

From Theory to Orbit: Security Proofs as Drivers for Space-Based QKD System Architecture

L. Trotta^{*a}, M. Ottavi^{†a}, C. G. Carosella^a, A. Galdini^a, M. Savaresi^a, L. Renella^a, S. Denaro^a, A. Pisano^a

^aThales Alenia Space – Italia, Via Saccomuro, 24, 00131 Rome, Italy

^{*}laura.trotta@thalesaleniaspace.com

[†]martina.ottavi@thalesaleniaspace.com

ABSTRACT

Quantum Key Distribution (QKD) offers unprecedented security for the exchange of cryptographic keys, relying on the principles of quantum mechanics. However, the confidence in this security comes from rigorous security proofs, which are mathematical demonstrations bounding the power of any adversary, and quantifying the achievable security in real, noisy, and lossy systems. For satellite QKD missions, the choice and implementation of security proofs have a profound impact on system architecture, subsystem requirements, protocol selection, and network feasibility. This article analyzes, from a systems engineering perspective, how the security proof and their practical "finite-size" implications influence the design, operation, and performance evaluation of space-based QKD networks and viceversa. We discuss key driving parameters, highlight the required technological adaptations, and propose guidelines for aligning mission and security requirements in ongoing and future satellite QKD constellations.

Keywords: QKD, Quantum Communications, Optical Communications, Space Communications, Security Proofs

1. INTRODUCTION

Quantum Key distribution (QKD) is a method for establishing cryptographic keys between two distant parties whose security rests on the laws of quantum mechanics rather than on the computational hardness of a mathematical problem. A security proof is the rigorous mathematical demonstration that quantifies exactly how much information an eavesdropper could, in principle, extract from a given QKD implementation, and it is this proof — not the protocol alone — that ultimately certifies the key as secure.

The rapid advancement of quantum computing technologies poses an existential threat to asymmetric public-key cryptography (e.g., RSA, ECC) through Shor's algorithm. In response, QKD has emerged as a physically secure key distribution method that guarantees Information-Theoretic Security (ITS) based on the laws of quantum mechanics rather than computational hardness assumptions. While terrestrial fiber-based QKD networks have demonstrated commercial viability over regional distances (<100-200 km), exponential photon attenuation in optical fibers severely restricts long-distance global deployment.

Space-based QKD leverages satellite platforms, operating primarily in Low Earth Orbit (LEO), to bypass terrestrial channel losses. Because atmospheric optical attenuation drops rapidly above 10 km, free-space laser links between satellites and Optical Ground Stations (OGT) exhibit diffraction-dominated channel losses that scale quadratically with distance rather than exponentially. Consequently, satellite constellations represent the primary viable topology for building a global-scale Quantum Internet.

However, transitioning QKD from pristine laboratory optical benches to dynamic space environments introduces severe engineering challenges. Satellites operate under stringent mass, volume, power, and thermal constraints, subjected to harsh radiation environments, extreme temperature gradients, and high dynamic

{OPEN}

Doppler shifts. Crucially, a LEO satellite pass over an OGS typically lasts between 300 and 600 seconds. This brief contact window severely restricts the total number of raw quantum pulses (N) exchanged per pass.

In classical QKD theoretical formulations, security proofs often assume an asymptotic regime ($N \rightarrow \infty$). In space systems, this assumption fails catastrophically. The small block sizes enforce a finite-size security regime, wherein statistical fluctuations in error estimation, privacy amplification overheads, and failure probability parameters (ϵ) [6] dramatically degrade the Secret Key Rate (SKR). Therefore, security proofs must not be treated as passive mathematical verifications applied post-facto; rather, they must serve as active primary design drivers that govern the end-to-end systems engineering of satellite QKD payloads, platforms, and network topologies.

