Security
of Infocommunication Systems
and Internet of Things

2026 Vol 4, No 1

https://doi.org/10.31861/sisiot2026.1.01021

Received 10 June 2026; revised 24 June 2026; accepted 27 June 2026; published 30 June 2026

Implementation Security of Practical Decoy-State QKD: A Dynamic Source-Deviation Model

Maksym Danyliuk[1,*] and Yuliya Tanasyuk[2]

[1]Department of Radio Engineering and Information Security, Yuriy Fedkovych Chernivtsi National University, Chernivtsi, Ukraine
[2]Department of Computer Systems and Networks, Yuriy Fedkovych Chernivtsi National University, Chernivtsi, Ukraine

*Corresponding author (E-mail: danyliuk.maksym.i@chnu.edu.ua)

ABSTRACT This paper develops a theoretical model for source-side implementation security in practical decoy-state quantum key distribution (QKD). The research object is a weak-coherent-pulse transmitter in which the emitted mean photon number is affected not only by the selected decoy setting, but also by semiconductor-laser dynamics, electrical drive response, intensity-modulator memory, residual optical effects, and slow drift. The transmitter is described at two modelling levels. The first layer is a nonlinear continuous-time carrier-photon-phase model used to explain physical mechanisms. The second layer is a pulse-indexed validation surrogate obtained by sampling the emitted pulse train under a declared operating regime and stroboscopic extraction rule. This distinction avoids treating a local discrete model as a globally valid replacement for nonlinear gain-switched laser dynamics. The model maps the selected intensity sequence to the actual pulse mean photon number, defines an operational memory length, and introduces vacuum-safe deviation metrics, residual-correlation diagnostics, conditional intensity laws, and photon-number probability intervals. These quantities are explicitly distinguished from composable security parameters. The security interpretation is an assumption audit: if the emitted intensity or phase statistics are history dependent, the standard decoy-state reduction to setting-independent photon-number yields and error rates is no longer automatic. The proposed framework therefore does not claim a new complete QKD security proof; it identifies measurable source quantities that must be exported to an appropriate finite-key or imperfect-source proof. The result is a mathematically traceable bridge between transmitter dynamics, source validation, and implementation-security requirements for practical decoy-state QKD systems. The objective of this paper is to develop a mathematically traceable dynamic source-deviation model for practical decoy-state QKD transmitters and to show how transmitter memory affects the assumptions used in decoy-state security analysis.

KEYWORDS QKD, decoy-state, implementation security, source memory, laser dynamics.

I. INTRODUCTION

Decoy-state QKD was introduced to make weak coherent laser sources usable in practical BB84 systems despite photon-number-splitting attacks [1-3]. Its central idea lies at the protocol level: Alice (the sender) randomly varies the source intensity and uses the observed gains and error rates at different intensities to estimate the contribution of single-photon pulses. This idea is powerful, but it is valid only relative to a source model. In practical high-speed transmitters, that source model is not merely a static Poissonian light source followed by attenuation. The laser, electrical driver, intensity modulator, timing electronics, and thermal environment form a dynamical transmitter system whose memory can affect the emitted pulse sequence [4-7].

This paper studies the implementation-security consequence of these transmitter dynamics. The objective of this paper is to develop a mathematically traceable dynamic source-deviation model for practical decoy-state QKD transmitters and to show how transmitter memory affects the assumptions used in decoy-state security analysis. To achieve this objective, the paper addresses the following tasks: formalizing the ideal decoy-state source assumptions; connecting semiconductor-laser and transmitter dynamics with the emitted pulse mean photon number; defining an operational memory length and diagnostic deviation metrics for source validation; and identifying proof-compatible quantities that must be bounded when emitted intensity or phase statistics are history dependent. The theoretical research object is a prepare-and-measure decoy-state QKD transmitter emitting phase-randomized weak coherent pulses with nominal intensity labels $u_k \in \{s, d, v\}$, where s denotes a signal setting, d – a weak-decoy setting, and v – a vacuum or near-vacuum setting. The input to the model is the selected intensity sequence together with physical transmitter parameters, drive waveforms, or measured pulse traces. The output is the actual pulse mean photon number μ_k, its history dependence, and validation quantities that indicate which assumptions of a standard decoy-state proof must be replaced by implementation-specific bounds.

The contribution is neither a new attack nor a complete finite-key security proof. It is a dynamic source-deviation model. The model connects semiconductor-laser rate equations to emitted pulse energy, defines a pulse-to-pulse sampled transition map, introduces a local state-space surrogate for validation, and shows how history-dependent photon-number probabilities weaken ideal decoy-state assumptions. The aim is to provide an explicit modelling chain from physical source characterization to proof-compatible quantities such as an operational correlation range, conditional intensity distributions, photon-number probability intervals, and phase-randomization bounds.

