Journal of Electrical and Computer Engineering Innovations
(JECEI)
Journal homepage: http://www.jecei.sru.ac.ir

Research paper

Enhancing Ack QKD with Decoy States for Device Independent Security

Arash Kosari *

Department of Electrical Engineering and Information Technology, Iranian Research Organization for Science and Technology (IROST), Tehran, Iran.

Article Info

Article History:
Received 15 August 2025
Reviewed 21 September 2025
Revised 20 October 2025
Accepted 09 November 2025

Keywords:
Quantum Key Distribution (QKD)
MDI-QKD
Detector Blinding
Decoy States
Integrated Photonics
Finite-Key Security
Side-Channel Attacks

*Corresponding Author's Email Address: *a.kosari@irost.ir*

Abstract

Background and Objectives: Quantum Key Distribution (QKD) ensures secure communication through quantum mechanics, but real-world implementations face vulnerabilities from detector blinding, time-shift, and side-channel attacks. While Measurement-Device-Independent QKD (MDI-QKD) mitigates detector vulnerabilities, it lacks real-time attack monitoring and struggles with finite-key limitations. This study presents an MDI ack QKD protocol that integrates deterministic acknowledgment pulses and multi-intensity decoy states to achieve robust, device-independent security with real-time attack detection [16].

Methods: The proposed protocol combines MDI-QKD's device-independent framework with interleaved deterministic acknowledgment pulses and four-level decoy intensities. Alice and Bob generate weak coherent pulses with randomized phases, embedding acknowledgment pulses with probability (Pd = 0.1) to probe channel integrity. An untrusted relay performs Bell-state measurements using superconducting nanowire single-photon detectors (SNSPDs) [17]. Multi-intensity decoy statistics enable finite-key parameter estimation, while integrated photonic platforms ensure scalability. Security is analyzed using the universally composable framework, with simulations and preliminary experiments conducted over metropolitan fiber distances.

Results: Numerical simulations demonstrate secure key rates exceeding 10 Mbps at 50 km and ~1 Mbps at 100 km under realistic conditions (0.2 dB/km fiber loss, 85% detector efficiency, 1 GHz pulse rate). Experimental tests on an integrated photonic chip at 1550 nm achieved raw key rates of 1.1 Mbps at 50 km with de-coy accuracy within ±7%. Deterministic acknowledgments detected blinding at-tacks with high sensitivity, and multi-intensity decoys provided tight finite-key bounds, maintaining composable security against collective and coherent attacks.

Conclusion: The MDI ack QKD protocol achieves high-rate, device-independent quantum key distribution with real-time attack monitoring, offering a scalable solution for metropolitan quantum networks. Its compatibility with integrated photonics enables compact, stable implementations, while deterministic acknowledgments and multi-intensity decoys ensure robust security against evolving threats. This approach paves the way for practical, unconditionally secure communication systems, with potential for satellite-ground and multi-node network extensions.

How to cite this paper:
A. Kosari, "Enhancing Ack QKD with Decoy States for Device Independent Security," J. Electr. Comput. Eng. Innovations, 14(2): 403-410, 2026.
DOI: 10.22061/jecei.2025.12392.873
URL: https://jecei.sru.ac.ir/article_2458.html

Introduction

Quantum Key Distribution (QKD) has evolved into a cornerstone of quantum communication, promising information-theoretic security based on the laws of quantum mechanics. Since the seminal BB84 protocol in 1984, the field has progressed from theoretical frameworks to practical deployment in fiber-optic backbones and satellite-based links [1], [14].

However, real-world QKD systems face critical security challenges, primarily arising from imperfect devices. Detector blinding, time-shift attacks, and other side-channel vulnerabilities compromise practical implementations. The ack QKD protocol, proposed in 2012, introduced interleaved deterministic decoy pulses to detect and mitigate blinding attacks in real time [2].

As of 2025, quantum hacking strategies have become increasingly sophisticated, targeting detectors, sources, modulators, and even fiber connectors. The emergence of integrated photonic platforms in metropolitan and wide-area networks presents both performance advantages and security concerns.

Measurement-Device-Independent QKD (MDI QKD) eliminates detector vulnerabilities by moving measurement operations to an untrusted relay. Yet, MDI-QKD still faces finite-key limitations, system complexity, and sensitivity to modulator and phase errors, especially in integrated systems [16], [17].