The remainder of this article is organized as follows. Section 2 introduces the systems engineering paradigm shift required for space QKD, framing formal security proofs and practical security engineering as complementary pillars within a continuous co-engineering loop between mathematical assumptions and physical platform design. Section 3 lays out the mathematical foundations of the finite-key regime, deriving how block size orbital pass geometry, and elevation-dependent channel loss jointly bound the extractable secret key, and compares analytical and numerical proof techniques as two complementary paths to certifying that bound. Section 4 translates these proof-level requirements into concrete subsystem specifications for the space segment, covering intensity modulator stability, polarization optics, quantum random number generation, pointing and tracking precision, and radiation-induced detector aging. Section 5 examines how the choice of security proof shapes architecture-level trade-offs, comparing downlink and uplink topologies and trusted-node versus entanglement-based network design. Section 6 concludes and outlines a roadmap for aligning mission and security requirements in future satellite QKD constellations.

1.1 INSTITUTIONAL CONTEXT

Today's QKD systems operate in a rapidly expanding market, with many organizations working in parallel to build fully integrated and secure QKD infrastructures.

Europe has its own strategy for quantum technologies, built on three research pillars: quantum computing, quantum sensing, and quantum communication. The strategy's five main objectives are to coordinate a large number of partners at the European Union level, to secure long-term programmatic commitments (such as the Quantum Flagship initiative and the Digital Europe Programme), to foster a pan-European quantum ecosystem, to establish standardized infrastructures such as EuroQCI, and to position Europe as a global leader in quantum technologies. Substantial funding has been allocated to the projects underpinning this roadmap.

Thales Alenia Space Italia aims to become a key player in the development of satellite-based quantum technologies and in the definition of global-scale quantum networks. Drawing on over 40 years of experience and a unique combination of skills, expertise, and cultures, Thales Alenia Space delivers cost-effective solutions for telecommunications, navigation, Earth observation, environmental management, exploration, science, and orbital infrastructures. The company's roadmap in this domain centers on strengthening laboratories, research activities, and enabling projects in quantum technologies.

The company's main initiatives in recent years include:

- In coordination with ESA: the Security And CryptoGraphic (SAGA) Mission, 1st Generation. The ESA SAGA project will design, develop, and validate the EuroQCI space segment.
- In coordination with the European Commission: LAIQA (Horizon), a technology-intensive research and innovation action to build a global space-based quantum network.
- In coordination with the European Commission: QUDICE (Horizon), focused on the development of multi-platform QKD technology.

{OPEN}

- In coordination with ESA: Quantum Security Validation Platform (QSVP), an integrated reference architecture designed to analyse and validate quantum and post-quantum technologies for Space systems.
- In coordination with the European Commission: QUID, for the realization of Italian quantum communication network.
- In coordination with the Italian Government: National Quantum Science and Technology Institute (NQSTI), realization of a hybrid (free-space + fiber) QKD link definition, design and simulation of a space-based Quantum Network System for distributed Quantum Sensing and Computing.
- In coordination with ASI: Robust Entanglement Source (RES), realization of a prototype polarization-entangled photon-pair source for QKD-based quantum key distribution, intended for use in satellite missions.
- In coordination with ASI: Optima, and end-to-end optical terminals system.

Thales Alenia Space is currently in Phase B2 of SAGA, the pilot project for demonstrating QKD protocols and their security. The system design was conceived to accommodate the full range of trade-offs between performance and security, with the security proof playing a guiding role throughout. To this end, an end-to-end testbed was designed and built to validate unit-level functionality. The design of these units was driven by the results of two distinct security proof approaches, both accounting for real component non-idealities and their impact on the security of the implemented QKD protocol. The outcome is a rigorous mathematical demonstration of the system's invulnerability against adversaries with unbounded resources. Through these advances, the security proof has moved beyond the purely theoretical domain into a concrete application, tested in Thales Alenia Space Italia's laboratories. The resulting units will be integrated into the SAGA satellite, Europe's first demonstrator to deliver information-theoretically secure cryptographic key generation and distribution to real users.