II. DECOY-STATE SOURCE ASSUMPTIONS AND IMPLEMENTATION PROBLEM

The usual decoy-state model begins with a phase-randomized weak coherent pulse [1-3]. If the intended mean photon number is a, phase randomization makes the optical state diagonal in the photon-number basis,

$$\rho_a = \sum_{n=0}^{\infty} p_n(a)|n\rangle\langle n|, \qquad p_n(a) = e^{-a}\frac{a^n}{n!} \tag{1}$$

For a finite set of intensity labels, Alice records the selected label, but Eve (eavesdropper) should not be able to distinguish a signal-labelled n-photon pulse from a decoy-labelled n-photon pulse except through the photon number itself. Under this same-n indistinguishability condition, the observed gain and error gain satisfy Eqs. (2) and (3):

$$Q_a = \sum_n p_n(a) Y_n, \tag{2}$$

$$E_a Q_a = \sum_n p_n(a) e_n Y_n \tag{3}$$

Here Y_n is the conditional detection probability for an n-photon pulse and e_n is the corresponding error probability. Eqs. (2) and (3) are the mathematical reason decoy-state estimation works: the coefficients $p_n(a)$ change with intensity, while the unknowns Y_n and e_n are shared across intensities [2-3].

The implementation assumptions behind this linear structure are stronger than they may look. The emitted mean photon number must be known or bounded for every intensity setting. Phase randomization must be adequate; otherwise, the Poisson mixture model is not justified. Side-channel degrees of freedom of an n-photon pulse must not reveal whether the pulse came from the signal or decoy setting. Standard finite-key sampling arguments also require independence or a proof-compatible treatment of correlations. Imperfect-source and finite-size analyses show that these details are part of the source model rather than cosmetic hardware details [8].

A static calibration of the average signal and decoy intensities is therefore insufficient when the actual pulse energy depends on recent history. The ideal source assumption is

$$\mu_k = \mu_{u_k} \tag{4}$$

In a physical transmitter, the actual value may be affected by previous settings and hidden source states. A decoy pulse following several signal pulses may have a different energy from a decoy pulse following several vacuum pulses. The nominal label u_k is then not enough to determine the photon-number distribution. This is the implementation problem addressed below.

III. DYNAMIC SOURCE-DEVIATION MODEL

A. Continuous physical model. A directly driven single-mode semiconductor laser can be represented by nonlinear rate equations for carrier density $N(t)$, photon density $S(t)$, and, when phase behaviour is relevant, optical phase $\phi(t)$. With gain compression and Langevin noise terms, a convenient model [9] is

$$\frac{dN}{dt} = \frac{I(t)}{qV} - \frac{N}{\tau_n} - \frac{g(N-N_0)}{1+\epsilon S}S + F_N(t), \tag{5}$$

$$\frac{dS}{dt} = \Gamma\frac{g(N-N_0)}{1+\epsilon S}S - \frac{S}{\tau_p} + \Gamma\beta\frac{N}{\tau_n} + F_S(t), \tag{6}$$

$$\frac{d\phi}{dt} = \frac{\alpha}{2}\left[\Gamma g(N-N_0) - \frac{1}{\tau_p}\right] + F_\phi(t) \tag{7}$$

The variables and parameters have their standard meanings: $I(t)$ is the injection current, q – the elementary charge, V – the active volume, τ_n – the carrier lifetime, τ_p – the photon lifetime, Γ – the optical confinement factor, β – the spontaneous-emission coupling factor, g – the differential gain, N_0 – the transparency carrier density, ϵ – the gain-compression parameter, and α – the linewidth-enhancement factor. The stochastic terms model spontaneous-emission seeding, amplitude jitter, and phase diffusion.

The phase equation is included only to mark the boundary of the intensity-memory model. Residual cavity photons do not by themselves imply failure of a protocol. Their relevance is narrower: if the optical phase is not sufficiently randomized under the declared operating conditions, the emitted pulses are not exactly described by the phase-randomized weak-coherent-state mixture in Eq. (1), and an imperfect-phase-randomization proof or additional source bound is required [6-7].

