

Integration of high photon efficiency optical communication with optical key distribution for physical layer security

Mateusz Kucharczyk^{a,b}, Paweł Jacewicz^{b,c}, Karol Łukanowski^c, Marcin Jarzyna^c, and Konrad Banaszek^{b,c}

^aQuantum Optical Technologies sp. z o.o., ul. Lisa Kuli 4, 35-032 Rzeszów, Poland

^bFaculty of Physics, University of Warsaw, ul. Pasteura 5, 02-093 Warsaw, Poland

^cCentre for Quantum Optical Technologies, Centre of New Technologies, University of Warsaw, ul. Banacha 2c, 02-097 Warsaw, Poland

ABSTRACT

Optical key distribution (OKD) provides information-theoretic protection for space optical communication links against passive eavesdropping. However, in the photon-starved deep-space regime, the standard pulse-by-pulse OKD protocol is no longer applicable when an eavesdropper has access to significantly higher signal levels. To overcome this limitation, we introduce a superframe OKD protocol tailored for high-order pulse position modulation (PPM) links. By aggregating consecutive PPM frames into logical superframes and finely modulating pulse intensities within those superframes, our scheme restores noise overlap required to obscure OKD bits from an advantaged adversary with up to +10 dB more optical power available. Simultaneously, dual-threshold discrimination applied to superframe photocount numbers extracts raw key bits at the legitimate receiver, which are subsequently reconciled with the transmitter using low-density parity-check coding (LDPC). End-to-end simulations demonstrate concurrent error-free classical 2^{20} -PPM data transmission at 5.8 Mbps alongside robust key distribution with a secret key rate of 386 bps under an incident flux of 10^6 photons/s. Crucially, this security enhancement is achieved purely through signaling architecture with minor optical hardware modifications.

Keywords: Physical Layer Security, Optical Key Distribution, Deep-Space Communications, Pulse Position Modulation

1. INTRODUCTION

Free-space optical communication is emerging as a critical technology for modern space missions, offering unprecedented bandwidth and freedom from radio-frequency spectrum licensing restrictions.^{1,2} As optical links are tested for prospective planetary missions and deep-space probes—such as NASA’s Deep Space Optical Communications demonstration—ensuring the confidentiality and integrity of transmitted data will be of paramount importance for their future deployment. Traditional cryptographic security relies on digital-layer algorithms whose guarantees stem from computational complexity assumptions. However, physical layer security (PLS) provides an information-theoretic alternative, exploiting the intrinsic noise and physical properties of the quantum optical channel to prevent eavesdropping regardless of the adversary’s computational power.³ In space scenarios, beam divergence over vast distances creates a broad footprint at the receiver plane, allowing a passive eavesdropper (Eve) positioned in orbit or on the ground to intercept a fraction of the optical signal without interfering with the direct transmission path to the legitimate receiver (Bob), as illustrated in Fig. 1.

Recent studies have demonstrated the feasibility of integrating data transmission with PLS via optical key distribution (OKD). Initial analysis validated concurrent data delivery and OKD for Near-Earth scenarios, specifically Low Earth Orbit (LEO)-to-ground links,⁴ with comprehensive channel modelling that incorporated atmospheric turbulence.⁵ This approach was subsequently extended to deep-space regimes by combining OKD intensity modulation with high-order Pulse Position Modulation (PPM).⁶ By leveraging intensity modulation for both photon-efficient data transmission and key distribution, these dual-purpose links establish secret keys without requiring separate hardware channels or dedicated physical resources.

