Satellite-Based Quantum Key Distribution: Protocols, Network Architectures, and Continuous-Variable Implementation Challenges

Cássio de Castro Silva[1], Rodrigo Dias Paolillo[1], Antônio Pereira Junior[1], Adriane Martins Alves[1], Yasmin da Silva Bonfim[1], Paulo Monteiro de Carvalho Monson[1], Adler Lima Botelho de Azevedo[1], Luiz Fernando Taboada Gomes Amaral[1], Braian Pinheiro da Silva[1]*, Valéria Loureiro da Silva[1]
[1]QuIIN, SENAI CIMATEC University; Salvador, Bahia, Brazil

Losses and attenuation are the main limitations to implementing secure quantum networks based on fiber or free-space optical links over long distances. A hybrid satellite–ground approach offers an effective solution to overcome these constraints and achieve higher key transmission rates. This article presents a systematic review of publications on satellite quantum communication, providing an overview of quantum key distribution with satellites, the use of satellite networks with emphasis on commonly adopted orbits, and the role of satellites in such architectures. Special attention is given to the implementation of continuous-variable QKD (CV-QKD) in satellite-based channels, highlighting its challenges and potential for integration into future satellite-based quantum networks
Keywords: Quantum Key Distribution. Satellite. Satellite-based QKD. Free-Space Optics. Continuous-Variable QKD.
Abbreviations: QKD, Quantum Key Distribution. DV-QKD, Discrete-Variable Quantum Key Distribution. CV-QKD, Continuous-Variable Quantum Key Distribution. SatQKD, Satellite-based Quantum Key Distribution. FSO, Free-Space Optics. GEO, Geostationary Orbit. LEO, Low Earth Orbit. SNR, Signal-to-Noise Ratio. PATS, Pointing Acquisition and Tracking Subsystem. LO, Local Oscillator. SKR, Secure Key Rate. QPSK, Quadrature Phase-Shift Keying.

Despite the predominance of classical systems in everyday applications such as television, the internet, and GPS, advances in quantum communication are transforming the telecommunications sector, particularly in data security. Quantum Key Distribution (QKD) enables encrypted information exchange with enhanced security and is being tested in projects such as satellite communications to protect data against interception, even by agents with advanced technology.

A systematic review is a research method that analyzes the literature on a topic using explicit criteria for searching and synthesizing information. This approach minimizes bias, consolidates evidence, and identifies gaps in knowledge [1]. The process involves three steps: (1) planning (defining objectives and selection criteria), (2) execution (filtering studies and extracting data), and (3) analysis and synthesis [2]. In rapidly evolving areas such as satellite-based quantum optical communication, where studies are abundant but dispersed, this methodology is essential for mapping the state of the art, guiding future research, and validating scientific results.

Materials and Methods

This study conducted a targeted search on QKD in satellite communications using LENS.org, Web of Science, and IEEE Xplore. The search focused on experimental and space-oriented applications, considering journal and conference articles published between 2015 and 2025. The initial results included 266 records from LENS.org, 116 from Web of Science, and 52 from IEEE Xplore. Python scripts were used to remove duplicates and correct metadata inconsistencies. The query applied was: ("quantum key distribution" OR "QKD" OR "CV-QKD" OR "continuous variable

Received on 26 October 2025; revised 18 January 2026.
Address for correspondence: Braian Pinheiro da Silva. Av. Orlando Gomes, 1845 - Piatã, Salvador – BA – Brazil, Zipcode: 41650-010. E-mail: braian.silva@fieb.org.br

J Bioeng. Tech. Health 2026;9(2):162-168

QKD") AND ("satellite" OR "space-based" OR "space- to-ground" OR "inter-satellite" OR "orbital" OR "LEO" OR "GEO" OR "space link" OR "optical space link" OR "SAT-QKD") AND ("experiment" OR "demonstration" OR "implementation" OR "field trial") NOT ("fiber" OR "terrestrial network" OR "optical fiber").

