Realistic vulnerabilities of decoy-state quantum key distribution

I. S. Sushchev,[1, 2, *] K.E. Bugai,[1, 3] S.N. Molotkov,[4] D. S. Bulavkin,[1] A.S. Sidelnikova,[1]
D.M. Melkonian,[1] V.M. Vakhrusheva,[1, 2] R. Yu. Lokhmatov,[1] and D.A. Dvoretskiy[1, 3]

[1] *SFB Laboratory, LLC, 127273 Moscow, Russia*
[2] *Quantum Technology Centre, Faculty of Physics,*
Lomonosov Moscow State University, 119991 Moscow, Russia
[3] *Bauman Moscow State Technical University, 2nd Baumanskaya Str. 5-1, Moscow, 107005, Russia*
[4] *Institute of Solid State Physics, Russian Academy of Sciences, Chernogolovka, Moscow Region 142432, Russia*

We analyze realistic vulnerabilities of decoy-state quantum key distribution (QKD) arising from the combination of laser damage attack (LDA) and unambiguous state discrimination (USD). While decoy-state QKD is designed to protect against photon-number-splitting and beam-splitting attacks by accurately estimating the single-photon fraction, it relies on stable attenuation to prepare pulses with fixed mean-photon numbers. An eavesdropper (Eve) can exploit LDA to irreversibly alter the optical components on Alice's side, effectively increasing the mean-photon numbers beyond the decoy-state security regime. We show that once the alteration exceeds a critical threshold—on the order of 10–20 dB—Eve can implement an efficient USD-based intercept-resend strategy using current off-the-shelf technology, thus obtaining the entire secret key. Numerical simulations confirm that for sufficiently elevated mean-photon numbers, Eve's conclusive measurement outcomes skew the decoy-state statistics, yet remain undetected by standard security checks. We further demonstrate how a modified USD setup employing an additional beam splitter can reduce the required threshold, facilitating Eve's attack. Our findings emphasize the need for robust safeguards against high-power laser damage in QKD systems, including careful hardware selection, rigorous testing under high-power illumination, and real-time monitoring to ensure the integrity of the decoy-state protocol.

INTRODUCTION

Quantum key distribution (QKD) is believed to provide a secure communication guaranteed by the laws of quantum physics. For the majority of QKD protocols the security proof is present for single-photon implementation. However, real-world QKD systems usually operate with faint laser pulses, since appropriate single-photon sources are not widely available. This inconsistency is often resolved by the GLLP approach [1] combined with the decoy-state method [2], which allow legitimate parties (Alice and Bob) to produce a secret key, even though the unwanted multiphoton component is present. QKD then becomes resilient to multiphoton-component attacks, such as photon number splitting (PNS) [3], beam splitting (BS) [4] and unambiguous state discrimination (USD) [5]. This, however, is only the case when the proper operation of the decoy-state method is implied, i.e. the mean-photon numbers in Alice's pulses are fixed. In turn, an eavesdropper (Eve) can launch the laser damage attack (LDA) [6–9] to alter the attenuation at Alice's side. In this paper, we show that once the alteration of attenuation caused by LDA exceeds some critical value of several dB, Eve can steal the entire secret key using just a copy of Bob's setup, deceiving the decoy-state method. Unlike PNS [10, 11], this USD attack can be conducted using current off-the-shelf technologies.

LDA is a well-known strategy to affect the mean photon numbers in Alice's pulses by altering the attenuation of the fixed or variable attenuators using high-power radiation [6, 8, 9]. It has been reported that the continuous-wave radiation with 0.3 – 5 W mean power can reduce the attenuation coefficient by up to 10 dB and more for the fixed attenuators [6, 8, 9] and by up to 14.5 dB for the variable attenuators [6]. It has been postulated that such alteration compromises the security of the decoy-state QKD [12], making it vulnerable to PNS attack. However, to complete PNS, Eve needs to handle quantum non-demolition (QND) measurement of the photon number, save the quantum state into the quantum memory and replace the quantum channel with a lossless line. This is argued to be beyond the present-day technologies [10, 11], although some progress has arisen in this area [13, 14]. A simpler approach is to launch the BS attack, which does not require non-demolition measurements [4]. BS is known to be less effective than PNS, never giving the full information on key to an eavesdropper. Yet, the realistic BS attack has never been demonstrated. In this paper, we show that it is the USD attack that poses a real threat to security of today's QKD systems.