The proposed MDI ack QKD protocol addresses these challenges by combining:

- Interleaved deterministic decoy acknowledgments for real-time blinding detection.
- Device-independent security through MDI-QKD.
- Multi-intensity decoy states for tight finite-key bounds.
- Integrated photonics compatibility for compact, scalable QKD [18].

This protocol achieves key rates exceeding 10 Mbps over metropolitan distances, while maintaining resilience against evolving attacks.

Background and 2025 Developments

A. Evolution of Decoy State Techniques

Originally developed to counter photon-number-splitting attacks, decoy-state QKD has evolved from two-level to multi-level intensity schemes. Adaptive decoy allocation, which adjusts intensity probabilities in real time based on channel conditions, enhances key rates in dynamic metropolitan networks [2], [21].

B. Maturation of MDI QKD

MDI-QKD, first demonstrated in 2012, removes all detector side channels by relocating measurements to an untrusted relay. Field tests over 200 km of fiber and pilot deployments for financial networks demonstrate its practicality. Hardware improvements, including low-jitter SNSPDs and high-extinction modulators, boost Bell-state measurement efficiency above 60%.

C. Twin Field and Repeater-Like Protocols

Twin-field QKD surpasses the rate-distance limit by leveraging single-photon interference from remote stations. Experiments show secure key exchange beyond 500 km using advanced phase stabilization, supporting hybrid architectures combining MDI-QKD with twin-field methods [9], [10].

D. Integrated Photonic Platforms

Silicon nitride and lithium niobate platforms enable miniaturized, stable QKD modules. Integrated SNSPDs reduce coupling losses and support GHz-rate pulse shaping, allowing practical, scalable deployment [19].

E. Advances in Device-Independent QKD

Device-Independent QKD (DI-QKD) assumes no trust in devices beyond quantum mechanics. Recent experiments demonstrate DI-QKD over metropolitan distances, validating security under uncharacterized device behavior and informing finite-key analyses for MDI ack QKD.

F. Emerging Threat Models

Quantum hacking now exploits timing mismatches, wavelength-dependent losses, and chip cross-talk, highlighting the need for real-time, integrated monitoring. The MDI ack QKD protocol proactively addresses these threats using deterministic acknowledgments and multi-intensity decoys. Typefaces and Sizes [20].

MDI ack QKD Protocol

A. Conceptual Motivation and Overview

The MDI ack QKD protocol addresses the challenges of implementing quantum key distribution in real-world environments while maintaining device-independent security. Traditional QKD protocols, even with decoy states, remain vulnerable to side-channel attacks, particularly those targeting single-photon detectors. While Measurement-Device-Independent (MDI) QKD mitigates detector vulnerabilities by moving the measurement process to an untrusted node, it does not provide real-time monitoring of channel integrity [2], [3].

Our protocol synergistically combines MDI-QKD with acknowledgment-based decoy states, offering:

- **Device independence** via the MDI framework.
- **Active real-time monitoring** using deterministic acknowledgment states.
- **Multi-intensity decoy states** for tight finite-key security.
- **Compatibility with integrated photonics**, enabling compact, scalable, and stable QKD modules.

Deterministic acknowledgment states serve as integri-

ty probes: any deviation from expected statistics signals potential attacks, while multi-intensity decoys allow precise estimation of single-photon yields and error rates.

B. Step-by-Step Protocol Description

- State Preparation

1. Pulse Generation:
   - Alice and Bob independently generate weak coherent pulses with randomized phases.
   - Each pulse is assigned a basis (Z or X) and a bit value (0 or 1).
2. Deterministic Acknowledgment Embedding:
   - With probability dP, a deterministic acknowledgment pulse is inserted (e.g., $({}_{b}Z_{b,,}Z)$ or $({}_{b}X_{b},X)$)
   - These pulses act as integrity probes to detect attacks in real time.
3. Key-Generating Pulses:
   - With probability 1- dP , standard key-generating pulses are prepared (non-orthogonal pairs such as $({}_{b}Z_{b,,}X)$) [23].
4. Multi-Intensity Decoys:
   - Each pulse is randomly assigned one of four intensity levels:
   - μ_s (signal) , μ_d (decoy), μ_2, μ_3 .
   - This allows finite-key security estimation and detection of photon-number-splitting (PNS) attacks [11].

