Research Article | Vol. 0, No. 0 / 00 00 0000 / Optics Express 1

Optics EXPRESS

Optical-pumping attack on a quantum key distribution laser source

MAXIM FADEEV,[1,2,*] ANASTASIYA PONOSOVA,[1,3] QINGQUAN PENG,[4] ANQI HUANG,[4] ROMAN SHAKHOVOY,[3,5] AND VADIM MAKAROV[1,6,3]

[1]*Russian Quantum Center, Skolkovo, Moscow 121205, Russia*
[2]*ITMO University, St. Petersburg 197101, Russia*
[3]*NTI Center for Quantum Communications, National University of Science and Technology MISIS, Moscow 119049, Russia*
[4]*College of Computer Science and Technology, National University of Defense Technology, Changsha 410073, China*
[5]*QRate, Moscow 143026, Russia*
[6]*Vigo Quantum Communication Center, University of Vigo, Vigo E- 36310, Spain*
[*]*mfadeev2022@gmail.com*

Abstract: We report a new type of vulnerability based on a physical principle that has not been previously exploited in quantum hacking—optical pumping of a laser in practical implementations of quantum key distribution (QKD) systems. We show that it is possible to increase the pulse energy of a source laser diode not only by injection-locking it with external light near its emission wavelength of 1550 nm, but also by optically pumping it at a much shorter wavelength. We experimentally demonstrate a 10% increase in pulse energy when exposing the laser diode to continuous-wave (cw) laser light at 1310 nm with a power of 1.6 mW via its fiber pigtail. This effect may allow an eavesdropper to steal the secret key. A possible countermeasure is to install broadband optical filters and isolators at the source output and to characterize them during security certification.

1. Introduction

Quantum key distribution (QKD) is a technology to generate a true random secret key by remote users using single photons [1,2]. The impossibility of compromising QKD protocols via direct measurement of single photons and independence of its security on computation algorithms make QKD an attractive cryptographic tool, especially with the rise of computational technologies. However, attempts at cryptanalysis of practical QKD implementations reveal many imperfections in their hardware implementations, such as bandwidth limitations of modulators [3], intensity correlation [4], shot noise measurement [5] or imperfections in source of quantum states [6]. Active quantum-hacking strategies have been proposed that create vulnerabilities in a "healthy" system imperceptible for its legitimate users [7–11]. To meet hard requirements on cryptographic resistance, practical QKD implementations are studied, and countermeasures to ensure physical security of the system hardware are developed and improved.

One of the imperfect devices in practical QKD systems is a photon source. Today, strongly attenuated laser pulses from semiconductor laser diodes (LDs) are used instead of true single-photon sources. In several studies, vulnerabilities in QKD are created by seeding Alice's LD by Eve's light injected through the quantum channel [12–14]. The attackers use laser light at about 1550 nm, which is near the LD operating wavelength. Injected power in the range of 100–160 nW can be sufficient to control the intensity of Alice's pulses [12,13]. Power as low as 1 nW might be enough to partially control the phase of Alice's pulses [14].

#562406 https://doi.org/10.1364/OE.562406
Journal © 0000 Received 24 Mar 2025; revised 16 Sep 2025; accepted 19 Sep 2025; published 00 00 0000

Optics EXPRESS

In this paper, we investigate the effects of optical pumping [15–17] of the QKD source of coherent radiation by 1310-nm illumination from the attacker Eve. This wavelength is a particular case of a broad wavelength band that is absorbed by the InGaAsP crystal within the laser [18]. This absorption creates an additional inversion population, resulting in an increase in output power. Appendix A describes the underlying physical process of the optical-pumping attack and provides a simple theoretical model of it. Here, we select a wavelength of 1310 nm due to its prevalence and accessibility, which consequently increases the potential risks of the attack. We demonstrate that QKD source based on a 1550-nm gain-switched laser diode is vulnerable to an optical-pumping attack, which results in an increase the energy of pulses emitted by Alice and might compromise the security of the key.

Our study indicates that the sufficient attenuation of Eve's light entirely mitigates the optical-pumping attack. However, QKD systems may be vulnerable to it due to the spectral selectivity of their passive countermeasures. The analysis of an industrial QKD system [11] reveals that active-state-preparation Alice modules may already be immune to this attack. Conversely, passive state-preparation QKD systems without modulators [19–22] are at greater risk due to the weaker requirements for passive countermeasures. But here we demonstrated the attack in principle at a single wavelength, while an adversary could exploit the entire absorption spectrum of the laser diode material. Effectiveness of the attack at different wavelengths will depend significantly on the practical implementation of a QKD system, including its LD architecture. Thus, comprehensive testing and evaluation are essential to certify QKD systems against this novel attack across the entire LD absorption band.

2. Experimental setup

Our experimental setup (Fig. 1) simulates a hacking scenario when Eve injects light into QKD source at a wavelength significantly shorter than the QKD operating one. A 1550-nm laser diode (LD1550; Agilecom WSLS-934010C4124-82) mimics Alice. However, contrary to the usual industry practice, it lacks a built-in isolator in order to demonstrate effects using low-power attacker's source (otherwise the isolator would add about 10 dB attenuation at 1310 nm). We conduct measurements of QKD source characteristics in both cw and pulsed regimes. In cw regime, LD1550 is powered only by a laboratory power supply (Keysight E3648A). For operating in a gain-switching pulsed mode [23], the bias current provided by the power supply is 3 mA, and pulses from the pulse generator (Highland Technology P400) are applied at 10 MHz repetition rate. In this regime, LD1550 produces 700-ps-wide optical pulses and has an average power of 14±0.1 μW.