RESULTS

USD attacks

Let us consider the attack against weak+vacuum decoy-state BB84 QKD (see Methods). First, Eve launches LDA and modifies mean photon numbers for

[*] sushchev.is16@physics.msu.ru

the signal and decoy states as follows:

$$\tilde{\mu} = \kappa\mu \quad (1)$$

$$\tilde{\nu} = \kappa\nu, \quad (2)$$

where κ is the attenuation alteration coefficient, determined by the particular high-power radiation effect on the attenuator under attack.

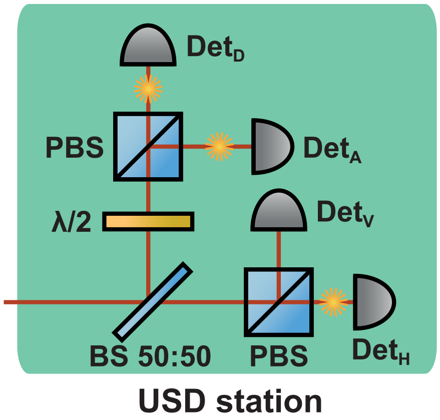

FIG. 1. Eve's polarization-encoding setup for the USD attack with a conclusive outcome for horizontally polarized state. Det$_{\rm H,V,D,A}$, detectors for horizontal, vertical, diagonal and anti-diagonal polarization; PBS, polarization beam-splitter; BS 50:50, symmetric beam-splitter; $\lambda/2$, half-wave plate for diagonal basis selection. The same setup can be designed for phase encoding.

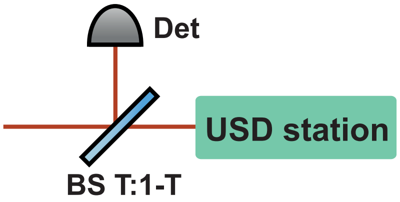

FIG. 2. Eve's setup for the modified USD attack. Det, additional detector for "odd" photons monitoring; BS T:1-T, asymmetric beam-splitter.

Next, we consider the USD strategy without QND measurements and quantum memory, hence, achievable by today's technologies. In fact, Eve only needs a copy of Bob's setup with passive basis choice for the full key distinction (Fig. 1). Having a conclusive outcome, when strictly 3 detectors have clicked (meaning that the two clicks in one basis are wrong, and the single click in another basis is correct), she sends a corresponding classical pulse to Bob, so he detects it with near-100% probability. The gains are then determined by the probability of Eve's conclusive measurements outcome.

It turns out that there exists the critical value for κ where the decoy-state secret key length estimation starts giving non-zero value, while the whole key leaks. This threshold κ_{USD} can be found numerically. However, for small $\tilde{\mu}$ and $\tilde{\nu}$, the approximate analytical estimation takes place:

$$\kappa_{USD} = 2 + \frac{2}{\mu - \nu} \ln \frac{\mu}{\nu} = 2\kappa_{3ph}, \quad (3)$$

where κ_{3ph} is the threshold for 3-photon PNS attack (see Methods). As seen, Eve needs additional 3 dB to exceed this 3-photon threshold. This result illuminates that $n > 3$ photon component gain complicates concealing the multiphoton attack.

Modified USD attack

Eve can then modify her setup and use an additional beam splitter with transmittance T to detect "odd" photons and suppress multiphoton yields for $n > 3$ (Fig. 2). Although, the gains at Bob's side will drop, it will provide the reduced USD threshold value κ_T:

$$\kappa_T = \frac{2}{2-T}\left(1 + \frac{1}{\mu - \nu} \ln \frac{\mu}{\nu}\right) = \frac{2\kappa_{3ph}}{2-T} \quad (4)$$

Surprisingly, stronger blocking the multiphoton signals with $n > 3$ even for conclusive outcomes increases the efficiency of USD attack and reduces the critical value κ_T. Asymptotically, κ_T coincides with 3-photon attack limit κ_{3ph} for $T \to 0$. However, the gain Q_μ will drop significantly:

$$\lim_{T\to 0} Q_\mu = \frac{T^3}{32} e^{-\tilde{\mu}} \tilde{\mu}^3 \quad (5)$$

Therefore, this strategy should be applied carefully, as gain drop may cause a timeout error at Bob's side.