M.K.: E-mail: mateusz.kucharczyk@qopt.tech

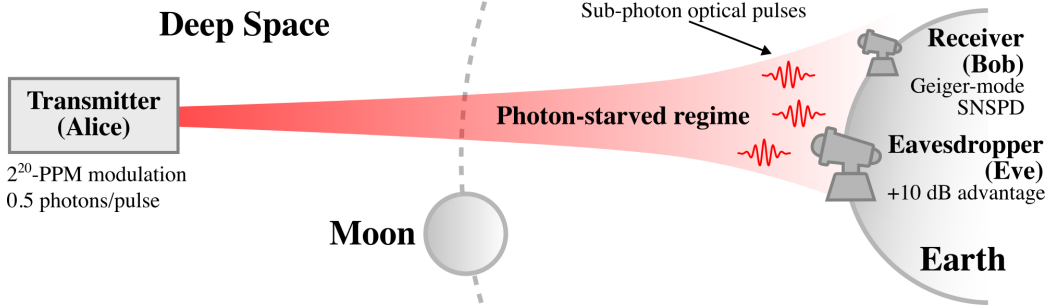


Figure 1. System scenario for physical layer security in deep-space optical communications. A deep-space probe (Alice) transmits high-order 2^{20} -PPM optical signal in the photon-starved regime ($n_f = 0.5$ photons/pulse) towards a legitimate Ground Station (Bob) equipped with a Geiger-mode SNSPD. Beam divergence over interplanetary distances creates an extended spatial footprint, allowing a passive Eavesdropper (Eve) with a +10 dB collection advantage to intercept a fraction of the optical flux.

Despite these advances, extending PLS to extreme deep-space scenarios presents a fundamental physical challenge: the photon-starved regime.⁷ In links spanning interplanetary distances (e.g., Earth-Mars), severe geometric attenuation reduces the received signal to sub-photon levels per pulse, with mean photon numbers dropping below $n_f < 1$ per PPM frame. Under such low flux, applying intensity modulation to individual PPM pulses no longer works. At individual pulse scales, quantum shot noise is insufficient to obscure the intensity states when an adversary possesses a significant collection advantage (e.g., a larger aperture or favorable atmospheric conditions). Under a strong passive eavesdropper advantage per-pulse intensity modulation allows Eve to discriminate key states with high fidelity, compromising secrecy distillation.

To overcome this challenge, we introduce and validate numerically a novel *superframe* architecture specifically tailored for extreme deep-space optical links. Rather than modulating the optical energy of individual PPM pulses, our approach aggregates multiple consecutive PPM frames into single OKD superframes. By modulating the collective mean photon number of the superframe between two few-photon levels, we deliberately restore the quantum shot-noise overlap required to mask the key signal from a privileged eavesdropper, even when individual detected pulses carry on average less than one photon.

Through detailed numerical simulations of a 2^{20} -PPM data link under a 0 dB to 10 dB eavesdropper's advantage, we demonstrate that this superframe framework successfully guarantees simultaneous error-free classical data transmission and information-theoretic secure key distribution. Crucially, this dual capability is achieved purely via signaling architecture—specifically by modulating the aggregate superframe photon statistics—requiring zero additional physical optical components at the transmitter or receiver.

2. HIGH-ORDER PPM DATA TRANSMISSION

In extreme deep-space optical communication, energy efficiency dominates system design. To maximize the transmitted information per received photon,⁸ pulse-position modulation (PPM) with a large alphabet size M is commonly employed. In this work, we adopt a high-order M -PPM scheme with $M = 2^{20} = 1,048,576$ time slots per frame. Each PPM frame conveys $b = \log_2 M = 20$ bits of raw information by emitting a single optical pulse in one of the M temporal slots.

2.1 Photon-Starved Channel and Detection Model

In interplanetary links spanning astronomical units, extreme geometric beam spreading reduces the optical power at the receiver to a photon-starved level. We model the receiver as a binary Geiger-type photon counting detector, such as a superconducting nanowire single-photon detector (SNSPD), operating in a click/no-click mode.⁹ In addition to the signal pulse with mean photon number n_f (set to an average of $n_f = 0.5$ photons per pulse), the model incorporates background noise and dark counts with a mean photon count per slot of $n_b = 10^{-9}$. Under binary Geiger detection, the detector registers a click whenever $n \geq 1$. The overall detection probability in a signal slot is given by:

$$P_{\text{click}}(n_f, n_b) = 1 - \exp[-(n_f + n_b)] \approx 1 - \exp(-n_f) \quad (1)$$

