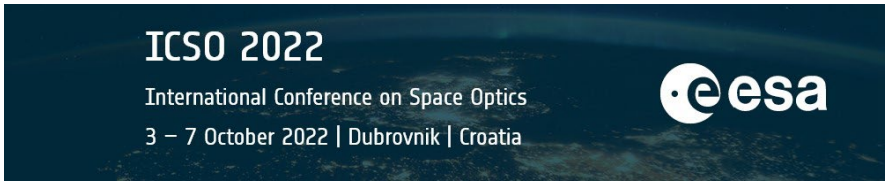
International Conference on Space Optics—ICSO 2022

Dubrovnik, Croatia

3–7 October 2022

Edited by Kyriaki Minoglou, Nikos Karafolas, and Bruno Cugny,



Modelling concurrent IM/DD key distribution and data transmission over an optical LEO-to-ground link

International Conference on Space Optics — ICSO 2022, edited by Kyriaki Minoglou, Nikos Karafolas, Bruno Cugny, Proc. of SPIE Vol. 12777, 127771B · © 2023 ESA and CNES · 0277-786X · doi: 10.1117/12.2689278

Modelling concurrent IM/DD key distribution and data transmission over an optical LEO-to-ground link

Michał Jachura*[a], Mikołaj Lasota[b], Piotr Kolenderski[b], Konrad Banaszek[a]
[a]Centre for Quantum Optical Technologies, CeNT, University of Warsaw, Banacha 2c, 02-097 Warszawa, Poland
[b] Faculty of Physics, Astronomy and Informatics, Nicolaus Copernicus University, Grudziądzka 5, 87-100 Toruń, Poland

ABSTRACT

We propose and analyze numerically concurrent intensity modulation/direct detection (IM/DD) optical key distribution (OKD) combined with conventional data transmission over a LEO-to-ground optical link. The idea is validated by numerical simulations which indicate that in a realistic scenario it is possible to generate simultaneously up to 200 Mbits of a secret key and downlink transmit up to 140 Gbits of data during a single nearly-zenithal pass of a LEO satellite. Such lengths of the secret key are three orders of magnitude higher in comparison to typical quantum key distribution systems, although they are generated under different security assumptions. The simplicity and robustness of IM/DD OKD protocols could make them an attractive and cost-effective option to provide security in the physical layer of space communication systems.

Keywords: optical key distribution; quantum key distribution; optical communication; satellite communication

1. INTRODUCTION

Intensity modulation/direct detection optical key distribution (IM/DD OKD) has the capability to generate a cryptographic key over free-space optics links that is secure against attacks using present or near term technology [1-3], while placing much less stringent requirements on the amount of tolerable noise and losses contributed by the physical channel as well as the performance of optoelectronic components compared to standard quantum key distribution (QKD). IM/DD approach is also well-suited to optical communication implemented using satellite optical terminals relying on non-coherent modulation formats such as on-off-keying (OOK) or pulse-position-modulation (PPM). In contrast to QKD, which relies on single photon generation and detection or shot-noise-limited coherent detection, optical key distribution requires in principle only a relatively minor modification of transmitters and receivers and can be realized using standard telecommunication components such as electro-optic modulators, fiber amplifiers and linear photodetectors. The purpose of this contribution is to provide estimates for the amount of a cryptographic key that can be generated using an IM/DD OKD protocol and the amount of data transferable during a single pass of a LEO satellite equipped with suitably modified optical communication terminal. The results are based on recent theoretical results presented in [4] that specify the attainable key rates under passive eavesdropping depending on the fractions of the optical signal collected by the authorized and unauthorized receivers and the noise of their respective detection subsystems. Following the customary naming convention these two parties will be referred to in the following text as Bob (authorized receiver) and Eve (potential eavesdropper).

This paper is organized as follows. In Sec. 2 we introduce the idea of optical key distribution and identify bit rates attainable in secret key generation and data transmission. In Sec. 3 we present numerical simulations of the proposed key distribution and data transmission scheme. Finally, Sec. 4 concludes the paper.

*m.jachura@cent.uw.edu.pl

2. OPTICAL KEY DISTRIBUTION

2.1 Modified on-off keying

The simplest realization of concurrent optical key distribution and data transmission relies on the modified OOK modulation format extended to three symbol values s_0, s_1, s_2. The zero-intensity symbol s_0 encodes information bit value **0**, while, in contrast to standard OOK, the non-zero intensity symbol encoding bit value **1** is replaced by a pair of symbols s_1, s_2 differing slightly in their amplitude. The optimal amplitude difference between symbols s_1, s_2 has been identified in [4]. As a rule of thumb when both authorized receiver and potential eavesdropper collect similar fractions of incoming light the separation is of the order of the standard deviation of the measured intensity distributions. Both non-zero intensity symbols s_1, s_2 encode information bit **1**, wherein s_1 encodes key bit *0* and s_2 encodes key bit *1*. The three-symbol constellation described above has been depicted in Fig.1 (a).

