Machinery & Energetics
Vol. 16, No. 4. 2025

Journal homepage:
https://technicalscience.com.ua/en

UDC 621.39:003.5
DOI: 10.31548/machinery/4.2025.09

Ihor Limar*
PhD in Technical Sciences, Senior Lecturer
State University of Intelligent Technologies and Telecommunications
65023, 1 Kuznechna Str., Odesa, Ukraine
Engineering and Technology Institute "Biotekhnika" of the National Academy of Agrarian Sciences of Ukraine
67667, 26 Mayakska Road Str., Khlibodarske village, Ukraine
https://orcid.org/0000-0002-8972-9935

Yevhen Sevastieiev
Master, Senior Lecturer
State University of Intelligent Technologies and Telecommunications
65023, 1 Kuznechna Str., Odesa, Ukraine
https://orcid.org/0000-0003-1165-1119

Quantum cryptography: Theoretical foundations and practical implementations for the protection of critical infrastructure

Abstract. The purpose of the article was to theoretically determine harmonised criteria for the applicability of quantum key distribution for the protection of critical infrastructure, taking into account the long-term risk of decryption by adversaries possessing quantum computational resources and traffic archiving capabilities. The methodology relied on a theoretical systems analysis of three Quantum Key Distribution subsystems – sources, detectors, and channels (fibre/free space) – complemented by simplified models of the link budget and bit error probability. A concise scenario analysis was conducted for banking networks, energy systems, and government communications, taking into account scalability, compatibility, and cost. The main results showed that laser intensity stability of 1-2% and higher detector efficiencies – 60-70% for Avalanche Photodiodes and 80-90% for Superconducting Nanowire Single-Photon Detectors – extended practical distances and reduced errors. Without trusted nodes in fibre, 150-200 km was achievable; for urban Free-Space Optics lines, 5-20 km was optimal, while longer distances required network segmentation or satellite segments. Architecturally, it was justified that: for banks – rings with trusted nodes and Free-Space Optics reserve; for energy systems – dual fibre channels "control centre-substation" with a local key cache; for government communications – segmented domains with interagency gateways and satellite redundancy. In all scenarios, a Quantum Key Distribution+Post-Quantum Cryptography hybrid with short key rotation and operational countermeasures against attacks on detectors and channels was appropriate, confirming practical suitability for urban and regional networks. The practical significance lay in providing engineering teams in banking, energy, and government communications with ready-made architectural profiles – from rings and dual fibre channels to segmented domains – with Key Management System/Hardware Security Module integration, definition of Service Level Objective/Service Level Agreement, and phased roadmaps. For regulators and operators, this formed a basis for updating requirements and audits, as well as for planning redundancy (Free-Space Optics/satellite) and Total Cost of Ownership categories

Keywords: key distribution; laser sources; photonic detectors; optical fibre; free-space communication; trusted nodes; banking networks

INTRODUCTION

Relevance was driven by the need of critical infrastructure for service continuity, strict timing guarantees, and fault tolerance. Banking systems required secure scalable channels between data centres, processing nodes, and branches; the energy sector required low latency between control centres and substations; government communications

Article's History: Received: 01.08.2025; Revised: 03.11.2025; Accepted: 27.11.2025.

Suggested Citation:
Limar, I., & Sevastieiev, Ye. (2025). Quantum cryptography: Theoretical foundations and practical implementations for the protection of critical infrastructure. *Machinery & Energetics,* 16(4), 9-20. doi: 10.31548/machinery/4.2025.09.

*Corresponding author

required intercity and interagency routes with redundancy and access segmentation. Against the backdrop of the long-term "store now – decrypt later" risk, interest in quantum key distribution (QKD) as a physically grounded complement to classical cryptography was growing, although deployment was complicated by channel losses, atmospheric factors, network heterogeneity, and requirements for interagency key management.

The reviewed studies systematised two main families of QKD protocols – prepare-and-measure and entanglement-based – in discrete-variable and continuous-variable implementations, focusing on the relationship between acceptable Quantum Bit Error Rate (*QBER*) levels and the secret rate on the one hand and source and detector parameters on the other. The works emphasised the criticality of intensity and frequency stability, jitter, background radiation levels, quantum efficiency, dark counts, and recovery time, as well as the role of synchronisation and correct calibration of polarisation/phase. The meta-review by L. Gyongyosi *et al.* (2019) additionally emphasised the importance of decoy states, Measurement-Device-Independent/Device-Independent (MDI/DI) settings, and finite-key corrections for network scenarios, but mostly in general terms, without deriving unified engineering criteria for specific classes of critical infrastructure and without a holistic comparison of technical requirements with architectural and economic constraints.

A separate body of work devoted to modelling the Bennett-Brassard 1984 (BB84) protocol detailed the impact of channel losses, background events, basis mismatch, the choice of timing-window width, discrimination thresholds, gating and filtering parameters on the secret rate, the intrusion-detection threshold, and achievable distance. In a number of studies, including T.-T. Nguyen *et al*. (2023), practical approaches were proposed for tuning receiver paths for fibre and Free-Space Optics (FSO) links, forming a basis for technical and technological recommendations. At the same time, existing models typically considered isolated configurations or laboratory conditions, accounted only limitedly for hybrid topologies combining fibre, FSO, and satellite segments, integration with key-management systems and Service Level Objective/Service Level Agreement (SLO/SLA) requirements, and almost did not propose harmonised suitability criteria specifically for banking networks, energy systems, and government communications. This structural limitation delineated the problem space for further research.

Reviews of 6G and URLLC services highlighted the fundamental need to combine physically protected key distribution with post-quantum cryptography (PQC), and to embed crypto functions into Software-Defined Networking/Network Functions Virtualisation (SDN/NFV) architectures with separation of control/user planes and strict latency budgets under Precision Time Protocol/Synchronous Ethernet (PTP/SyncE). However, cross-sector reviews lacked domain-specific, quantitative criteria for critical infrastructure – banking networks, energy, and government communications – tied to target SLOs and component parameters. The study by M. Hoschek (2021) emphasised slice isolation, distributed key caches, and telemetry for SLA control, but did not establish a direct link between telemetry and the link budget and secret rate, nor with orchestration of Key Management System/Hardware Security Module (KMS/HSM) under specific time budgets. The work by D. Rahmayanti (2025) outlined the applicability of QKD in 5G/6G transport with account taken of radio and FSO channels, showing "windowed" availability due to turbulence, precipitation, and daytime illumination and justifying spatial-spectral filtering, adaptive apertures, auto-tracking, and route redundancy, but did not reduce these factors to unified suitability and life-cycle cost profiles for specific domains.

S. Rajpoot *et al*. (2023) systematised requirements for trusted-node networks and highlighted trade-offs between route length, key rotation, and acceptable *QBER*, but without SLO-oriented integration with SDN/NFV and without comparing fibre/FSO/satellite hybrids specifically for critical-infrastructure tasks. The review by I.B. Djordjevic (2022) substantiated layered complementarity of the physical layer, QKD, and PQC with Perfect Forward Secrecy (PFS) support and KMS/HSM integration, but left open the numerical norms for components and the direct impact on ηtot, *QBER*, and achievable SLOs in applied scenarios. Results by P. Dharanish *et al*. (2024) demonstrated the viability of Field-Programmable Gate Array (FPGA) implementations of PQC (acceleration of KEM and signatures), but did not define policies for allocating quantum keys between flows with different latency requirements and session lifetimes.