For $n_f = 0.5$, $P_{\text{click}} \approx 0.3935$, meaning that approximately 60.65% of the transmitted PPM frames contain no detected signal photons ($n = 0$), resulting in symbol *erasures*. The residual noise level $n_b = 10^{-9}$ yields a false-alarm click probability in non-signal slots of $p_{\text{err}} = 1 - \exp(-n_b) \approx 10^{-9}$, corresponding to an overall symbol decision error probability of $p_{\text{err}} \cdot (M - 1) \approx 0.001$. Furthermore, when key distribution is superimposed, the pulse intensity is modulated between $n_f = 0.4$ and 0.6 photons/pulse; these minor power fluctuations induce small variations in the erasure rate that are readily absorbed by the forward error correction code without compromising data recovery.

2.2 Erasure Mitigation via Gauss-Jordan Elimination Codes

To achieve reliable data delivery across a channel with an erasure rate exceeding 60%, we employ modular forward error correction (FEC) codes based on Gauss-Jordan elimination.¹⁰ The code is parameterized by sub-block parameters $T = 16$, $n = 2,000$, $k = 320$, and an overlap parameter $m = 32$. This configuration maps $K = 4,640$ information symbols onto a total codeword length of $N = T \times n = 32,000$ transmitted PPM symbols (channel uses). The code rate R is:

$$R = \frac{K}{N} = \frac{4,640}{32,000} = 0.145 \text{ symbols per channel use.} \quad (2)$$

Since each transmitted pulse carries on average $n_f = 0.5$ photons, the Photon Information Efficiency (PIE) achieved by the data link is:

$$\text{PIE} = \frac{2.9 \text{ bits/symbol}}{0.5 \text{ photons/symbol}} = 5.8 \text{ bits/photon} \quad (3)$$

Across all numerical simulation runs, the Gauss-Jordan erasure code achieved 100% error-free data recovery (0 bit errors) at an effective throughput rate of 5.8 Mbps under an incident flux of 10^6 photons/s.

3. SUPERFRAME ARCHITECTURE FOR OPTICAL KEY DISTRIBUTION

While high-order PPM effectively mitigates the energy constraints of deep-space communications, it does not inherently protect the physical layer against unauthorized interception. To secure the link, we superimpose an OKD protocol over the data transmission. However, applying intensity-modulated OKD directly to individual PPM frames fails in extreme deep-space regimes. With an average of only 0.5 photons per pulse, the quantum shot noise is insufficient to obscure the modulated intensity states from a well-equipped adversary. To overcome this limitation, we introduce the concept of OKD superframes.

3.1 The OKD Superframe Concept

The core innovation of our protocol relies on aggregating multiple consecutive PPM frames into a single, extended logical structure termed a *superframe*. For this implementation, we group $S = 10$ consecutive 2^{20} -PPM frames into one superframe, as shown in Fig. 2.

This structural grouping combines seamlessly with data transmission. As detailed in Section 2, a single forward error correction (FEC) codeword comprises $N = 32,000$ PPM frames. By adopting a superframe length of $S = 10$, each data codeword aligns perfectly with exactly 3,200 superframes. This deterministic mapping ensures that Alice and Bob can maintain synchronization between the data demodulation and the key distillation processes without requiring any additional physical signaling headers.

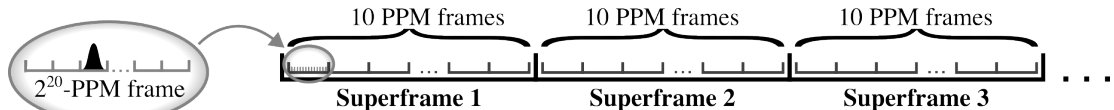


Figure 2. OKD superframe structural aggregation. (Left) A single 2^{20} -PPM frame conveying data via a single optical pulse across $M = 2^{20}$ temporal slots. (Right) Grouping of $S = 10$ consecutive PPM frames into individual logical superframes, forming the baseline unit for intensity-modulated key distribution.