B. From waveform to pulse mean photon number. For decoy-state analysis, the relevant scalar observable is the emitted mean photon number per pulse. Let t_k be the trigger time of the k-th pulse, and T_p – the integration gate. The output pulse energy and mean photon number are

$$E_k^{\text{out}} = \int_{t_k}^{t_k+T_p} P_{\text{out}}(t)\,dt, \tag{8}$$

$$\mu_k = \frac{E_k^{\text{out}}}{h\nu} \tag{9}$$

If photon density is used directly, then

$$\mu_k = \eta_{\text{ext}} C_S \int_{t_k}^{t_k+T_p} S(t)\,dt, \tag{10}$$

where C_S is the proportionality constant between photon density and output power, and η_{ext} includes attenuation and external optical losses. In an externally modulated transmitter, the corresponding expression is given by

$$\mu_k = \frac{\eta_{\text{ext}}}{h\nu}\int_{t_k}^{t_k+T_p} T_{\text{IM}}(t;u_k,x_k)P_{\text{LD}}(t)\,dt \tag{11}$$

Eq. (11) makes explicit that the protocol label u_k first enters the physical drive or modulator waveform. Thus, the modelling chain is as follows: $u_k \to I(t)$ or $T_{\text{IM}}(t) \to P_{\text{out}}(t) \to \mu_k$. The same scalar μ_k is later used in the decoy-state photon-number distribution.

C. Exact sampled transition map and local discrete surrogate. The transmitter is modelled at two distinct levels. Eqs. (5, 6), and (7) form the continuous-time

physical mechanism model. Source validation, however, works with pulse-indexed data. For a fixed clock period T and a fixed stroboscopic extraction rule S, the continuous dynamics induce an exact sampled map:

$$\begin{aligned} x_{k+1} &= F_S(x_k, u_k) + w_k, \\ \mu_k &= H_S(x_k, u_k) + \zeta_k \end{aligned} \tag{12}$$

Here x_k denotes the hidden transmitter state at the chosen sampling event. It may include residual carrier state, electrical or modulator-memory state, slow thermal state, and residual optical-field variables. The functions F_S and H_S are generally nonlinear and may depend on the operating regime and sampling rule.

The discrete linear model used in this paper is introduced only after Eq. (12), as a local validation-level surrogate of the sampled nonlinear map. Around a declared operating trajectory (x_k^0, u_k^0), the deviations are defined as $\delta x_k = x_k - x_k^0$, $\delta\mu_k = \mu_k - \mu_k^0$ and $\delta u_k = u_k - u_k^0$. A first-order approximation gives

$$\delta x_{k+1} = A_k \delta x_k + B_k \delta u_k + w_k, \tag{13}$$

$$\delta\mu_k = C_k \delta x_k + D_k \delta u_k + \zeta_k \tag{14}$$

A time-invariant form is acceptable only if the fitted Jacobians are approximately constant over the declared operating regime:

$$\begin{aligned} \delta x_{k+1} &= A\delta x_k + B\delta u_k + w_k, \\ \delta\mu_k &= c^T \delta x_k + d\delta u_k + \zeta_k \end{aligned} \tag{15}$$

This model is not asserted to be a globally valid replacement for nonlinear gain-switching dynamics. If one matrix pair is too coarse across signal, decoy, and vacuum settings, a switched-affine or nonlinear surrogate should be used. The scientific role of Eq. (15) is to represent measurable pulse-to-pulse memory while preserving μ_k as the output quantity used in source validation.

D. History-dependent source map and operational memory length. The practical source map is given as

$$\mu_k = \mu(u_k, u_{k-1}, \dots, u_{k-L}; \theta_k), \tag{16}$$

where θ_k represents hidden transmitter states, such as carrier recovery, electrical waveform tails, modulator bias memory, thermal drift, stochastic noise, or residual optical-field effects. The memory length L should not be interpreted as a claim that physical memory is exactly finite. It is an operational truncation length under a declared operating regime, tolerance, and confidence level.

Let $h_k^{(\ell)}$ denote the most recent ℓ-pulse history, while g and g' denote two possible older histories. Define $\Delta_{\mathrm{TV}}(\ell)$ as the maximum total-variation distance between the conditional intensity laws obtained when the recent ℓ-pulse history is fixed and only the older history is changed:

$$\Delta_{\mathrm{TV}}(\ell) = \max d_{\mathrm{TV}}\left(F_{u,h,g}^{(\ell)}, F_{u,h,g'}^{(\ell)}\right).$$

Then a distributional operational memory length is

$$L_{\mathrm{op}}(\varepsilon_{\mathrm{mem}}, \delta_{\mathrm{mem}}) = \min\{\ell : \Delta_{\mathrm{TV}}(\ell) \le \varepsilon_{\mathrm{mem}}\} \tag{17}$$

with confidence of at least $1 - \delta_{\mathrm{mem}}$ on the declared operating set. If only conditional means are available, the distributional criterion can be replaced by a weaker mean-based dependence measure:

$$\Delta_\mu(\ell) = \max\left|\mathbb{E}\left[\mu_k \mid u, h^{(\ell)}, g\right] - \mathbb{E}\left[\mu_k \mid u, h^{(\ell)}, g'\right]\right|$$

The corresponding mean-based operational memory length is then defined as

$$L_\mu(\varepsilon_\mu, \delta_\mu) = \min\{\ell : \Delta_\mu(\ell) \le \varepsilon_\mu\} \tag{18}$$

with confidence of at least $1 - \delta_\mu$ on the declared operating set.