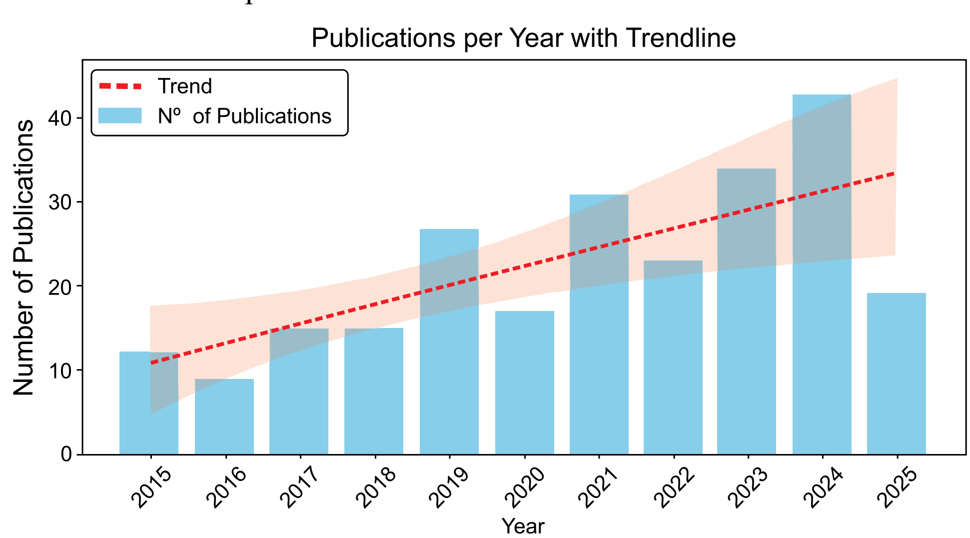
After automated and manual screening, 245 relevant publications remained. Figure 1 shows the annual distribution of satellite-based QKD research, with a linear trendline confirming steady growth. Most (79.2%) address satellite-based QKD, whereas only 6.8% specifically examine CV-QKD protocols. The remainder cover broader theoretical discussions or less-defined approaches. These results underscore the predominance of satellite-based QKD research, with CV-QKD emerging as a promising subfield. All references in subsequent sections were drawn from this systematic search.

Quantum Key Distribution Protocols

Quantum key distribution protocols are classified into discrete variable (DV-QKD) and continuous variable (CV-QKD) schemes, differing in their implementation requirements and operational principles. DV-QKD protocols encode information in the polarization, phase, or time-bin degree of freedom of single photons, requiring expensive single-photon detectors [3], whereas CV-QKD uses coherent states with quadrature modulation, enabling high-efficiency homodyne or heterodyne detection and leveraging existing telecommunications infrastructure for enhanced scalability [4]. The foundational DV-QKD protocol, BB84, encodes information in the polarization states of photons, allowing communicating parties (Alice and Bob) to detect eavesdropping (Eve) through quantum superposition principles and No-cloning theorem [5, 6]. Enhanced with decoy-state methods, this protocol has demonstrated robust satellite implementations resistant to photon number-splitting attacks [3,7-9].

A critical challenge in satellite-mediated QKD involves establishing trust in the orbital platform, which typically relays signals between ground stations without direct connection [3]. While conventional BB84 requires treating the satellite as a trusted node, measurement-device-independent (MDI) protocols circumvent this limitation by having the satellite (Charlie) perform Bell measurements on quantum states from both parties before broadcasting results [10,11]. This approach enables secure key establishment without relying on Charlie's integrity, although atmospheric turbulence in free-space optics poses implementation challenges [10]. Nevertheless,

Figure 1. Annual distribution of publications from 2015 to 2025 with linear trendline.



multiple studies have confirmed the feasibility of MDI-QKD [11-13], including satellite-based CV-QKD demonstrations [14].

Entanglement-based protocols represent another significant advancement, with extensive theoretical [15-20] and experimental [21] developments. In these schemes, Charlie distributes entangled photon pairs to Alice and Bob, who perform measurements and basis reconciliation via authenticated channels. The BBM92 protocol extends BB84 by incorporating entanglement measurements, eliminating reliance on Charlie's trustworthiness [16].

Satellite-Based Quantum Key Distribution Networks

With advances in quantum technologies, satellite communication is becoming essential for the realization and scalability of future quantum networks [7]. Although they have their own limitations, especially related to complications involving the link, positioning, and distribution of satellites, functional applications of quantum key distribution are already known in the literature [3,8,14,22].

The use of satellites in QKD depends on factors such as the distance between ground stations, the number of satellites available, and the protocol adopted. The last one is particularly critical, as it influences and adapts to the other parameters.

