Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Temporal Side-Channel Vulnerability of Decoy-State Quantum Key Distribution under Quantum Non-Demolition Eavesdropping

A. S. Kalashnikova

batmankuro99@gmail.com

National University of Science and Technology "MISIS"

D. V. Sych

P.N. Lebedev Physical Institute of the Russian Academy of Sciences

Research Article

Keywords: quantum cryptography, quantum communication, quantum key distribution, side-channel attack, QND measurement, BB84-decoy state

Posted Date: November 10th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-11062023/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

Temporal Side-Channel Vulnerability of Decoy-State Quantum Key Distribution under Quantum Non-Demolition Eavesdropping

A. S. Kalashnikova[1*] and D. V. Sych[1,2†]

[1*]National University of Science and Technology "MISIS", Leninsky Prospekt, 4, Moscow, 119049, Russia.
[2]Lebedev Physical Institute of the Russian Academy of Sciences, Leninsky Prospekt, 53, Moscow, 119991, Russia.

*Corresponding author(s). E-mail(s): batmankuro99@gmail.com;
Contributing authors: denis.sych@gmail.com;
†These authors contributed equally to this work.

Abstract

Quantum key distribution promises information-theoretic security, but practical implementations are vulnerable to side-channel attacks that exploit unintended non-operational physical degrees of freedom. A particularly subtle threat arises from the temporal distinguishability of signal and decoy pulses in decoy-state BB84 protocol. If an eavesdropper can discriminate quantum state by its timing, she can tag the intensity class and break the central assumption of the decoy-state method. In this work, we analyze a temporal side-channel attack in which the eavesdropper employs a realistically imperfect quantum non-demolition measurement module to extract timing information without absorbing the photon. We show that the maximum-likelihood discrimination probability of signal and decoy pulses reaches 0.68 after 60 km of standard single-mode fiber, well above the random-guessing baseline of 0.5. With the quantum non-demolition module placed at 70 km, the discrimination probability increases to 0.70–0.73, depending on the interaction time, while at short distances ($<$ 5 km) it remains nearly independent of the quantum non-demolition parameters. The secure key rate, evaluated within a modified GLLP framework, drops to zero beyond 36 km in both cases—with the maximum-likelihood discrimination alone and with the imperfect-quantum non-demolition module—differing only in overall efficiency. To obtain these results, we develop a comprehensive model that combines realistic fiber propagation with a non-ideal quantum non-demolition interaction and

statistical decision theory. The proposed methodology provides a practical toolbox for quantifying temporal side-channel vulnerabilities and can serve as a foundation for future security analyses of quantum key distribution systems.

Keywords: quantum cryptography; quantum communication; quantum key distribution; side-channel attack; QND measurement; BB84-decoy state.

1 Introduction

Quantum Key Distribution (QKD) enables two remote parties to establish a provably secure secret key by encoding information in quantum states and detecting eavesdropping through unavoidable quantum disturbances Bennett and Brassard (2014); Gisin et al. (2002). In the asymptotic limit and under ideal assumptions, unconditional security proofs have been established for a range of protocols, including BB84 and its decoy-state variants Lo et al. (2005); Wang (2005); Hwang (2003).

However, the practical security of QKD remains a central challenge. Physical devices inevitably deviate from the idealized models employed in security proofs, opening side channels through which an eavesdropper may gain partial information without introducing visible errors. A side channel is any unintended non-operational degree of freedom whose observable behavior correlates with the secret bit or basis choice during quantum preparation, transmission, or detection. Over the past decade, the investigation of side channels has evolved into a critical area of research, driven by a growing number of successful attacks on commercial and experimental systems Lydersen et al. (2010); Gerhardt et al. (2011); Weier et al. (2011); Duplinskiy and Sych (2021).

In this work, we focus on a specific side channel: the temporal side channel of the light source Lamas-Linares and Kurtsiefer (2007). In practical QKD setups, timing of a photon may depend on the encoded quantum state. Such state—timing correlations can arise from imperfections in the source electronics, modulator responses, or wavelength-dependent optical paths. Crucially, an eavesdropper capable of resolving these timing differences could sort detection events into distinguishable groups, e.g. signal states and decoy states in a decoy-state QKD protocol, thus breaking the central assumption of the decoy-state method and severely compromising the security proof Miller (2025).

Measuring the photon's arrival time, however, presents a fundamental difficulty: a conventional time-resolving detector would absorb the photon, collapsing its quantum state and destroying the key bit. To circumvent this problem, we turn to the concept of quantum non-demolition (QND) measurement Brune et al. (1990). A QND measurement extracts information about a specific observable—here, the photon presence or arrival time—without absorbing the photon or projecting its polarization state Grangier et al. (1998); Guerlin et al. (2007). In principle, a QND timing module placed before the legitimate receiver could allow an adversary to tag the state group (signal or decoy) while leaving the qubit intact. This possibility makes the temporal side channel both technically subtle and theoretically dangerous.

The present article is dedicated to a systematic evaluation of this threat. We analyze a temporal side-channel attack against a decoy-state BB84 protocol and quantify its impact on the secure key rate. By modeling the timing response of a realistic QKD transmitter and the capabilities of an eavesdropper armed with an ideal QND timing measurement, we derive bounds on the information leakage and determine the maximum tolerable timing distinguishability.