Simulation results

The yields for the described USD attacks are determined by the probabilities for Eve's conclusive measurements outcome for n–photon component. Considering such yields, we have simulated the decoy-state single-photon gain estimation Q_1 over different attenuation alterations κ (Fig. 3). As seen, the estimated single-photon gain starts to rise rapidly after exceeding the threshold. The critical κ values correspond to those, derived by numerically solving Eq. (15). In the worst studied case, corresponding to decoy-state parameters $\mu = 0.5$ and $\nu = 0.1$, the threshold lies near 11 dB, which can be further reduced below 10 dB by proper selection of the beam splitter transmittance T in the modified USD. The reported experimental demonstrations of more than 10 dB attenuation alteration [6, 9] thus provide strong evidence of the practical attainability of the proposed attack. Table I shows the comparison between these numerical values with 0.1 dB rounding precision and analytical values from Eq. (3). There is a noticeable difference around 1 dB between numerical and analytical values. However, analytical estimations are conservative, which makes it acceptable to use them during security analysis.

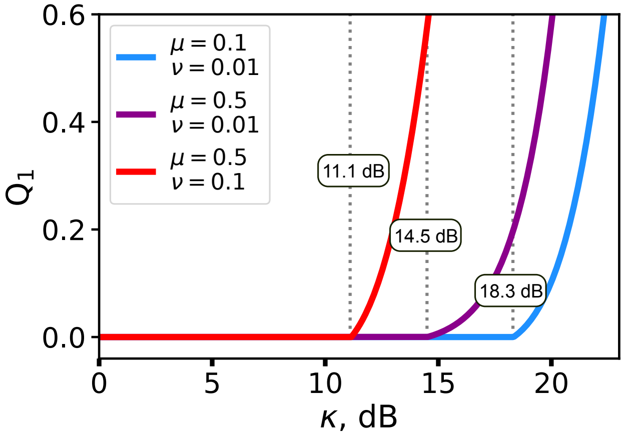

FIG. 3. Simulated single-photon gain estimation dependence on the attenuation alteration for different decoy-state parameters during the USD attack: $\mu = 0.5$, $\nu = 0.1$ (red); $\mu = 0.5$, $\nu = 0.01$ (purple); $\mu = 0.1$, $\nu = 0.01$ (blue). The threshold values (11.1 dB, 14.5 dB and 18.3 dB, respectively) are highlighted with the grey lines.

The rapid rise of the single-photon gain estimation in Fig. 3 gives Eve the possibility to set the desirable Q_1 value by slightly adjusting κ. The typical Q_1 values for proper functioning QKD systems are dependent on the channel length, mean-photon number μ and detection efficiency and lie in the region $10^{-6} - 10^{-2}$. The total gain Q_μ is also dependent on mentioned parameters and usually should be of the same order of magnitude as Q_1. Eve can reach this picking up the proper beam-splitter for the modified USD. Operating with typical altered mean-photon numbers $\tilde{\mu} \approx 5 - 15$ Eve can tune the gain to match the expected values at Bob's station by selecting the proper T value (Fig. 4).

TABLE I. Critical κ value (threshold) estimation by solving numerical transcendental equation (15) and from analytical equation (3) for different decoy-state parameters

	Numerical threshold	Equation (3)
$\mu = 0.5$, $\nu = 0.1$	11.1 dB	10.0 dB
$\mu = 0.5$, $\nu = 0.01$	14.5 dB	12.5 dB
$\mu = 0.1$, $\nu = 0.01$	18.3 dB	17.2 dB

DISCUSSION

We have described a realistic attack on QKD systems, which combines the laser damage and the USD. We have presented Eve's USD setup, which is essentially a copy of Bob's station. We have also presented the setup for modified USD by adding an asymmetric beam-splitter, which advances the efficiency of the attack. Unlike PNS or BS attack, such USD can be implemented using present-day technologies.