2. THE SYSTEMS ENGINEERING PARADIGM SHIFT: SECURITY PROOFS AS PRIMARY DESIGN DRIVERS

Traditional space mission design follows a top-down waterfall architecture: science/mission goals dictate data throughput requirements, which derive Link Budgets, specifying Payload Apertures and Transmitter Power, ultimately sizing Power Subsystems (EPS) and Mass Margins. In a satellite in QKD mission, this linear methodology breaks down because quantum channel capacity cannot be scaled simply by boosting transmitted power. Increasing laser pulse power introduces multi-photon states, exposing the protocol to Photon Number Splitting (PNS) attacks and severely reducing secret key yield.

Consequently, space QKD requires a bidirectional Co-Engineering Loop where security proof assumptions directly drive subsystem specifications, while physical orbit and hardware limitations feed back into proof bounds.

To build an integrated system framework, it is vital to recognize that mathematical security proofs and practical security engineering represent two complementary, mutually reinforcing pillars of space system security. While a formal security proof guarantees Information-Theoretic Security (ITS) against quantum eavesdropping techniques, such as photon number splitting or collective state manipulation, it operates strictly under idealized abstraction models. In a real-world space deployment, physical vulnerabilities fall outside the theoretical scope of quantum proofs. Risks such as Trojan-horse optical reflection attacks, laser-seeding exploits, power side-channel leaks, and firmware tampering on onboard processors must be systematically addressed by security engineering practices. Rather than viewing these two domains as isolated efforts, security proofs protect against mathematically modeled channel threats, whereas security engineering safeguards the physical platform and surrounding infrastructures.

{OPEN}

Achieving a truly resilient satellite architecture requires embedding theoretical security models within a continuous Security Risk Assessment (SRA) lifecycle. Physical hardware deviations identified during dynamic threat modeling feed directly back into the security proof equations as system noise parameters. Simultaneously, security engineering enforces supply chain verification, optical isolator placement to block side-channel reflections, and secure boot architectures for onboard FPGA controllers. This ensures that the physical satellite platform strictly abides by the foundational operational assumptions required for mathematical security proofs to remain valid throughout the satellite operational lifespan.

3. MATHEMATICAL FOUNDATIONS & FINITE-KEY EFFECTS IN SATELLITE CHANNELS

Secret Key Rate Formulation under Finite-Size Regime

To quantify the impact of security proofs on space systems, consider the standard finite-key formulation for decoy state BB84 protocol. The extracted secret key length (ℓ) from a raw block of size N is expressed as [8]:

$$\ell = \lfloor s_{X,0} + s_{X,1}(1 - h(\phi_X)) \rfloor - \lambda_{EC} - 6 \log_2 \frac{21}{\epsilon_{sec}} - \log_2 \frac{2}{\epsilon_{cor}}$$

where $s_{X,0}$ and $s_{X,1}$ represent the lower bounds on zero-photon (vacuum) and single-photon counts in the X-basis; ϕ_X is the upper bound on the phase error rate of single photon events; $h(x) = -x \log_2 x - (1 - x) \log_2 (1 - x)$ is the binary entropy function; λ_{EC} is the number of bits published during Error Correction; and ϵ_{sec} , ϵ_{cor} denote the secrecy and correctness security parameters.

In an asymptotic regime ($N \rightarrow \infty$), statistical fluctuation vanish, and ϕ_X converges precisely to the measured bit error rate e_{bit} . In real satellite pass, however, the number of exchanged pulses N is necessary finite, typically on the order of 10^6 to 10^8 per pass, and the phase error rate cannot be measures directly; it must instead be interferred from the error rate observed on a limited sample. Standard statistical tail bounds, such as Hoeffding's Inequality or Chernoff Bounds [8][10], are used to convert this finite sample into a conservative upper bound on the true phase error rate, at the cost of an additional statistical margin that must be added to guard against an unlucky, non-representative sample.