Practical countermeasures proposed by C.-L. Chen *et al*. (2025) – Quantum Random Number Generator (QRNG), decoy states, active monitoring of sources and detectors, checks against blinding attacks – were not tied to standardised telemetry thresholds and the impact on SLO/Total Cost of Ownership (TCO) under operational conditions. Thus, the existing literature set out principles (QKD + PQC hybrid, SDN/NFV manageability, trusted-node topologies, "windowed" FSO/satellite operation), but did not form a unified, quantitatively defined, domain-oriented set of criteria. The article proposed to close this gap: to normalise source and detector parameters and synchronisation requirements, to build suitability maps for fibre, FSO, and satellite channels, to define SLO classes and TCO profiles for three domains, and to determine orchestration policies for KMS/HSM and quantum-key allocation in the QKD + PQC hybrid with account taken of latency budgets and traffic prioritisation.

The problem space, therefore, lay in the absence of a harmonised systematisation of requirements for components and channels with a direct linkage to banking networks, energy-system control, and government communications, as well as in the shortage of theoretical compatibility and cost models that allow comparison of integration options at the architectural level.

The purpose of the study was to form a systemic framework for evaluating the feasibility of implementing QKD in three typical critical-infrastructure scenarios – banking networks, energy-system control, and government communications – taking into account scalability requirements, integration with fibre, free-space, and satellite channels, and full life-cycle costs. The research hypothesis was that integrating physically grounded key distribution with key life-cycle management and compatible transport infrastructure would provide a practically suitable level of security, fault tolerance, and scalability over urban and regional distances without unacceptable costs.

MATERIALS AND METHODS

The study was purely theoretical in nature and was based on a systems analysis of three classes of QKD subsystems: radiation sources, photonic detectors, and quantum communication channels. For sources, intensity and frequency stability, polarisation constancy, timing jitter, and background radiation were considered; for detectors – quantum efficiency, dark count rate, dead time, and timing jitter; for channels – the loss budget and fluctuations. Closed-form estimates of the link budget and errors were used: optical losses in fibre were modelled as (formula 1):

$$A(d) = \alpha_f d + A_{conn}\,, \tag{1}$$

where α_f – fibre-specific loss (dB/km); d – route length (km); A_{conn} – total losses at connectors/splices (dB). Analysis: increasing d or α_f linearly increases attenuation, compressing the achievable range; a large A_{conn} creates a "fixed penalty" even on short spans. Typically, $\alpha_f \approx$ 0.17-0.25 dB/km; each connector adds ≈0.2-0.5 dB. Total transmission (formula 2):

$$\eta_{tot} = \eta_{src} \times 10^{-\frac{A}{10}} \times \eta_{det}, \tag{2}$$

where η_{src} – the useful fraction of the photon flux from the source (accounts for intensity/polarisation stability); $10^{-A/10}$ – the channel transmission fraction, which depends on attenuation A; η_{det} – detector quantum efficiency. Analysis: a decline in due to intensity/polarisation fluctuations, or an increase in A, exponentially reduces η_{tot}; increasing η_{det} (APD ≈ 0.6-0.7; SNSPD ≈0.8-0.9) directly raises the probability of useful events and "compensates" for part of the channel loss. The approximate bit error was evaluated by formula (3).

$$BER \approx \frac{p_{dc} + e_{mis} p_{sig}}{p_{sig} + p_{dc}}, \tag{3}$$

where p_{sig} – the probability of detecting a useful signal per pulse; p_{dc} – the probability of dark counts (detector noise); e_{mis} – the fraction of errors due to basis/alignment mismatch (polarisation, timing windows, phase shifts). Analysis: a decrease in p_{sig} (due to low η_{tot}) or an increase in p_{dc} raises *QBER*; reducing emis through polarisation/phase stabilisation and timing-window optimisation directly reduces *QBER*. For CV-QKD, increased phase noise effectively increased emis through quadrature imbalance; active phase locking reduced this contribution. For DV-QKD, "decoy" intensities were taken into account; for CV-QKD – SNR of homodyne/heterodyne measurement and phase stability. Parameters were varied within practical intervals aligned with industry practice, and the output metrics were achievable distance, secret key rate, and *QBER*. No physical experiments were performed; no equipment list was provided.

Assumptions for detectors were as follows: APDs operated in Geiger mode with active gating (windows 0.5-1.5 ns, dead time 50-100 ns, jitter 50-80 ps), and discrimination thresholds were selected by the criterion of minimising total error. SNSPDs were considered in continuous counting mode (without gating) with efficiency 0.8-0.9, dark-count rate ⩽10^1 cps, and typical receiver windows of 0.1-0.3 ns. These modes fixed the initial conditions for calculating p_{sig}, *QBER*, and the secret rate. For each applied domain (banking networks, energy systems, government communications), a set of candidate topologies and integration policies (TLS/IPsec, KMS/HSM, PQC hybrids) was preliminarily formed, target SLOs for availability/latency were set, and deployment staging was fixed. For banking profiles, ring schemes with trusted nodes and an FSO reserve were considered; QKD keys were assigned to short-lived TLS/IPsec sessions with PFS for critical flows, while mass channels were protected by PQC, with mandatory integration with KMS/HSM. For trunks, a fibre + LEO/MEO satellite-link hybrid with key buffering and route redundancy was assumed. Fault-tolerance requirements were implemented through two physically independent routes (fibre + FSO or two fibres from different operators) combined with a path-diversity policy at the level of network management.

Comparative modelling was performed for three transport classes: point-to-point fibre segments without trusted nodes, fibre networks with trusted nodes/key routing, and free-space (FSO) links, as well as the combination with satellite segments. For fibre, an exponential attenuation law (via α_f) with additional connector losses was applied; for FSO – windowed availability models taking into account turbulence, precipitation, and background illumination; for satellite links – pointing geometry and atmospheric losses with time "visibility windows". For each configuration, the following were evaluated: (1) indicative secret-key rate (orders of magnitude), (2) probability of meeting target SLOs for availability, (3) sensitivity to degradation of component parameters. Topological analysis covered rings and stars with trusted nodes, fibre + FSO hybrids, and inclusion of satellite segments for intercity routes. The obtained estimates served as the basis for distance ranges, availability indicators, and key-rate profiles, subsequently summarised in results tables. First, p_{sig} and *QBER* were obtained from the link budget and configurations without a positive secret rate were filtered out. For suitable variants, the secret-key rate was calculated and binned by order of magnitude: kbit/s, 10 kbit/s, 100+ kbit/s. Availability (SLO) was classified by classes: A ⩾ 99.99%, B = 99.95-99.99%, C = 99.9-99.95%, D = 99.0-99.9%, E<99.0%. Sensitivity was determined under parameter variations of ±10% or +1 dB to losses: low – ⩽10% rate drop; medium – 10-30%; high – >30% or loss of a positive

secret rate. For further calculations, normalised ranges of source, detector, and synchronisation parameters were fixed (intensity, polarisation, linewidth, detection efficiency, dark counts, dead time, jitter, timing windows, and monitoring). The bounds were selected with account taken of practical intervals: intensity stability ⩽1-2% RMS, polarisation stability ⩾25-30 dB, APD efficiency 60-70% and SNSPD 80-90%, dark counts for APD ⩽10^2-10^3 cps and for SNSPD ⩽10^1 cps, typical timing windows 0.2-1.0 ns. The stated intervals were used as input constraints in all link-budget models, η_{tot}/*QBER* calculations, and scenario comparisons of channels and topologies. Parameterisation covered the following subsystems and protocols: laser source for DV-QKD (BB84 with "decoy" intensities), local oscillator for CV-QKD (GMCS); APD detectors for DV-QKD and SNSPD detectors for DV and CV implementations; synchronisation subsystems for DV-QKD (BB84 + decoy, MDI), for CV-QKD (GMCS), and for entanglement-based variants (E91/BBM92); monitoring subsystems for DV-QKD (BB84 + decoy, MDI), CV-QKD (GMCS), and entanglement-based (E91/BBM92). All listed components were included in the link-budget calculations, ηtot estimates, *QBER*, and secret-key rate.