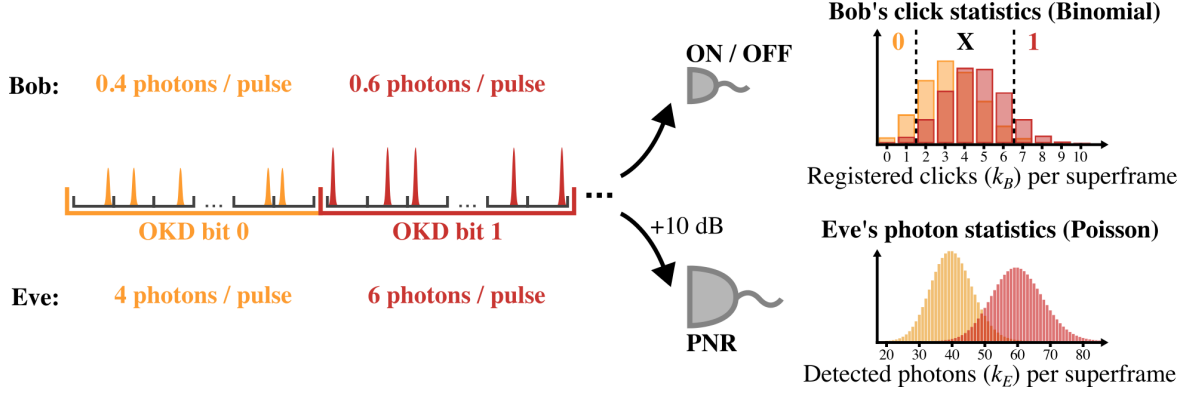


Figure 3. Receiver detection statistics and sifting mechanism for OKD superframes. Bob receives mean fluxes of 0.4 and 0.6 photons/pulse (for OKD bits 0 and 1) using an ON/OFF single-photon detector. He registers binomial click counts $k_B \in \{0, \dots, 10\}$ across $S = 10$ frames and applies dual-threshold discrimination to extract key bits (0, 1) or discard ambiguous events (X). An eavesdropper (Eve) possessing +10 dB more optical power collects on average 4 or 6 photons/pulse using a Photon-Number-Resolving (PNR) detector. The physical overlap between Eve's resulting Poisson distributions $P_E(k_E)$ enforces quantum shot-noise uncertainty, securing the key.

3.2 Passive Eavesdropping Model and Detection Statistics

To rigorously evaluate the security of the proposed architecture, we consider a highly privileged passive eavesdropper, Eve, as illustrated in the overall system diagram in Fig. 3. We assume Eve is optimally positioned within the diffractive footprint of the beam or utilizes a wiretap, granting her a significant signal-to-noise ratio (SNR) advantage over the legitimate recipient, Bob. In our conservative security model, we grant Eve a 10 dB signal advantage, meaning she collects ten times more signal photons than Bob.¹¹

As Alice modulates the intensity between two levels corresponding to mean photon numbers $n_0 = 4$ (OKD bit 0) and $n_1 = 6$ (OKD bit 1) registered by Bob per superframe, the physical constraints of the respective receiver setups lead to fundamentally different statistical distributions for Bob and Eve:

- **Bob's Detection (Binomial Distribution):** Bob utilizes Geiger-mode single-photon detectors (e.g., SNSPDs) operating in a click/no-click regime. Within a single superframe comprising $S = 10$ discrete frames, Bob registers a maximum of S clicks. The total registered click count k_B follows a binomial distribution, as shown in the top-right plot of Fig. 3. For a per-frame click probability $p_{\text{click}}(n_a) = 1 - \exp(-n_a/S)$, Bob's probability of registering k clicks is given by:

$$P_B(k_B|n_a) = \binom{S}{k_B} [p_{\text{click}}(n_a)]^{k_B} [1 - p_{\text{click}}(n_a)]^{S-k_B}, \quad k_B \in \{0, 1, \dots, S\} \quad (4)$$

where $a = 0, 1$. To extract raw key bits, Bob applies dual decision thresholds to this binomial distribution, assigning high-confidence outcomes to bit values 0 and 1 while discarding ambiguous intermediate click counts (X), as detailed in Subsection 3.3.