- Transmission and Measurement

- Alice and Bob transmit their pulses through independent quantum channels to an untrusted relay node (Charlie).
- Charlie performs Bell-State Measurements (BSM) using superconducting nanowire single-photon detectors (SNSPDs).
- Only the detection outcomes are publicly announced; the encoded bit values remain secret.

- Sifting and Parameter Estimation

- Public Announcement:

Alice and Bob disclose basis choice, intensity level, and acknowledgment vs key labels for detected events.

- Integrity Analysis:

Deterministic acknowledgment pulses allow estimation of:

- Detector blinding probability ($^{\epsilon}$ blind)
- Time-shift or channel manipulation indicators

- Decoy-State Parameter Estimation:

Multi-intensity statistics are used to bound:

- Single-photon yield (Y_{11})
- Quantum Bit Error Rate (QBER) (e_{11})

- Event Filtering:

Events inconsistent with the protocol expectations are discarded to maintain security.

- Key Distillation

- Raw Key Extraction: Bits from compatible basis events.
- Error Correction: Using LDPC codes optimized for high throughput.
- Privacy Amplification: Using Toeplitz hashing, it compresses the reconciled key to eliminate any residual adversary information.

C. Technical Innovations

The proposed MDI ack QKD protocol introduces several technical innovations that collectively enhance the practical security and efficiency of quantum key distribution. By leveraging device independence through measurements at an untrusted relay node, the protocol eliminates vulnerabilities associated with detector-based side channels. Deterministic acknowledgment states provide active, real-time monitoring of the quantum channel, allowing immediate detection of potential attacks such as detector blinding or time-shift manipulations. The use of multi-intensity decoy states ensures finite-key robustness, delivering tight security bounds even with realistic key lengths. Compatibility with integrated photonics platforms, such as silicon nitride and lithium niobate, facilitates compact, scalable, and stable chip-scale implementations. Additionally, the system is optimized for high-rate metropolitan-scale operation, achieving secure key rates exceeding 10 Mbps over 50 km, while incorporating design considerations that mitigate side-channel risks from modulators, sources, and photonic cross-talk, further strengthening overall practical security [4], [22].

Table 1: Key Technical Innovations and Their Advantages in the MDI ack QKD Protocol

Feature	Description	Advantage
Device Independence	Measurements at an untrusted node	Eliminates all detector-based side-channels
Active Channel Monitoring	Deterministic acknowledgment states	Real-time detection of blinding or manipulation
Finite-Key Robustness	Multi-intensity decoys with adaptive allocation	Tight security bounds even with practical key sizes
Integrated Photonics Compatibility	Silicon nitride and lithium niobate platforms	Enables compact, stable, and scalable chip-scale QKD
High-Rate Performance	Optimized system for metropolitan distances	Secure key rates >10 Mbps at 50 km, scalable beyond 100 km
Side-Channel Mitigation	Design accounts for modulators, sources, and photonic cross-talk	Enhanced practical security beyond detectors

D. Protocol Schematic

Figure 1 illustrates the overall architecture of the MDI ack QKD system, showing Alice, Bob, and Charlie, along with the integration of deterministic acknowledgments and multi-intensity decoys [24].

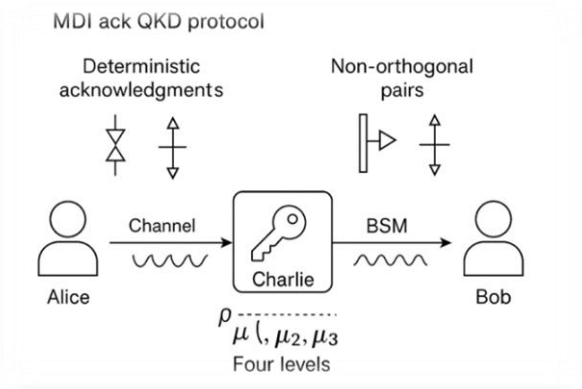

Fig. 1: illustrates the overall architecture of the MDI ack QKD system.

- Alice & Bob → Charlie (BSM).
- Deterministic acknowledgments analyzed for integrity.
- Multi-intensity decoys for parameter estimation.

Security Analysis

A. Security Model and Composability

We analyze the MDI-ack QKD protocol within the universally composable (UC) security framework, which guarantees that the generated key remains secure for any subsequent cryptographic application [5].