Scenario analysis was conducted for three applied critical-infrastructure domains: banking networks, energy-system control, and government communications. For each scenario, architectural profiles were formed: recommended topology; integration with classical protocols (Transport Layer Security (TLS) and Internet Protocol Security (IPsec)), KMS/HSM and PQC hybrids; requirements for latency, availability, and fault tolerance; a phased deployment plan. Hybrid trunk: fibre – the primary transport; LEO/MEO satellite links – reserve/bridge for intercity sections with "windowed" availability. Quantum-key exchange was performed opportunistically, key material was buffered in edge KMS/HSM with lifetime limits and used to bridge pauses between "windows". Route redundancy ensured path diversity under SDN control, with automatic switching to an alternative path (fibre priority). Compatibility was assessed at the network level (SDN/NFV manageability, Wavelength-Division Multiplexing (WDM) coexistence for Continuous-Variable Quantum Key Distribution (CV-QKD), optical isolation for Discrete-Variable Quantum Key Distribution (DV-QKD)) and at the application level (key life-cycle policies, rotation frequency, PFS). For DV-QKD with "decoy" intensities, automated calibration of the "signal/decoy" power ratio and continuous monitoring of parasitic ASE with pre-set alert thresholds were envisaged; procedures were performed at initialisation and periodically during the session for timely recalibration. The economic component was implemented as a structured TCO model: Capital Expenditures (CapEx) (optics, detectors, satellite inserts), Operating Expenditures (OpEx) (calibration, monitoring, audit), integration costs (KMS/HSM, node upgrades), staff training, and risk costs. Threat modelling was also carried out: attacks on measurement modules (blinding, timing shifts), "Trojan" injections, store-now/decrypt-later with the use of quantum memory. For each threat, technical (MDI/DI) paradigms, power/spectrum monitoring, randomised window sampling), organisational (HSM, domain segmentation, audit), and operational countermeasures were defined, as well as residual risk. The combination of the stated methods directly produced the normalised component ranges, channel suitability maps, and applied profiles.

RESULTS

Systematised quality criteria for sources and detectors

For radiation sources, it was established that intensity stability within ⩽1-2% RMS over the operating interval and linear polarisation stability of no worse than 25-30 dB ensured reproducibility of state encoding in prepare-and-measure protocols. For discrete-variable implementations with decoy intensities, automated calibration of power ratios and monitoring of parasitic amplified spontaneous emission (ASE) background radiation with alert thresholds were recommended. In continuous-variable (CV-QKD) implementations, stability of the local-oscillator phase and low source phase noise were critical; within the study, normalisation was adopted at the level of a narrow frequency band (a few hundred kHz) for sources aligned with local oscillators.

For detectors, it was established that detection efficiency ⩾60-70% for avalanche photodiodes (APD) in Geiger mode and ⩾80-90% for superconducting nanowire single-photon detectors (SNSPD) substantially reduced requirements for channel length or intensity. In parallel, lower bounds for dark counts in the range ⩽10^2-10^3 cps for APD and ⩽10^1 cps for SNSPD reduced the contribution to *QBER* and increased the usable key-sifting rate. Dead time ⩽50-100 ns for APD and ⩽20-50 ns for SNSPD, and jitter ⩽50-80 ps, were defined as practical reference points for urban and regional profiles. In Table 1, the recommended parameter ranges for sources, detectors, and synchronisation were systematised (intensity, polarisation, linewidth, efficiency, dark counts, dead time, jitter, timing windows, and monitoring).

Table 1. Recommended parameter ranges for sources and detectors

Subsystem	Protocol/class	Key parameters	Recommended range/note
Source (laser)	DV-QKD (BB84 + decoy)	Intensity stability (RMS)	⩽1-2% over the session interval
		Linear polarisation	Stability ⩾25-30 dB
		Linewidth	Narrow (hundreds of kHz) for stable interference
Source (local oscillator)	CV-QKD	Phase noise	Low: σφ⩽0.1-0.2 rad; SSB PN ⩽-90/-120/-140 dBc/Hz @10 kHz/100 kHz/⩾1 MHz; Δν⩽100-300 kHz; active phase locking
		Relative intensity noise	Minimisation of ASE, real-time monitoring: C-band ±1-1.5 nm from the carrier (windows 0.2-0.4 nm ≈ 25-50 GHz); RIN 10 kHz-20 MHz

Continued Table 1.

Subsystem	Protocol/class	Key parameters	Recommended range/note
Detector (APD)	DV-QKD	Detection efficiency	⩾60-70% (near-IR)
		Dark counts	⩽10^2-10^3 cps; active gating
		Dead time / jitter	⩽100 ns/⩽80 ps
Detector (SNSPD)	DV/CV	Detection efficiency	⩾80-90%
		Dark counts	⩽10^1 cps
		Dead time / jitter	⩽50 ns/⩽50 ps
Synchronisation	DV-QKD (BB84 + decoy, MDI); CV-QKD (GMCS); Entanglement-based (E91/BBM92)	Coincidence window	Tunable, optimisation for SNR and *QBER*: 0.2-1.0 ns (APD 0.5-1.5 ns; SNSPD 0.1-0.3 ns)
Monitoring	DV-QKD (BB84 + decoy, MDI); CV-QKD (GMCS); Entanglement-based (E91/BBM92)	Security parameters	Detection of blinding, "Trojan" injections, afterpulsing: power threshold -35...-25 dBm; out-of-band monitoring ±2-5 nm (windows 0.2-0.4 nm); tail monitoring 0.1-10 μs (APD 1-10 μs; SNSPD ⩽0.5 μs)

Note: low local-oscillator phase noise: $\sigma\varphi \leqslant 0.1$-$0.2$ rad (RMS, band 1 kHz-10 MHz); SSB PN ⩽ -90 dBc/Hz @ 10 kHz, ⩽-120 dBc/Hz @ 100 kHz, ⩽-140 dBc/Hz @⩾1 MHz; source/LO linewidth $\Delta\nu \leqslant 100$-300 kHz; residual phase-tracker error ⩽ 5-10° (RMS). Active phase locking – mandatory. near-IR – near-infrared

Source: compiled by the authors based on D.V. Reddy *et al.* (2020), Y. Shao *et al.* (2021), C. Yu *et al.* (2024)

For DV-QKD, intensity stability at the level of ⩽1-2% RMS preserved the correctness of selecting "decoy" intensities and reduced statistical biases; deterioration to ~3-5% increased the conservatism of intrusion estimation and reduced the secret rate in weak-signal regimes. Linear polarisation stability of around 25-30 dB ensured selectivity in the bases, whereas ≈20 dB already noticeably increased *QBER* due to degraded orthogonality. For CV-QKD, low local-oscillator phase noise and active locking maintained the SNR of homodyne/heterodyne measurement; without these measures, quadrature variance increased, and the secret rate fell under an unchanged loss budget. Detector efficiency remained key: approximately 60-70% for APD and 80-90% for SNSPD increased the registration probability and "absorbed" several decibels of additional loss; a decrease by ~10 pp reduced the practical range by tens of kilometres. Limiting dark counts (on the order of 10^2-10^3 cps for APD and 10^1 cps for SNSPD) reduced the background contribution to *QBER*; exceeding these levels required either narrowing timing windows with the risk of losing useful events, or reducing the sifting rate, which directly reduced the key rate. Within detector dynamics, dead time and jitter should be kept at the level of "tens of nanoseconds" and "tens of picoseconds" respectively, so as not to limit pulse rate and the accuracy of time correlation. The defined reference points were integrated into acceptance-testing procedures: verification of intensity stability under thermal fluctuations, analysis of dark counts with temperature taken into account, assessment of afterpulsing, and modelling of blinding and "Trojan" injections. For timely detection of degradation, telemetry was applied at a rate of at least 1 Hz for sources and 10-100 Hz for detectors, ensuring continuity of critical-infrastructure services.