- **Eve's Detection (Poisson Distribution):** Conversely, Eve's massive signal advantage enables her to utilize ideal photon-number-resolving (PNR) detectors¹² to directly measure the photon number of the entire superframe. Assuming a coherent laser source, Eve's detected photon count k_E retains the inherent quantum shot noise of the optical field and follows a Poisson distribution centered around $n_{E,0} = 40$ and $n_{E,1} = 60$, as shown in Fig. 3:

$$P_E(k_E|n_{E,a}) = \frac{(n_{E,a})^{k_E} e^{-n_{E,a}}}{k_E!}, \quad k_E \in \{0, 1, 2, \dots\} \quad (5)$$

Because Eve's Poisson distributions for the two bit states exhibit variance equal to their means ($\sigma_a^2 = n_{E,a}$), the two probability mass functions significantly overlap. This residual uncertainty prevents Eve from executing a flawless, error-free discrimination of every superframe, which forms the fundamental physical basis for secure key generation.

3.3 The OKD Processing Stack

To distill a secure cryptographic key from the overlapping click and photon distributions, Alice and Bob execute a standard post-processing protocol over an authenticated public channel. After Alice modulates the superframes according to her raw key bits ($n_0 = 4$ for bit 0, $n_1 = 6$ for bit 1), she publicly discloses a random 10% fraction of her sequence. Bob utilizes these calibration slots to fit his binomial detection statistics and determine optimal dual-click thresholds. Following sifting—where Bob discards ambiguous intermediate click counts and retains only high-confidence events—the parties perform reverse reconciliation using LDPC code to correct residual bit errors. Finally, the reconciled key is compressed via privacy amplification using a SHA-3 cryptographic hash function, completely eliminating Eve’s partial information advantage to produce the final symmetric secret key.

4. SIMULATION RESULTS

To rigorously evaluate the proposed superframe OKD framework over a photon-starved 2^{20} -PPM link, we performed a numerical simulation composed of two distinct stages. First, we generated superframe detection distributions across a parameter search space to dynamically identify the optimal transmitter photon counts registered by Bob (n_0, n_1) and receiver dual decision thresholds (k_0, k_1) across eavesdropper advantages ranging from 0 to 10 dB.¹¹ Second, using these optimized parameters, we conducted a full end-to-end numerical simulation for the critical 10 dB worst-case scenario, implementing the complete post-processing chain including sifting, LDPC error correction, and privacy amplification using SHA3 hash function.

In the initial parameter search phase, Alice modulated superframes of $S = 10$ PPM slots using target mean number of photons n_0 and n_1 registered by Bob. The intensity gap $\Delta n = n_1 - n_0$ balances bit discrimination at Bob against quantum shot-noise overlap, which limits Eve’s information leakage. Simultaneously, Bob applied dual decision thresholds k_0 and k_1 to discard ambiguous click counts ($k_0 < k < k_1$) per superframe, suppressing the raw key bit error rate (RKBER) at the expense of sifted yield. Fig. 4(a) maps this parameter space for the 10 dB case, plotting asymptotic secret key rate K against raw bit bias $|p_0 - 0.5|$. The search identified $n_0 = 4, n_1 = 6$ with $k_0 = 1, k_1 = 7$ as the optimal configuration (marked by the gold star), achieving an asymptotic maximum of $K = 0.003$ bits/superframe at an RKBER of 16.3%.

Fig. 4(b) and Table 1 summarize these theoretically optimized operational points across varying levels of Eve’s channel advantage. Comparing an adaptive per-point re-optimization strategy against a static configuration fixed