While our simulations addressed the ideal-case scenario, we believe that the real-world limitations can be easily bypassed by Eve. First, we assume that Eve can place her laboratory near Alice's station, therefore, we neglect the channel losses. If this is not the case and the signal must travel through, say, 10 km of standard optical fiber from Alice, the resulting channel loss would raise the threshold by approximately 2 dB. Second, Eve's imperfect detection with her SPADs efficiency η_E compensates for the LDA signal amplification, hence, the critical value for realistic USD equals $\kappa_{RUSD} = \kappa_{USD}/\eta_E$. For typical InGaAs SPADs efficiency values $\eta_E = 5 - 30\%$ it means that Eve needs additional 5–15 dB to reach the attack threshold. It then appears that the required attenuation alteration is significantly larger than the experimentally reported 10–14 dB. While for some QKD solutions this may seem like a safeguard, others often employ two attenuators in series (e.g., a variable and a fixed attenuator, as in Ref.[15]), whose combined attenuation may fall even below this "pragmatic" threshold. Moreover, Eve can avoid these limitations for QKD systems operating in the visible region (free-space QKD), where she can use high-efficiency Si SPADs. She can also upgrade her apparatus by using superconducting detectors with near-unity efficiency, which are available for purchase [16]. Thus, considering the worst-case scenario, we imply that Eve possesses sufficient resources to buy (or steal) state-of-the-art apparatus.

Another practical limitation for Eve is noise, which can originate either from imperfect state preparation – such as finite polarization extinction ratio or limited interference visibility – or from detector dark counts. While the first contribution is typically significant and may result in an error detection probability of 1–2% [10], the impact of dark counts is likely negligible over short distances. For example, consider the case where Eve detects altered mean photon numbers $\tilde{\mu} \sim 0.5$ and $\tilde{\nu} \sim 0.1$ with a typical detector efficiency of $\eta_E \sim 0.1$, while the dark count probability of InGaAs-based single-photon detectors in QKD is usually no more than $10^{-6} - 10^{-5}$.

Imperfect detection of quantum states may lead to two parasitic scenarios for Eve. The first is four-photon detection. As stated above, filtering out the "odd" photons reduces the attack threshold, albeit at the cost of slightly lower gain for Eve. The second is three-photon detection with an incorrect measurement outcome, which may introduce QBER after Eve's signal is imposed on the legitimate channel. However, maintaining the QBER below the critical threshold (11% for BB84) appears to be easily achievable by Eve.

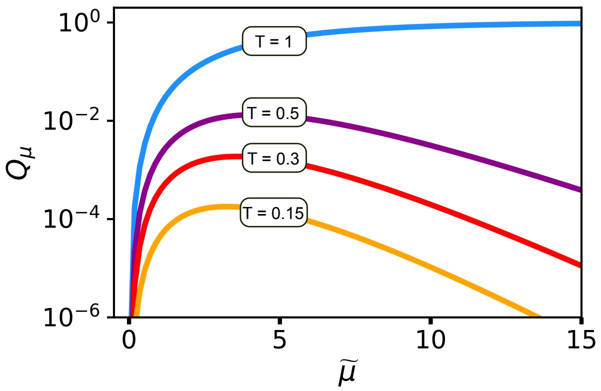

FIG. 4. Simulated signal pulses gain dependence on the altered mean-photon number for modified USD attack with different beam-splitter transparency T: $T = 1$ (blue); $T = 0.5$ (purple); $T = 0.3$ (red); $T = 0.15$ (yellow).

To trigger a click at Bob's side Eve could decide to use classical pulses with a large number of photons to compensate the drop in detection rate. This, however, may cause some irregularities in detection statistics, such as an increase of double-click rate in mismatched bases or QBER lowering, which, in principle, may be monitored by Bob. QBER lowering may arise from Eve's use of USD and her ability to enforce a detection event by sending a classical pulse with near-unity probability. However, this is unlikely to be a significant issue for Eve. By adjusting the repetition rate of her pulses, she can ensure that Bob's gain matches the expected value, thereby maintaining the dark-count to signal-count ratio and keeping the QBER close to its nominal level. If needed, Eve can even introduce a controlled amount of additional QBER by sending noise pulses – although such imperfections are likely to occur naturally due to non-ideal state preparation, as discussed above.