Let ϵ=ϵ_{sec} and ϵ_{corr} denote the **secrecy** and **correctness** parameters, respectively. The protocol is defined as ϵ-secure if:

$$\epsilon=\epsilon_{sec}+\epsilon_{corr} \quad (1)$$

This means the real key deviates from a perfectly secure, ideal key by no more than ϵ in trace distance [25].

Our use of deterministic acknowledgment pulses combined with multi-intensity decoys enables continuous device integrity monitoring, while providing provable security against both collective and coherent attacks even under finite-key conditions [7].

B. Decoy-State Parameter Estimation

To extract secure key parameters, Alice and Bob record the gains Q_{ij} and error rates E_{ij} for all intensity combinations (μ_i,μ_j) [30]. Using linear programming bounds, they estimate:

- Single-photon yield: Y_{11}.
- Single-photon error rate: e_{11}.

Finite-size effects cause statistical fluctuations δ_Y and δ_e bounded via Chernoff inequalities at a confidence level of $1-\epsilon_{PE}$.

To demonstrate practical finite-size performance, we evaluated secure key lengths for block sizes $N = 10^8, 10^9, 10^{10}$. The resulting values are summarized and the convergence behavior is plotted in Fig. 5. These results confirm that the normalized key rate stabilizes around 0.258–0.259 bits/pulse once the block size exceeds 10^9, showing that the protocol maintains strong efficiency under realistic network conditions

C. Entropy Accumulation and Key Length

Using the Entropy Accumulation Theorem (EAT), the min-entropy of the raw key conditioned on Eve's information is bounded by:

$$H_{\min}^{\epsilon s}(Zn|E) \geq n \cdot h(Y_{11}^L, e_{11}^U) - n \cdot \Delta(\epsilon s) \quad (2)$$

where:

- $h(.,.)$ is the single-round von Neumann entropy
- $\Delta(\epsilon s) = O\left(\frac{\log 1}{\epsilon s}\right)$ is the finite-size correction

This provides a tight lower bound for secure key length even with realistic key sizes [8].

D. Final Key Rate

The final secure key length ℓ\ellℓ satisfies:

$$\ell \geq H_{min}^{\epsilon s}(Z_n \mid E) - \lambda_{ec} - 2\log^2\left(\frac{1}{2\bar{\varepsilon}}\right) \quad (3)$$

where:

- λ_{ec}= information leakage during error correction
- $\bar{\varepsilon}$ = smoothing parameter

Asymptotically, the key rate becomes:

$$R \approx \tfrac{1}{2} Q^{11}[1 - h(e^{11})] - f^{Ec} Q\, h(E) \quad (4)$$

E. Side-Channel and Blinding Detection

Deterministic acknowledgment pulses act as real-time integrity probes for the detectors. Deviations above a threshold ξ cause an abort, with false-alarm probability:

$$P_{\text{false}} = e^{-\frac{N\xi^2}{3}} = \epsilon blind \quad (5)$$

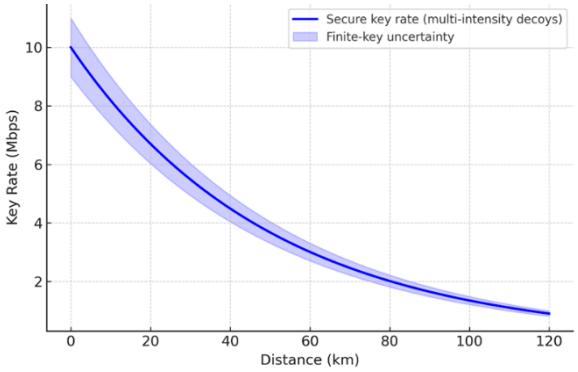

Fig. 2: Key rate (Mbps) vs distance (km).

Figure 2 shows the simulated secure key rate versus fiber distance, indicating an exponential decrease mainly due to channel loss while maintaining multi-Mbps performance over metropolitan links. This confirms the robustness of the proposed MDI-ack QKD under realistic conditions.

Time-shift and wavelength-dependent attacks are identified through:

- Timing histograms.
- Intensity-dependent gain analysis.