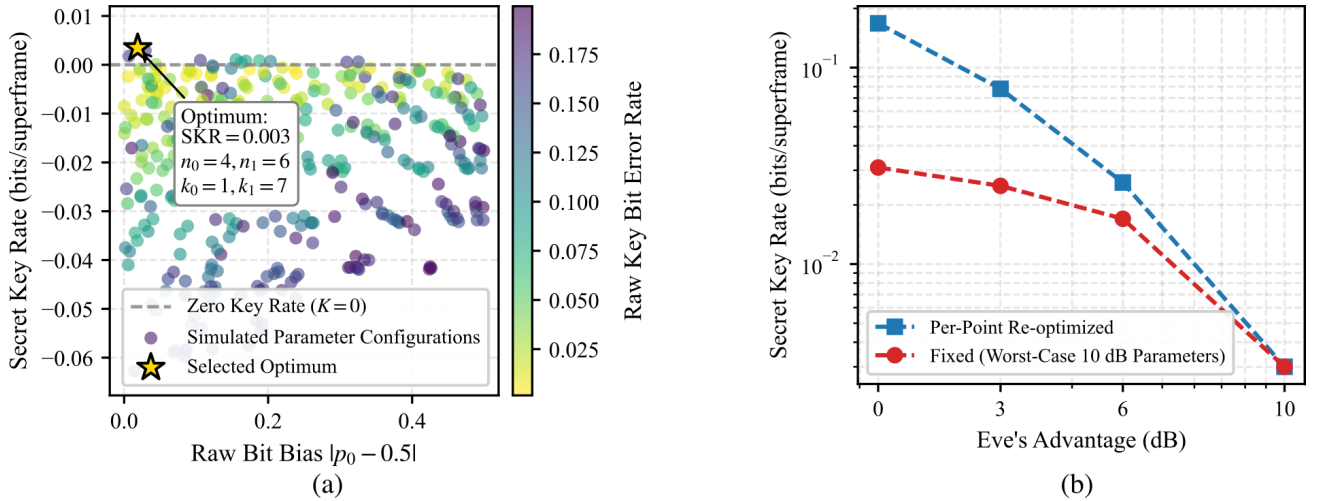


Figure 4. Joint parameter optimization and secret key rate performance. (a) Search space showing secret key rate (SKR) versus raw bit bias $|p_0 - 0.5|$, color-coded by raw key bit error rate (RKBER). The gold star indicates the optimal operational point ($n_0 = 4, n_1 = 6, k_0 = 1, k_1 = 7$) yielding maximum SKR near zero bit bias. (b) SKR performance as a function of Eve’s advantage, comparing dynamic per-point re-optimization (blue squares) against fixed worst-case operation (red circles).

at the 10 dB worst-case parameters demonstrates that dynamic tuning yields nearly an order of magnitude higher key yield in low-advantage regimes (0–3 dB), reaching $K = 0.168$ bits/superframe at 0 dB.

Finally, to validate practical feasibility, we executed the full end-to-end protocol simulation for the 10 dB extremal case using the pre-optimized parameters ($n_0 = 4, n_1 = 6, k_0 = 1, k_1 = 7$). We transmitted 100,000 consecutive superframes through the channel. Sifting via Bob’s dual-threshold discrimination yielded 12,600 raw key bits with a post-sifting error rate of 16.3%. These raw bits were subsequently error-corrected using an LDPC code with a code rate of 0.3 and an efficiency of 1.09, followed by privacy amplification via a SHA-3 cryptographic hash function. Following full distillation, the realized end-to-end secret key rate was $K_{\text{realized}} = 0.00194$ bits/superframe, corresponding to an operational key generation rate of 386 bps. The slight reduction from the theoretical search bound (0.003 bits/superframe) reflects realistic finite block-length overheads and practical reconciliation efficiencies, confirming that information-theoretic key generation remains robust under full system execution.

Table 1. Adaptively optimized parameters across varying eavesdropper advantages to maximize the secret key rate (SKR).

Eve’s Advantage [dB]	n_0	n_1	k_0	k_1	$p(\text{bit} = 1)$ [%]	RKBER [%]	SKR (bits/superframe)
0	1	5	1	4	56.8	4.3	0.168
3	2	5	1	5	56.6	8.5	0.078
6	3	6	1	6	46.3	8.7	0.026
10	4	6	1	7	51.9	16.3	0.003

5. CONCLUSION

We presented a superframe-based optical key distribution (OKD) architecture that enables physical layer security for photon-starved deep-space links. By aggregating consecutive 2^{20} -PPM frames into logical superframes and modulating their collective photon statistics, our framework restores the quantum shot-noise overlap necessary to obscure cryptographic keys from an eavesdropper with up to a +10 dB optical power advantage.

