).

The lower bound on the secret key rate can be established via the security analysis based on bases imbalance estimation [17]. As a result, the key rate significantly drops even at the very high visibility value $V = 0.499$, and almost vanishes at the moderate visibility value $V = 0.45$. The upper bound on the secret key rate can be established via the security analysis based on explicit eavesdropping attacks that take into account passive light source side channels. The easiest attack of this kind is the intercept-resend attack [18]. As a result, the key rate is almost unaffected even at the visibility value $V = 0.2$.

5. Results and discussion
As we can see, there is a huge gap between the lower and upper bounds on the key rate, thus the security of the currently operating QKD devices is under question. The typical measurable interference contrast of fiber-based optical schemes is around 20dB to 30dB (corresponds to the visibility values around 0.49 to 0.499), which results in the several times decrease of the secure communication distance, compared to the simplified security analysis ignoring the side channels.
The straightforward direction to resolve this issue is to design optical schemes which have higher interference contrast. Integrated optics offers much better contrast compared to the fiber optics, thus it will be a useful feature of the future chip-based optical devices. Another possible solution is to make tighter estimations of the upper and lower bounds. The upper bound is given by the explicit eavesdropping attacks, thus the design and analysis of the novel attacks is a very promising direction. The lower bounds can also be tightened, since the original security considerations were very optimistic for the eavesdropper.

A counter-measure against passive light source side channel attack can be connected with the development of novel protocols. For example, the use of more quantum states in the communication alphabet [7–9] makes state discrimination more difficult, which lowers Eve’s information. The use of single-mode QKD protocols, such as phase-shift keying of coherent states [1, 2], might also be profitable for this purpose. Eventually, the extreme simplification of the protocol to just two letters can also be a possible solution [19–23].

Acknowledgements
The work is supported by Russian Foundation for Basic Research grant 20-32-51004.

References
[1] Sych D and Leuchs G 2010 New Journal of Physics 12 053019
[2] Sych D and Leuchs G 2010 Optics and Spectroscopy 108 326–330
[3] Sych D, Řeháček J, Hradil Z, Leuchs G and Sánchez-Soto L L 2012 Phys. Rev. A 86 052123
[4] Leuchs G, Dong R and Sych D 2009 New J. Phys. 11 113040
[5] Sych D 2016 Journal of Russian Laser Research 37 556–561
[6] Averchenko V, Reiß D A, Sych D and Leuchs G 2020 Physica Scripta 95 034012
[7] Sych D V, Grishanin B A and Zadkov V N 2004 Phys. Rev. A 70 052331
[8] Sych D, Grishanin B and Zadkov V 2004 Laser Physics 14 1314–1321
[9] Sych D V, Grishanin B A and Zadkov V N 2005 Quantum Electronics 35 80–84
[10] Sych D, Averchenko V and Leuchs G 2017 Phys. Rev. A 96 053847
[11] Averchenko V, Sych D, Schunk G, Vogl U, Marquardt C and Leuchs G 2017 Phys. Rev. A 96 043822
[12] Averchenko V, Sych D, Marquardt C and Leuchs G 2020 Phys. Rev. A 101 013808
[13] Sych D and Leuchs G 2009 New J. Phys. 11 013006
[14] Shcherbatenko M, Elezov M, Manova N, Sedykh K, Korneev A, Korneeva Y, Dryazgov M, Simonov N, Feimov A, Goltsman G and Sych D 2021 Applied Physics Letters 118 181103
[15] Sych D V, Grishanin B A and Zadkov V N 2006 Laser Physics Letters 3 102–105
[16] Sych D and Leuchs G 2015 Foundations of physics 45 1613–1619
[17] Duplinskiy A and Sych D 2019 ArXiv:1908.04703
[18] Babukhin D and Sych D 2020 J. Phys.: Conf. Series 1695 012119
[19] Sych D and Leuchs G 2016 Phys. Rev. Lett. 117(20) 200501
[20] Shcherbatenko M, Elezov M, Sych D and Goltsman G N 2020 J. Phys.: Conf. Series 1695 012140
[21] Elezov M, Shcherbatenko M, Sych D and Goltsman G 2018 J. Phys.: Conf. Series 1124 051014
[22] Elezov M, Shcherbatenko M, Sych D and Goltsman G 2019 EPJ Web of Conferences 220 03011
[23] Shcherbatenko M L, Elezov M S, Goltsman G N and Sych D V 2020 Phys. Rev. A 101 032306