Increased double-click rates, in contrast, may represent a more sensitive signature of the attack, as they result from a higher probability of multiphoton events in Eve's classical pulses. The double-click probability grows approximately with the square of the pulse intensity μ^2 reaching Bob. To mitigate this, Eve can reduce the pulse intensity to match pre-attack levels. While this may make the modified USD attack more challenging – since losses introduced by the beam splitter T can no longer be compensated by increased intensity – our standard USD attack, as well as the modified version using a highly transparent beam splitter, remain unaffected. As a further option, Eve may resort to sending single photons to Bob in order to almost completely suppress double-clicks. Although this adds some technical complexity, it is entirely feasible with current technology, as commercial single-photon sources are readily available (see, for instance, [17]).

It is worth noting that, according to the reported experimental results [6, 9], the attenuation alteration induced by LDA is inherently unpredictable. This leads to two possible scenarios for the adversary. In the first case, the alteration does not exceed the required threshold, and the attack fails. In the second case, the attenuation alteration exceeds the threshold, but its exact value remains unknown to Eve. The latter scenario is of primary interest in our analysis, as we focus on conditions under which the attack becomes feasible – even if such conditions are not always guaranteed in practice. After applying LDA, Eve may seek to verify whether the modification was successful and to estimate the actual attenuation alteration in order to select optimal parameters for the subsequent USD attack. This can be accomplished, in principle, using optical reflectometry techniques [18], or by directly measuring the intensity of Alice's radiation with a high-sensitivity power meter or a single-photon detector. Once this measurement is performed, Eve can acquire the necessary information to initiate the USD attack and proceed with the USD attack as outlined above.

We have found that such USD attacks give the whole key to Eve whenever the attenuation alteration threshold is overcome. It is the 3-photon nature of these USD attacks that accounts for the existence of the threshold, which is found to lie in the region of 10–20 dB, depending on the decoy-state parameters. Such attenuation alterations have been previously experimentally demonstrated for several types of attenuators under high-power radiation [6, 9].

Therefore, one must make sure that the attenuators used in a QKD system are resilient to LDA. One mitigation approach is to monitor the functioning of optical components during the QKD session by placing a beam splitter with a high-sensitivity photodetector at the output of Alice's setup. Another option is to detect external light injection using a watchdog detector, which, however, can be circumvented by Eve [19]. A more promising method is the use of passive monitoring devices, such as optical fuses, which are permanently damaged under high-power radiation, thereby interrupting the communication. This effect can be achieved through the fiber-fuse phenomenon [20] or by employing carbon nanomaterials [21]. Finally, appropriate types of attenuators should be selected – those experimentally shown to be more resistant to high-power radiation, such as neutral filters [8] or manual variable attenuators [6]. The actual sustainability of the attenuators used in a particular QKD system should be tested as part of the certification process [6, 9, 15]. In that case, the security of the QKD will be preserved.

METHODS

Decoy-state method

The decoy-state QKD utilizes auxiliary coherent states and monitors their detection statistics. Two decoy states with mean photon numbers ν_1 and ν_2 are known to be sufficient for the estimation of the single-photon fraction. The relative secret key rate for the decoy-state BB84 is expressed as follows [2]:

$$\ell = \frac{Q_1}{Q_\mu}\Big[1 - h(E_1)\Big] - leak, \tag{6}$$

where Q_1 is the single-photon gain, Q_μ is the gain for signal pulses with mean photon number μ, E_1 is the quantum bit error rate (QBER) for the single-photon fraction, $leak$ is the information spent on the error correction, $h(x) \equiv -x\log_2 x - (1-x)\log_2(1-x)$ is the binary entropy function. For simplicity, we assume an infinite key length and the lack of side channels.

Next we consider the optimal vacuum+weak decoy-state variant ($\nu_1 \equiv \nu$, $\nu_2 \equiv 0$). The decoy-state method considers an estimation of Q_1 and E_1 given by:

$$Q_1 = Y_1 \mu e^{-\mu} \tag{7}$$

$$Y_1 \geq Y_1^L \equiv \frac{\mu}{\nu(\mu-\nu)}\left[Q_\nu e^{\nu} - \frac{\nu^2}{\mu^2} Q_\mu e^{\mu} - \frac{\mu^2 - \nu^2}{\mu^2} Q_0\right] \tag{8}$$

$$E_1 \leq E_1^U \equiv \frac{E_\nu Q_\nu e^{\nu} - E_0 Q_0}{\nu Y_1^L}, \tag{9}$$

where $Q_{\mu,\nu,0}$ are the measured gains for signal, decoy and vacuum states, $E_{\nu,0}$ is the QBER for decoy and vacuum states correspondingly, Y_1 is the yield for the single-photon component.