As an attacker, we use a 1310-nm laser diode (LD1310; Nolatech FPL-FBG-1310-14BF) in cw regime. Its emission is injected into LD1550 via a fiber-optic circulator. The output power is controlled with a variable optical attenuator (VOA; OZ Optics BB-100) in a range from 23 nW to 1.6 mW at port 2 of the optical circulator OC. This power is limited by the available maximum power of LD1310. A polarisation controller PC is adjusted to maximise Eve's power at port 2 of OC.

We investigate several characteristics of LD1550 under optical pumping by LD1310: its light–current characteristic and differential quantum efficiency in cw mode, pulse area and shape, and average power in the pulsed regime. The average optical power is measured using an optical power meter (Thorlabs PM400 with a photodiode sensor S154C). The backreflected light at 1310 nm makes a contribution to 1550 nm average power measurements at port 3 of OC. We correct for this by measuring the reflected power with LD1550 switched off and subtracting it from the total measured power in each experiment. This correction is stable and is of the same order of magnitude or less than the effects observed. Pulse shape is recorded by a p-i-n photodiode (Laserscom PDI35-10G, 10 GHz bandwidth) connected to an oscilloscope (LeCroy 735Zi, 3.5 GHz bandwidth).

Optics EXPRESS

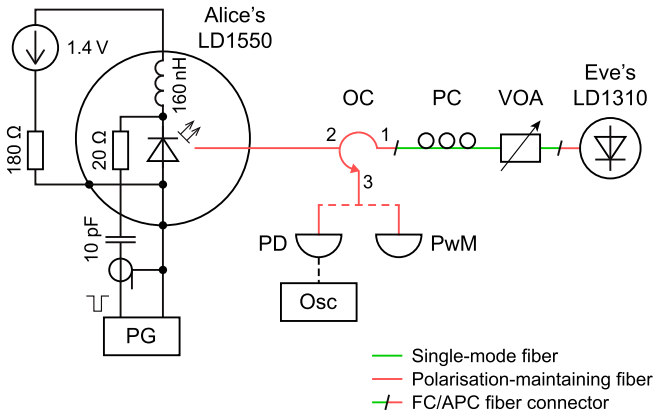

Fig. 1. Scheme of experiment. LD, laser diode; PG, pulse generator; OC, optical circulator; PD, photodiode; Osc, oscilloscope; PwM, power meter; PC, polarisation controller; VOA, variable optical attenuator. External electrical connections of LD1550 for pulsed operation are shown. Port 3 of OC is interchangeably connected to either PD or PwM.

First, all the characteristics of LD1550 are measured before exposure. Then, they are characterised under exposure to a constant power level of LD1310 emission. In the experiments conducted on the cw 1550-nm LD, we gradually reduce Eve's injected power, beginning from its maximum value. We terminate the experiment when we observe several instances of unchanged characteristics in the 1550-nm LD operation under exposure. Conversely, in the tests of Alice's pulsed source, we gradually increase the 1310-nm power, starting from its minimum value.

3. Experimental results

We demonstrate how Eve can manipulate the characteristics of Alice's laser by 1310 nm wavelength radiation of different powers. We quantify the influence of Eve's pumping via differential quantum efficiency [24,25]. It indicates how efficiently a laser medium converts injected electron-hole pairs into emitted photons. The theoretical limit for this coefficient is 1. Here we explore how additional optical pumping changes this efficiency.

Figure 2 demonstrates differential quantum efficiency of LD1550 depending on the pump power injected through its fiber pigtail. For thus, we measure the output power of LD1550 in cw regime depending on current under different power levels of pumping illumination (inset in Fig. 2). We extract the experimental value of optical power – current slope. We then calculate the differential quantum efficiency

$$\eta = \frac{2e}{\hbar\omega}\frac{dP}{dI}, \tag{1}$$

where e is the elementary charge, $\hbar$ is the reduced Planck's constant, ω is the laser frequency, and $\frac{dP}{dI}$ is the power–current slope averaged over 7 to 25 mA range.

Our data confirms that, at a fixed bias current, Alice's diode emits higher power under optical pumping. However, the change in the differential quantum efficiency is less than 1% in the investigated range of pumping power. With a decrease in pump power from 1.6 to 0.6 mW, the differential quantum efficiency decreases linearly, and then, under the lower pumping power of 140 μW and less, it becomes constant and remains the same even immediately after exposure but higher comparing to the pre-exposure level. It recovers to the initial value within a day. Both pre- and after-exposure levels are marked with dashed lines in Fig. 2. Additional research is required for an explanation of this effect.