Attenuation *A(d)* increased linearly with length and the number of connections; an increase of +1 dB reduced the transmission fraction 10-A/10 by approximately 20%, and even a small fixed penalty A_{conn} substantially limited the operating range. Converting attenuation into the channel transmission fraction and then accounting for source and detector efficiencies showed that an additional 1-2 dB of loss reduced η_{tot} by ≈18-36%, with ηtot scaling proportionally with η_{src} and η_{det}. Transitioning from APD to SNSPD increased path efficiency by on the order of 15-30% under otherwise equal conditions. *QBER* estimation revealed that reducing p_{sig} as a result of increasing total channel attenuation A to ≳ 15-20 dB (e.g., 80-120 km of fibre with $\alpha_f \approx 0.2$ dB/km plus 6-8 connectors of 0.2-0.5 dB) or even adding +1...+2 dB to the baseline directly increased the error rate, because ηtot ∝ 10-A/10 decreased by ≈18-36% and the relative contribution of dark counts p_{dc} increased. By contrast, reducing emis through polarisation/phase stabilisation and timing-window optimisation (approximately 0.2-1.0 ns) consistently decreased *QBER* by several percentage points. In CV-QKD, increased phase noise raised effective e_{mis}, but active phase locking recovered part of the operating region in range; in DV-QKD, the use of "decoy" intensities stabilised estimates of p_{sig} in weak-signal regimes and maintained a positive secret rate on longer links. Configurations with above-threshold *QBER* were removed from further comparisons, which explains the reduction of usable range in high-loss scenarios. Sensitivity analysis identified critical points at which an additional connector (~0.2-0.5 dB) triggered a transition from a positive to a zero-secret rate; increasing η_{src} and η_{det} partly compensated fibre losses, reduced *QBER*, and extended the operating range without increasing source power. Collectively, these dependencies showed that managing line losses and path efficiency determines the useful signal p_{sig} and, consequently, the error level, shaping the observed ranges and secret rates.

Comparative modelling results for quantum channels and topologies

The second block of results concerned a comparative analysis of communication channels and basic topologies. Three operating regimes were aligned: (1) point-to-point optical fibre without intermediate trusted nodes, (2) fibre segments with trusted nodes and key routing, (3) free-space optical

(FSO) communication for urban routes and satellite segments for intercity. The analysis was conducted with account taken of losses, fluctuations, background illumination, weather factors, and service-availability requirements.

For fibre lines, practical ranges of 150-200 km without nodes were confirmed, provided the parameters in Table 1 were met and "decoy" intensities were used. For longer distances, segmentation with trusted nodes was deemed appropriate, shifting requirements from the physical layer to organisational and cryptographic policies (physical security, HSM, audit). For urban FSO, typical routes of 5-20 km were aligned, with sensitivity to meteorological factors; nighttime windows and adaptive apertures/trackers improved the availability profile. For trunks, a hybrid was recommended: terrestrial fibre segments + satellite (Low Earth Orbit (LEO) and Medium Earth Orbit (MEO)) segments with key buffering and route redundancy. In Table 2, the suitability of channels and topologies for different environments and distances was summarised with typical losses, target availability, and orders of key-generation rate.

Table 2. Suitability of channels and topologies for distances/environments

Channel/Topology	Typical environment	Distance (km)	Indicative losses/ factors	Target availability	Indicative key rate*
Fibre P2P without nodes	Urban/regional	50-200	0.17-0.25 dB/ km + connectors	99.9%	tens of kbit/s
Fibre with trusted nodes	Regional/intercity	200-1,000+	Total losses by segment; node requirements	99.95%+	hundreds of kbit/s (aggregation)
Urban FSO	"Rooftop-to-rooftop" links	5-20	Turbulence, rain/fog, background light	99.0-99.9% (climate-dependent)	units-tens of kbit/s
Inter-building FSO reserve	Intra-urban reserve	1-5	Low loss budget, short baselines	99.9%	tens of kbit/s
Satellite (LEO/MEO)	Intercity/interstate	500+ (projection)	Atmosphere, pointing, cloud cover	Windowed availability	from units to tens of kbit/s

Note: * – rate depends on protocol, losses, and the parameters in Table 1; typical orders are given for planning
Source: compiled by the authors based on M. Ghalaii *et al.* (2023), A. Rayhan *et al.* (2025)

The range of 50-200 km for "pure" fibre without trusted nodes corresponded to a practical loss budget of 8-20 dB (including splices/connectors), within which the parameters in Table 1 made it possible to keep *QBER* below threshold values for a positive secret rate. Crossing the ~200 km boundary without nodes, even with high-efficiency detectors, theoretically required either unacceptably low error rates from ideal components or a substantial reduction in the key rate, which made the service uneconomic for most applied critical-infrastructure scenarios.

Fibre networks with trusted nodes extended geographical coverage to hundreds and thousands of kilometres via an organisational trust model: each segment ensured locally high quality, while the key was routed through nodes. Technically, this enabled aggregation of key rates (hundreds of kbit/s in total), but shifted requirements to physical security, HSM, audit, and segmentation of access domains, which had to be accounted for in TCO. FSO links of 5-20 km provided effective urban connections at low deployment cost, but availability of 99.0-99.9% depended strongly on climate: rain, fog, and daytime illumination reduced time windows of stable operation. For this reason, FSO was appropriate either as a reserve to fibre (1-5 km with 99.9% availability due to short baselines) or as a primary channel in scenarios where windowed availability profiles were acceptable (for example, night-time windows with illumination control in dense urban areas).

Satellite segments (LEO/MEO) logically imposed a windowed availability regime and requirements for pointing/atmospheric transparency. Despite modest orders of key rates (units-tens of kbit/s), such segments opened a practical path for intercity/interstate trunks where continuous fibre rings with trusted nodes were economically or organisationally difficult. Thus, the "fibre + FSO/satellite" hybrid optimised both range and fault tolerance. In summary, for designing critical-infrastructure networks it was rational to combine fibre segments (as a high-availability base) with FSO inserts (as an economical reserve or local primary channel) and satellite links (as an intercity reserve or temporary bridge), achieving compliance with SLO without disproportionate cost growth.

Applicability for banks, energy systems, and the state

The third block of results transformed technical norms into applied architectural profiles for three scenarios, in each of which a recommended topology, an integration policy with classical protocols and KMS/HSM, latency and fault-tolerance requirements, an indicative cost category, and a phased implementation plan were formed. For banking networks, the suitability of branch-to-hub and processing-centre interactions in the form of rings with trusted nodes was established, enabling routing of key material with local aggregation and rotation aligned with the transaction profile. For critical payments, QKD keys were used as material for one-time or partially one-time TLS/IPsec sessions (PFS + PQC hybrid), while standard flows remained on PQC algorithms with higher throughput. Due to high sensitivity to outages, fault tolerance was ensured via two independent physical routes (fibre + FSO or two fibres from different operators).

In energy-system management, the suitability of dual "control centre – substation" channels with geo-redundancy

was confirmed, where QKD provided keys to protect critical telemetry and control commands (including for IEC 62351-compatible profiles), while classical channels served as backup or transport. Strict requirements for latency and determinism directed the design towards fibre segments with a minimal number of intermediate nodes and a local key cache at the edge. For government communications, hybrid architectures were formed with segmentation of access domains, in which QKD keys remained within the domain, and inter-domain exchange took place through gateways with HSM and trust policies. Satellite segments were used for intercity backbones and redundancy, while urban segments were built on fibre with nodes. Table 3 summarised the applied deployment profiles for banking networks, energy systems, and government communications: topologies, integration with classical cryptography, SLOs, TCO categories, and implementation phasing.