Hybrid ground-space integration offers a promising solution to mitigate high attenuation in fiber channels and atmospheric losses in free-space optical (FSO) links. China has demonstrated this approach with an integrated quantum network combining fiber and satellite-to-ground links, achieving a 4,600 km range and a key rate of 47.0 kbps in 2021 [3].

A major challenge in such systems is maintaining alignment between moving satellites. Studies from Australia and Singapore indicate that with a residual pointing error of 10 μrad, operation is feasible up to 400 km; however, the Pointing, Acquisition, and Tracking Subsystem (PATS) experiences Signal-to-Noise Ratio (SNR) limitations beyond 150 km due to weak tracking-beacon signals [23].

The successful implementation of satellite-based QKD systems fundamentally depends on the alignment between orbital mechanics and quantum communication requirements. Different orbital configurations present distinct advantages for QKD applications, with altitude, inclination, orbital period, and coverage characteristics directly influencing protocol selection, link performance, and system viability.

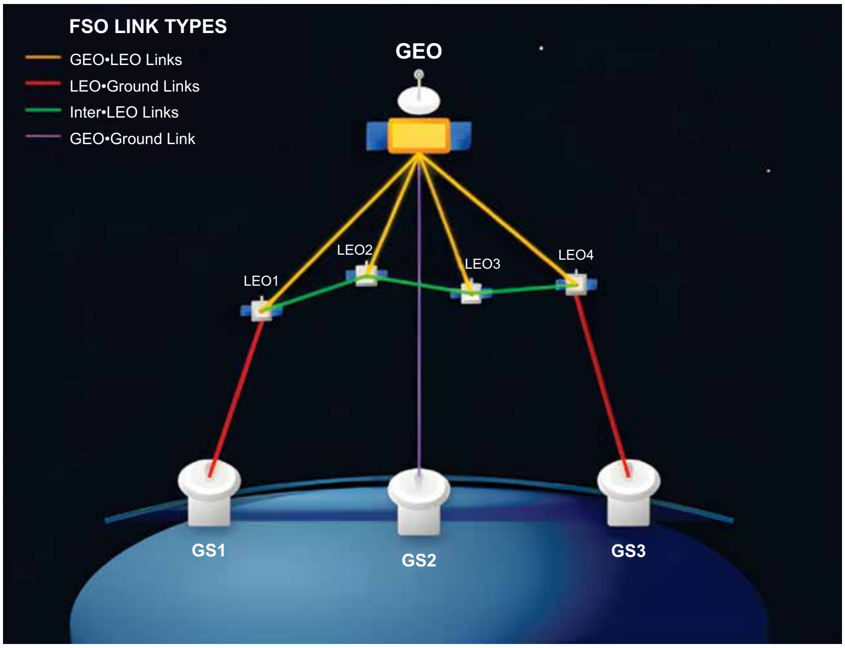
These parameters critically determine key distribution efficiency, as quantum communication performance exhibits strong dependence on satellite elevation, access duration, and ground station visibility windows. A systematic evaluation of orbital dynamics reveals how specific orbital regimes optimize different aspects of QKD implementations.

<u>Low Earth Orbit</u>

Low Earth Orbit (LEO) satellites (500-1,200 km altitude) are crucial for quantum communications, as demonstrated by China's Micius satellite [24,25]. However, these systems face significant signal attenuation (20-30 dB downlink, up to 69 dB uplink) [26], with atmospheric turbulence causing transmittance fluctuations that impair protocol efficiency [18,27]. Their Earth proximity offers advantages including reduced diffraction losses [28], relaxed pointing requirements, and simplified adaptive optics needs [29] (Figure 2).

The BB84 protocol remains the preferred PM-DV- QKD choice due to its simplicity and proven security [28], typically implemented in S/C bands where single-photon detectors perform optimally [28]. Operational challenges include intermittent coverage with brief access windows (minutes per day) [3, 30] and demanding tracking requirements due to orbital motion [31]. While finite-size effects impact key rates, their effect is less pronounced in LEO [24].

Figure 2. Schematic diagram of the communication between a constellation of satellites and earth stations.



Yellow lines represent optical links between the GEO satellite and LEO CubeSats, which are interconnected by green lines. The red line indicates the link between an LEO and the ground stations (GSs), while the purple line shows the link from the GEO to the GSs.