2 Channel Model and Temporal Distributions

We consider a decoy-state BB84 protocol implemented with eight laser diodes, each encoding one of four polarization states (H, V, D, A) in either the signal or the decoy intensity class. The signal and decoy states are prepared with mean photon numbers $\mu = 0.3$ and $\nu = 0.1$, respectively. The lasers emit at a central wavelength $\lambda_0 = 1550\,\mathrm{nm}$ with individual detunings λ_k on the order of picometers.

The channel is modeled as a discretized span from 0 to $L = 70$ km with a step of 2 km; at each distance all subsequent quantities are evaluated. The fiber is standard single-mode with chromatic dispersion coefficient $D_l = 17\,\mathrm{ps}/(\mathrm{nm}\cdot\mathrm{km})$, polarization-mode dispersion coefficient $D_{\mathrm{PMD}} = 0.1\,\mathrm{ps}/\sqrt{\mathrm{km}}$, and group index $n_g = 1.47$. Optionally, a dispersion-compensating fiber (DCF) module is appended at the receiver side to compress the pulses before detection.

We model the arrival time of a photon at the channel output as a Gaussian random variable whose mean and variance are determined by several physical effects:

1. **Chromatic dispersion**. The group-velocity dispersion parameter is given by $\beta_2 = -(\lambda_0+\lambda_k)^2 D_l/(2\pi c)$. An initial transform-limited pulse of width T_0 broadens to $T_1 = T_0\sqrt{(1 + C\beta_2 L/T_0^2)^2 + (\beta_2 L/T_0^2)^2}$, where C is the laser chirp parameter Agrawal (2021). The corresponding temporal variance is $\sigma^2_{\mathrm{chrom}} = T_1^2/2$.
2. **Polarization-mode dispersion (PMD)**. The PMD-induced temporal shift and broadening are modeled as $\Delta t_{\mathrm{PMD}} = \frac{1}{2}\mathrm{DGD}\cos\big[2(\theta_k - \theta_{\mathrm{fast}})\big]$ and $\sigma_{\mathrm{PMD}} = \frac{\mathrm{DGD}}{\sqrt{3}}\big|\cos(2\theta_k)\big|$, where $\mathrm{DGD} = D_{\mathrm{PMD}}\sqrt{L}$ and θ_k is the polarization angle of the k-th laser relative to the fast axis of the fiber.
3. **Individual laser offsets**. Each laser diode possesses a hardware-specific temporal offset δt_k (on the order of tens of picoseconds) arising from electronic path-length differences and modulator characteristics.
4. **Detection jitter**. A Gaussian timing jitter of $\sigma_{\mathrm{jitter}} = 15\,\mathrm{ps}$ is added to model the finite resolution of practical detectors.

The total temporal distribution of the k-th laser at distance z is therefore Gaussian with mean

$$\mu_k(z) = \delta t_k + D_l z \lambda_k + \frac{D_{\mathrm{PMD}}\sqrt{z}}{2}\cos\big[2(\theta_k - \theta_{\mathrm{fast}})\big]$$

and standard deviation

$$\sigma_k(z) = \sqrt{\sigma^2_{\mathrm{chrom},k}(z) + \sigma^2_{\mathrm{PMD},k}(z) + \sigma^2_{\mathrm{jitter}}}.$$

At each distance z, the temporal distribution of the k-th laser state ($k = 1, \ldots, 8$) is represented by a diagonal density matrix on the discrete time-bin Hilbert space $\mathcal{H}_{\text{time}}$:

$$\rho_{\text{time}}^{(k)}(z) = \sum_{j=1}^{n(z)} p_k(t_j; z)\, |t_j\rangle\langle t_j|,$$
$$p_k(t_j; z) = \mathcal{N}\big(t_j; \mu_k(z), \sigma_k(z)\big).$$

The eight matrices are grouped by intensity class: $\{\rho_{\text{time}}^{(1)}, \ldots, \rho_{\text{time}}^{(4)}\}$ correspond to signal states, and $\{\rho_{\text{time}}^{(5)}, \ldots, \rho_{\text{time}}^{(8)}\}$ to decoy states.

These eight time-bin density matrices form the basis of Eve's classification decision.

In the decoy-state BB84 protocol, each laser prepares a weak coherent pulse whose photon-number statistics follow a Poisson distribution. The photon-number density matrix is now represented in the three-dimensional basis $\{|0\rangle, |1\rangle, |\mathcal{M}\rangle\}$, where $|0\rangle$ the vacuum state, $|1\rangle$ denotes a single-photon state, and $|\mathcal{M}\rangle$ denotes the multi-photon subspace ($k \geq 2$). It takes the form:

$$\rho_{\text{ph}} = \begin{pmatrix} e^{-x} & 0 & 0 \\ 0 & xe^{-x} & 0 \\ 0 & 0 & 1 - e^{-x} - xe^{-x} \end{pmatrix},$$

where x is the average intensity. The diagonal elements correspond to the probabilities $p_0 = e^{-x}$, $p_1 = xe^{-x}$, and $p_m = 1 - e^{-x} - xe^{-x}$, with $x = \mu$ for signal states and $x = \nu$ for decoy states.

The overall state of the k-th laser at distance z is the tensor product

$$\rho^{(k)}(z) = \rho_{\mu/\nu} \otimes |\psi_k\rangle\langle\psi_k| \otimes \rho_{\text{time}}^{(k)}(z),$$

where $|\psi_k\rangle \in \{|H\rangle, |V\rangle, |D\rangle, |A\rangle\}$ is the encoded polarization state, $\rho_{\text{time}}^{(k)}(z)$ describes the temporal degree of freedom at distance z, and the intensity class (signal or decoy) determines whether $\rho_{\mu/\nu}$ equals ρ_μ or ρ_ν.