For a fitted stable linear surrogate satisfying $\| A^j \| \le Kr^j$ with $0 < r < 1$, a sufficient design rule is to choose L as the smallest integer for which $Kr^L \le \varepsilon_{\mathrm{dyn}}$. This is a model-based shortcut, not a substitute for validation from data.

E. Linearized memory estimation. For small deviations around calibrated intensities, a first-order predictive memory model can be used as a diagnostic:

$$\mu_k = \mu_{u_k} + \sum_{j=1}^{L} \alpha_j \psi_{k-j} + \xi_k \tag{19}$$

The predictors ψ_{k-j} should be centered setting variables or centered nominal intensities rather than raw labels. Let y collect the measured deviations $\mu_k - \mu_{u_k}$, and A_{reg} contain the past predictors, the least-squares estimate is as follows

$$\begin{aligned} y &= A_{\mathrm{reg}}\alpha + \xi, \\ \hat{\alpha} &= \left(A_{\mathrm{reg}}^T A_{\mathrm{reg}}\right)^{-1} A_{\mathrm{reg}}^T y \end{aligned} \tag{20}$$

provided that $A_{\mathrm{reg}}^T A_{\mathrm{reg}}$ is nonsingular; otherwise, a pseudoinverse or regularized estimator should be used.

The coefficients α_j characterize a local predictive kernel, not a security parameter. Confidence intervals should account for serial dependence in ξ_k, for example through block resampling or a dependence-robust covariance estimate. Structured residuals indicate that a longer history, nonlinear terms, setting-pair terms, or conditional distributions are needed.

As summarized in Fig. 1, the linearized memory model is not the physical laser model itself; it is a pulse-indexed validation surrogate fitted after the emitted pulse-mean sequence has been extracted from the transmitter dynamics.

IV. SOURCE-DEVIATION METRICS AND PARAMETER ESTIMATION

The model produces a sequence of actual mean photon numbers. The following quantities are diagnostic statistics for source validation. They summarize deviation and memory but do not by themselves establish a composable security guarantee.

A. Vacuum-safe intensity deviation. For non-vacuum settings, the relative deviation can be defined with a calibration floor $\tau > 0$:

$$\varepsilon_k^{(\tau)} = \frac{|\mu_k - \mu_{u_k}|}{\max(\mu_{u_k}, \tau)} \tag{21}$$

For the non-vacuum settings,

$$V_{\mathrm{nonvac}} = \max_{k : u_k \in \mathcal{U}_+} \varepsilon_k^{(\tau)} \tag{22}$$