Table 3. QKD deployment profiles – topology, integration, SLO, TCO, phasing

Scenario	Recommended topology	Integration with classical cryptography	SLO requirements	TCO category (5 years)	Phased implementation
Banking networks	Ring with trusted nodes + FSO backup	TLS/IPsec with PFS; PQC hybrid; KMS + HSM	99.95%+, low RTO/RPO	Medium-high	Urban pilot → regional rings → intercity backbones
Energy systems	Dual control centre – substation channels	IEC-compatible protection; local key cache	Low latency, high determinism	Medium	Backbone section → critical nodes → scaling to substation classes
Government communications	Segmented domains + satellite segments	Gateways with HSM; access policies	High availability and segmentation	High	Urban cores → intercity routes → inter-agency gateways

Note: TCO categories (5 years) are interpreted as follows: medium – basic fibre infrastructure without expensive components; medium-high – rings with trusted nodes and backup (FSO/second route) and increased availability requirements; high – intercity/satellite segments with enhanced hardware security and complex integration
Source: compiled by the authors based on M. Stanley *et al.* (2022), J. Faba *et al.* (2025)

For banking networks, ring topologies with trusted nodes ensured uniform availability and the ability to route the key even if an individual segment failed. FSO backup enabled rapid service restoration during fibre incidents, keeping RTO/RPO within strict limits. The QKD + PQC hybrid made it possible to allocate QKD keys to transaction-critical flows (short TLS sessions with frequent rotation), while high-performance channels were handled by PQC algorithms without a bottleneck on the quantum key generation side. In the TCO profile, CapEx on nodes and KMS/HSM and OpEx on audit/logging dominated.

In energy systems, determinism and low latency were decisive. Dual fibre channels between control centres and substations minimised the risk of losing control. A local edge key cache removed peak load on generation during short "bursts" of control commands; the compatibility profile with the IEC family of protocols meant practical integration without violating existing SLAs. TCO here was formed by a balance of moderate CapEx on fibre routes/nodes and OpEx for maintaining determinism (synchronisation, regular monitoring of the timing budget).

For government communications, access-domain segmentation and intercity/interstate links were key. Satellite segments added geographic flexibility and route redundancy, but increased the complexity of managing availability windows. Inter-domain exchange policies required gateways with HSM, multifactor access, logging, and thorough audit. The high TCO category was explained both by the cost of satellite components and by organisational security requirements. Thus, each profile demonstrated how technical norms of components and channels were transformed into applied architectures with realistic SLOs and costs, confirming the hypothesis about the practical suitability of hybrid QKD networks for critical infrastructure.

Scalability, compatibility, cost, and future risks

The fourth block of results integrated aspects of scalability, compatibility with existing infrastructure, life-cycle economics, and evolutionary risks. It was generalised that scaling QKD networks required coordination at three levels: physical (channel and component quality), network (topological and routing decisions), and application (key management, compatibility with protocols and services). All levels were "tied together" through SLOs (availability, latency, key throughput) and security policies (trust domain, isolation, audit).

Compatibility with existing infrastructure was achieved through hybrid cryptoprofiles: QKD provided high-quality symmetric material injected into TLS/IPsec/into application protocols as session keys, while post-quantum algorithms (PQC) carried scalable flows where QKD key material was a limited resource. For telecom operators, an SDN/NFV approach with cryptographic functions as services was considered appropriate, enabling centralised management of rotation and key distribution policies and observability of network state.

The economic part of the results was presented as structured TCO drivers: capital expenditure on optics/detectors/satellite segments; operating expenditure on calibration, monitoring, audit; costs of integration with KMS/HSM and upgrading network elements; costs of staff training; risk costs (penalties/downtime) in case of failure. It was determined that phased deployment (pilots, limited operation, scaling) minimised TCO through gradual capability build-up and reuse of developed templates. Table 4 presented a risk map of deployment and corresponding countermeasures, with an assessment of residual risk and operational policies.

Table 4. Deployment risks and aligned countermeasures

Risk/attack	Nature of the threat	Aligned countermeasures	Residual risk	Operational policies
Detector blinding	Driving the APD into linear mode	Power monitoring, filtering, MDI-QKD, liveness tests	Low-medium	Periodic testing, telemetry logging
"Trojan horse"	Light injection into the module	Optical isolators, back-reflection detectors, alarms	Low	Strict cabling policies, tamper sealing
Time/window shift	Manipulation of time windows	Dynamic windows, random discretisation, audit	Low	Synchronisation checks, test packets
Store-now/decrypt-later	Archiving traffic until quantum computers emerge	QKD+PQC hybrid, short key rotation	Low	Clear RKP (retention/rotation) policies
Atmospheric/weather factors (FSO)	Loss of availability	Geo-redundancy, combined routes, window planning	Medium	SLAs with alternative carriers
Trusted-node compromise	Organisational risk	Physical security, HSM, separation of duties, audit	Low-medium	Access checks, logging, SOC integration

Note: RKP – Retention/Rotation Key Policies, SOC-integration – Security Operations Centre
Source: compiled by the authors based on M.P. Lingaraju *et al.* (2019)

Risk contours confirmed the appropriateness of technical and organisational countermeasures. For detector blinding, the simultaneous presence of optical filtering, power monitoring at the module input, and periodic liveness tests reduced the probability of a successful attack to a low/medium level, while MDI-QKD additionally shifted trust to the central joint-measurement node, removing the class of detector attacks at the endpoints. The "Trojan horse" attack was neutralised by isolators and back-radiation sensors; residual risk remained low, provided strict cabling policies and access control to optical panels were enforced.

Manipulations of time windows were mitigated by adaptive windows and randomised offsets, making the attack less predictable; regular synchronisation audits prevented drift from accumulating to levels that would be noticeable in *QBER* only after the fact. The store-now/decrypt-later risk was conceptually reduced by the QKD + PQC hybrid and short key rotation, which made sessions cryptographically short-lived for deferred analysis, even with the emergence of powerful quantum computers. For FSO channels, medium residual risk was compensated by geo-redundancy and SLAs with alternative transport, as well as planning of operating "windows" taking into account local climate patterns. Finally, the organisational risk of trusted nodes was substantially reduced through HSM, separation of duties, tamper sealing, video surveillance, and SOC monitoring with immutable logs. From a scalability perspective, the results confirmed that segmentation into trust domains and gateways between those domains allowed the network to grow without disproportionate risk growth: an incident was localised within a domain, component migrations occurred gradually, and policies for key-material exchange remained under centralised KMS control.

The TCO structure was formed from four classes of costs: CapEx on optics/detectors/satellite segments; OpEx on calibration, monitoring, and audit; costs of integration with KMS/HSM and upgrading network elements; costs of staff training. Phased deployment – first an urban pilot on short fibre or FSO (5-20 km), then regional rings with nodes, then intercity inclusion via satellite or leased backbones – spread costs evenly and reduced integration risks. Compatibility with existing transports improved with CV-QKD (better alignment with WDM), while DV-QKD required stricter optical isolation and channel separation; in application protocols, short TLS/IPsec sessions with frequent key rotation were recommended for critical flows in order to use the limited quantum key rate efficiently.

Development trajectories relevant to the studied scenarios were outlined: the emergence of quantum repeaters and intermediate technologies without state disclosure (extending distance without trusted nodes), broader use of MDI/DI paradigms (reducing dependence on the honesty of the measurement module), hardware improvements in detectors and sources (fewer dark events, lower jitter, better phase stability), and "native" integration with PQC in network stack services. Threats from quantum memory – i.e., the ability to store states and analyse these states later – were neutralised by design choices of the QKD + PQC hybrid, short key-rotation policies, and minimising session lifetimes; in the government segment, record-retention regulations and mandatory PFS settings were additionally taken into account.