Critically, this margin shrinks only as the inverse square root of the sample size: doubling the number of detected events does not halve the margin, but reduces it by only about thirty percent, so its effect fades slowly rather than quickly. When the number of detected signals is small, as is often the case during a short or low-elevation satellite pass, this statistical margin dominates the phase error rate estimate, pushing it toward its maximum plausible value and, through the entropy penalty in the key-length formula, collapsing the provable secret key length to zero. This mathematical reality enforces a strict minimum threshold for collected photons per pass.

Impact of Orbital dynamics on block formation

In a typical LEO pass (e.g., altitude 500 km), the slant range varies dynamically from ~ 1695 km at 10° elevation down to 500 km at zenith. Channel loss fluctuate due to free-space path loss ($L_{FSP} \propto \left(\frac{4\pi R}{\lambda}\right)^2$), atmospheric absorption, and beam wander caused by atmospheric turbulence. Because free-space path loss scales with the square of the slant range, low elevation passes are disproportionately loss-limited even before atmospheric effects are added.

As demonstrated in [18], at low elevation angles ($<10^\circ$), higher channel loss causes detector dark counts to domanite, driving QBER above 6%. under finite-size security proofs, data gathered at such elevations yields zero secret key bits after finite-key correction. For this reason, mission operators should define a pre-committed elevation mask at the protocol design stage, fixed independently of the statistics observed in any given pass, below which data is excluded from key generation. Discarding low-elevation segments only after observing a

{OPEN}

high error rate would constitute an outcome-dependent post-selection, which is incompatible with the assumptions underlying composable finite-key security proofs.

Mathematical methodologies for Security Proofs: Analytical vs. Numerical Frameworks

Certifying the Information-Theoretic Security of a QKD protocol against general attacks (e.g. coherent attacks) requires calculating a tight lower bound on the secret key rate. In literature, two main theoretical paradigms are employed to perform this analysis: analytical proof techniques and convex numerical frameworks.

The analytical approach relies on exact mathematical inequalities, such as Entropic Uncertainty Relations [15], smooth min-entropy formulations [16], or the Gottesman-Lo- Lütkenhaus-Preskill theorem [17], to derive closed-form expressions for both asymptotic and finite-key secret rates. The primary advantage of this methodology lies in its ability to provide clear physical insights into how individual operational parameters directly impact key generation, while requiring virtually no computational overhead since it relies on direct formula evaluation. However, analytical proofs depend heavily on strict mathematical symmetries, such as those present in idealized symmetric BB84 protocols. Consequently, when confronted with complex, asymmetric, or real-world device imperfections-such as source intensity correlations, state preparation flaws, or arbitrary basis misalignments-analytical bounds tend to become overly pessimistic or mathematically intractable.

Conversely, the numerical framework bridges the gap between ideal quantum theory and real-world imperfect hardware by reformulating secret key rate estimation as a convex optimization problem over valid density matrices. Pioneered by tools based on Semidefinite Programming (SDP) (pioneered by Coles, Winick, Lütkenhaus et al. [14]), this approach minimizes quantum relative entropy subject to linear constraints derived directly from experimental statistics. The main strength of the numerical methodology lies in its high versatility and tight key rate bounds for practical deployments, as it seamlessly accommodates unstructured protocols lacking symmetry, spatial and polarization mode mismatches, and memory effects in hardware components. Despite its higher computational cost and reliance on specialized numerical solvers with strict convergence tolerances to prevent invalid security bounds, the numerical framework offers the necessary flexibility to model practical space-grade optical payloads operating under dynamic orbital and environmental conditions.

4. SUBSYSTEM TRADE-OFFS & HARDWARE REQUIREMENTS DRIVEN BY PROOF ASSUMPTIONS

Space segment: Transmitter & Optical Payload

Security Proofs for Weak Coherent Pulse (WCP) decoy-state protocols assume that multi-photon states, single-photon states, and vacuum states are identical in all degrees of freedom except photon number. Any side-channel leak, such as spectral differences, pulse-shape variations, or spatial mode mismatches between intensity levels, allows Eve to distinguish state types without altering the quantum channel.