For the gains $Q_{\mu,\nu}$ we have:

$$Q_{\mu,\nu} = \sum_{n=0}^{\infty} p_{\mu,\nu}(n) Y_n, \tag{10}$$

where $p_{\mu,\nu}(n)$ is a Poisson probability function for a photon number n and the mean value μ or ν. Here, we have implied a proper functioning of Alice's apparatus which guarantees that the desired mean-photon numbers are prepared. The yields for n–photon components Y_n can be modified by Eve during PNS, BS or USD attack. That, however, will be detected by the decoy-state method and reflected in the single-photon fraction value estimation.

Analytical estimation for USD thresholds

When the USD attack is performed, the gains are determined by the probability of Eve's conclusive measurements outcome:

$$Q_\mu = (1 - e^{-\frac{\tilde{\mu}}{2}})(1 - e^{-\frac{\tilde{\mu}}{4}})^2 \tag{11}$$

$$Q_\nu = (1 - e^{-\frac{\tilde{\nu}}{2}})(1 - e^{-\frac{\tilde{\nu}}{4}})^2 \tag{12}$$

Here, we considered perfect noiseless detection at Eve's station and ideal bit imposition. Such strict requirements, in principle, can be relaxed (See "Discussion").

Let us derive the critical value for κ where the secret key length estimation starts giving a non-zero value:

$$Y_1^L(\kappa_{USD}) = 0 \tag{13}$$

Considering $Q_0 << 1$, eq. (13) takes the following form:

$$\frac{\Big[1 - \exp\Big(-\frac{\tilde{\nu}}{2}\Big)\Big]\Big[(1 - \exp\Big(-\frac{\tilde{\nu}}{4}\Big)\Big]^2}{\Big[1 - \exp\Big(-\frac{\tilde{\mu}}{2}\Big)\Big]\Big[1 - \exp\Big(-\frac{\tilde{\mu}}{4}\Big)\Big]^2}\frac{\mu^2}{\nu^2}e^{-(\mu-\nu)} = 1 \tag{14}$$

Modifying the left part of the expression we obtain the transcendental equation for κ_{USD}:

$$\frac{\sinh(\frac{\kappa_{USD}\nu}{4})\sinh^2(\frac{\kappa_{USD}\nu}{8})}{\sinh(\frac{\kappa_{USD}\mu}{4})\sinh^2(\frac{\kappa_{USD}\mu}{8})}\frac{\mu^2}{\nu^2}e^{\frac{\kappa_{USD}-2}{2}(\mu-\nu)} = 1 \tag{15}$$

This equation can be solved numerically. However, for approximate estimation, we will use the Taylor expansion of the left part:

$$\frac{\sinh(\frac{\kappa_{USD}\nu}{4})\sinh^2(\frac{\kappa_{USD}\nu}{8})}{\sinh(\frac{\kappa_{USD}\mu}{4})\sinh^2(\frac{\kappa_{USD}\mu}{8})} \lesssim \Big(\frac{\nu}{\mu}\Big)^3 \tag{16}$$

That results in equation (3).

For the modified USD attack with an additional beamsplitter the gains are modified as follows:

$$Q_\mu = e^{-(1-T)\tilde{\mu}}(1 - e^{-\frac{T\tilde{\mu}}{2}})(1 - e^{-\frac{T\tilde{\mu}}{4}})^2 \tag{17}$$

$$Q_\nu = e^{-(1-T)\tilde{\nu}}(1 - e^{-\frac{T\tilde{\nu}}{2}})(1 - e^{-\frac{T\tilde{\nu}}{4}})^2 \tag{18}$$

For the transcendental equation we have:

$$\frac{\sinh(\frac{T\kappa_T\nu}{4})\sinh^2(\frac{T\kappa_T\nu}{4})}{\sinh(\frac{T\kappa_T\mu}{4})\sinh^2(\frac{T\kappa_T\mu}{4})}\frac{\mu^2}{\nu^2}e^{(\kappa_T - 1 - \frac{T\kappa_T}{2})(\mu-\nu)} = 1 \tag{19}$$

Using approximation (16) we found an estimate for κ_T resulting in equation (4).