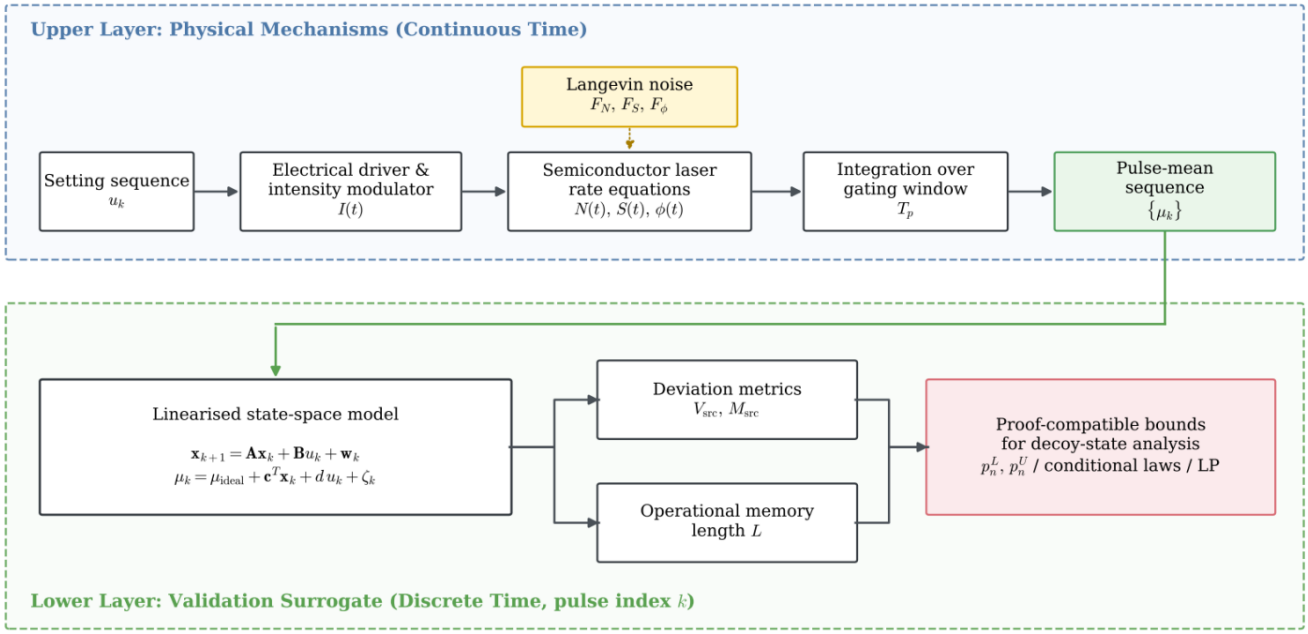

FIG. 1. Two-layer modelling chain for dynamic source-deviation analysis in practical decoy-state QKD. The upper layer represents continuous-time transmitter mechanisms that map the selected setting sequence to the emitted pulse-mean sequence. The lower layer represents the pulse-indexed validation surrogate that converts the emitted sequence into deviation metrics, operational memory length, and proof-compatible bounds for decoy-state security analysis.

For a vacuum or near-vacuum setting, relative error is not meaningful. The corresponding diagnostic should be absolute:

$$V_{\text{vac}} = \max_{k:u_k=v} \mu_k \tag{23}$$

If an outlier-sensitive maximum is unsuitable for a measurement campaign, the same definitions can be replaced by one-sided confidence bounds or conditional quantiles under each setting and history class.

B. Residual memory diagnostics. Autocorrelation should not be computed directly on raw μ_k, because the raw sequence contains deliberate decoy modulation. The residuals are defined as

$$r_k = \mu_k - \hat{m}\left(u_k, h_k^{(m)}\right), \tag{24}$$

where $\hat{m}$ is either a setting-only empirical mean or a fitted short-history conditional mean. The residual autocorrelation at phase lag j is

$$\hat{\rho}_r(j) = \frac{\sum_{k=j+1}^{N}(r_k - \bar{r})\,(r_{k-j} - \bar{r})}{\sum_{k=1}^{N}(r_k - \bar{r})^2} \tag{25}$$

An aggregate residual memory diagnostic over the operational window L is

$$M_{\text{src}} = \sum_{j=1}^{L} |\hat{\rho}_r(j)| \tag{26}$$

This diagnostic is useful for detecting leftover serial dependence after known setting structure has been removed. It is not sufficient for security, because two sources with similar autocorrelation may have different conditional intensity laws.

C. Aggregate engineering score. For hardware comparison one may define

$$D_{\text{src}} = w_1 V_{\text{nonvac}} + w_2 M_{\text{src}} + w_3 V_{\text{vac}}, \quad w_i \geq 0 \tag{27}$$

The weights are engineering choices. D_{src} is a summary index for monitoring and design comparison, not a composable security parameter. Its correct role is to trigger a more precise source-characterization step.

D. Conditional intensity laws and photon-number intervals. The proof-facing validation object is the conditional law of the emitted mean photon number,

$$F_{u,h}(m) := P(\mu_k \leq m \mid u_k = u, h_k = h) \tag{28}$$

The induced photon-number probability is then a mixed-Poisson law given by Eq. (29).

$$p_n(u,h) = \int_0^\infty e^{-\mu}\frac{\mu^n}{n!}\, dF_{u,h}(\mu) \tag{29}$$

If source characterization provides only an interval $I_{u,h} = \left[\underline{\mu}(u,h), \overline{\mu}(u,h)\right]$, conservative bounds are

$$\underline{p}_n(u,h) = \inf_{\mu \in I_{u,h}} e^{-\mu}\frac{\mu^n}{n!}, \tag{30}$$

$$\overline{p}_n(u,h) = \sup_{\mu \in I_{u,h}} e^{-\mu}\frac{\mu^n}{n!} \tag{31}$$

Because $e^{-\mu}\mu^n/n!$ is unimodal in μ, the extrema are obtained at interval endpoints and, for the upper bound, also at $\mu = n$ when n lies inside the interval. These bounds are suitable outputs of the validation layer; the security proof must determine how they enter the final key analysis.

E. Numerical validation workflow. In the absence of device-specific calibration data, this paper does not present numerical results. A scientifically grounded validation workflow would proceed as follows: define the continuous source model and operating regime; simulate or measure the pulse train under randomized decoy sequences; extract μ_k by the declared integration rule; fit the local pulse-to-pulse surrogate; examine residuals; estimate L, V_{nonvac}, V_{vac}, and M_{src}; construct $F_{u,h}$ or interval bounds; and

export photon-number probability bounds to the chosen proof framework. Any further simulation should label parameters as device-specific, literature-based illustrative, or dimensionless sensitivity parameters.