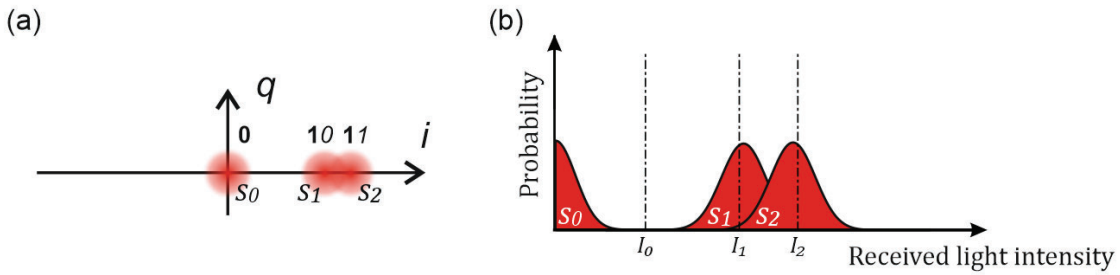


Figure 1. (a) Constellation diagram showing the set of three symbols used in concurrent data transmission and key distribution. The zero-amplitude symbol encodes only the information bit value **0,** while the non-zero amplitude pulses encode the information bit value **1** and the cryptographic key bit *0* or *1* depending on their amplitude. (b) Light intensity thresholds implemented in a hard-decoded linear optical receiver.

The probabilities of sending symbols s_0, s_1, and s_2 are $p_0 = 1/2$ and $p_1 = p_2 = 1/4$ respectively. The signal collected by the optical ground station is detected using a linear photodetector such as an avalanche photodiode with a transimpedance amplifier (APD-TIA). Based on the measured intensity I information bits and key bits are hard-decoded using the following decision criteria:

$$\begin{aligned} I \le I_0 &\text{ information bit } \mathbf{0}\text{, no key bit} \\ I_0 < I < I_1 &\text{ information bit } \mathbf{1}\text{, key bit } \boldsymbol{0} \\ I_1 \le I \le I_2 &\text{ information bit } \mathbf{1}\text{, no key bit} \\ I > I_2 &\text{ information bit } \mathbf{1}\text{, key bit } \boldsymbol{1} \end{aligned} \tag{1}$$

In numerical simulations we used optimal values of thresholds I_1 and I_2 which maximize the key generation rate [4]. A natural choice for the threshold I_0 is $I_0 = I_1/2$ which minimizes the raw bit-error-rate (BER) for Gaussian distributions associated with symbols s_0 and s_1 [5].

2.2 Data rate and secret key rate

As assumed in the numerical example studied in Sec. 3, the communication link is established only when detected light power is high enough to ensure very small raw BER $\le 10^{-10}$. Thus for the sake of simplicity we did not take into account any data overhead resulting from forward error-correction. In the on-off keying each symbol encodes a single information bit hence the data transmission bitrate equals to $1/T$ where T is the time slot duration of a single symbol.

According to the detailed theoretical model presented in [4] the average number of secret key bits per symbol in IM/DD OKD depends on the ratio:

$$R = \left(\frac{\tau_B \sigma_E}{\tau_E \sigma_B}\right)^2, \tag{2}$$

where σ_B and σ_E are standard deviations of the Gaussian noise measured by Bob and Eve, while τ_B and τ_E are power transmission factors from the satellite transmitter to their optical receiver setups (associated with their respective light collection capabilities). As an example when both Bob and Eve detect the same light power sent from the transmitter and similarly their detection noise is the same the ratio $R = 1$. The dependence of the average number of secret key bits per symbol on the ratio R has been presented in Fig. 2, where the basic IM/DD OKD protocol has been taken which uses only symbols s_1 and s_2 from the constellation shown in Fig. 1. The key bits per symbol figure multiplied by the symbol rate $1/T$ yield the key rate in bits per second.