Optics EXPRESS

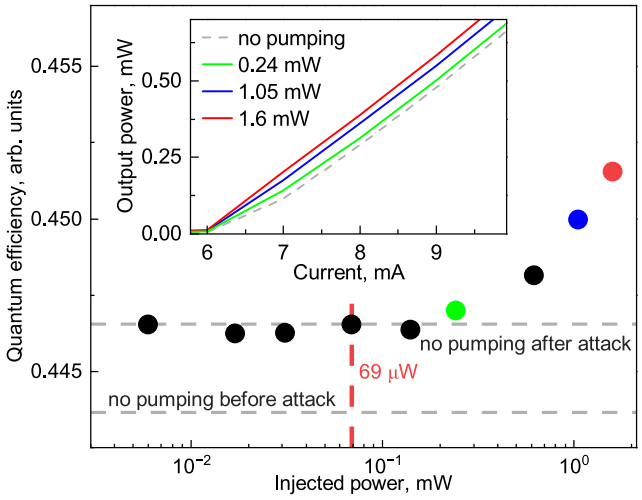

Fig. 2. Dependence of differential quantum efficiency on the injected cw power of Eve. "No pumping after attack" shows the level of differential quantum efficiency immediately after exposure. The inset shows measured light–current characteristics of LD1550 in cw regime.

This behaviour might result in an increase of the mean photon number emitted by Alice. To estimate the effect of optical pumping on QKD security, we measure LD1550's output characteristics in the pulsed regime in the presence of attack. Figure 3 shows the increase in the average output power of Alice's laser when injecting a different amount of power at 1310 nm. A notable and stable increase takes place when Eve's pump power reaches 69 μW. With a further pump power increase, the LD1550's power rises linearly. It reaches 21.7% at pump power of 1.6 mW.

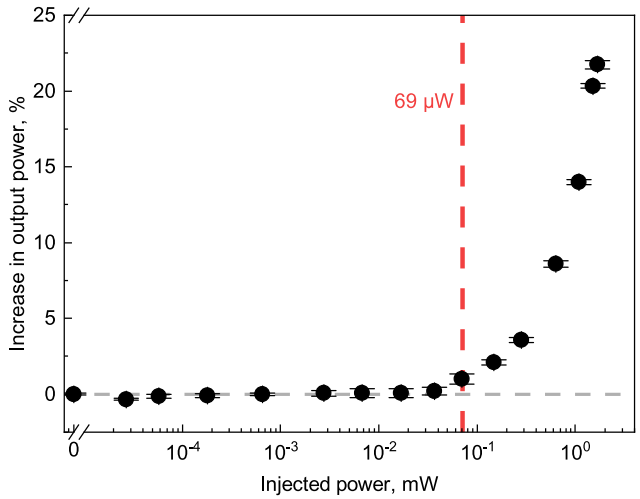

Fig. 3. Average output power of pulsed LD1550 under exposure to 1310-nm light. Standard deviation is less than 1% of measured average power.

We also measure the shape of pulses emitted by Alice under Eve's illumination. For each experimental point, we record 200k pulses, calculate the mean pulse area and its standard deviation, and draw a normalised pulse energy as the pulse area under exposure divided by the

Optics EXPRESS

initial pulse area before exposure. The result is shown in Fig. 4. Here, the maximum increase in pulse energy is about 10% at the maximum LD1310 power. A stable increase in the pulse energy is observed starting from 140 μW pump power. However, the pulse shape changes even under the lowest applied pump power of just 23 nW (inset in Fig. 4). The observed shifting of pulses under attack by about 75 ps is an order of measurement accuracy.

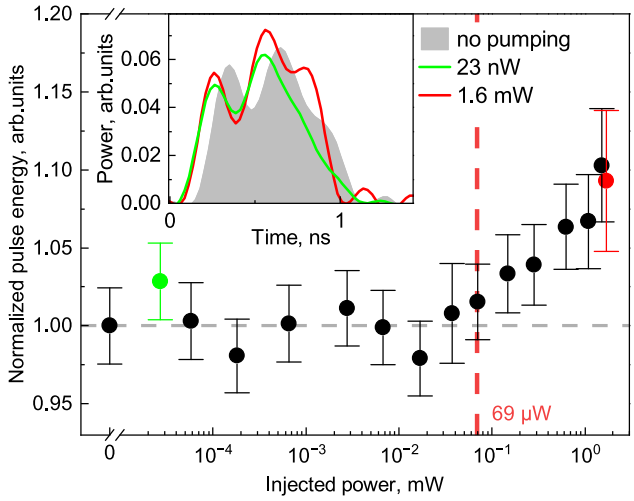

Fig. 4. Pulse energy of LD1550's pulses under Eve's illumination, normalised to their energy without pumping. Error bars present the standard deviation. Inset shows typical single-shot pulse shapes before exposure and under exposure to the minimum and maximum 1310-nm laser powers. The pulses change shape. Their mean timing, however, does not change; the time shift visible in the plot is the result of a random jitter of individual pulses.

The behaviour of the pulse energy differs quantitatively from that of the average output power. In Fig. 4, even a decrease of the pulse energy is observed. This discrepancy may be caused by spontaneous luminescence of LD1550 under continuous pumping by LD1310, which cannot be distinguished in our measurements.

In summary, our experimental results show that just about 23 nW of 1310-nm light might change characteristics of Alice's pulses, while about 140 μW should reach her laser diode to induce an increase in its pulse energy.

4. Discussion

As shown in 3, optical pumping induces an increase of both the average power and pulse energy. Let us discuss the implications of each for QKD security.

Increase in average power. In our experiment done at a low duty cycle, we notice that the increase in average power under pumping is higher than the increase in pulse energy. The difference reaches 10% under the highest attacker's power. This can be explained by an emission of LD1550 between signal pulses, induced by the optical pumping. However, the emission power between the pulses is about 1000 times lower than in the pulses. It might be difficult for Eve to exploit.