The theoretical study fulfilled the stated aim: aligned criteria for sources, detectors, and channels were formed; comparative profiles of channels and topologies for urban and regional distances were proposed; applied architectural solutions for banking, energy, and government communications were built; issues of scalability, compatibility, and life-cycle economics were integrated; risks and effective countermeasures were systematised. The obtained results confirmed the working hypothesis: integrating physically grounded key distribution with key life-cycle management and compatible transport infrastructure provides a practically usable level of security, resilience, and scalability over urban and regional distances without unacceptable costs, while phased deployment made it possible to achieve target SLOs with controlled risks and predictable TCO.

DISCUSSION

In this section, the obtained results were analysed – link budgets, the sensitivity of the secret key rate to dark-count

events and jitter, as well as SLO profiles for the banking, energy, and government domains – and compared with the conclusions of other researchers. The emphasis was not on a literature review, but on comparison: where the results coincided, where these findings diverged, what this meant for practical implementation, and why it mattered for long-term cyber resilience. The obtained results are consistent with a broad body of research and, at the same time, refine the boundaries of applicability for critical infrastructure. The practical secret key rate was determined by a combination of intensity stability (⩽1-2% RMS), polarisation stability (~25-30 dB), and low dark-event rate together with detection efficiency; similar dependencies were reported by M. Kumar & B. Mondal (2025). The transition from APD ≈ 60-70% to SNSPD ≈ 80-90% effectively "recovered" several decibels and extended the operating distance without changing the topology, while accounting for receiver time-window jitter refined the boundary of a positive secret key rate. For CV-QKD, the stability of the local-oscillator phase remained critical: the degradation of SNR in homodyne and heterodyne measurements under uncontrolled phase noise was described in detail by S. Kundu *et al*. (2025), which is consistent with the phase-noise and linewidth norms adopted in this work. The combination of authentication, modern error correction, and decoy intensities with narrow time windows reduced statistical biases in single-photon estimation; the corresponding effects were demonstrated by C. Anilkumar *et al.* (2024), and in the developed model this reduced *QBER* without modernising the optics, with deviations from the stated estimates explained by tighter gating and stricter tolerances for intensity stability.

The evolutionary trajectory of the network – from trusted-node to entanglement-based architectures with quantum repeaters – was substantiated by Q. Jude (2024); the obtained profiles confirm the viability of such an approach, provided that sites are reserved for repeaters and DI verification is prepared in urban and regional pilots. The strengthening of cryptographic security through entangled states in a "one-time pad" was demonstrated by G. Pradeep & M.D.S. Nandhini (2024); in applied policy, this meant allocating the quantum key to short-lived critical TLS/IPsec sessions with PFS priority, while bulk high-bitrate flows were encrypted using PQC algorithms for scalability. The heterogeneity of availability in 5G/6G and IoT and the need for geo-redundancy with combined transports are consistent with the conclusions of Durr-E-Shahwar *et al.* (2024); the "fibre + FSO/satellite" hybrid achieves target SLOs with moderate TCO if FSO is used as an urban backup over 1-5 km, and the satellite as an intercity "bridge". Additionally, the operational observations of S.V.S. Pillai & K. Polimetla (2024) were taken into account, that centralisation of key generation increases delays and costs; local edge caches with eviction policies synchronised with rotation smooth "bursts" of control commands and unload backbone links.

Interoperability and manageability were ensured through an SDN/NFV framework with crypto functions as services and centralised KMS/HSM control loops – approaches set out in detail in S. Brightwood *et al.* (2024); on this basis, the architecture avoided "crypto islands" during migration and scaling, and orchestration was tied to SLO classes and domain constraints. The stratification of roles of the physical channel, the key distribution system, and application protocols, generalised by S. Akter (2023), confirms the practicality of separation of duties and simplifies SLO validation. For cloud solutions with artificial intelligence (AI) components, zero-trust principles based on post-quantum algorithms, described by A. Sreerangapuri (2024), envisaged telemetry of the status of quantum components, liveness tests, access audits, and checks of encryption modes in OT environments.

Industrial cases of adopting PQC without breaking existing stacks were generalised by H.C. Ukwuoma *et al*. (2022); the obtained hybrid policy shifted bulk channels to PQC, while the quantum key was reserved for short critical sessions. The outcomes of the NIST process and the arguments in favour of hybridisation, presented by R. Bavdekar *et al*. (2023), were reflected in TCO estimates for different domains. Aspects of corporate governance and risk management in migration to PQC, highlighted by Y.-K. Liu & D. Moody (2024), were supplemented with requirements for regular implementation audits, staff training programmes, and side-channel control; technical issues of compatibility and leakage mitigation were detailed by S. Li *et al*. (2023). The "store now – decrypt later" risk was systematised by S. Singh *et al.* (2024); in practical profiles, this was implemented by short key rotation and mandatory PFS in critical channels, with immutable logs and domain segmentation for government communications. Performance data on CRYSTALS-Kyber and the advisability of hardware offloads at network nodes were provided by M.S.C. Laule *et al*. (2024), while the integration of lattice-based schemes on OpenTitan was demonstrated by T. Stelzer *et al.* (2025) – together, this substantiated encrypting large flows "in hardware" without loss of cryptographic security in banking and energy backbones. The discipline of modes and ciphertext variability as a way to reduce leakage through side channels was detailed by P.-A. Berthet (2024); in regulations, this was implemented through regular compliance tests, non-conformance logs, and rapid configuration rollbacks. The long-term security of lattice-based schemes in hybrid profiles was confirmed by J. Shunza (2019), and A. Dadheech (2021). In elevated-risk scenarios, the complementary role of chaotic dynamics was considered by M.H. Al Hasani & K.A. Al Naimee (2019).

The integration of cryptography into PKI and OT networks with domain segmentation and HSM gateways was described by J.O. del Moral *et al.* (2024), while models for integrating KMS and key-distribution policies in multi-domain environments were presented by A. Geremew & A. Mohammad (2024); comparison with the chosen architecture of inter-agency gateways and centralised management attests to interoperability.

Taken together, manageable standardisation of components (intensity stability, polarisation stability, detector efficiency and noise characteristics), protocol engineering (decoy states, gating, authentication and error correction), and the choice of transports/topologies (fibre with FSO/satellite backup and a "development window" for MDI/DI and repeaters) ensure the achievement of target SLOs without radical replacement of physical infrastructure. For banking networks, rings with trusted nodes and edge key caching are appropriate; for energy systems – deterministic latency in dual fibres "control centre – substation"; for government communications – domain segmentation and HSM gateways with satellite "bridges" for intercity routes. The practical importance lies in outlining a manageable migration trajectory towards long-term cyber resilience: from urban pilots – to regional rings and then to architectures with MDI/DI and quantum repeaters, with a hybrid cryptopolicy QKD + PQC that operates at scale without "crypto islands".

CONCLUSIONS

The study was purely theoretical in nature and, in accordance with its aim, aligned the requirements for three key QKD subsystems: radiation sources with controlled frequency and intensity stability and stable polarisation, photon detectors with high efficiency at low dark-count events and low jitter, and quantum communication channels in optical fibre and free space, taking into account the loss budget and fluctuations.

It was established that, without trusted nodes, practically achievable fibre distances are about 150-200 km; for urban FSO lines, routes of 5-20 km are appropriate; scaling up requires segmentation via a network of trusted nodes, satellite segments, or the emergence of quantum repeaters. Applied architectural profiles were formed: for banking networks, rings with FSO backup and session rotation based on QKD keys; for energy-system control, dual fibre channels between control centres and substations with a local key cache; for government communications, segmented domains with inter-agency gateways and satellite redundancy.