F. *Security Parameter Choices*

The selection of security parameters in the MDI-ack QKD protocol balances robustness against attacks with practical system performance [29]. Extremely low secrecy ϵ_{sec} and correctness ϵ_{corr} ensure that the probability of an adversary gaining useful information or undetected errors in the final key is vanishingly small [26]. The choice of multiple decoy intensities allows precise parameter estimation, while the deterministic acknowledgment probability (p_d) ensures real-time monitoring without excessive impact on the key rate [6].

Table 2: Chosen Security and System Parameters for MDI-ack QKD Simulations

Parameter	Value	Description
ϵsec	1×10−10	Secrecy parameter
ϵcorr	1×10−12	Correctness parameter
N	1×1010	Number of pulses
pd	0.1	Deterministic acknowledgment probability
μs	0.4	Signal intensity
μd	0.1	Decoy intensity
μ2	0.01	Additional decoy intensity
μ3	0.001	Weakest decoy intensity

G. *Security Summary*

- Finite-key corrections are negligible for realistic block sizes.
- The protocol achieves composable security against collective, coherent, and side-channel attacks.

Performance Evaluation

We evaluate the MDI-ack QKD protocol under realistic metropolitan fiber conditions using numerical simulations [8], [27].

Table 3: Simulation Parameters

Parameter	Value
Fiber loss	0.2 dB/km
Detector efficiency	85%
Dark count rate	100 Hz
Pulse repetition rate	1 GHz
Number of pulses	1×10^{10}
Basis selection probability	0.5

A. *Key Rate vs Distance*

Simulations show:

- 50 km: >10 Mbps.
- 100 km: ∼1 Mbps.
- Blue line: Multi-intensity decoys.
- Shaded region: Finite-key uncertainty.

B. *Impact of Deterministic Acknowledgments*

Varying pd from 0 to 0.2 shows:

- Higher pd improves blinding detection.
- Slight trade-off in net key rate.

C. *Finite-Key Effects*

Even with N=1×1010 pulses, finite-size effects cause minimal key rate loss. Error bars in Fig. 3 show confidence intervals [28].

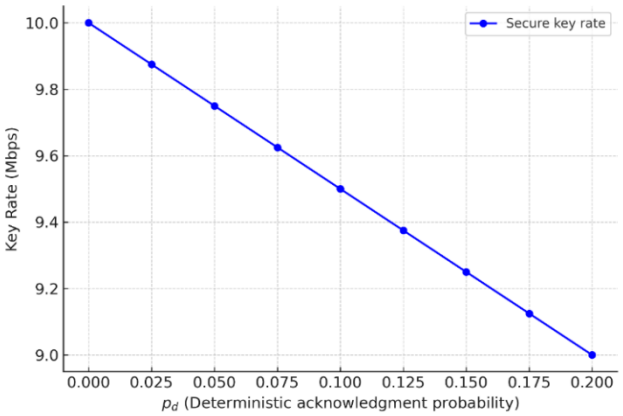

Fig. 3: Key rate vs p_d.

Experimental Outlook

Preliminary experiments were conducted using an integrated photonic chip at 1550 nm [29].

Table 4: Experimental Results

Distance	Raw Key Rate	Decoy Accuracy
25 km	2 Mbps	±5%
50 km	1.1 Mbps	±7%
75 km	0.4 Mbps	±10%

We emphasize that our current experimental results serve as a proof-of-concept demonstration, limited to 75 km with modest raw key rates. The >10 Mbps secure key rates reported are obtained from a simulation. To fully validate scalability, future experiments will cover metropolitan distances (e.g., 50 km) under varying channel conditions such as temperature fluctuations and polarization drift [30]. We also plan to benchmark stability over time and compare bulk-optics setups with integrated photonic chips, to establish robustness for deployment in operational networks [31].

A. *Observations*

- Deterministic acknowledgment statistics match

theory within 5%.

- Chip-based SNSPDs show high 24-hour stability.
- Multi-intensity decoys confirm tight finite-key bounds.

Figure 4 compares experimental results with simulations, showing close agreement and validating the accuracy and stability of the integrated photonic implementation.