V. SECURITY INTERPRETATION FOR DECOY-STATE QKD

In the ideal model, the photon-number probability in round k depends only on the selected intensity label:

$$P(n \mid u_k = a) = e^{-\mu_a} \frac{\mu_a^n}{n!} \tag{32}$$

For the special case in which the emitted mean photon number is deterministic conditional on the selected setting and recent history, the photon-number probability becomes

$$P(n \mid u_k = a, h_k = h) = e^{-\mu(a,h)} \frac{[\mu(a,h)]^n}{n!} \tag{33}$$

If residual conditional intensity fluctuations remain, the mixed-Poisson representation in Eq. (29) should be used instead.

The security implication is an assumption audit. Standard decoy-state formulas rely on source conditions under which observed detection statistics can be decomposed into photon-number contributions with setting-independent, or otherwise proof-compatible, single-photon parameters. If transmitter dynamics make μ_k depend on recent history, the usual reduction to common Y_n and e_n is not automatic, because pulses carrying the same photon number n may still be distinguishable through intensity, phase, temporal profile, or other degrees of freedom.

The ideal Eqs. (2) and (3) must therefore be replaced, at the validation interface, by history-conditioned relations of the form

$$Q_{a,h} = \sum_n p_n(a,h) Y_{n,a,h}, \tag{34}$$

$$E_{a,h} Q_{a,h} = \sum_n p_n(a,h) e_{n,a,h} Y_{n,a,h} \tag{35}$$

Eqs. (34) and (35) are not presented here as a new security proof. They show where the standard assumptions are weakened. An appropriate proof may use conservative photon-number intervals, conditional intensity laws, overlap or fidelity bounds, phase-randomization quality parameters, or other source-characterization data. The diagnostic quantities V_{nonvac}, V_{vac}, M_{src}, and D_{src} are therefore not inserted directly into a key-rate formula. They must first be translated into proof-compatible bounds [4-7].

For phase randomization, the same discipline applies. Residual intracavity photons or insufficient phase diffusion do not imply automatic key compromise. They indicate that the emitted pulse train may not be exactly diagonal in the photon-number basis under the standard abstraction. If phase is relevant, the validation output should include a bound on the conditional phase distribution or an equivalent proof-facing parameter [6-7].

VI. COUNTERMEASURES AND VALIDATION REQUIREMENTS

The model suggests that countermeasures should be evaluated dynamically, not only through static optical power calibration. Source monitoring can estimate pulse energy before the quantum channel and detect drift, abnormal correlations, or history-dependent deviations. The monitor must itself be calibrated and bounded; otherwise, it remains an informal diagnostic rather than proof evidence.

Transmitter design should also reduce pattern effects. Electrical pre-emphasis, bandwidth-aware waveform shaping, stable modulator bias control, and architectures with stationary operating points can reduce dependence of current pulse energy on previous settings. The dynamic model provides a common comparison basis through μ_k, V_{nonvac}, V_{vac}, M_{src}, conditional intensity laws, and photon-number intervals.

If correlations cannot be made negligible, the next step is a correlation-aware parameter-estimation procedure. The validation report should state the declared operating envelope, sampling rule, calibration uncertainty, estimated memory length, residual-correlation results, conditional intensity intervals, and phase-randomization evidence where applicable. Standards facing documentation should connect those source-characterization artefacts to the security proof and module protection claims [10-11].

VII. DISCUSSION

The novelty of the proposed model is its traceability chain. Existing proof frameworks already contain several local abstractions: finite-key decoy-state bounds, imperfect-source models, phase-randomization bounds, correlation ranges, conditional distributions, overlap or fidelity constraints, and certification evidence. This paper does not replace those results. Instead, it organizes the corresponding validation quantities around a hardware-grounded dynamic source object: a transmitter whose emitted mean photon number and possibly phase statistics are functions of recent setting history and hidden physical state.

The model is intentionally limited. It focuses on source intensity memory in practical decoy-state QKD. Phase and leakage are discussed as extensions because they interact with the same source model, but the paper does not attempt to provide a complete multi-mode side-channel proof. It also does not claim that any single diagnostic score determines the final secret-key length. These quantities are useful only after translation into proof-compatible bounds.

The next stage of this research is numerical and experimental validation. A numerical study should simulate or identify the sampled transition map under a declared operating regime, fit the memory kernel, and compare conditional intensity distributions against static calibration. An experimental study should use calibrated pulse traces to estimate the same quantities with confidence intervals. A later security-rate-cost study could compare hardware improvements, monitoring precision, proof penalties, and final key rate, but such trade-off curves are not the core theoretical claim of this article.