3 Discrimination Procedure

Based on the measured arrival time t, Eve must decide whether the photon originated from a signal or decoy state. This is a binary hypothesis test. Assuming equal a priori probabilities for both classes, the optimal decision rule is the maximum-likelihood classifier:

$$\hat{c}(t) = \begin{cases} S, & p_S(t) > p_D(t), \\ D, & \text{otherwise.} \end{cases}$$

where $p_S(t)$ and $p_D(t)$ are the temporal probability densities of the signal and decoy classes, respectively.

The probability of correct classification is given by

$$P_{\text{discrim}} = \frac{1}{2}\big[P(\text{correct} \mid S) + P(\text{correct} \mid D)\big],$$

where

$$P(\text{correct} \mid C) = \sum_{t_j \in \mathcal{T}_C} p_C(t_j), \quad C \in \{S, D\},$$

where $\mathcal{T}_S = \{t_j : p_S(t_j) > p_D(t_j)\}$ and $\mathcal{T}_D = \{t_j : p_S(t_j) \leq p_D(t_j)\}$.

The quantity P_{discrim} directly quantifies the fraction of detection events for which Eve correctly identifies whether the photon originated from a signal or decoy state. Note that this classification leads to the photon absorption, hence cannot be directly applied as an eavesdropping strategy.

Figure 1 presents the temporal pulse profiles of the eight laser states at the transmitter output. The initial and final distributions are plotted as probability densities as functions of arrival time. After propagation, the pulses are broadened and shifted relative to one another due to chromatic dispersion, PMD, and individual laser offsets. The corresponding discrimination probability of signal and decoy pulses, evaluated directly from these distributions, is $P_{\text{discrim}} \approx 0.68$ after 60 km and before the DCF and $P_{\text{discrim}} \approx 0.62$ after DCF.

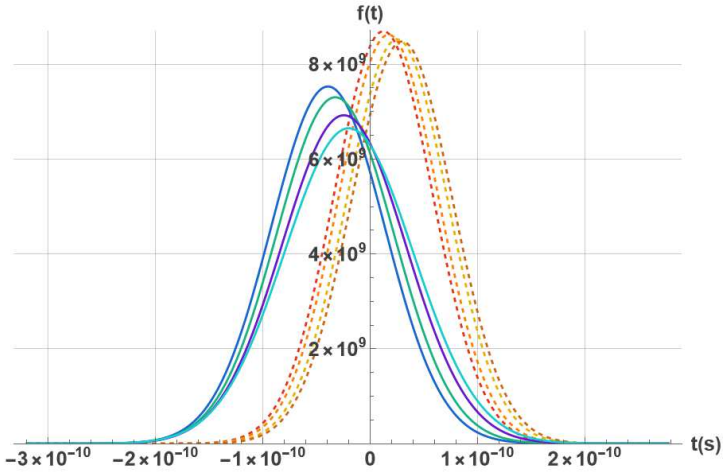


Fig. 1 Temporal probability distributions of the eight laser states at the transmitter output. The signal states are shown as solid lines (blue for $|H\rangle$, teal for $|V\rangle$, purple for $|D\rangle$, cyan for $|A\rangle$) and the decoy states as dashed lines (red for $|H\rangle$, orange for $|V\rangle$, yellow for $|D\rangle$, brown for $|A\rangle$), respectively.

4 QND Measurement

To extract timing information without absorbing the photon, Eve employs a QND measurement scheme Brune et al. (1990). For example,the physical architecture is

based on a single-atom mirror resonator Dong et al. (2009): a one-dimensional waveguide terminated at one end by a conventional mirror, with a two-level atom (qubit) positioned at a distance a from the mirror. When the photon frequency is resonant with the atomic transition, the atom acts as a second, tunable mirror, forming an intrinsic cavity that traps the photon between the physical mirror and the atom.

The QND interaction is described by an effective Hamiltonian in the rotating frame Sathyamoorthy et al. (2014); Besse et al. (2018):

$$H = \hbar \int dt\xi(t)\big(a^\dagger b(t) + ab^\dagger(t)\big) + \hbar\Omega\big(a^\dagger a \otimes \sigma_x\big), \tag{1}$$

where the first term describes the coupling of the incoming photon to the resonator mode, with $\xi(t)$ representing the temporal profile of the wave packet, and the second term implements a dispersive interaction between the photon number operator $a^\dagger a$ and the meter qubit σ_x Blais et al. (2004). Because $[a^\dagger a, H] = 0$, the photon number is preserved during the measurement, guaranteeing the QND property.

In our model the ideal QND scheme is supplemented by two realistic imperfection channels Lindblad (1976):

1. **Photon loss.** The resonator mode suffers from intrinsic losses due to imperfect mirror reflectivity and atomic scattering into non-resonant modes Reiserer and Rempe (2015). These processes are described by a Lindblad term with decay rate κ, which transfers population from the $\{|1\rangle, |\mathcal{M}\rangle\}$ subspace to the vacuum state $|0\rangle$ and to the state $|\mathcal{M} - 1\rangle$, respectively. In our numerical simulations we set $\kappa = 1 \times 10^8$ s^{-1}, corresponding to a photon lifetime of $\tau = 1/\kappa = 10$ ns. This value is consistent with the parameters of high-Q microcavities operating at 1550 nm, where quality factors of $Q \approx 10^7$ have been demonstrated Ilchenko et al. (2001).
2. **Polarization rotation.** The dispersive coupling $\hbar\Omega(a^\dagger a \otimes \sigma_x)$ induces a state-dependent phase on the meter qubit, but the atom-field interaction may also weakly couple to the photon's polarization degree of freedom. This leads to a slow continuous rotation of the polarization vector during the photon's residence in the resonator, modeled by the unitary operator U_{rot} with rate α Arnardottir (2018); Brennecke et al. (2007). In our numerical simulations we set $\alpha = 2\pi \times 1$ MHz, which corresponds to a typical polarization modulation frequency in cavity-QED systems and is consistent with the demonstrated capability to manipulate single-photon polarization in such devices Arnold et al. (2015).