End-to-end simulations demonstrated that this approach supports simultaneous, error-free classical data transmission at 5.8 Mbps alongside robust secret key generation. Utilizing dual-threshold sifting, low-density parity-check error correction, and SHA-3 privacy amplification, the system achieved a secret key rate of 386 bps under the worst-case +10 dB eavesdropper advantage. Crucially, this dual-purpose capability is achieved purely through software-defined signaling architecture, requiring zero modifications to existing optical hardware, thereby offering a highly practical security solution for future interplanetary missions.

ACKNOWLEDGMENTS

M.K.’s contribution was supported by the “Industrial Doctorate” programme financed by the Ministry of Science and Higher Education of the Republic of Poland, contract no. DWD/8/0353/2024. The “Quantum Optical Technologies” (FENG.02.01-IP.05-0017/23) project is carried out within the Measure 2.1 International Research Agendas programme of the Foundation for Polish Science, co-financed by the European Union under the European Funds for Smart Economy 2021-2027 (FENG). This work was supported by the European Union’s Horizon Europe research and innovation programme under the project “Quantum Security Networks Partnership” (QSNP, Grant Agreement No. 101114043).

REFERENCES

- [1] Hemmati, H., [*Deep space optical communications*], John Wiley & Sons (2006).
- [2] Boroson, D. M., Robinson, B. S., Murphy, D. V., Burianek, D. A., Khatri, F., Kovalik, J. M., Sodnik, Z., and Cornwell, D. M., “Overview and results of the lunar laser communication demonstration,” in [*Free-Space Laser Communication and Atmospheric Propagation XXVI*], **8971**, 213–223, SPIE (2014).

- [3] Bloch, M. and Barros, J., [*Physical-layer security: from information theory to security engineering*], Cambridge University Press (2011).
- [4] Jachura, M., Lasota, M., Kolenderski, P., and Banaszek, K., “Modelling concurrent IM/DD key distribution and data transmission over an optical LEO-to-ground link,” in [*International Conference on Space Optics — ICSO 2022*], **127777**, 127771B, International Society for Optics and Photonics, SPIE (2023).
- [5] Czerwinski, A., Lasota, M., Jarzyna, M., Kucharczyk, M., Jachura, M., and Banaszek, K., “Modeling optical key distribution over a satellite-to-ground link under weak atmospheric turbulence,” *IEEE Journal of Selected Topics in Quantum Electronics* **32**(1: Advances in Free Space Laser Communications), 1–13 (2026).
- [6] Lukanowski, K., Kucharczyk, M., Jachura, M., Jarzyna, M., and Banaszek, K., “Physical layer security for photon-starved communication links,” in [*International Conference on Space Optics — ICSO 2024*], **13699**, 136994H, International Society for Optics and Photonics, SPIE (2025).
- [7] Banaszek, K., Kunz, L., Jachura, M., and Jarzyna, M., “Quantum limits in optical communications,” *J. Lightwave Technol.* **38**(10), 2741–2754 (2020).
- [8] Dacha, S. K., Essiambre, R.-J., Ashikhimin, A., Blanco-Redondo, A., Kschischang, F. R., Banaszek, K., and Zhang, Y., “Communicating at a record 14.5 bits per received photon through a photon-starved channel,” *Phys. Rev. Res.* **7**, 033108 (2025).
- [9] Natarajan, C. M., Tanner, M. G., and Hadfield, R. H., “Superconducting nanowire single-photon detectors: physics and applications,” *Superconductor science and technology* **25**(6), 063001 (2012).
- [10] Ozaydin, B., Médard, M., and Duffy, K. R., “Coding and decoding in high photon information efficiency systems,” *J. Lightwave Technol.* **43**(19), 9117–9127 (2025).
- [11] Banaszek, K., Jachura, M., Kolenderski, P., and Lasota, M., “Optimization of intensity-modulation/direct-detection optical key distribution under passive eavesdropping,” *Opt. Express* **29**(26), 43091–43103 (2021).
- [12] Hadfield, R. H., “Single-photon detectors for optical quantum information applications,” *Nature Photonics* **3**(12), 696–705 (2009).