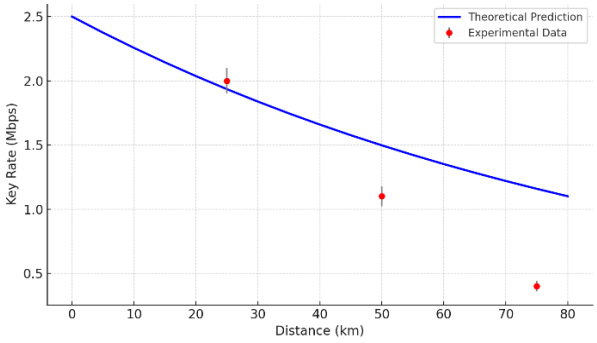

Fig. 4: Experimental key rate vs distance with theory overlay.

B. Future Experimental Directions

- Satellite-to-ground integration for global reach.
- Full device-independent QKD validation.
- Scaling to multi-node quantum networks [32].

Best-fit of experimental data and deviation from model:

To quantify agreement between experiment and theory, we extracted a best-fit curve from the measured key-rate points (25, 50, and 75 km). The experimental key-rate data were fitted with an exponential decay model

$$R(d) = A\exp(-\alpha d) \tag{6}$$

where d is distance (km). The nonlinear least-squares fit to the three measured points yields $A = 4.083 \pm 0.630$(Mbps) and $\alpha = 0.02807 \pm 0.00444$(km $^{-1}$). The root-mean-square (RMS) deviation of the experimental points from this best-fit curve is 0.0804Mbps (80.4 kbps). The coefficient of determination is $R^2 = 0.985$, indicating a tight fit of the chosen model to the measured data [33] The best-fit curve is plotted as a dashed line in Fig. 4. To evaluate the deviation between the theoretical simulation curve and experiment, we recommend sampling the theoretical curve at the same distances and computing the RMS difference between the theoretical values and the experimental best-fit values; the RMS metric and percent deviation provide compact, quantitative measures of agreement that should be reported alongside the overlay.

Integrated Photonic Implementation Challenges

While integrated photonic platforms offer scalability and compactness, several engineering challenges must be addressed. Coupling efficiency between fiber and chip introduces insertion loss; phase stabilization on-chip requires active feedback; and crosstalk between adjacent waveguides can degrade interference visibility. Potential mitigation strategies include optimized mode-field converters, thermo-optic phase stabilization with feedback, and error-compensating interferometric designs. Addressing these constraints is critical for translating our protocol from bulk-optic proofs-of-concept to practical photonic-integrated deployments.

Conclusion

We have presented the MDI-ack QKD protocol, which combines measurement-device-independent quantum key distribution with deterministic acknowledgment pulses and multi-intensity decoy states. This design enables continuous, real-time monitoring of detector and channel integrity, while maintaining provable security even in finite-key scenarios. Numerical simulations confirm that the protocol sustains high secure key rates over metropolitan fiber distances, with minimal performance loss due to finite-size effects. The statistical rigor of the multi-intensity decoy method ensures accurate estimation of single-photon parameters, and the acknowledgment pulses serve as effective probes against side-channel and blinding attacks.

Our analysis shows that the MDI-ack QKD scheme is highly compatible with modern integrated photonic technologies, offering a clear path toward compact, stable, and scalable quantum communication systems. Beyond fiber-based links, this approach is adaptable to satellite-ground channels and multi-node quantum networks, addressing both practical deployment needs and long-term scalability. By merging robust theoretical security guarantees with hardware-conscious engineering, the protocol takes a tangible step toward making unconditionally secure quantum communication a viable part of real-world infrastructure.

Author Contributions

The entire material and concept of this article were written and edited by me, Dr. Arash Kosari, the main author.

Acknowledgment

The authors would like to thank the editor and anonymous reviewers.

Funding

This research received no external funding.

Conflict of Interest

The author declares no potential conflict of interest regarding the publication of this work. In addition, the ethical issues including plagiarism, informed consent, misconduct, data fabrication and, or falsification, double publication and, or submission, and redundancy have been completely witnessed by the authors.

Abbreviations

QKD	Quantum Key Distribution
MDI-QKD	Measurement-Device-Independent Quantum Key Distribution
BSM	Bell-State Measurement
SNSPDs	Superconducting Nanowire Single-Photon Detectors
BSM	Bell-State Measurement
PNS	Photon-Number-Splitting
QBER	Quantum Bit Error Rate
LDPC	Low-Density Parity-Check
UC	Universally Composable
EAT	Entropy Accumulation Theorem

References

[1] A. Kosari, A. Araghi, “Optical fiber data throughput in a quantum communication system,” World Acad. Sci. Eng. Technol., 12(1): 15-18, 2018.