Geostationary Orbit (GEO)

GEO satellites, located at an altitude of 35,786 km, have complementary characteristics that can be valuable for global quantum networks. This configuration allows permanent connections between the satellite and fixed ground stations, eliminating the complexity of handover between multiple satellites in LEO constellations.

Experiments with Micius have shown that with each handover in LEO, the system requires precise telescope realignment, new negotiation of QKD parameters, and interruption of the quantum key stream [3,25]. With the extended visibility of the GEO orbit, this problem would be mitigated, allowing continuous data accumulation [24], coverage also simplifies network management by reducing tracking complexity.

This operational difference is particularly relevant in CV-QKD, where link stability is crucial for error correction and privacy amplification protocols allowing the implementation of advanced post- processing schemes that require prolonged iterative exchanges between parties [32]. They offer the advantage of maintaining a continuous connection for extended periods, allowing extended QKD operations, and provide 24/7 availability without orbital restrictions [30]. A GEO system can point to a target user on demand in a short time, without the orbital constraints imposed on a LEO system by orbital mechanics [30]. Measurements of quantum-limited signals from a geostationary satellite can show total losses of 69 dB [26].

Satellite-Based CV-QKD: Challenges and Approaches

Satellite-based CV-QKD employs space-qualified optical communication hardware, enabling high- speed operation with IQ modulators and coherent receivers, making it a scalable and cost-effective option for global quantum networks [16,24,27,33,34].

CV-QKD protocols may have a practical advantage in free-space applications, especially in satellite-based channels, because a homodyne detector, in which the signal is coupled to an intense, narrow-band local oscillator (LO) beam, intrinsically filters out background radiation at non-coincident wavelengths [26], this suggests that CV-QKD can operate in strong stray light conditions and potentially during the day, which for discrete variable protocols would require additional filtering, increasing attenuation and complexity [29].

CV-QKD in FSO and satellite-to-ground links has been investigated theoretically [24], detailed analyses address the feasibility of CV-QKD with Gaussian modulation in uplink scenarios, considering practical factors such as atmospheric turbulence and pointing errors under dynamic and time-varying orbital parameters [32].

Studies also analyze satellite-to-ground CV-QKD in the downlink scenario, which is more favorable for the transmission [33,35], preliminary experiments were carried out on signal transmission in FSO and satellite-to-ground links [24]. More recent proposals include the use of optical phase-shift keying (QPSK) signaling and dual heterodyne/threshold detection receivers to increase the reliability and feasibility of satellite entanglement-based FSO-CV-QKD systems [34].

One of the main challenges of CV-QKD is its lower robustness to transmission losses compared to DV-QKD [32]. With current homodyne detectors, positive secure key rates (SKR) can be achieved only for losses not exceeding 20–25 dB, which is very challenging in satellite-to-ground links [29]. For comparison, positive secure key rates with channel losses exceeding 69 dB (over fiber) have been demonstrated with DV-QKD [29].

Satellite-to-ground links are characterized by strongly variable channel attenuation (fading) [18], atmospheric turbulence induces phenomena such as beam wandering and beam broadening, which increase the average link loss [33] to higher orbits, key generation is affected by finite size effects, due to the limited number of symbols exchanged in a single satellite pass for high-loss channels [26], these can be mitigated by achieving higher transmission rates or considering multiple satellite passes [24].

Although CV-QKD employs standard telecom components, the need for a phase-stabilized local oscillator can raise implementation costs [27]. Atmospheric turbulence is stronger in the uplink, where the signal is affected early in the channel [33], whereas in the downlink most of the path is in vacuum, reducing turbulence effects [7, 35].

Simulations indicate that uplink QKD in the Micius orbit remains highly challenging and is more feasible in lower orbits [32]. To enhance uplink CV-QKD performance, optimization of orbital parameters, beam spot size, receiving aperture, and modulation variance has been proposed [32].

Segmenting the satellite pass and extracting keys from each segment, rather than from the entire pass, improves robustness against channel noise and enables secure key generation even under active collective attacks; this approach also mitigates fading, increasing the secure key rate and enabling communication with higher-altitude satellites [26].