Increase in pulse energy. This increases the mean photon number emitted. Its effect on the security of different QKD protocols is well-studied, particularly for the standard decoy-state BB84 and MDI QKD protocols [12]. For instance, in a typical BB84 system [26], an unaccounted increase in the pulse energy by 10% leads to an overestimate of the secret key rate by 11% at the distance of 40 km of fiber [12], which makes the QKD system insecure. Hereinafter, we

Optics EXPRESS

present calculations indicating that the attack can be entirely mitigated by employing sufficient attenuation of the eavesdropper's light. With the implemented countermeasure, this attack will not increase Alice's pulse intensity and affect the secret key rate.

Countermeasures. To prevent the optical-pumping attack, different known techniques might be considered. They include real-time calibration of Alice's intensity using variable optical attenuators with feedback, monitoring incoming light from the quantum channel, using optical power limiting devices [14,27,28], and providing a sufficiently high total isolation [29] to suppress the injected light from the quantum channel to a safe level.

In our experiment, the 1310-nm pump power required to observe a stable increase of both differential quantum efficiency and 1550-nm pulse energy is about 140 μW (-8.5 dBm). It is several orders of magnitude higher comparing to the laser-seeding attacks [12–14]. Therefore, the optical-pumping attack should be easily preventable by a proper isolation level.

A major limiting factor for Eve is the power-handling ability of the quantum channel and of the last component in the QKD source setup. Owing to the lack of experimental and theoretical data on this, we assume that the last component in the QKD source is a fiber-optic isolator and its damage threshold at 1310 nm equals that at 1550 nm, which is on order of 4 W (36 dBm) [29]. Then, Alice needs isolation at 1310 nm just above 44.5 dB to prevent the optical-pumping attack. Meanwhile, a Raman fiber laser based on a standard single-mode fiber (OFS SMBD0980B) of about 250 W cw power at 1310 nm is reported in [30]. In this case, the required isolation is 62.5 dB.

The estimated safe isolation boundaries are significantly lower than the typical isolation at 1550 nm of practical active-state-preparation Alice modules in their backward direction [11,31,32]. Unfortunately, systems might be vulnerable to the optical-pumping attack owing to the spectral dependency of the isolation of an optical scheme. Some of the passive elements used to prevent attacks, such as fiber-optic isolators and dense-wavelength-division multiplexers (DWDMs), often have vulnerabilities at wavelengths differing from their operating one [33–37]. Figure 5 shows typical wavelength-dependence of loss of 1550-nm telecommunication fiber-optic isolators and DWDM near 1310 nm. At 1550 nm, a typical single-stage isolator provides isolation of about 30 dB [29] and dual-stage isolator of about 50 dB. At 1310 nm, they provide isolation of only about 10 and 15 dB. DWDM filters also have the same issue with the lack of isolation outside their operating range, as shown in Fig. 5. Their isolation at 1310 nm between the common input and channel output fluctuates around a few decibel. So, the spectral dependence of the system components might open a loophole for Eve to conduct the optical-pumping attack and should be considered in the system design.

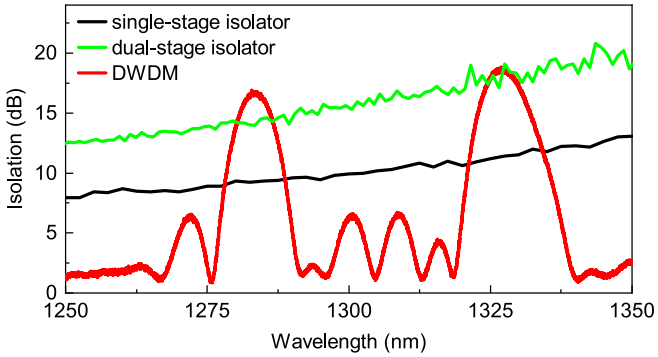

Fig. 5. Spectral characteristics near 1310 nm of typical 1550-nm fiber-optic isolators in backward direction and a dense-wavelength-division multiplexer (DWDM; Prointech DWDM-1T-MOD777-34) measured from its common port to the port of channel 34.

Optics EXPRESS

However, if the QKD system lacks modulators, it is not susceptible to the light-injection attacks and might not have enough isolation installed, such as passive-state-preparation schemes [19,22,26,38–41]. Then it's important to ensure it is protected against the optical-pumping attack.

5. Risk evaluation for a practical QKD implementation

We estimate the success of the optical-pumping attack on an industrial-prototype prepare-and-measure QKD system, on the example of a real optical scheme of Alice produced by QRate [42] that is analysed in detail in [11]. Figure 6 shows it. Alice uses intensity and phase modulators IM and PM1 to prepare her states, and isolators Iso1 and Iso2 to protect them against the Trojan-horse attack. Laser diode LD1 emits signal pulses and is the target of our attack. The following calculations consider the optical path of Eve's light to it. The total isolation at 1310 nm is calculated as a sum of loss in backward direction of each component, and is

$$\begin{aligned}\alpha_{1310} = \ & \alpha_{\mathrm{Iso2}} + \alpha_{\mathrm{Iso1}} + \alpha_{\mathrm{DWDM2}} + \alpha_{\mathrm{Att}} + \alpha_{\mathrm{VOA1}} \\ & + \alpha_{\mathrm{DWDM1}} + \alpha_{\mathrm{BS}} + \alpha_{\mathrm{PM1}} + \alpha_{\mathrm{IM}} + \alpha_{\mathrm{LD1}},\end{aligned} \tag{2}$$

where α_{Iso} is the isolation value of the optical isolator at 1310 nm wavelength, α_{LD1} is the isolation of LD1's built-in isolator, α_{DWMD}, α_{Att}, α_{VOA1}, α_{BS}, α_{PM1}, and α_{IM} are insertion losses of components in Fig. 6.