3-photon PNS attack

Let us consider a specific PNS strategy with blocking all n–components with $n \neq 3$. This strategy leads to a more significant drop in secret key rate in comparison to the standard PNS strategy with preserving $n = 2$ component. This 3-photon attack, however, does not require a quantum memory as the measurements in two different bases can be conducted simultaneously. Hence, only classical memory for the measurements outcome is required.

We consider the zero yields for 3-photon attack, except for the Y_3:

$$\begin{aligned} Y_{n\neq 3} &= 0 & (20)\\ Y_{n=3} &\neq 0 & (21)\end{aligned}$$

LDA modifies mean photon numbers as dictated by eq. (1) and (2). The gains are then:

$$\begin{aligned} Q_\mu &\approx Y_3\frac{\tilde{\mu}^3}{6}e^{-\tilde{\mu}} & (22)\\ Q_\nu &\approx Y_3\frac{\widetilde{\nu}^3}{6}e^{-\tilde{\nu}} & (23)\end{aligned}$$

The critical value for κ where the secret key length estimation starts giving non-zero value can be derived from the following equation:

$$Y_1^L(\kappa_{3ph}) = 0 \tag{24}$$

Considering $p_{dcr} << 1$, we obtain the equation:

$$Q_\nu e^\nu = \frac{\nu^2}{\mu^2}Q_\mu e^\mu, \tag{25}$$

Solving equation (25) for κ_{3ph} we obtain the 3-photon attack threshold:

$$\kappa_{3ph} = 1 + \frac{1}{\mu - \nu}\ln\frac{\mu}{\nu} \tag{26}$$

The threshold is proportional to those for the described USD attacks (3) and (4). This underlines the 3-photon nature of the described USD strategies.

Simulation of USD attack

Considering noiseless and lossless detection at Eve's station, we can express the yields for the USD attack, i.e. the probabilities of conclusive measurements outcome for n–photon components. For this, we use the binomial distribution of photons after the 50:50 beamsplitter and pick up the scenarios, when only 3 detectors click (we assume Eve using threshold detectors without photon number resolution):

$$\begin{aligned} Y_n^{USD} &= \sum_{k=1}^{n}\binom{n}{k}\left(\frac{1}{2}\right)^k\left(\frac{1}{2}\right)^{n-k}\\ &\times\sum_{m=1}^{n-k-1}\binom{n-k}{m}\left(\frac{1}{2}\right)^k\left(\frac{1}{2}\right)^{n-k-m} = 1 - \frac{3^n-1}{2^{2n-1}},\end{aligned} \tag{27}$$

where the first sum denotes the probability of k photons to arrive at the correct-basis measurement side and the second sum denotes the probability of the the remaining $n-k$ photons to be divided along two paths in the incorrect-basis measurement side.

For the modified USD attack the yields are multiplied by the probability of n photons passing through the beamsplitter T:

$$Y_n^T = T^n \cdot Y_n^{USD} \tag{28}$$

We have simulated the single-photon gain estimation and the total gain for signal pulses using equations (7)–(8), (10), (27)–(28) for different decoy-state parameters. The series in Eq. (10) was truncated at $n = 600$, since the cumulative probability of the Poisson distribution beyond this point becomes negligible within the precision of the 8-digit floating-point arithmetic used in our simulations. The results are presented in "Simulation results".

DATA AVAILABILITY

All the data that support the results of the current work are available from the corresponding authors upon reasonable request.

CODE AVAILABILITY

The code for simulation is available from the corresponding author upon reasonable request.

ACKNOWLEDGMENTS

I.S.S. thanks S.P. Kulik for numerous discussions. I.S.S. also acknowledges the scholarship from the Foundation for the Advancement of Theoretical Physics and Mathematics "BASIS".

AUTHOR CONTRIBUTION

I.S.S. developed the theoretical framework and wrote the manuscript, I.S.S. and K.E.B. introduced the scenario for combined LDA and USD attack, I.S.S. and R.Yu.L. executed the numerical simulations, D.S.B., A.S.S., V.M.V. and D.M.M. aided in interpreting the results and worked on the manuscript, S.N.M. and D.A.D. conceptualized and supervised the work.

COMPETING INTERESTS

The authors declare no competing interests.

[1] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Security of quantum key distribution with imperfect devices, Proc. IEEE Int. Symp. Inf. Theory (ISIT), p. 136 (2004).