The evolution of the joint Eve–photon density matrix is governed by the Lindblad master equation

$$\dot{\rho} = -\frac{i}{\hbar}[H, \rho] + \kappa\Big(a\rho a^\dagger - \frac{1}{2}\{a^\dagger a, \rho\}\Big), \tag{2}$$

where the second term describes photon loss from the resonator at a rate κ. In addition, there is a slow continuous rotation of the polarization state.

Equation (2) is solved numerically by splitting the evolution into small time steps $\delta t = \tau/N$, where τ is the total interaction time and N is the number of steps. At each step, the following parameters and operators are computed:

$$p = 1 - e^{-\kappa \delta t}, \qquad \theta = \alpha \delta t,$$

$$K_0^{(\mathrm{vac})} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \sqrt{1-p} & 0 \\ 0 & 0 & \sqrt{1-p} \end{pmatrix},$$

$$K_1^{(\mathrm{vac})} = \begin{pmatrix} 0 & 0 & \sqrt{p} \\ 0 & \sqrt{p} & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

$$U_{\mathrm{rot}} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

The operators $K_0^{(\mathrm{vac})}$ and $K_1^{(\mathrm{vac})}$ act on the three dimensional photon-number space $\{|1\rangle, |0\rangle, |\mathcal{M}\rangle\}$. $K_0^{(\mathrm{vac})}$ describes the no-loss event: the single-photon and multi-photon amplitudes are multiplied by $\sqrt{1-p}$, while the vacuum component remains unchanged. $K_1^{(\mathrm{vac})}$ describes the loss of one photon: it maps the multi-photon state $|\mathcal{M}\rangle$ to the single-photon state $|1\rangle$ with amplitude $\sqrt{p}$, and the single-photon state $|1\rangle$ to the vacuum state $|0\rangle$ with amplitude $\sqrt{p}$. The rotation operator U_{rot} acts on the polarization subspace and is unchanged.

The operators $K_0^{(\mathrm{vac})}$ and $K_1^{(\mathrm{vac})}$ act on the vacuum-single-photon subspace and are extended to the full Hilbert space via tensor products with identity matrices on the polarization, time, and Eve subsystems:

$$K_i = I_{\mathrm{Eva}} \otimes (K_i^{(\mathrm{vac})} \otimes I_{\mathrm{pol}} \otimes I_{\mathrm{time}}), \quad i = 0, 1.$$

Similarly, the polarization rotation is extended as

$$U_{\mathrm{rot}} = I_{\mathrm{Eva}} \otimes I_{\mathrm{vac}} \otimes U_{\mathrm{rot}} \otimes I_{\mathrm{time}}.$$

The density matrix is then updated sequentially: unitary evolution ($e^{-iH\delta t}\rho e^{+iH\delta t}$), photon loss ($K_0\rho K_0^\dagger + K_1\rho K_1^\dagger$), polarization rotation ($U_{\mathrm{rot}}\rho U_{\mathrm{rot}}^\dagger$).

The values are chosen in accordance with typical parameters of solid-state microcavity systems Arnardottir (2018); Brennecke et al. (2007).

The QND interaction maps the photon's arrival time onto the phase of the meter qubit. For a photon detected at time t, the probability that the meter qubit is found in the excited state is

$$P_+(t) = \cos^2 \phi(t), \qquad \phi(t) = 2\Omega \int_0^t |\xi(t')|^2 \, dt',$$

where $|\xi(t)|^2 = p(t)$ is the temporal probability density of the photon. The phase is accumulated as

$$\phi_j = 2\Omega \sum_{i=1}^{j} p_i \, \delta t,$$

with $p_i = p(t_i; z)$ being the probability at the i-th time. The meter response is then $P_+(t_j) = \cos^2 \phi_j$. The total probability that the meter registers an excitation for a given input state k is obtained by

$$P_{\text{total}}^{(k)} = \sum_j p_k(t_j; z)\, P_+(t_j).$$

The quantity $P_+(t_j)$ gives the probability that the meter qubit is found in the excited state at time bin t_j.

Figure 2 illustrates the response of Eve's QND meter, showing the probability $P(t)$ as a function of time for an interaction time $\tau = 5\,\text{ns}$ with Eve's module positioned at $z = 60\,\text{km}$. Under these conditions, the corresponding discrimination probability between signal and decoy states is $P_{\text{discrim}} \approx 0.71$.