To preserve this theoretical equivalence and prevent side-channel exploits in space, the optical payload must meet stringent hardware requirements across several key subsystems:

- **Intensity Modulator Stability:** Modulators must maintain extinction ratio stability within ± 0.1 dB under thermal fluctuations across the orbit. Fluctuations in decoy state intensities degrade $s_{X,1}$ estimation precision.
- **Polarization Extinction Ratio (PER):** For polarization-encoded BB84, payload optical elements (dichroic mirrors, beam splitters, steering mirrors) must guarantee a system PER exceeding 30 dB (1000:1) to keep intrinsic optics QBER below 0.5% [11].

{OPEN}

- Quantum Random Number Generators (QRNG): The security proof relies on perfectly unbiased numbers for state preparation and basis selection. Space-qualified QRNGs must achieve high throughput (>1 Gbps) with continuous real-time entropy validation compliant with NIST SP 800-90B.

Pointing, Acquisition, and Tracking (PAT) & Jitter Noise

Space-to-ground optical links require sub-microradian pointing accuracy. Pointing jitter introduces spatial power fluctuations at the ground receiver, creating scintillation-like fading. Furthermore, offset pointing degrades spatial filtering efficiency, increasing background noise collection. From a security proof standpoint, pointing jitter induces intensity fluctuations that Eve can exploit via statistical blinding or channel state estimation attacks. High-precision Fine Steering Mirrors (FSM) backed by closed-loop quad-sensor tracking are mandatory to constrain jitter-induced QBER fluctuation to within <0.2%.

Space Radiation & Single-Photon Detector Aging

One of the most critical space-environment drivers for satellite QKD payloads is ionizing radiation, from trapped protons encountered in regions such as the South Atlantic Anomaly to galactic cosmic rays. Single-photon detectors, whether silicon avalanche photodiodes or InGaAs-based devices, accumulate displacement damage over the course of a mission, gradually degrading their dark count performance. As the dark count rate rises, it contributes an increasing background of spurious detection events indistinguishable from genuine signal, which manifests directly as an increase in the observed quantum bit error rate. Because the security proof bounds the tolerable error rate before secret key generation collapses, this radiation-driven degradation effectively imposes a finite operational lifetime on the detector subsystem, and by extension on the mission’s useful key-generation capacity, unless actively mitigated.

Systems engineering responses to this degradation generally fall into three categories. The first is active thermal control: operating detectors at deeply reduced temperatures suppresses the thermally-activated component of the dark count rate, though it does not reverse the underlying radiation damage and typically comes with a non-trivial power and thermal-subsystem cost. The second is periodic thermal annealing, in which detectors are deliberately warmed for a sustained period to partially heal radiation-induced lattice defects; this can recover a meaningful fraction of the detector’s original performance but requires careful scheduling, since the detector is unavailable for key generation during the annealing cycle itself. The third is shielding, physically reducing the flux of damaging particles reaching the detector housing; this is effective but never complete, since sufficiently energetic particles cannot be fully stopped by mass budgets compatible with a satellite payload, and shielding choices must also account for the possibility of secondary radiation generated within the shielding material itself. In practice, a satellite QKD payload typically combines these strategies, since none alone is sufficient across the full expected radiation environment and mission lifetime, and their relative weighting is itself a mission-specific trade-off between mass, power, and required detector longevity.

5. SATELLITE CONSTELLATION ARCHITECTURES & PROTOCOL TRADE-OFFS

Downlink vs. Uplink Topology

A primary system architectural decision is choosing between Downlink QKD (Quantum transmitter on satellite, receiver on ground) and Uplink QKD (Transmitter on ground, receiver on satellite). Table 1 shows the comparison between the two QKD system architectures.

Table 1 Architectural Comparison: Downlink vs. Uplink Space QKD Configurations.