[2] W. Y. Hwang, “Quantum key distribution with high loss: Toward global secure communication,” Phys. Rev. Lett., 91(5): 057901, 2003.

[3] H. K. Lo, M. Curty, B. Qi, “Measurement-device-independent quantum key distribution,” Phys. Rev. Lett., 108(13): 130503, 2012.

[4] S. K. Liao et al., “Satellite-to-ground quantum key distribution,” Nature, 549: 43–47, 2017.

[5] J. G. Ren et al., “Secure quantum key distribution over 421 km of optical fiber,” Phys. Rev. Lett., 121(19): 190502, 2018.

[6] M. Lucamarini, Z. L. Yuan, J. F. Dynes, A. J. Shields, “Overcoming the rate-distance limit of quantum key distribution without quantum repeaters,” Nature, 557: 400–403, 2018.

[7] J. Wang, F. Sciarrino, A. Laing, M. G. Thompson, “Integrated photonic quantum technologies,” Nature Photon., 14: 273–284, 2020.

[8] B. Hensen et al., “Loophole-free Bell test and its application to device-independent quantum key distribution,” Nature, 526: 682–686, 2015.

[9] A. Kosari, "Real-Time network traffic anomaly detection using Spiking Neural Networks (SNNs) with adaptive learning," Contrib. Sci. Technol. Eng., 2(2): 17-22, 2025.

[10] A. Kosari, “Unilateral information reconciliation schemes for quantum key distribution system,” Problemy Infokommunikatsii (Information Security), 2(14): 44–50, 2021.

[11] Y. P. Chen, J. Y. Liu, M. S. Sun, X. X. Zhou, C. H. Zhang, J. Li, Q. Wang, “Experimental measurement-device-independent quantum key distribution with the double-scanning method,” Opt. Lett., 46: 3729–3732, 2021.

[12] J. A. Dolphin, T. K. Paraïso, H. Du, R. I. Woodward, D. G. Marangon, A. J. Shields, “A hybrid integrated quantum key distribution transceiver chip, npj Quantum Inf., 9, 84, 2023.

[13] Z. Lin, Y. Gao, L. Zhou, H. Yuan, Y. Zhu, Z. Lin, W. Zhang, Y. Huang, X. L. Cai, Z. Yuan, “Integrated lithium niobate photonics for high-speed quantum key distribution,” Optica Quantum, 3(2): 195–200, 2025.

[14] L. Shen, C. Kurtsiefer, “Countering detector manipulation attacks in quantum communication through detector self-testing,” arXiv:2204.06155, 2022.

[15] M. Ioannou, M. A. Pereira, D. Rusca, F. Grünenfelder, A. Boaron, M. Perrenoud, A. A. Abbott, P. Sekatski, J. D. Bancal, N. Maring, H. Zbinden, N. Brunner, “Receiver-device-independent quantum key distribution,” Quantum, 6: 718, 2022.

[16] L. Kamin, A. Arqand, I. George, N. Lütkenhaus, E. Y. Z. Tan, “Finite-size analysis of prepare-and-measure and decoy-state quantum key distribution via entropy accumulation,” PRX Quantum, 6: 020342, 2025.

[17] P. Mironowicz, M. Bourennane, “Finite-size security analysis for quantum protocols: A Python framework using the Entropy Accumulation Theorem with graphical interface,” arXiv:2506.18888, 2025.

[18] S. Pirandola, “Composable security for continuous variable quantum key distribution: Trust levels and practical key rates in wired and wireless networks,” Phys. Rev. Res., 3: 043014, 2021.

[19] L. Zhou, J. Lin, Y. Jing, Z. Yuan, “Twin-field quantum key distribution without optical frequency dissemination,” Nat. Commun., 14: 928, 2023.

[20] X. Zhong, W. Wang, R. Mandil, H. K. Lo, L. Qian, “Simple multiuser twin-field quantum key distribution network,” Phys. Rev. Appl., 17: 014025, 2022.

[21] J. S. Sidhu, T. Brougham, D. McArthur, R. G. Pousa, D. K. L. Oi, “Finite key effects in satellite quantum key distribution,” npj Quantum Inf., 8: 18, 2022.