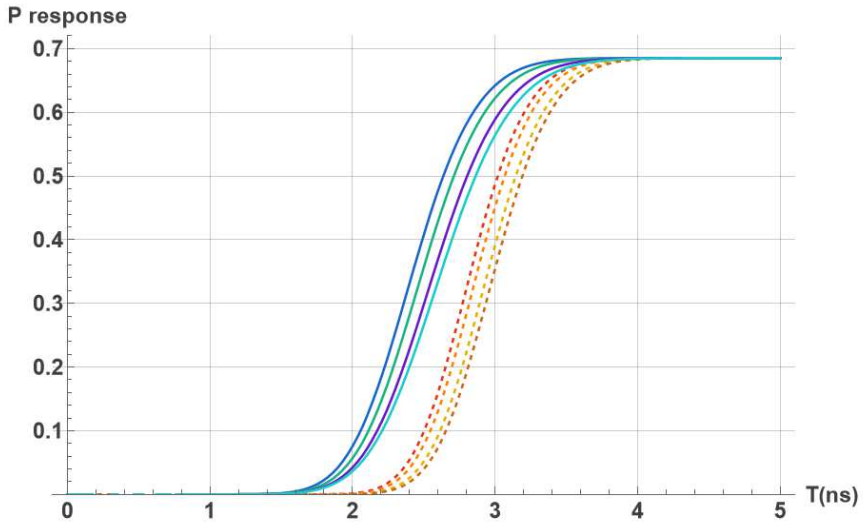


Fig. 2 The probability of excitation of the measuring qubit. The signal states are shown as solid lines (blue for $|H\rangle$, teal for $|V\rangle$, purple for $|D\rangle$, cyan for $|A\rangle$) and the decoy states as dashed lines (red for $|H\rangle$, orange for $|V\rangle$, yellow for $|D\rangle$, brown for $|A\rangle$), respectively.

Figure 3 presents the discrimination probability P_{discrim} after the QND interaction as a function of the distance z at which the QND module is placed. Three curves are shown, corresponding to interaction times $\tau = 1, 3, 5$ ns. The lower bound of $\tau = 1$ ns is chosen because shorter interaction times yield insufficient phase accumulation to resolve the temporal profiles of the signal and decoy states, rendering the QND measurement ineffective. The upper bound of $\tau = 5$ ns is set by Bob's detection window: interaction times beyond this limit risk exceeding the typical gate duration

of single-photon detectors, so that the QND module would begin to alter the temporal structure of the pulses within Bob's acceptance window.

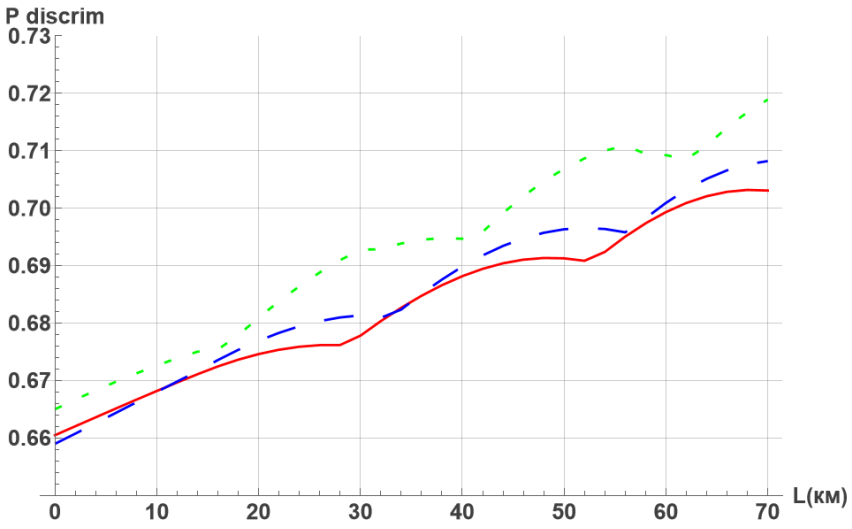


Fig. 3 The probability of distinguishing signal states from decoy states after QND interaction. Three curves are shown, corresponding to interaction times $\tau = 1, 3, 5$ ns (red solid, blue dashed, and green dotted, respectively).

5 Security Analysis

The standard GLLP formula for the secure key rate (per pulse) in the asymptotic limit reads

$$R \geq \frac{1}{2}\big[Q_1\big(1 - h_2(e_1)\big) - Q_\mu\, f\, h_2(E_\mu)\big],$$

where Q_μ is the overall gain for signal pulses — the probability that Bob detects a signal when Alice sends a pulse of intensity μ, E_μ is the corresponding bit error rate on Bob's side, Q_1 is the single-photon gain, e_1 is the single-photon error rate, $h_2(\cdot)$ is the binary entropy function, and $f = 1.2$ is the error-correcting codes efficiency factor Babukhin and Sych (2024).

To assess the impact of the non-ideal QND attack on the secure key rate, we evaluate the key generation rate within the standard GLLP model Gottesman et al. (2004), with parameters modified to account for the effects of the QND interaction.

1. **Modified gain.** The QND module introduces additional photon loss. The probability that a photon survives the QND interaction and is subsequently detected by Bob is obtained from the post-interaction density matrix. The modified gains are

computed using the three-component photon-number decomposition:

$$Q_\mu = p_{\mathrm{vac},S}\, Y_0 + p_{1,S}\, Y_1 + p_{m,S}\, Y_2,$$

$$Q_\nu = p_{\mathrm{vac},D}\, Y_0 + p_{1,D}\, Y_1 + p_{m,D}\, Y_2,$$

where $p_{\mathrm{vac},S}$, $p_{1,S}$, and $p_{m,S}$ are the probabilities of zero, one, and multiple ($k \geq 2$) photons in the signal state after the QND interaction, extracted from the diagonal elements of the reduced photon-number density matrix $\rho^{(\mathrm{ph})}_{\mathrm{int},S}$:

$$p_{1,S} = \big[\rho^{(\mathrm{ph})}_{\mathrm{int},S}\big]_{11}, \qquad p_{\mathrm{vac},S} = \big[\rho^{(\mathrm{ph})}_{\mathrm{int},S}\big]_{22}, \qquad p_{m,S} = \big[\rho^{(\mathrm{ph})}_{\mathrm{int},S}\big]_{33}.$$