Architectural Metric	Downlink Topology (Transmitter in Space)	Uplink Topology (Receiver in Space)
----------------------	---	-------------------------------------

{OPEN}

Atmospheric Turbulence Impact	Low (Beam expands in space before hitting atmosphere).	High (Beam expands early near ground, causing high jitter)
Ground Aperture Requirement	Large (1.0 m-1.0 m OGS Telescope)	Small (20 cm-40 cm ground transmitter)
Detector Complexity & Cooling	Low (Detectors situated at ground station)	High (Cryogenic cooling & shielding required in orbit)
Daytime Operation Feasibility	Higher SNR via spatial/narrowband filtering at OGS	Extremely difficult due to solar background clutter
Radiation Vulnerability	Minimal (Transmitter optics/modulators are radiation-hard)	Severe (Sensors degrade continuously due to radiation)
Security Proof Bounds	Favored: higher key rate due to lower attenuation	Constrained: higher QBER reduces finite-key generation window

Dowlink topologies are strongly favored from a security proof prospective. Higher link efficiency minimizes attenuation to 25-35 dB, ensuring raw key sizes $N > 10^7$ per pass, which is essential to mitigate finite-key statistical penalty factors.

Trusted Node vs. Entanglement-Based Quantum Repeaters

Current near-term constellations rely on trusted node architectures [12] [13]. The satellite performs QKD with Ground Station A, stores the key K_A in secure memory, flies over Ground Station B, performs QKD to generate K_B , and transmits $K_A \oplus K_B$ over a public authenticated channel. The security proof implication that permits this process is that the satellite itself must be fully trusted. If an adversary gains physical or side-channel control of the payload, overall security is completely compromised.

To eliminate trusted nodes, Entanglement Distribution (BBM92 Protocol) uses an on-board Entangled Photon Source (EPS) to send photon pairs simultaneously to Station A and Station B. Security proofs for BBM92 allow the satellite platform to be untrusted. However, because both optical links must be closed simultaneously, total channel loss equals $L_{tot} = L_a + L_b$ (e.g., 30 dB + 30 dB = 60 dB). At 60 dB attenuation, finite-key extraction requires multi-gigahertz sources and multi-meter ground apertures, highlighting a direct trade-off between physical security trust assumptions and link availability.

6. CONCLUSIONS AND ROADMAP

This article has argued that, in space-based QKD systems, security proofs cannot be treated as a downstream mathematical formality validated after the payload is built. The severe pass-time and block-size constraints imposed by LEO satellite geometry push every mission into the finite-key regime, where statistical margins — not idealized asymptotic bounds — determine whether a given link yields any usable secret key at all. As shown throughout this work, this reality propagates upward through the entire system stack: it shapes the tolerances required of intensity modulators, polarization optics, and random number generators; it dictates pointing and tracking precision; it sets the pace at which radiation-hardening strategies must be scheduled against detector lifetime; and it ultimately governs high-level architectural choices between downlink and uplink topologies, and between trusted-node and entanglement-based network designs.

A recurring theme is that the security proof and the physical platform must be co-engineered rather than designed sequentially. Treating the proof as a fixed mathematical input to which hardware must merely comply, or conversely as a formality to be satisfied loosely after the platform is built, both lead to systems that either underperform their theoretical potential or, more critically, fail to deliver the security guarantees they claim. The guidelines discussed in this work — pre-committing elevation masks at the protocol design stage rather than adapting them to observed statistics, budgeting link margins against finite-key thresholds rather than asymptotic rates, and selecting the trust model appropriate to a mission's operational and

{OPEN}

jurisdictional context — are intended to help bridge this gap for near-term satellite QKD demonstrators and for the multi-node constellations expected to follow them.

Looking forward, the transition from single-link demonstrations to interoperable, multi-orbit QKD constellations will place increasing pressure on the alignment of security-proof frameworks across independently operated space and ground segments. As numerical security-proof techniques mature and become computationally tractable for near-real-time use, and as standardization efforts extend composable security definitions across heterogeneous network segments, satellite QKD is positioned to move from a sequence of scientific demonstrations toward a dependable, and rigorously certified, component of the future quantum-secured communication infrastructure.