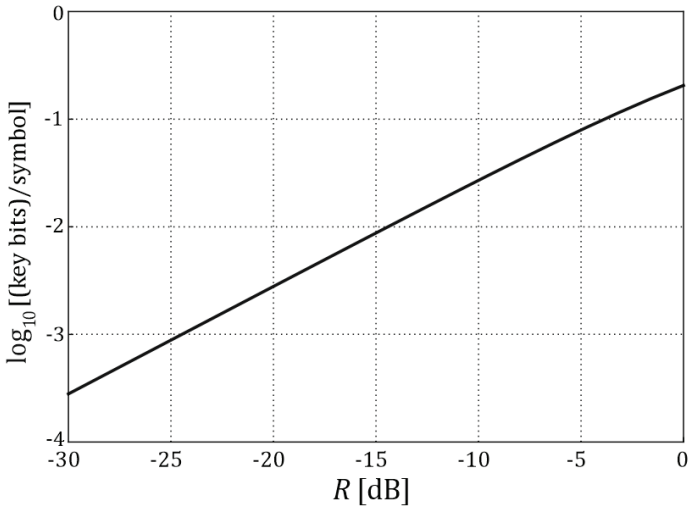


Figure 2. The average number of secret key bits per symbol in hard-decoded IM/DD OKD. The amount of the key depends on the ratio $R = (\tau_B \sigma_E / \tau_E \sigma_B)^2$ where σ_B and σ_E are standard deviations of the Gaussian noise measured by Bob and Eve, while τ_B and τ_E are power transmission factors from the satellite transmitter to their optical receiver setups (associated with their respective light collection capabilities). Detailed analytical derivation of the average number of key bits per symbol is presented in [4].

When Bob and Eve use linear APD-TIA detectors, their detection noise levels σ_B and σ_E are dominated by the thermal noise. However one may also consider the fundamental lower bound on the detection noise resulting from the Poisson photon number statistics. In that case the dominating noise contribution results from the shot-noise which cannot be anyhow suppressed by Eve and presents a fundamental limit on the light intensity detection noise. Let us note that in the extended on-off keying protocol described in Sec. 2.1 the probability of sending a non-zero amplitude symbol s_1 or s_2 (encoding a key bit) equals 1/2, hence in the concurrent key distribution/data transmission scenario the key rates indicated in Fig. 2 should be reduced by a factor of 2.

3. DATA TRANSMISSION AND KEY DISTRIBUTION

The numerical simulations were carried out using a set of typical parameters of the satellite orbit (resembling that of the International Space Station), the optical transmitter [6,7], and the optical receiver [7,8] summarized in the Table 1. We have assumed that the optical transmitter onboard LEO satellite is able to send optical symbols in the modified on-off keying modulation format. The scenario is illustrated in Fig. 3(a) with the optical ground station (OGS) located at the

latitude of Warsaw, Poland (52°N). Fig. 3(b) shows the elevation angle (EA) of the satellite observed from the ground station over an arbitrarily selected 24 h time period, while panels in Fig. 3(c) depict four examples of an orbital pass over the station. The simulation relies on mathematical models presented in [8].

The duration of a communication session within a single orbital pass depends on the power threshold of the photodetector. We have used the data provided by a manufacturer of an APD-TIA detector which ensures acceptable level of raw BER $\leq 10^{-10}$ for detected average optical power above or equal to -38 dBm and symbol duration above or equal to 0.8 ns [9]. The duration of a communication session also depends on the maximal elevation angle of the orbital pass and it reaches its maximum for a zenithal pass (EA = 90°).

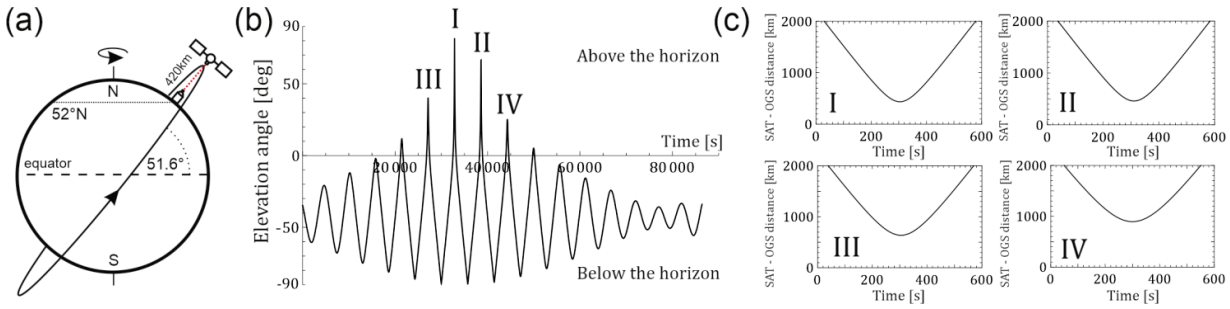


Figure 3. (a) LEO satellite orbiting around the Earth and equipped with an onboard optical terminal implementing the IM/DD OKD protocol concurrently with data transmission during an orbital pass over the optical ground station. Orbit parameters were taken akin to International Space Station i.e. 51.64° inclination angle, zero eccentricity (circular orbit) and 420 km apogee/perigee. The optical ground station is located at the latitude of Warsaw, Poland (52°N) (b) Elevation angle of the satellite visible form the ground station over 24h time period. Approaches with highest elevation angles were depicted using Roman numerals (c) Four examples of LEO satellite orbital pass as it approaches optical ground station with a maximum elevation angle of I: 84.07°, II: 69.60°, III: 40.72°, IV: 25.46°.