The probabilities for the decoy state, $p_{\mathrm{vac},D}$, $p_{1,D}$, and $p_{m,D}$, are extracted analogously from $\rho^{(\mathrm{ph})}_{\mathrm{int},D}$. Here $Y_k = 1 - (1 - Y_0)(1 - \eta)^k$ is the conditional detection probability for a k-photon state, $\eta = \eta_{\mathrm{total}} = \eta_{\mathrm{det}}\, \eta_{\mathrm{channel}}$ is the overall efficiency, $Y_0 = 10^{-6}$ is the dark-count probability, and $\eta_{\mathrm{channel}} = 10^{-\alpha L/10}$ with $\alpha = 0.2\,\mathrm{dB/km}$. For the multi-photon component we use Y_2 as the worst-case (lowest) detection probability among all $k \geq 2$ states.

2. **Modified error rate.** The QND interaction degrades the polarization states, introducing an additional error contribution. The polarization fidelity after the interaction is evaluated by projecting the post-QND polarization density matrix onto the ideal state:
$$P^{(k)}_{\mathrm{pol}} = \mathrm{Tr}\big[\rho^{(k)}_{\mathrm{pol}}\, |\psi_k\rangle\langle\psi_k|\big],$$
where $\rho^{(k)}_{\mathrm{pol}}$ is the polarization matrix of the k-th state after the QND interaction. The mean polarization fidelity over the four states is $\bar{P}_{\mathrm{pol}}$, and the additional polarization error is $e_{\mathrm{pol}} = 1 - \bar{P}_{\mathrm{pol}}$. The combined error is
$$e_{\mathrm{opt}} = e_{\mathrm{det}} + e_{\mathrm{pol}} - 2\, e_{\mathrm{det}}\, e_{\mathrm{pol}},$$
which accounts for two independent sources of bit-flip errors: the baseline detector error $e_{\mathrm{det}} = 0.01$ and the polarization-induced error e_{pol}. The total error rates for signal and decoy pulses are
$$E_\mu Q_\mu = e_0 Y_0 + e_{\mathrm{opt}}\big(p_{1,S}\, \eta + p_{m,S}\, (1 - (1 - \eta)^2)\big),$$
$$E_\nu Q_\nu = e_0 Y_0 + e_{\mathrm{opt}}\big(p_{1,D}\, \eta + p_{m,D}\, (1 - (1 - \eta)^2)\big),$$
where $e_0 = 0.25$ is the error rate for dark counts, $\eta = \eta_{\mathrm{total}}$ is the overall channel efficiency, $p_{1,S}$ and $p_{m,S}$ are the single-photon and multi-photon probabilities in the signal state, and $p_{1,D}$, $p_{m,D}$ are the corresponding probabilities in the decoy state. The term $p_1\, \eta$ is the single-photon detection probability, while $p_m\, (1 - (1 - \eta)^2)$ is the multi-photon detection probability evaluated for $k = 2$ as a conservative upper bound.
3. **Inclusion of temporal side-channel.** Beyond the direct loss and polarization effects, the QND measurement enables Eve to partially distinguish signal from decoy states via their temporal distributions. This information leakage is quantified

by the fidelity between the post-interaction temporal density matrices of signal and decoy states. For a given pair of states (k_S, k_D) sharing the same polarization basis, the temporal fidelity is $F = \left(\mathrm{Tr}\sqrt{\sqrt{\rho}\,\sigma\sqrt{\rho}}\right)^2$.

The average fidelity $\bar{F}_{SD}$ over the four basis states yields the QND-induced distinguishability parameter

$$\delta = \frac{1}{2}\left(1 - \sqrt{\bar{F}_{SD}}\right).$$

This parameter quantifies the fraction of single-photon events that can no longer be reliably assigned to either the signal or the decoy intensity class. Following the approach of Babukhin and Sych (2024), the upper bound on the single-photon error rate is further relaxed to

$$e = e_1 + 4(1-\Delta)\Delta(1-2e_1) + 4(1-2\Delta)\sqrt{\Delta(1-\Delta)e_1(1-e_1)},$$

where $\Delta = \delta/Y_L$, and e_1 is the theoretical error from eavesdropping incorporated into the single-photon error of the decoy-state method.

Figure 4 shows the secure key rate R as a function of distance, computed using the GLLP formula with parameters modified to account for the QND-induced loss and polarization errors.