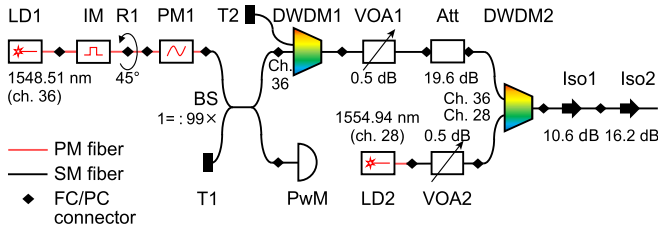

Fig. 6. Optical scheme of a commercial QKD transmitter [11]. LD, laser diode; IM, intensity modulator; R, FC/PC connector with 45° rotation; PM, phase modulator; T, optical terminator; BS, beamsplitter; DWDM, dense-wavelength-division multiplexer; Ch., DWDM channel number; VOA, variable optical attenuator; PwM, power meter; Att, fixed attenuator; Iso, polarisation-independent isolator.

The isolation values at 1310 nm used for the calculation in Eq. (2) are listed in Table 1. To estimate Alice's setup isolation at 1310 nm, we measure insertion loss of components similar to those listed in [11]. We cannot disclose model numbers for most of them, owing to our confidentiality agreements with QKD system manufacturer. They are standard off-the-shelf fiber-optic products. Fixed attenuator (Thorlabs FA20T) and fiber-optic 99:1 beamsplitter (Thorlabs TW1550R1A2) specify loss at 1310 nm in their data sheets. A phase modulator based on Ti-diffused lithium niobate is characterised using our PwM and LD1310. Insertion loss of IM is assumed to be the same as that of PM. All the other components are characterised using a broadband light source and optical spectrum analyser (Hewlett-Packard 70004A), using methodology from Appendix E of [11]. The isolation of LD1's built-in isolator is assumed to be the same as that of the single-stage isolator.

The total calculated isolation at 1310 nm is 97.6 dB, which is higher comparing to our maximum required value of 62.5 dB. Thus, the system is resilient against the optical-pumping attack at 1310 nm. However, to ensure its security, both the efficiency of optical pumping and insertion loss of the source components must be characterised in a wide spectral range [11,36].

Optics EXPRESS

Table 1. Insertion loss of components similar to those from the QKD system [11] measured at 1310 nm. The variable optical attenuator can be set anywhere in the range 0.5–30 dB, of which the worst case of 0.5 dB is assumed here

Element	Symbol	Loss, dB
Isolator 2	α_{Iso2}	16.2
Isolator 1	α_{Iso1}	10.6
DWDM2	α_{DWMD2}	3.0
Fixed attenuator	α_{Att}	19.6
Variable optical attenuator	α_{VOA1}	0.5
DWDM1	α_{DWMD1}	4.1
Beamsplitter	α_{BS}	24.0
Phase modulator	α_{PM1}	4.5
Intensity modulator	α_{IM}	4.5
LD1's built-in isolator	α_{LD1}	10.6

6. Conclusion

We have proposed a new kind of attack on real QKD systems—the optical-pumping attack on the transmitter. It allows the eavesdropper to increase the intensity of the prepared states by injecting light into Alice at a wavelength corresponding to a semiconductor absorption band of her laser source. We experimentally demonstrate 10% increase in pulse energy of 1550-nm Alice's source using Eve's injected power of 1.6 mW at 1310 nm.

Our study shows that the power required for the success of this attack is at least three orders of magnitude higher than that of the laser-seeding attack. At the same time, characteristics of passive countermeasures in practical QKD systems are wavelength-dependent and might be ineffective against this type of attack in a wide spectral range. Thus, the optical-pumping attack should be considered a possible threat to QKD security. As part of the certification process, QKD systems must be tested to confirm their countermeasures effectively mitigate this attack.

Finally, we analyse the risk of this attack on the example of the industrial QKD system [11,42]. The analysis indicates that systems with proper protection against the light-injection attacks may be resilient against the optical-pumping attack with existing countermeasures. Therefore, the latter should be strongly considered in QKD systems that do not require protection against the light-injection attacks, such as the systems using passive state preparation [19–22,26,38–41].

A. Supplementary materials

Distributed feedback (DFB) laser diodes are widely used in quantum key distribution (QKD) systems because they offer low noise, high-frequency stability, and a narrow linewidth. The DFB laser achieves high-performance emission by combining an active medium (gain semiconductor) with a diffraction grating along the entire length of the cavity. This design allows for precise selection of the wavelength.