The use of squeezed states extends CV-QKD operation to higher loss and noise levels under given security assumptions, though compression must be optimized for collective-attack scenarios [18]. CV-QKD with discrete modulation offers lower implementation requirements, acceptable key rates, and compatibility with existing infrastructure. In satellite-to-ground links, where payload weight is critical, the homodyne protocol with QPSK shows greater tolerance to excessive noise [33,34].

Conclusion

The coexistence of classical and quantum applications in different satellite orbits demonstrates the potential for faster and more secure global communication. While GEO satellites offer broad coverage for QKD over long distances, LEO satellites stand out for their low latency, essential for real-time applications.

Hybrid integration, as demonstrated by the Micius fiber-optic network, is already a reality and is expected to expand as satellite constellations evolve. The most promising solution for global quantum networks may lie precisely in the synergistic integration of these two approaches, combining the high transmission rate of LEO satellites with the continuous coverage provided by GEO satellites [32].

This integration will, however, require significant advances on several fronts, including the development of dedicated QKD satellites, more robust protocols for operation in high-attenuation conditions, and the standardization of interfaces between the ground and space segments. The studies analyzed suggest that, with appropriate investment and technological development, satellite-based quantum networks could become an operational reality within the next decade, thus revolutionizing the secure communications landscape on a global scale.

Acknowlegement

This work has been fully/partially funded by the project Implementação do sistema CV-QKD em uma rede quântica real supported by Quantum Industrial Innovation (QuIIN) - EMBRAPII CIMATEC Competence Center in Quantum Technologies, with financial resources from the PPI IoT/Manufatura 4.0 of the MCTI grant number 053/2023, signed with EMBRAPII.

References

1. Rosana Ferreira Sampaio and Marisa Cotta Mancini. Estudos de revisão sistemática: um guia para síntese criteriosa da evidência científica. Brazilian journal of physical therapy, 11:83–89, 2007.
2. Barbara Kitchenham et al. Procedures for performing systematic reviews. Keele, UK, Keele University, 33(2004):1–26, 2004.
3. Yu-Ao Chen, Qiang Zhang, et al. An integrated space-to-ground quantum communication network over 4,600 kilometres. Nature, 589(7841):214–219, 2021.
4. Zhen Qu and Ivan B Djordjevic. High-speed free-space optical continuous-variable quantum key distribution enabled by three-dimensional multiplexing. Optics Express, 25(7):7919–7928, 2017.
5. Wimar Klop, Rudolf Saathof, et al. Qkd optical ground terminal developments. In International Conference on Space Optics—ICSO 2020, volume 11852, pages 388–403. SPIE, 2021.
6. Murali Krishna Pasupuleti. Quantum key distribution protocols: Security analysis and real-world implementations. International Journal of Academic and Industrial Research Innovations(IJAIRI), 05:267–278, 06 2025.
7. Sheng-Kai Liao, Wen-Qi Cai, et al. Satellite-to-ground quantum key distribution. Nature, 549(7670):43–47, 2017.
8. Sheng-Kai Liao, Hai-Lin Yong, et al. Long-distance free-space quantum key distribution in daylight towards inter-satellite communication. Nature Photonics, 11(8):509–513, 2017.
9. Giulia Guarda, Domenico Ribezzo, et al. Bb84 decoystate qkd protocol over long-distance optical fiber. In 2023 23rd International Conference on Transparent Optical Networks (ICTON), pages 1–4. IEEE, 2023.
10. Yuan Cao, Yu-Huai Li, et al. Long-distance free-space measurement-device-independent quantum key distribution. Physical Review Letters, 125(26):260503, 2020.
11. Xingyu Wang, Chen Dong, et al. Feasibility of space-based measurement-device-independent quantum key distribution. New Journal of Physics, 23(4):045001, 2021.
12. Dong Chen, Zhao Shang-Hong, et al. Measurement-device-independent quantum key distribution with q-plate. Quantum Information Processing, 14(12):4575– 4584, 2015.
13. Hoi-Kwong Lo, Marcos Curty, et al. Measurement-device-independent quantum key distribution. Physical review letters, 108(13):130503, 2012.
14. Qingquan Peng, Ying Guo, et al. Satellite-to-submarine quantum communication based on measurement-device-independent continuous-variable quantum key distribution. Quantum Information Processing, 21(2):61, 2022.
15. Dong Chen, Shang-Hong Zhao, et al. Measurement-device-independent quantum key distribution with pairs of vector vortex beams. Physical Review A, 93(3):032320, 2016.
16. Minh Q Vu, Hoang D Le, et al. Entanglement-based satellite fso/qkd system using dual-threshold/direct detection. In ICC 2022-IEEE International Conference on Communications, pages 3245–3250. IEEE, 2022.
17. Xinliang Wei, Lei Fan, et al. Optimizing satellite-based entanglement distribution in quantum networks via quantum-assisted approaches. In 2024 International Conference on Quantum Communications, Networking, and Computing (QCNC), pages 280–287. IEEE, 2024.
18. Nedasadat Hosseinidehaj and Robert Malaney. Cv-qkd with gaussian and non-gaussian entangled states over satellite-based channels. In 2016 IEEE Global Communications Conference (GLOBECOM), pages 1–7. IEEE, 2016.