Quantitative indicators showed that, without trusted nodes in fibre, 150-200 km is practically achievable with a loss budget of ~8-20 dB, with secret key rates at the level of tens of kbit/s; at the component level, maintaining intensity stability $\leqslant$1-2%, polarisation stability $\geqslant$25-30 dB, and detection efficiency of 60-70% (APD) and 80-90% (SNSPD) extends operating distances; the transition APD→SNSPD adds approximately 15-30%, while an additional +1 dB of loss reduces the secret-key-rate margin by roughly 20%.

The obtained values confirm the proposed hypothesis about the practical suitability of a QKD + PQC hybrid for urban and regional networks with achievable SLOs without unacceptable TCO. Compatibility with existing infrastructure was shown through a QKD plus PQC hybrid with integration into TLS or IPsec and KMS or HSM under SDN or NFV policy control, as well as a predictable life-cycle cost structure. A phased deployment was recommended, from an urban pilot to regional rings and intercity backbones, with prioritisation of critical flows, short rotation, and PFS.

The limitations of the conclusions are linked to the absence of empirical validation, the climatic sensitivity of FSO, and dependence on assumed component parameters. Further directions include quantum repeaters, broader MDI or DI verification, improving the quality of sources and detectors, and native integration of QKD plus PQC hybrids into network services of Ukraine's critical infrastructure.

ACKNOWLEDGEMENTS

None.

FUNDING

None.

CONFLICT OF INTEREST

None.

REFERENCES

[1] Akter, S. (2023). Quantum cryptography for enhanced network security: A comprehensive survey of research, developments, and future directions. *Arxiv*. doi: 10.48550/arxiv.2306.09248.

[2] Al Hasani, M.H., & Al Naimee, K.A. (2019). Impact security enhancement in chaotic quantum cryptography. *Optics & Laser Technology*, 119, article number 105575. doi: 10.1016/j.optlastec.2019.105575.

[3] Anilkumar, C., Lenka, S., Neelima, N., & Sathishkumar, V.E. (2024). A secure method of communication through BB84 protocol in quantum key distribution. *Scalable Computing Practice and Experience*, 25(1), 21-33. doi: 10.12694/scpe.v25i1.2152.

[4] Bavdekar, R., Chopde, E.J., Agrawal, A., Bhatia, A., & Tiwari, K. (2023). Post quantum cryptography: A review of techniques, challenges and standardizations. In *2023 international conference on information networking* (pp. 146-151).Bangkok: IEEE. doi: 10.1109/ICOIN56518.2023.10048976.

[5] Berthet, P.-A. (2024). Ciphertext malleability in lattice-based KEMs as a countermeasure to side channel analysis. *Arxiv*. doi: 10.48550/arXiv.2409.16107.

[6] Brightwood, S., Jarry, H., Frank, E., & Olusegun, J. (2024). *Network security and Quantum cryptography: Challenges and opportunities*. Retrieved from https://surli.cc/rlkwmt.

[7] Chen, C.-L., Zeng, K.-W., Li, W.-Y., Lee, C.-F., Liu, L.-C., & Deng, Y.-Y. (2025). Lightweight post-quantum cryptography: Applications and countermeasures in internet of things, blockchain, and E-learning. *Engineering Proceedings,* 103(1), article number 14. doi: 10.3390/engproc2025103014.

[8] Dadheech, A. (2021). Post-quantum lattice-based cryptography: A quantum-resistant cryptosystem. In N. Kumar, A. Agrawal, B.K. Chaurasia & R.A. Khan (Eds.), *Limitations and future applications of quantum cryptography* (pp. 102-123). Hershey: IGI Global Scientific Publishing. doi: 10.4018/978-1-7998-6677-0.ch006.
[9] del Moral, J.O., iOlius, A.D., Vidal, G., Crespo, P.M., & Martinez, J.E. (2024). Cybersecurity in critical infrastructures: A post-quantum cryptography perspective. *IEEE Internet of Things Journal*, 11(18), 30217-30244. doi: 10.1109/IIOT.2024.3410702.
[10] Dharanish, P., Kokila, S., Mythily, M., & Balachandran, A. (2024). FPGA implementation of post quantum cryptography for high performance. In V. Sharmila, S. Kannadhasan, A.R. Kannan, P. Sivakumar & V. Vennila (Eds.), *Challenges in information, communication and computing technology*: *Proceedings of the 2nd international conference on challenges in information, communication, and computing technology* (pp. 209-213). London: CRC Press. doi: 10.1201/9781003559092.
[11] Djordjevic, I.B. (2022). Physical-layer security, quantum key distribution, and post-quantum cryptography. *Entropy*, 24(7), article number 935. doi: 10.3390/e24070935.
[12] Durr-E-Shahwar, Imran, M., Altamimi, A.B., Khan, W., Hussain, S., & Alsaffar, M. (2024). Quantum cryptography for future networks security: A systematic review. *IEEE Access*, 12, 180048-180078. doi: 10.1109/ACCESS.2024.3504815.
[13] Faba, J., Brito, J.P., Cresta, J., Pastor, A., López, D., Brito, R., Buruaga, J.S., & Martin, V. (2025). A hybrid approach to address the transition to quantum-resistant cryptography in telecommunication environments. In *2025 international conference on quantum communications, networking, and computing* (pp. 122-126). Nara: IEEE. doi: 10.1109/QCNC64685.2025.00027.
[14] Geremew, A., & Mohammad, A. (2024). Preparing Critical infrastructure for post-quantum cryptography: Strategies for transitioning ahead of cryptanalytically relevant quantum computing. *International Journal on Engineering Science and Technology*, 6(4), 338-365. doi: 10.46328/ijonest.240.
[15] Ghalaii, M., *et al*. (2023). Satellite-based quantum key distribution in the presence of bypass channels. *PRX Quantum*, 4, article number 040320. doi: 10.1103/PRXQuantum.4.040320.
[16] Gyongyosi, L., Bacsardi, L., & Imre, S. (2019). A survey on quantum key distribution. *Infocommunications Journal,* 11(2), 14-21. doi: 10.36244/ICJ.2019.2.2.
[17] Hoschek, M. (2021). Quantum security and 6G critical infrastructure. *Serbian Journal of Engineering Management*, 6(1), 1-8. doi: 10.5937/SJEM2101001H.
[18] Jude, Q. (2024). *Quantum entanglement and the future of secure quantum computing*. Retrieved from https://surl.li/baztmk.
[19] Kumar, M., & Mondal, B. (2025). A brief review on quantum key distribution protocols. *Multimedia Tools and Applications*, 84(27), 33267-33306. doi: 10.1007/s11042-024-20535-x.
[20] Kundu, S., Gupta, T., Sardar, A., Bandyopadhyay, A., Swain, S., & Mallik, S. (2025). A survey on quantum computing: Transforming cryptography, AI/ML, blockchain, and network communication. *Franklin Open*, 12, article number 100371. doi: 10.1016/j.fraope.2025.100371.
[21] Laule, M.S.C., Silva, J.E.O., & Hanco, H.N. (2024). Lattice-based cryptography: Development and analysis of a new variant of the crystals-kyber algorithm. *Interfaces,* 20, 165-184. doi: 10.26439/interfases2024.n020.7383.
[22] Li, S., Chen, Y., Chen, L., Liao, J., Kuang, C., Li, K., Liang, W., & Xiong, N. (2023). Post-quantum security: Opportunities and challenges. *Sensors*, 23(21), article number 8744. doi: 10.3390/s23218744.
[23] Lingaraju, M.P., Kumar, B.T., & Jayachandra, C. (2019). Quantum entanglement and its implications for secure communication. *World Journal of Advanced Research and Reviews*, 1(1), 82-88. doi: 10.30574/wjarr.2019.1.1.0003.
[24] Liu, Y.-K., & Moody, D. (2024). Post-quantum cryptography and the quantum future of cybersecurity. *Physical Review Applied*, 21, article number 040501. doi: 10.1103/PhysRevApplied.21.040501.
[25] Nguyen, T.-T., Khac, T.-V., & Quynh, L.-N. (2023). Simulation of the BB84 quantum key exchange protocol. In *2023 15th international conference on knowledge and systems engineering* (pp. 1-4). Hanoi: IEEE. doi: 10.1109/KSE59128.2023.10299471.
[26] Pillai, S.V.S., & Polimetla, K. (2024). Analyzing the impact of quantum cryptography on network security. In *2024 international conference on integrated circuits and communication systems* (pp. 1-6). Raichur: IEEE. doi: 10.1109/ICICACS60521.2024.10498417.
[27] Pradeep, G., & Nandhini, M.D.S. (2024). Towards efficient quantum cryptography: Enhancing QOTP with entanglement based techniques. *Journal of Dynamics and Control,* 8(11), 166-183. doi: 10.71058/jodac.v8i11017.
[28] Rahmayanti, D. (2025). Quantum key distribution (QKD) as a wireless telecommunications security solution. *Journal of Informatics and Computer Technology*, 5(1), 10-26. doi: 10.55606/jitek.v5i1.5765.
[29] Rajpoot, S., Singh, K., Singh, C.P., & Sharma, B.K. (2023). Security challenges and future research in quantum key distribution networks. In *2023 10th IEEE uttar pradesh section international conference on electrical, electronics and computer engineering* (pp. 95-100). Gautam Buddha Nagar: IEEE. doi: 10.1109/UPCON59197.2023.10434510.
[30] Rayhan, A., Bushra, Z.I., Chowdhury, S., Faruqui, N., & Barua, B. (2025). Performance analysis of free space optical communication in urban rain environment. In *2025 international conference on electrical, computer and communication engineering* (pp. 1-6). Chittagong: IEEE. doi: 10.1109/ECCE64574.2025.11013976.
[31] Reddy, D.V., Nerem, R.R., Nam, S.W., Mirin, R.P., & Verma, V.B. (2020). Superconducting nanowire single-photon detectors with 98% system detection efficiency at 1550 nm. *Optica*, 7(12), 1649-1653. doi: 10.1364/OPTICA.400751.
[32] Shao, Y., Wang, H., Pi, Y., Huang, W., Li, Y., Liu, J., Yang, J., Zhang, Y., & Xu, B. (2021). Phase noise model for continuous-variable quantum key distribution using a local local localoscillator. *Physical Review A*, 104, article number 032608. doi: 10.1103/PhysRevA.104.032608.