An injection current transfers carriers to the active region of LD. When this current reaches a sufficient level to create a population inversion, lasing—or stimulated emission—occurs as a result of carrier recombination: electrons from the conduction band recombine with holes in the valence band. Optical pumping excites electrons from the valence band into the conduction band inside the active region of LD. Figure 7 provides a schematic illustration of the conduction and valence bands. For a detailed explanation of the actual band structure in InGaAsP materials typically applied in 1550-nm laser diodes, refer to [43].

Optics EXPRESS

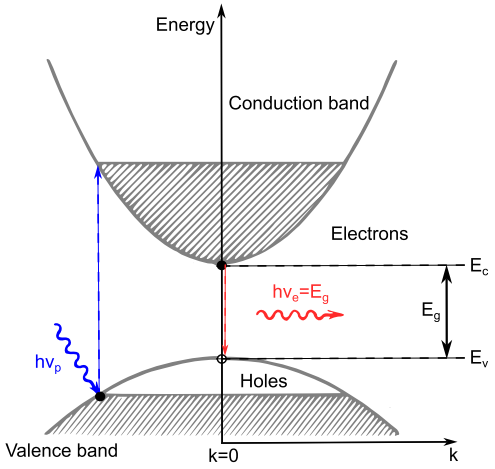

Fig. 7. Schematic view of the conduction and valence bands in semiconductor material. The pump light is in blue, and the emission light is in red. E_c represents the energy level at the bottom of the conduction band, and E_v the energy level at the top of the valence band.

In the presence of injection current alone, the laser rate equation for the carrier number N is expressed as follows:

$$\dot{N} = I/e - N/\tau_e - QG/(\Gamma\tau_{\rm ph}). \tag{3}$$

The effect of continuous optical pumping at a wavelength of 1310 nm is reduced to the addition of the optical pumping rate $R_{\rm opt}$ to the right hand side of the laser rate equation for the carrier number N. The system of rate equations can thus be written as follows:

$$\begin{aligned} \dot{N} &= I/e + R_{\rm opt} - N/\tau_e - QG/(\Gamma\tau_{\rm ph}), \\ \dot{Q} &= (G-1)Q/\tau_{\rm ph} + C_{\rm sp}N/\tau_e, \end{aligned} \tag{4}$$

where Q is the normalized electric field intensity corresponding to the photon number inside the laser cavity and related to the output power by $P = Q\eta\hbar\omega_0/(2\Gamma\tau_{\rm ph})$, where $\hbar\omega$ is the photon energy (ω is the central angular frequency of the 1550-nm laser), η is the differential quantum output, Γ is the confinement factor, $\tau_{\rm ph}$ is the photon lifetime inside the cavity, and the factor $1/2$ takes into account that the output power is measured only from one facet. Onwards, I is the pump current, e is the absolute value of the electron charge, τ_e is the effective lifetime of the electron, the factor $C_{\rm sp}$ corresponds to the fraction of spontaneously emitted photons that end up in the active mode, and the dimensionless gain G is defined by

$$G = \frac{N - N_0}{N_{\rm th} - N_0}\frac{1}{\sqrt{1 + 2\gamma_Q Q}}, \tag{5}$$

where N_0 and $N_{\rm th}$ are the carrier numbers at transparency and threshold, respectively, and γ_Q is the dimensionless gain compression factor. The optical pumping rate, in turn, can be written as

$$R_{\rm opt} = \epsilon_{\rm opt}\frac{P_{1310}}{\hbar\omega_{1310}}, \tag{6}$$

where $\epsilon_{\rm opt}$ is the pumping efficiency, P_{1310} is the optical pumping power, and $\hbar\omega_{1310}$ is the corresponding photon energy.

The actual characteristics of laser diodes required for near-practical simulation, such as the absorption cross-sections of the semiconductor, the material properties, and the coupling efficiency

Optics EXPRESS

with optical fibre, are unknown because manufacturers keep this information confidential. For simulations we have used laser and pump current parameters listed in Table 2. Simulations of the output signal with and without optical pumping are shown in Fig. 8. It was assumed that the pump current is a sequence of rectangular pulses and can be written as $I(t) = I_b + I_p(t)$, where I_b is the bias current, and the modulation current $I_p(t)$ varied from 0 to I_p^{max} (the peak-to-peak value of the modulation current).

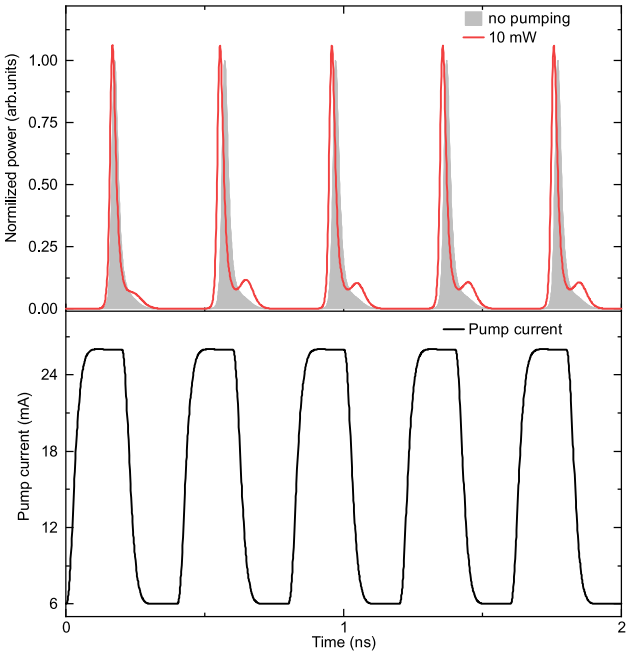

Fig. 8. Simulations of the output signal with and without optical pumping.