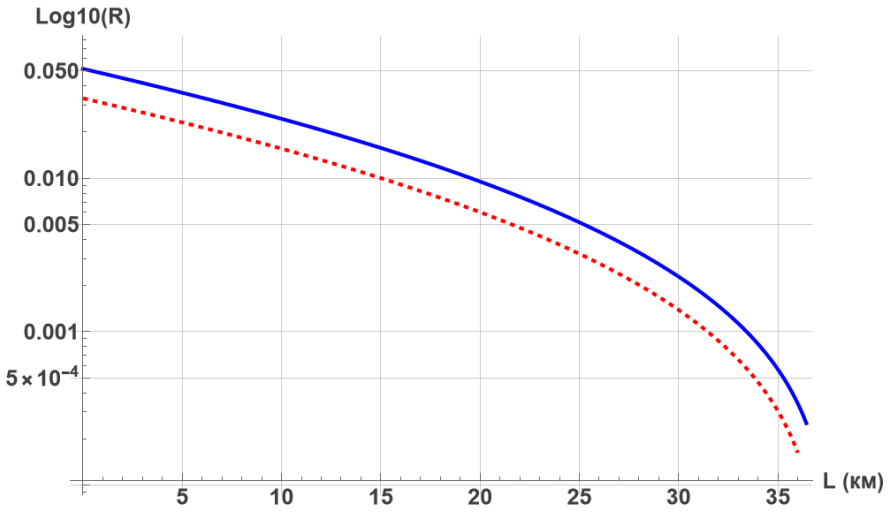


Fig. 4 The secure key rate is plotted against transmission distance for the QND temporal attack with Eve's optimal strategy, QND (red dashed) and for the case where state groups are distinguished by the maximum likelihood method (blue solid), respectively.

6 Conclusion

The maximum-likelihood discrimination probability of signal and decoy pulses at the fiber output after 60 km of standard single-mode fiber reaches $P_{\text{discrim}} \approx 0.68$, significantly exceeding the random-guessing baseline of 0.5 and indicating the vulnerability of the decoy-state method. At the distance of 60 km, the discrimination probability after the QND interaction reaches its maximum, ranging from $P_{\text{discrim}} \approx 0.70$ for $\tau = 1\,\text{ns}$ to $P_{\text{discrim}} \approx 0.71$ for $\tau = 5\,\text{ns}$. At short distances (< 5 km), the discrimination probability is nearly independent of τ, with all curves clustered near 0.66–0.67. As the distance increases, the spread among the curves widens, indicating that the choice of interaction time becomes increasingly consequential. The QND measurement improves Eve's discrimination capability, although photon loss and polarization rotation within the QND module partially offset this gain.

The nonlinear behavior of the curves shown in Fig. 3 distinguishing the two groups of states arises from the nonlinear interaction of chromatic dispersion and polarization-mode dispersion. These two effects, which are of a different physical nature, manifest themselves at different transmission distances, with the strength of their impact varying nonlinearly, so that their combined influence leads to the observed deviations from linearity. Thus, the resulting shape of the curves is determined by the cumulative effect contributed by each type of dispersion and by their complex interplay as the distance changes.

The secure key rate as a function of distance is shown in Fig. 4. The blue curve lies consistently above the red curve by a factor of 1.5–2 in the absolute key rate. Beyond 30 km, both curves drop to zero and exhibit the same cutoff distance. This indicates that the two methods differ only in overall efficiency while sharing the same noise resilience. It is precisely this factor-of-1.5–2 gap between the curves that constitutes the security breach of the protocol.

The results of this work demonstrate that the temporal side channel poses a measurable threat to the security of the decoy-state BB84 protocol. An eavesdropper equipped with a realistically imperfect QND measurement module can achieve a discrimination probability significantly above the random-guessing baseline, compromising the central assumption of the decoy-state method and reducing the secure key rate.

It should be emphasized that the present analysis is a theoretical exploration of the vulnerability, and several idealizations remain. The QND architecture, while based on experimentally demonstrated building blocks, has not been realized as a complete, field-deployable device. Nevertheless, the mere existence of a physically motivated attack pathway—without the need for a perfect QND measurement—indicates that the temporal degree of freedom of photonic qubits deserves more attention in security proofs. At the same time, this work establishes a concrete theoretical framework—including a channel model, a discrimination procedure, and modified GLLP formulae—that can be applied to quantify temporal side-channel leakage in practical QKD systems.

Declarations

Funding. No funds, grants, or other support was received. **Competing interests.** The authors have no relevant financial or non-financial interests to disclose. **Ethics approval and consent to participate.** Not applicable. **Consent for publication.** Not applicable. **Data availability.** Not applicable. **Materials availability.** Not applicable. **Code availability.** Not applicable. **Author contribution.** All authors contributed to the study conception and design. Material preparation, data collection and analysis were performed by A. S. Kalashnikova and D. V. Sych. All authors read and approved the final manuscript.

References

Arnold, C., Demory, J., Loo, V., Lemaître, A., Sagnes, I., Glazov, M., Krebs, O., Voisin, P., Senellart, P., Lanco, L.: Macroscopic rotation of photon polarization induced by a single spin. Nat. Commun. **6**, 6236 (2015) https://doi.org/10.1038/ncomms7236

Agrawal, G.P.: Fiber-Optic Communication Systems, 5th edn. Wiley, Hoboken, NJ (2021)

Arnardottir, K.B.: Cavity QED effects in low dimensional systems. PhD thesis, Nanyang Technological University, Singapore (2018). https://doi.org/10.32657/10356/75866

Bennett, C.H., Brassard, G.: Quantum cryptography: Public key distribution and coin tossing. Theoretical Computer Science **560**, 7–11 (2014) https://doi.org/10.1016/j.tcs.2014.05.025 . Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84

Brennecke, F., Donner, T., Ritter, S., Bourdel, T., Köhl, M., Esslinger, T.: Cavity qed with a bose–einstein condensate. Nature **450**(7167), 268–271 (2007) https://doi.org/10.1038/nature06120

Besse, J.-C., Gasparinetti, S., Collodo, M.C., Walter, T., Kurpiers, P., Pechal, M., Eichler, C., Wallraff, A.: Single-shot quantum nondemolition detection of individual itinerant microwave photons. Physical Review X **8**(2) (2018) https://doi.org/10.1103/physrevx.8.021003