VIII. CONCLUSION

This study developed a dynamic source-deviation model for practical decoy-state QKD transmitters and established a method for representing source memory at the interface between hardware validation and security analysis. The proposed model shows that a practical

transmitter cannot always be treated as a static Poissonian source with fixed calibrated intensities. When semiconductor-laser dynamics, modulator memory, residual optical effects, or drift make the emitted mean photon number dependent on recent settings, the source model required by standard decoy-state analysis must be checked dynamically.

The main result of the study is a two-layer modelling framework for dynamic source-deviation analysis in practical decoy-state QKD. The nonlinear carrier-photon-phase equations describe the physical origin of source dynamics, while the sampled pulse-to-pulse map and its local validation surrogate provide a practical way to estimate memory from measured or simulated pulse traces. This separation is useful because it avoids treating a local discrete approximation as a complete physical model, while still producing quantities that can be used in implementation assessment.

The introduced operational memory length, vacuum-safe deviation measures, residual-correlation diagnostics, conditional intensity laws, and photon-number probability intervals form a validation interface between transmitter characterization and security proofs. Rather than directly proving composable secrecy, the primary significance of these results lies in determining which source parameters must be bounded before applying a finite-key or imperfect-source proof to a physical device.

From the implementation-security perspective, the model clarifies why static optical-power calibration is insufficient for high-speed decoy-state QKD transmitters. Dynamic source characterization can reveal history-dependent deviations that may weaken the usual assumption of setting-independent photon-number yields and error rates. Therefore, practical QKD security should include not only protocol level analysis, but also documented validation of transmitter memory, phase-randomization quality, and conditional photon-number probability bounds. Future research should apply the proposed framework to numerical simulations and calibrated pulse-trace measurements, followed by integration of the obtained bounds into an appropriate finite-key security analysis.

AUTHOR CONTRIBUTIONS

M.D. – mathematical modelling, literature analysis, conceptualization, methodology, formal analysis, resources, investigation, validation, writing-original draft preparation, visualization; Y.T. – conceptualization, methodology, validation, writing-review and editing, supervision.

COMPETING INTERESTS

The authors declare no conflict of interest.

REFERENCES

[1] W.-Y. Hwang, “Quantum key distribution with high loss: Toward global secure communication,” *Phys. Rev. Lett.*, vol. 91, no. 5, Art. no. 057901, 2003. doi: 10.1103/PhysRevLett.91.057901.

[2] H.-K. Lo, X. Ma, and K. Chen, “Decoy state quantum key distribution,” *Phys. Rev. Lett.*, vol. 94, no. 23, Art. no. 230504, 2005. doi: 10.1103/PhysRevLett.94.230504.

[3] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, “Practical decoy state for quantum key distribution,” *Phys. Rev. A*, vol. 72, no. 1, Art. no. 012326, 2005. doi: 10.1103/PhysRevA.72.012326.

[4] V. Zapatero, A. Navarrete, K. Tamaki, and M. Curty, “Security of quantum key distribution with intensity correlations,” *Quantum*, vol. 5, Art. no. 602, 2021. doi: 10.22331/q-2021-12-07-602.

[5] X. Sixto, V. Zapatero, and M. Curty, “Security of decoy-state quantum key distribution with correlated intensity fluctuations,” *Phys. Rev. Appl.*, vol. 18, no. 4, Art. no. 044069, 2022. doi: 10.1103/PhysRevApplied.18.044069.

[6] S. Nahar, T. Upadhyaya, and N. Lütkenhaus, “Imperfect phase randomization and generalized decoy-state quantum key distribution,” *Phys. Rev. Appl.*, vol. 20, no. 6, Art. no. 064031, 2023. doi: 10.1103/PhysRevApplied.20.064031.

[7] A. Marcomini, G. Currás-Lorenzo, D. Rusca, A. Valle, K. Tamaki, and M. Curty, “Characterising higher-order phase correlations in gain-switched laser sources with application to quantum key distribution,” *EPJ Quantum Technol.*, vol. 12, Art. no. 38, 2025. doi: 10.1140/epjqt/s40507-025-00340-7.

[8] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, “Secure quantum key distribution with realistic devices,” *Rev. Mod. Phys.*, vol. 92, no. 2, Art. no. 025002, 2020. doi: 10.1103/RevModPhys.92.025002.

[9] L. A. Coldren, S. W. Corzine, and M. L. Mašanović, *Diode Lasers and Photonic Integrated Circuits*, 2nd ed. Hoboken, NJ, USA: Wiley, 2012. doi: 10.1002/9781118148167.