Table 2. Simulation parameters

Parameter	Value
Bias current I_b, mA	6.0
Maximum pump current I_p^{max}, mA	20.0
Carrier timelife τ_e, ns	1.0
Photon timelife τ_{ph}, ps	3.0
Pump current pulse width, ns	0.2
Pulse repetition rate, GHz	2.5
Confinement factor Γ	0.12
Threshold carrier number N_{th}	6.5×10^7
Transparency level N_0	5.5×10^7
Spontaneous emissions fraction C_{sp}	10^{-5}
Gain compression factor γ_Q	1.0×10^{-6}
Pumping efficiency ϵ_{opt}	0.1

Funding. Russian Science Foundation (21-42-00040); National Natural Science Foundation of China (62371459); Q1

Optics EXPRESS

Innovation Program for Quantum Science and Technology (2021ZD0300704); Galician Regional Government; NextGenerationEU (PRTR-C17.I1); Planes Complementarios de I+D+I con las Comunidades Autonomas; Ministerio de Economía y Competitividad; Postdoctoral Fellowship Program of CPSF (GZC20252817).

Disclosures. The authors declare no conflicts of interest.

Author contributions. R. S., A. H., and Q. P. assisted in planning the experiment. M. F. and A. P. conducted the experiment. R. S. and V. M. supervised the study. All authors analysed the results and contributed to writing the manuscript.

Data availability. Data underlying the results presented in this paper are not publicly available at this time, but may be obtained from the authors upon reasonable request.

References

1. C. H. Bennett, F. Bessette, L. Salvail, *et al.*, "Experimental quantum cryptography," J. Cryptology **5**(1), 3–28 (1992).
2. K. Horodecki, M. Horodecki, P. Horodecki, *et al.*, "Quantum key distribution based on private states: Unconditional security over untrusted channels with zero quantum capacity," IEEE Trans. Inf. Theory **54**(6), 2604–2620 (2008).
3. A. Gnanapandithan, L. Qian, and H.-K. Lo, "Hidden multidimensional modulation side channels in quantum protocols," Phys. Rev. Lett. **134**(13), 130802 (2025).
4. D. Trefilov, X. Sixto, V. Zapatero, *et al.*, "Intensity correlations in decoy-state BB84 quantum key distribution systems," Opt. Quantum **3**(5), 417–431 (2025).
5. N. A. Silva, D. Pereira, N. J. Muga, *et al.*, "Practical imperfections affecting the performance of CV-QKD based on coherent detection," in *2020 22nd International Conference on Transparent Optical Networks (ICTON)*, (2020), pp.1–4.
6. Z. Tang, K. Wei, O. Bedroya, *et al.*, "Experimental measurement-device-independent quantum key distribution with imperfect sources," Phys. Rev. A **93**(4), 042308 (2016).
7. H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," Nat. Photonics **8**(8), 595–604 (2014).
8. A. Dixon, J. Dynes, M. Lucamarini, *et al.*, "Quantum key distribution with hacking countermeasures and long term field trial," Sci. Rep. **7**(1), 1978 (2017).
9. F. Xu, X. Ma, Q. Zhang, *et al.*, "Secure quantum key distribution with realistic devices," Rev. Mod. Phys. **92**(2), 025002 (2020).
10. S. Sun and A. Huang, "A review of security evaluation of practical quantum key distribution system," Entropy **24**(2), 260 (2022).
11. V. Makarov, A. Abrikosov, P. Chaiwongkhot, *et al.*, "Preparing a commercial quantum key distribution system for certification against implementation loopholes," Phys. Rev. Appl. **22**(4), 044076 (2024).
12. A. Huang, Á. Navarrete, S. H. Sun, *et al.*, "Laser-seeding attack in quantum key distribution," Phys. Rev. Appl. **12**(6), 064043 (2019).
13. X.-L. Pang, A.-L. Yang, C.-N. Zhang, *et al.*, "Hacking quantum key distribution via injection locking," Phys. Rev. Appl. **13**(3), 034008 (2020).
14. V. Lovic, D. G. Marangon, P. R. Smith, *et al.*, "Quantified effects of the laser-seeding attack in quantum key distribution," Phys. Rev. Appl. **20**(4), 044005 (2023).
15. O. Svelto, *Pumping Processes*, (Springer US, Boston, MA, 1998), pp. 201–248.
16. T. Okamoto, N. Nunoya, Y. Onodera, *et al.*, "Optically pumped membrane BH-DFB lasers for low-threshold and single-mode operation," IEEE J. Sel. Top. Quantum Electron. **9**(5), 1361–1366 (2003).
17. M. Guina, A. Rantamäki, and A. Härkönen, "Optically pumped VECSELs: review of technology and progress," J. Phys. D: Appl. Phys. **50**(38), 383001 (2017).
18. M. Levinshtein, S. Rumyantsev, and M. Shur, *Handbook Series on Semiconductor Parameters, Vol. 2: Ternary and Quaternary A_3B_5 Semiconductors*, (World Scientific Publishing, Singapore, 1999).
19. V. Zapatero, W. Wang, and M. Curty, "A fully passive transmitter for decoy-state quantum key distribution," Quantum Sci. Technol. **8**(2), 025014 (2023).
20. C. Hu, W. Wang, K.-S. Chan, *et al.*, "Proof-of-principle demonstration of fully passive quantum key distribution," Phys. Rev. Lett. **131**(11), 110801 (2023).
21. F.-Y. Lu, Z.-H. Wang, V. Zapatero, *et al.*, "Experimental demonstration of fully passive quantum key distribution," Phys. Rev. Lett. **131**(11), 110802 (2023).
22. W. Wang, R. Wang, C. Hu, *et al.*, "Fully passive quantum key distribution," Phys. Rev. Lett. **130**(22), 220801 (2023).
23. O. Svelto, *Transient Laser Behavior*, (Springer US, Boston, MA, 2010), pp. 313–373.
24. D. T. Cassidy, "Differential quantum efficiency of a homogeneously broadened injection laser," Appl. Opt. **23**(17), 2870–2873 (1984).
25. T. Tomiyasu, T. Hiratani, D. Inoue, *et al.*, "High-differential quantum efficiency operation of GaInAsP/InP membrane distributed-reflector laser on Si," Appl. Phys. Express **10**(6), 062702 (2017).
26. L. C. Comandar, M. Lucamarini, B. Fröhlich, *et al.*, "Quantum cryptography without detector vulnerabilities using optically-seeded lasers," Nat. Photonics **10**(5), 312–315 (2016).
27. G. Zhang, I. W. Primaatmaja, J. Y. Haw, *et al.*, "Securing practical quantum communication systems with optical power limiters," PRX Quantum **2**(3), 030304 (2021).