[33] Shunza, J. (2019). *Lattice-based cryptosystems and post-quantum cryptography.* Kigali: African Institute for Mathematical Sciences. doi: 10.13140/RG.2.2.18756.50563.
[34] Singh, S., Jha, C.K., Bende, A., Rana, V., Patkar, S., Drechsler, R., & Merchant, F. (2024). MemSPICE: Automated simulation and energy estimation framework for MAGIC-based logic-in-memory. In *Proceedings of the 29th Asia and south pacific design automation conference* (pp. 282-287). Incheon: IEEE. doi: 10.1109/ASP-DAC58780.2024.10473924.
[35] Sreerangapuri, A. (2024). Post-quantum cryptography for ai-driven cloud security solutions. *International Journal for Multidisciplinary Research*, 6(5). doi: 10.36948/ijfmr.2024.v06i05.29032.
[36] Stanley, M., Gui, Y., Unnikrishnan, D., Hall, S.R.G., & Fatadin, I. (2022). Recent progress in quantum key distribution network deployments and standards. *Journal of Physics Conference Series*, 2416, article number 012001. doi: 10.1088/1742-6596/2416/1/012001.
[37] Stelzer, T., Oberhansl, F., Schupp, J., Karl, P., & Turcuman, H. (2025). Extended version: Enabling lattice-based post-quantum cryptography on the opentitan platform. *Journal of Cryptographic Engineering*, 15, article number 11. doi: 10.1007/s13389-025-00369-5.
[38] Ukwuoma, H.C., Arome, G., Thompson, A., & Alese, B.K. (2022). Post-quantum cryptography-driven security framework for cloud computing. *Open Computer Science*, 12(1), 142-153. doi: 10.1515/comp-2022-0235.
[39] Yu, C., Xu, Q., & Zhang, J. (2024). Recent advances in InGaAs/InP single-photon detectors. *Measurement Science and Technology,* 35(12), article number 122003. doi: 10.1088/1361-6501/ad76ca.

Ігор Лімарь
Кандидат технічних наук, старший викладач
Державний університет інтелектуальних технологій і зв'язку
65023, вул. Кузнечна, 1, м. Одеса, Україна
Інженерно-технологічний інститут «Біотехніка» Національної академії аграрних наук України
67667, вул. Маяцька дорога, 26, с. Хлібодарське, Україна
https://orcid.org/0000-0002-8972-9935

Євген Севастєєв
Магістр, старший викладач
Державний університет інтелектуальних технологій і зв'язку
65023, вул. Кузнечна, 1, м. Одеса, Україна
https://orcid.org/0000-0003-1165-1119

Квантова криптографія: теоретичні основи та практичні імплементації для захисту критичної інфраструктури

Анотація. Метою статті було теоретично визначити узгоджені критерії застосовності квантового розподілу ключів для захисту критичної інфраструктури з урахуванням довготривалого ризику дешифрування з боку супротивників, що володіють квантовими обчислювальними ресурсами та архівацією трафіку. Методологія спиралася на теоретичний системний аналіз трьох підсистем Quantum Key Distribution джерел, детекторів і каналів (волокно/вільний простір), доповнений спрощеними моделями лінк-бюджету та імовірності бітової помилки. Проведено стислий сценарний аналіз для банківських мереж, енергосистем і державних комунікацій з урахуванням масштабованості, сумісності та вартості. Основні результати показали, що стабільність інтенсивності лазерів 1-2 % і вища ефективність детекторів – 60-70 % для Avalanche Photodiode та 80-90 % для Superconducting Nanowire Single-Photon Detector – розширюють практичні відстані та знижують похибки. Без довірених вузлів у волокні досяжно 150-200 км; для міських Free-Space Optics ліній оптимальні 5-20 км, а більші дистанції потребують сегментації мережі чи супутникових відрізків. Архітектурно обґрунтовано: для банків – кільця з довіреними вузлами та Free-Space Optics резервом; для енергосистем – подвійні волоконні канали "диспетчерська-підстанція" з локальним кешем ключів; для держзв'язку – сегментовані домени з міжвідомчими шлюзами та супутниковим резервуванням. У всіх сценаріях доцільний гібрид Quantum Key Distribution+Post-Quantum Cryptography із короткою ротацією ключів і операційними контрзаходами проти атак на детектори та канали, що підтверджує практичну придатність для міських і регіональних мереж. Практична значимість полягає в наданні інженерним командам банків, енергетики та держзв'язку готових архітектурних профілів – від кілець і подвійних волоконних каналів до сегментованих доменів – з інтеграцією Key Management System/Hardware Security Module, визначенням Service Level Objective/Service Level Agreement та поетапними дорожніми картами. Для регуляторів і операторів це база для оновлення вимог і аудитів, а також для планування резервування (Free-Space Optics/супутник) і категорій Total Cost of Ownership

Ключові слова: розподіл ключів; лазерні джерела; фотонні детектори; оптичне волокно; зв'язок у вільному просторі; довірені вузли; банківські мережі