In order to calculate the duration of a communication session during each satellite pass we have used the standard link equation [10] to calculate received power P_r:

$$P_r = P_t \left(\frac{\pi D_t D_r}{4r\lambda}\right)^2 \mu\,, \tag{3}$$

where P_t is the transmitter power, D_t and D_r are the diameters of transmitter and receiver telescopes respectively, r is a distance between satellite and OGS, λ denotes the optical carrier wavelength and μ is the light collection efficiency in the receiver. Realistically D_t is related to the required minimum beam divergence of the transmitter output beam, which depends on the pointing precision of a laser beam characteristic for particular attitude determination and control system. Our simulation is based on the practically achievable beam divergence $2\theta = 0.06°$ [6], while the D_t is calculated using algebraic formula for Gaussian beam propagation $D_t = \frac{2\lambda}{\theta\pi} \approx 1.9$ mm. The desired beam divergence can be achieved using either an aspheric-lens fiber collimator or a telescope reflecting a suitably diverging light beam.

Table 1: Parameters of the satellite orbit, the optical transmitter and the optical receiver used in the numerical simulations of an IM/DD OKD link. Orbit properties are based on the international space station data, whereas the data for an optical transmitter are based on [6,7] and for an optical receiver are taken from [7,8].

Satellite orbit properties	
Inclination angle	51.64°
Orbit apogee/perigee	420km/420km

Orbital eccentricity	0
Orbital period	91 min 43 s
Transmitter parameters	
Beam power	P_t = 1 W
Slot duration	T = 1 ns
Beam divergence (full angle)	2θ = 0.06°
Transmitter collimated beam diameter	D_t = 1.88 mm
Wavelength	λ = 1550 nm
Receiver parameters	
Ground station latitude	52° N
Receive telescope diameter	D_r = 40 cm
Light collection efficiency	μ = 50%
Detection power threshold	$P_r > -38$ dBm

In numerical simulations we have analyzed 50 satellite passes with the maximal elevation angle varying from 0.19° to 87.2°. For approximately half of the passes the received power has not reached the threshold of −38 dBm and thus communication was impossible. For the other half the duration of communication session for a single satellite pass varied from 61 s to 146 s depending on the pass elevation angle. In Fig. 4 we present a total number of secret key bits which can be distributed during a single satellite pass along with the number of transferred classical information bits. In Fig. 4(a) the factor $R = -10$ dB, while in Fig. 5(a) the factor $R = -20$ dB. When detection noise levels of both Bob's and Eve's detectors are similar, this corresponds to the scenario when Eve collects approximately three times more or a ten times more signal than Bob respectively.

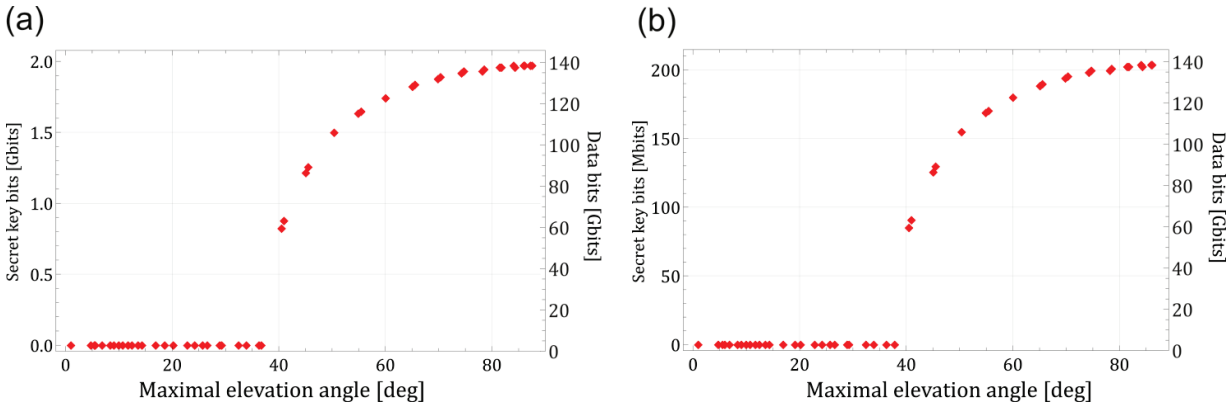


Figure 4. Total number of secret key bits (left axis) which can be distributed during a single LEO satellite pass along with the number of transferred classical information bits (right axis). (a) R = −10 dB (b) R = −20 dB