Brune, M., Haroche, S., Lefevre, V., Raimond, J.M., Zagury, N.: Quantum nondemolition measurement of small photon numbers by rydberg-atom phase-sensitive detection. Phys. Rev. Lett. **65**, 976–979 (1990) https://doi.org/10.1103/PhysRevLett.65.976

Blais, A., Huang, R.-S., Wallraff, A., Girvin, S.M., Schoelkopf, R.J.: Cavity quantum electrodynamics for superconducting electrical circuits: An architecture for quantum computation. Physical Review A **69**(6) (2004) https://doi.org/10.1103/physreva.69.062320

Babukhin, D.V., Sych, D.V.: Joint eavesdropping on the BB84 decoy state protocol with an arbitrary passive light-source side channel. Lobachevskii Journal of Mathematics **45**(6), 2454–2465 (2024) https://doi.org/10.1134/S1995080224602753

Dong, H., Gong, Z.R., Ian, H., Zhou, L., Sun, C.P.: Intrinsic cavity qed and emergent quasinormal modes for a single photon. Physical Review A **79**(6) (2009) https://doi.org/10.1103/physreva.79.063847

Duplinskiy, A., Sych, D.: Bounding passive light-source side channels in quantum key distribution via hong-ou-mandel interference. Phys. Rev. A **104**, 012601 (2021) https://doi.org/10.1103/PhysRevA.104.012601

Guerlin, C., Bernu, J., Deléglise, S., Sayrin, C., Gleyzes, S., Kuhr, S., Brune, M., Raimond, J.-M., Haroche, S.: Progressive field-state collapse and quantum non-demolition photon counting. Nature **448**(7156), 889–893 (2007) https://doi.org/10.1038/nature06057

Gerhardt, I., Liu, Q., Lamas-Linares, A., Skaar, J., Kurtsiefer, C., Makarov, V.: Full-field implementation of a perfect eavesdropper on a quantum cryptography system. Nature Communications **2**(1) (2011) https://doi.org/10.1038/ncomms1348

Gottesman, D., Lo, H.-K., Lutkenhaus, N., Preskill, J.: Security of quantum key distribution with imperfect devices. In: International Symposium onInformation Theory, 2004. ISIT 2004. Proceedings., p. 136 (2004). https://doi.org/10.1109/ISIT.2004.1365172

Grangier, P., Levenson, J.A., Poizat, J.-P.: Quantum non-demolition measurements in optics. Nature **396**(6711), 537–542 (1998) https://doi.org/10.1038/25059

Gisin, N., Ribordy, G., Tittel, W., Zbinden, H.: Quantum cryptography. Rev. Mod. Phys. **74**, 145–195 (2002) https://doi.org/10.1103/RevModPhys.74.145

Hwang, W.-Y.: Quantum key distribution with high loss: Toward global secure communication. Phys. Rev. Lett. **91**, 057901 (2003) https://doi.org/10.1103/PhysRevLett.91.057901

Ilchenko, V.S., Gorodetsky, M.L., Yao, X.S., Maleki, L.: Microtorus:a high-finesse microcavity with whispering-gallery modes. Opt. Lett. **26**(5), 256–258 (2001) https://doi.org/10.1364/OL.26.000256

Lindblad, G.: On the generators of quantum dynamical semigroups. Communications in Mathematical Physics **48**(2), 119–130 (1976) https://doi.org/10.1007/BF01608499

Lamas-Linares, A., Kurtsiefer, C.: Breaking a quantum key distribution system through a timing side channel. Opt. Express **15**(15), 9388–9393 (2007) https://doi.org/10.1364/OE.15.009388

Lo, H.-K., Ma, X., Chen, K.: Decoy state quantum key distribution. Phys. Rev. Lett. **94**, 230504 (2005) https://doi.org/10.1103/PhysRevLett.94.230504

Lydersen, L., Wiechers, C., Wittmann, C., Elser, D., Skaar, J., Makarov, V.: Hacking commercial quantum cryptography systems by tailored bright illumination. Nature Photonics **4**(10), 686–689 (2010) https://doi.org/10.1038/nphoton.2010.214

Miller, A.: Micius, the world's first quantum communication satellite, was hackable. In: 2025 International Conference on Quantum Communications, Networking, and Computing (QCNC), pp. 411–415 (2025). https://doi.org/10.1109/QCNC64685.2025.00070

Reiserer, A., Rempe, G.: Cavity-based quantum networks with single atoms and optical photons. Rev. Mod. Phys. **87**, 1379–1418 (2015) https://doi.org/10.1103/RevModPhys.87.1379

Sathyamoorthy, S.R., Tornberg, L., Kockum, A.F., Baragiola, B.Q., Combes, J., Wilson, C.M., Stace, T.M., Johansson, G.: Quantum nondemolition detection of a propagating microwave photon. Physical Review Letters **112**(9) (2014) https://doi.org/10.1103/physrevlett.112.093601

Wang, X.-B.: Beating the photon-number-splitting attack in practical quantum cryptography. Phys. Rev. Lett. **94**, 230503 (2005) https://doi.org/10.1103/PhysRevLett.94.230503

Weier, H., Krauss, H., Rau, M., Fürst, M., Nauerth, S., Weinfurter, H.: Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors. New Journal of Physics **13**(7), 073024 (2011) https://doi.org/10.1088/1367-2630/13/7/073024