19. Johannes Pseiner, Lukas Achatz, et al. Experimental wavelength-multiplexed entanglement-based quantum cryptography. Quantum Science and Technology, 6(3):035013, 2021.
20. Xiaoyu Ai, Robert Malaney, et al. Short codes and entanglement-based quantum key distribution via satellite. In 2017 Sensor Signal Processing for Defence Conference (SSPD), pages 1–5. IEEE, 2017.
21. Sebastian Ecker, Johannes Pseiner, et al. Advances in entanglement-based qkd for space applications. In International Conference on Space Optics—ICSO 2022, volume 12777, pages 925–945. SPIE, 2023.
22. Sheng-Kai Liao, Jin Lin, et al. Space-to-ground quantum key distribution using a small-sized payload on tiangong-2 space lab. Chinese Physics Letters, 34(9):090302, 2017.
23. Denis Naughton, Robert Bedington, et al. Design considerations for an optical link supporting intersatellite quantum key distribution. Optical Engineering, 58(1):016106–016106, 2019.
24. Daniele Dequal, Luis Trigo Vidarte, et al. Feasibility of satellite-to-ground continuous-variable quantum key distribution. npj Quantum Information, 7(1):3, 2021.
25. Aleksandr Khmelev, Alexey Duplinsky, et al. Eurasian-scale experimental satellite-based quantum key distribution with detector efficiency mismatch analysis. Optics Express, 32(7):11964–11978, 2024.
26. Ivan Derkach and Vladyslav C Usenko. Applicability of squeezed-and coherent-state continuous-variable quantum key distribution over satellite links. Entropy, 23(1):55, 2020.
27. Guoqi Huang, Ziang Song, et al. Enhanced performance of measurement-device-independent quantum key distribution over turbulent channels through adaptive optics: G. huang et al. Quantum Information Processing, 23(3):68, 2024.
28. Satya Ranjan Behera and Urbasi Sinha. Estimating the link budget of satellite-based quantum key distribution (qkd) for uplink transmission through the atmosphere. EPJ Quantum Technology, 11(1):66, 2024.
29. Davide Orsucci, Philipp Kleinpaß, et al. Assessment of practical satellite quantum key distribution architectures for current and near-future missions. International Journal of Satellite Communications and Networking, 43(3):164–192, 2025.
30. Angel Alvaro, Luis Pascual, et al. Caramuel: The future of space quantum key distribution in geo. In 2022 IEEE International Conference on Space Optical Systems and Applications (ICSOS), pages 57–65. IEEE, 2022.
31. Peide Zhang, Jaya Sagar, et al. End-to-end demonstration for cubesatellite quantum key distribution. IET Quantum Communication, 5(3):291–302, 2024.
32. Jin Cheng, Yujie Chen, et al. Feasibility and parameter optimization of ground-to-satellite uplink continuous-variable quantum key distribution. New Journal of Physics, 27(2):023011, 2025.
33. Jinyi Li, Jian Zhou, et al. Discrete modulation continuous variable quantum key distribution under fast fading channel. Physica Scripta, 99(11):115118, 2024.
34. Thang V Nguyen, Hoa T Le, et al. Enhancing design and performance analysis of satellite entanglement-based cv-qkd/fso systems. IEEE Access, 11:112097–112107, 2023.
35. Yichen Gao, Guanqun Song, and Ting Zhu. Optimizing global quantum communication via satellite constellations. arXiv preprint arXiv:2501.00280, 2024.