The number of secret key bits clearly exceeds the performance of QKD realized over satellite distances by several orders of magnitude [11] at the cost of the security level, guaranteed in the present scenario against a restricted class of attacks relying on passive eavesdropping. Apart from offering much higher key distribution speed IM/DD OKD has significantly lower technological requirements dispensing with single photon generation and detection or shot-noise-limited coherent detection. Thus OKD could serve as an attractive alternative to quantum key distribution in recently developed satellite optical communication systems especially if implemented as an additional functionality of the optical terminal.

4. CONCLUSIONS

We have proposed and numerically simulated concurrent data transmission and key distribution over a free-space optical link from a LEO satellite to optical ground station. Satellite-to-ground optical downlinks operate in very stringent conditions regarding onboard electrical power consumption and communication session duration. The essential advantage of the presented scheme is the simultaneous use of a single laser beam for both information transmission and secure key generation while preserving the total data volume transmitted during the communication session. Our simulations based on typical parameters of satellite orbit, optical ground station and optical transmitter show a clear advantage of optical key distribution over quantum key distribution in terms of attainable secret key rate. Under the assumptions discussed in the paper it is possible to generate up to 200 Mbits of a secret key during a single nearly zenithal pass of a LEO satellite which exceeds current QKD standards by approximately three orders of magnitude [11]. Additionally in contrast to QKD, implementing the OKD functionality would not require any major redesign of satellite optical transmitters which routinely utilize IM/DD modulation formats for regular data downlink. The security analysis of optical key distribution is based on potential eavesdropper signal detection capabilities such as detection noise and the receiver telescope size. Thanks to technological simplicity and high key bitrates offered by optical key distribution it can be in principle used for enhancing the security of free-space optical communication links in near-future missions.

ACKNOWLEDGMENTS

This work is a part of the project “Quantum Optical Technologies” carried out within the International Research Agendas Programme of the Foundation for Polish Science co-financed by the European Union under the European Regional Development Fund. ML and PK acknowledge financial support by the Foundation for Polish Science (FNP) (project First Team co-financed by the European Union under the European Regional Development Fund, POIR.04.04.00-00-3FD9/17).

REFERENCES

[1] T. Ikuta, K. Inoue, “Intensity modulation and direct detection quantum key distribution based on quantum noise,” New J. Phys. 18, 013018 (2016).
[2] N. Yamamori, K. Inoue, “Experimental demonstration of intensity- modulation/direct-detection secret key distribution,” Jpn. J. Appl. Phys. 59, 022003 (2020).
[3] P. V. Trinh, A. Carrasco-Casado, A. T. Pham, M. Toyoshima, “Secrecy analysis of FSO systems considering misalignments and eavesdropper’s location,” IEEE Trans. Commun. 68, 7810–7823 (2020).
[4] K. Banaszek, M. Jachura, P. Kolenderski, and M. Lasota, "Optimization of intensity- modulation/direct-detection optical key distribution under passive eavesdropping," Opt. Express 29, 43091-43103 (2021).
[5] R. Hui [Introduction to Fiber-Optics Communications], Academic Press, Cambridge, MA (2019).
[6] T. S. Rose, D. W. Rowen, S. D. LaLumondiere, N. I. Werner, R. Linares, A. C. Faler, J. M. Wicker, C. M. Coffman, G. A. Maul, D. H. Chien, A. C. Utter, R. P. Welle, and S. W. Janson, "Optical communications downlink from a low-earth orbiting 1.5U CubeSat," Opt. Express 27, 24382-24392 (2019).
[7] R. W. Kinsgsbury, [Optical Communications for Small Satellites], MIT, Cambridge, MA (2015).
[8] D. Roddy, [Satellite Communications 4th Edition], McGraw Hill, New York, 29-75 (2006).
[9] https://www.kyosemi.co.jp/mgt/wp-content/uploads/products/kpdxa1gk-t/kpdxa1gk-t_en.pdf
[10] Moision, B. and Farr, W., “Range dependence of the optical communications channel,” IPN Prog. Rep. 42-199, 1–10 (2014)
[11] R. Bedington, J. M Arrazola, A. Ling, “Progress in satellite quantum key distribution,” npj Quantum Inf 3, 30 (2017)