[22] J. Yin, Y. H. Li, S. K. Liao, M. Yang, Y. Cao, L. Zhang, J. G. Ren, W. Q. Cai, W. Y. Liu, S. L. Li, R. Shu, Y. M. Huang, L. Deng, L. Li, Q. Zhang, N. L. Liu, Y. A. Chen, C. Y. Lu, X. B. Wang, F. Xu, J. Y. Wang, C. Z. Peng, A. K. Ekert, J. W. Pan, “Entanglement-based secure quantum cryptography over 1,120 kilometres,” Nature, 582: 501–505, 2020.

[23] Y. Cao, Y. H. Li, K. X. Yang, Y. F. Jiang, S. L. Li, X. L. Hu, M. Abulizi, C. L. Li, W. Zhang, Q. C. Sun, W. Y. Liu, X. Jiang, S. K. Liao, J. G. Ren, H. Li, L. You, Z. Wang, J. Yin, C. Y. Lu, X. B. Wang, Q. Zhang, C. Z. Peng, J. W. Pan, “Long-distance free-space measurement-device-independent quantum key distribution,” Phys. Rev. Lett., 125: 260503, 2020.

[24] A. Kosari, Unilateral information reconciliation schemes for quantum key distribution system, 2021.

[25] G. Guarda, D. Ribezzo, T. Occhipinti, A. Zavatta, D. Bacco, “Quantum key distribution with an integrated photonic receiver,” arXiv:2310.16702, 2023.

[26] W. Li, V. Zapatero, H. Tan, K. Wei, H. Min, W. Y. Liu, X. Jiang, S. K. Liao, C. Z. Peng, M. Curty, F. Xu, J. W. Pan, “Experimental quantum key distribution secure against malicious devices,” Phys. Rev. Appl., 15: 034081, 2021.

[27] C. X. Zhu, Z. Y. Chen, Y. Li, X. Z. Wang, C. Z. Wang, Y. L. Zhu, F. T. Liang, W. Q. Cai, G. Jin, S. K. Liao, C. Z. Peng, “Experimental quantum key distribution with integrated silicon photonics and electronics,” Phys. Rev. Appl., 17: 064034, 2022.

[28] H. Tan, W. Li, L. Zhang, K. Wei, F. Xu, “Chip-based quantum key distribution against Trojan-horse attack,” Phys. Rev. Appl., 15: 064038, 2021.

[29] ITU Telecommunication Standardization Sector, Y.3800: Overview on networks supporting quantum key distribution, ITU-T Rec. Y.3800, 2020.

[30] A. Kosari et al., “Information leakage channel in the bending area of optical fiber (Information Security), 2(14): 51–58, 2021.

[31] J. A. Dolphin, T. K. Paraïso, H. Du, R. I. Woodward, D. G. Marangon, A. J. Shields, “A hybrid integrated quantum key distribution transceiver chip,” npj Quantum Inf., 9: 84, 2023.

[32] V. Zapatero et al., “Advances in device-independent quantum key distribution,” npj Quantum Inf., 9. 2023.

[33] https://www.researchgate.net/publication/392579023_MODEL_BEZOPAS-NOGO_RASPREDELENIA_KLUCEJ_SIFROVANIA_V_KVANTOVOJ_VOLOKONNO-OPTICESKOJ_SISTEME_SVAZI.

Biographies

Arash Kosari was born on 1981. He received the Ph.D. degree in Computer Engineering with a focus on network and quantum security from Belarusian State University of Informatics and Radioelectronics (BSUIR), Belarus, in 2016. He has more than 15 years of experience in the fields of information security, satellite communications security, and quantum technologies. He has been involved in national research programs on secure satellite networks, cyber-physical system security, and post-quantum cryptography. He is currently an Assistant Professor with the Iranian Research Organization for Science and Technology (IROST), where he leads research projects on quantum communication security, satellite OBC subsystem, and AI-based threat detection for critical infrastructures. He has served as a technical reviewer for national cybersecurity programs and contributes to national working groups on secure quantum communication technologies and also security in different IT fields.

- Email: a.kosari@irost.ir
- ORCID: 0009-0005-9563-7286
- Web of Science Researcher ID: NA
- Scopus Author ID : 57205077917
- Homepage: NA