Optics EXPRESS

28. Q. Peng, B. Gao, D. Wang, *et al.*, "Defending against a laser-seeding attack on continuous-variable quantum key distribution using an improved optical power limiter," Phys. Rev. A **108**(5), 052616 (2023).
29. A. Ponosova, D. Ruzhitskaya, P. Chaiwongkhot, *et al.*, "Protecting fiber-optic quantum key distribution sources against light-injection attacks," PRX Quantum **3**(4), 040307 (2022).
30. A. Grimes, A. Hariharan, I. Sun, *et al.*, "High-power, high-efficiency, semi-random Raman fiber lasers," in *Proc. SPIE 11981, Fiber Lasers XIX: Technology and Systems*, (2022), p. 119810J.
31. H. Tan, W. Li, L. Zhang, *et al.*, "Chip-based quantum key distribution against trojan-horse attack," Phys. Rev. Appl. **15**(6), 064038 (2021).
32. S. Sajeed, P. Chaiwongkhot, A. Huang, *et al.*, "An approach for security evaluation and certification of a complete quantum communication system," Sci. Rep. **11**(1), 5110 (2021).
33. N. Jain, B. Stiller, I. Khan, *et al.*, "Risk analysis of Trojan-horse attacks on practical quantum key distribution systems," IEEE J. Sel. Top. Quantum Electron. **21**(3), 168–177 (2015).
34. B. A. Nasedkin, I. M. Filipov, A. O. Ismagilov, *et al.*, "Analyzing transmission spectra of fiber-optic elements in the near IR range to improve the security of quantum key distribution systems," Bull. Russ. Acad. Sci.: Phys. **86**(10), 1164–1167 (2022).
35. A. V. Borisova, B. D. Garmaev, I. B. Bobrov, *et al.*, "Risk analysis of countermeasures against the Trojan-horse attacks on quantum key distribution systems in 1260–1650 nm spectral range," Opt. Spectrosc. **128**(11), 1892–1900 (2020).
36. H. Tan, M. Petrov, W. Zhang, *et al.*, "Wide-spectrum security of quantum key distribution," PRX Quantum (2025). In press.
37. B. Nasedkin, F. Kiselev, I. Filipov, *et al.*, "Loopholes in the 1500–2100-nm range for quantum-key-distribution components: Prospects for Trojan-horse attacks," Phys. Rev. Appl. **20**(1), 014038 (2023).
38. Z. L. Yuan, B. Fröhlich, M. Lucamarini, *et al.*, "Directly phase-modulated light source," Phys. Rev. X **6**(3), 031044 (2016).
39. G. L. Roberts, M. Lucamarini, J. F. Dynes, *et al.*, "A direct GHz-clocked phase and intensity modulated transmitter applied to quantum key distribution," Quantum Sci. Technol. **3**(4), 045010 (2018).
40. T. K. Paraïso, I. D. Marco, T. Roger, *et al.*, "A modulator-free quantum key distribution transmitter chip," npj Quantum Inf. **5**(1), 42 (2019).
41. Y. Kurochkin, M. Papadovasilakis, A. Trushechkin, *et al.*, "A practical transmitter device for passive state BB84 quantum key distribution," arXiv (2024).
42. Qrate QKD312, Hardware and software system for quantum key distribution (QKD), https://goqrate.com/projects/qrate_qkd312/, visited 10 August 2025.
43. Y. A. Goldberg and N. M. Schmidt, *Gallium Indium Arsenide Phosphide ($Ga_xIn_{1-x}As_yP_{1-y}$)* (World Scientific, London, 1999), vol. 2, chap. 7, pp. 153–179.