[10] European Telecommunications Standards Institute, *Quantum Key Distribution (QKD); Security Proofs*, ETSI GS QKD 005 V1.1.1, Dec. 2010.

[11] European Telecommunications Standards Institute, *Quantum Key Distribution (QKD); Common Criteria Protection Profile—Pair of Prepare and Measure Quantum Key Distribution Modules*, ETSI GS QKD 016 V2.1.1, Jan. 2024.

Maksym Danyliuk

Ph.D. student in Radio Engineering at the Department of Radio Engineering and Information Security of Physical, Technical and Computer Sciences Institute, Yurii Fedkovych Chernivtsi National University, Ukraine. Research interests and professional activities are as follows: cybersecurity, cyber-physical systems, microcontrollers, IoT, software development, mathematical modeling.

ORCID ID: 0009-0005-8583-0437

Yuliya Tanasyuk

Ph.D., associate professor at the Department of Computer Systems and Networks of Physical, Technical and Computer Sciences Institute, Yuriy Fedkovych Chernivtsi National University, Ukraine. Research interests and academic activities are as follows: programming, network information technologies, cybersecurity, IoT, software engineering.

ORCID ID: 0000-0001-8650-0521

Безпека реалізації практичного QKD з decoy-state протоколом: динамічна модель відхилень джерела

Максим Данилюк[1,*], Юлія Танасюк[2]

[1]Кафедра радіотехніки та інформаційної безпеки, Чернівецький національний університет імені Юрія Федьковича, Чернівці, Україна
[2]Кафедра комп'ютерних систем та мереж, Чернівецький національний університет імені Юрія Федьковича, Чернівці, Україна

*Автор-кореспондент (Електронна адреса: danyliuk.maksym.i@chnu.edu.ua)

АНОТАЦІЯ У цій роботі розроблено теоретичну модель безпеки реалізації на стороні джерела у практичних системах квантового розподілу ключів (QKD) зі станами-приманками (decoy-state). Об'єктом дослідження є передавач на основі слабких когерентних імпульсів, у якому випромінюване середнє число фотонів залежить не лише від обраного налаштування стану-приманки, але й від динаміки напівпровідникового лазера, відгуку електричного драйвера, пам'яті модулятора інтенсивності, залишкових оптичних ефектів та повільного дрейфу. У статті моделювання передавача розглядається на двох рівнях. Перший рівень – це нелінійна неперервна у часі модель «носії-фотони-фаза», яка використовується для пояснення фізичних механізмів. Другий рівень – це сурогатна модель валідації з індексацією імпульсів, отримана шляхом дискретизації послідовності випромінюваних імпульсів за визначеного режиму роботи та стробоскопічного правила вилучення. Таке розмежування дозволяє уникнути розгляду локальної дискретної моделі як глобально адекватної заміни нелінійної динаміки лазера з модуляцією підсилення. Модель відображає обрану послідовність інтенсивностей на фактичне середнє число фотонів в імпульсі, визначає операційну довжину пам'яті, а також уводить метрики відхилень, безпечні для вакууму, діагностику залишкової кореляції, умовні закони інтенсивності та інтервальні оцінки ймовірностей числа фотонів. Ці величини чітко відокремлені від компонованих (composable) параметрів безпеки. Інтерпретація безпеки є аудитом припущень: якщо статистика випромінюваної інтенсивності або фази залежить від передісторії, стандартне зведення станів-приманок до незалежних від налаштувань виходів фотонів та рівнів помилок більше не є автоматичним. Таким чином, запропонована структура не претендує на нове повне доведення безпеки QKD; вона визначає вимірювані характеристики джерела, які необхідно передати у відповідне доведення для скінченних ключів або недосконалих джерел. Результатом є математично простежуваний зв'язок між динамікою передавача, валідацією джерела та вимогами до безпеки реалізації для практичних систем QKD зі станами-приманками. Метою цієї статті є розробка математично простежуваної динамічної моделі відхилень джерела для практичних передавачів QKD зі станами-приманками та демонстрація того, як пам'ять передавача впливає на припущення, що використовуються в аналізі безпеки станів-приманок. Для досягнення цієї мети вирішено такі завдання: формалізовано припущення щодо ідеального джерела станів-приманок; пов'язано динаміку напівпровідникового лазера та передавача з середнім числом фотонів випромінюваного імпульсу; визначено операційну довжину пам'яті та діагностичні метрики відхилень, придатні для валідації джерела; а також визначено сумісні з доведенням безпеки величини, які необхідно обмежити, коли статистика випромінюваної інтенсивності або фази залежить від передісторії.

КЛЮЧОВІ СЛОВА QKD, decoy-state, безпека реалізації, пам'ять джерела, динаміка лазера.