REFERENCES

- [1] Bennett, C. H. and G. Brassard, "Quantum Cryptography: Public-Key Distribution and Coin Tossing", Proceedings of the International Conference on Computers, Systems and Signal Processing, Bangalore, India (1984).
- [2] Bennett, C. H., Brassard, G., & Mermin, N. D., "Quantum cryptography without Bell's theorem", *Physical review letters* 68(5), 557 (1992).
- [3] Scarani, V., Acin, A., Ribordy, G., & Gisin, N., "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations", *Physical review letters* 92(5), 057901 (2004).
- [4] Lo, H. K., Ma, X., & Chen, K., "Decoy state quantum key distribution", *Physical review letters* 94(23), 230504 (2005).
- [5] Zhao, Y., Qi, B., Ma, X., Lo, H. K., & Qian, L., "Experimental quantum key distribution with decoy states", *Physical review letters* 96(7), 070502 (2006).
- [6] Fung, Chi-Hang Fred, Xiongfeng Ma, and Hoi Fung Chau. "Practical issues in quantum-key-distribution postprocessing." *Physical Review A—Atomic, Molecular, and Optical Physics* 81.1 (2010): 012318.
- [7] J. Pan, "604 progress of the quantum experiment science satellite (QUESS) Micius project national report 2016–2018", *Chin. J. Space Sci.* 38(5), 604–609 (2018).
- [8] Lim, C. C. W., Curty, M., Walenta, N., Xu, F., Zbinden, H., "Concise security bounds for practical decoy-state quantum key distribution." *Physical Review A* 89.2, 022307 (2014).
- [9] Yin, H., Zhou, M., Gu, J., Xie, Y., and Lu, Y., Chen, Z., "Tight security bounds for decoy-state quantum key distribution." *Scientific Reports* 10.1, 1-10 (2020).
- [10] Curty, M., Xu, F., Cui, W., Lim, C. C. W., Tamaki, K., & Lo, H. K. (2014). Finite-key analysis for measurement-device-independent quantum key distribution. *Nature communications*, 5(1), 3732.
- [11] Stathis, A., Ntanos, A., Lyras, N. K., Giannoulis, G., Panagopoulos, A. D., & Avramopoulos, H. (2024, June). Toward converged satellite/fiber 1550 nm DS-BB84 QKD networks: Feasibility analysis and system requirements. In *Photonics* (Vol. 11, No. 7, p. 609). MDPI.
- [12] Liao, S. K., Cai, W. Q., Handsteiner, J., Liu, B., Yin, J., Zhang, L., ... & Pan, J. W. (2018). Satellite-relayed intercontinental quantum network. *Physical review letters*, 120(3), 030501.
- [13] Orsucci, D., Shrestha, A., & Moll, F. (2024). Review of Low-Earth Orbit Satellite Quantum Key Distribution. *Future Generation Optical Wireless Communications*, 68.
- [14] Winick, A., Lütkenhaus, N., & Coles, P. J. (2018). Reliable numerical key rates for quantum key distribution. *Quantum*, 2, 77
- [15] Tomamichel, M., & Renner, R. (2011). Uncertainty relation for smooth entropies. *Physical review letters*, 106(11), 110506.

{OPEN}

- [16] Renner, R. (2008). Security of quantum key distribution. *International Journal of Quantum Information*, 6(01), 1-127.
- [17] Gottesman, D., Lo, H. K., Lütkenhaus, N., & Preskill, J. (2002). Security of quantum key distribution with imperfect devices. *arXiv preprint quant-ph/0212066*.
- [18] Sidhu, J. S., Brougham, T., McArthur, D., Pousa, R. G., & Oi, D. K. (2022). Finite key effects in satellite quantum key distribution. *npj Quantum Information*, 8(1), 18.

{OPEN}