[2] H. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. 94, 230504 (2005).

[3] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Limitations on practical quantum cryptography, Phys. Rev. Lett. 85, 1330 (2000).

[4] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, Experimental quantum cryptography, J. Cryptol. 5, 3 (1992).

[5] H. P. Yuen, Quantum amplifiers, quantum duplicators, and quantum cryptography, Quantum Semiclass. Opt. 8, 939 (1996).

[6] A. Huang, R. Li, V. Egorov, S. Tchouragoulov, K. Kumar, and V. Makarov, Laser-damage attack against optical attenuators in quantum key distribution, Phys. Rev. Appl. 13, 034017 (2020).

[7] D. D. Ruzhitskaya, I. V. Zhluktova, M. A. Petrov, K. A. Zaitsev, P. P. Acheva, N. A. Zunikov, et al., Vulnerabilities in the quantum key distribution system induced under a pulsed laser attack, J. Sci. Tech. Inf. Tech. Mech. Opt. 136, 837 (2021).

[8] S. V. Alferov, K. E. E. Bugai, and I. A. Pargachev, Study of the vulnerability of neutral optical filters used in quantum key distribution systems against laser damage attack, JETP Lett. 116, 123 (2022).

[9] K. E. Bugai, A. P. Zyzykin, D. S. Bulavkin, S. A. Bogdanov, I. S. Sushchev, and D. A. Dvoretskiy, Laser damage attack on a simple optical attenuator widely used in fiber-based QKD systems, Proc. 2022 Int. Conf. Laser Optics (ICLO), p. 1 (2022).

[10] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, Rev. Mod. Phys. 74, 145 (2002).

[11] S. P. Kulik, K. S. Kravtsov, and S. N. Molotkov, Experimental resources needed to implement photon number splitting attack in quantum cryptography, Laser Phys. Lett. 19, 025203 (2022).

[12] A. Huang, Á. Navarrete, S. H. Sun, P. Chaiwongkhot, M. Curty, and V. Makarov, Laser-seeding attack in quantum key distribution, Phys. Rev. Appl. 12, 064043 (2019).

[13] W.-T. Liu, S.-H. Sun, L.-M. Liang, and J.-M. Yuan, Proof-of-principle experiment of a modified photon-number-splitting attack against quantum key distribution, Phys. Rev. A 83, 042326 (2011).

[14] A. Ashkenazy, Y. Idan, D. Korn, D. Fixler, B. Dayan, and E. Cohen, Photon number splitting attack—Proposal and analysis of an experimental scheme, Adv. Quantum Technol. 3, 2300437 (2024).

[15] V. Makarov, A. Abrikosov, P. Chaiwongkhot, A. K. Fedorov, A. Huang, E. Kiktenko, et al., Preparing a commercial quantum key distribution system for certification against implementation loopholes, Phys. Rev. Appl. 22, 044076 (2024).

[16] SCONTEL, Single-photon detectors (SSPD), www.scontel.ru/sspd (accessed April 17, 2025).

[17] Quandela, Single-photon sources, www.quandela.com/technology/the-power-of-single-photon-sources (accessed April 17, 2025).

[18] M. K. Barnoski and S. M. Jensen, Fiber waveguides: a novel technique for investigating attenuation characteristics, Appl. Opt. 15, 2112–2115 (1976).

[19] S. Sajeed, I. Radchenko, S. Kaiser, J. P. Bourgoin, A. Pappa, L. Monat, et al., Attacks exploiting deviation of mean photon number in quantum key distribution and coin tossing, Phys. Rev. A 91, 032326 (2015).

[20] K. E. Bugai, I. S. Sushchev, D. S. Bulavkin, R. Y. Lokhmatov, and D. A. Dvoretskiy, Protection method against powerful emission attacks based on optical-fiber fuse element, Proc. 2024 Int. Conf. Laser Optics (ICLO), p. 446 IEEE (2024).

[21] E. V. Borisova, A. A. Ponosova, B. I. Galagan, V. V. Koltashev, N. A. Rutyunyan, and V. V. Makarov, Optical fuse as a countermeasure against light injection attacks on quantum key distribution systems, Proc. 2024 Int. Conf. Laser Optics (ICLO), pp. 103-103, IEEE (2024).