Berra et al. *EPJ Quantum Technology* (2023) 10:27
https://doi.org/10.1140/epjqt/s40507-023-00185-y

EPJ Quantum Technology
a SpringerOpen Journal

EPJ.org

RESEARCH Open Access

Modular source for near-infrared quantum communication

Federico Berra[1*], Costantino Agnesi[1], Andrea Stanco[1], Marco Avesani[1], Sebastiano Cocchi[1], Paolo Villoresi[1,2] and Giuseppe Vallone[1,2,3]

*Correspondence:
federico.berra@phd.unipd.it
[1]Dipartimento di Ingegneria dell'Informazione, Università degli Studi di Padova, via Gradenigo 6B, 35131 Padova, Italy
Full list of author information is available at the end of the article

Abstract

We present a source of states for Quantum Key Distribution (QKD) based on a modular design exploiting the iPOGNAC, a stable, low-error, and calibration-free polarization modulation scheme, for both intensity and polarization encoding. This source is immune to the security vulnerabilities of other state sources such as side channels and some quantum hacking attacks. Remarkably, our intensity modulation scheme allows full tunability of the intensity ratio between the decoy and signal states, and mitigates patterning effects. The source was implemented and tested at the near-infrared optical band around 800 nm, of particular interest for satellite-based QKD. Furthermore, the modularity of the source simplifies its development, testing, and qualification, especially for space missions. For these reasons, our work paves the way for the development of the second generation of QKD satellites that can guarantee excellent performances at higher security levels.

Keywords: iPOGNAC; Near-infrared; QKD; Quantum; Quantum comunication; Quantum key distribution; Satellite

1 Introduction

Quantum Key Distribution (QKD) [1, 2] is essential to ensure the safe exchange of sensitive data between distant parties. Establishing its security on the principles of quantum mechanics and the characteristics of photons, QKD allows two distant parties to distill a secret key with unconditionally secure and bound the shared information with any adversarial eavesdropper [3]. Furthermore, unlike computationally-secure classical algorithms, QKD offers long-term privacy since algorithmic and technological advances for both classical and quantum computation do not threaten the security of keys generated with QKD.

Satellite-based QKD [4–6] is essential for the development of a global-scale network mainly because the achievable distance between parties with a satellite-assisted link is substantially larger than the distances compatible with optical fiber which is limited by exponential propagation losses to a few hundred of kilometers [7] in the absence of quantum repeaters. This has led to several pioneering works in satellite quantum communications [8–10], culminating in the development and launch of the Micius satellite by the Chinese Academy of Science [11] that demonstrated intercontinental QKD links [12]. In

Springer

this regard, the near-infrared (NIR) optical band around 800 nm has been often cited as an ideal wavelength for satellite-based quantum communications since it has good atmospheric transmission, enables the use of free-space coupled silicon-based single photon avalanche diode (SPADs), and is a good compromise in terms of beam divergence (which is proportional to the wavelength) especially when compared to longer wavelengths.

The technical solution employed by the Micius satellite to develop the QKD transmitter is based on a multiple light source approach, where each polarization state and each intensity state was emitted by an independent laser. This leads to a total of 8 lasers being used to implement the decoy-states BB84 protocol [13, 14]. This solution offers good performances in terms of stability and intrinsic QBER, but recent studies have highlighted that a fully secure implementation can be challenging [2, 15].

A first concern is related to the distinguishability of the optical pulses emitted by the independent laser sources and responsible for encoding the different polarization and intensity states. Any difference between the photonic degrees of freedom of the light pulses, such as in the spectral or temporal profiles, could enable an eavesdropper to perform a side-channel attack, obtaining information about the exchanged key without being detected and compromising the security of the protocol [16]. If not properly assessed and mitigated, the harsh space environment could exacerbate this security vulnerability since each individual laser could be subject to different temperature gradients or radiation doses, individually modifying their behavior and opening a side channel for a quantum hacker to exploit. The second vulnerability of the multiple light source approach is that it is susceptible to some quantum hacking attacks such as the Trojan Horse attack described by Lee *et al.* [17], where an eavesdropper can change the wavelength of the independent laser sources of different amounts, enabling him to obtain polarization information without performing a direct polarization measurement.

A possible solution to these security concerns is to change the design of the QKD transmitter to implement decoy-states BB84 with a single light source, an intensity modulator to generate the decoys, and a polarization modulator to encode the quantum states. This, however, comes with the technical challenge of developing intensity and polarization modulation stages that guarantee the required performances in terms of stability and state quality. Regarding, intensity modulation a large concern emerged with the patterning effect that commercial-off-the-shelf intensity modulators would exhibit and would cause a significant decrease in the achievable secure key rate [18–20]. However, the patterning effect can be mitigated with an active device [21] or passively with the design presented by Roberts *et al.* [22] at the cost of fixing the decoy state ratio at construction.

Regarding polarization modulation instead, the iPOGNAC[1] offers a stable, low-error, and calibration-free solution [23], which has currently been developed and tested only at 1550 nm. The implementation of the iPOGNAC at shorter wavelengths is more challenging due to several reasons. First of all, the availability and reliability of optical components such as high-speed lasers or phase modulators is lower compared to the high maturity of TELECOM components. Secondly, temperature fluctuations became more relevant at 800 nm with respect to 1550 nm due to a shortening of the beat length [24] and smaller core areas of the polarization maintaining (PM) fibers. This leads to more

[1]The iPOGNAC is object of the Italian Patent No. 102019000019373 filed on 21.10.2019 as well as of the International Patent Application no. PCT/EP2020/079471 filed on 20.10.2020.

stringent requirements on the alignment of the optical axis between PM fibers (Mating Sleeves). Therefore, the extension of the iPOGNAC at 800 nm is not straightforward.

In this work, we present a novel QKD source designed for satellite-based operations and working in the NIR optical band around 800 nm. This QKD source adopts a modular design approach, exploiting the iPOGNAC for both intensity and polarization modulation. In this way, patterning-effect-free intensity modulation is obtained passively with the added flexibility of effortless tuning the intensity ratio. Furthermore, polarization modulation with the iPOGNAC guarantees polarization states that are fixed with respect to the transmitter's reference frame eliminating the need for calibration between the transmitter and the receiver. Secondly, given its free-space output, it can be easily interfaced with a telescope, making it a promising solution for quantum communication with satellites.

The manuscript is organized as follows: The design and working principle of our modular QKD source are explained in Sect. 2, giving particular focus to the novel iPOGNAC-based intensity modulation scheme. Experimental validation of the source is performed in Sect. 3 that concludes with a proof-of-principle QKD experiment.

2 Methods

2.1 Intensity modulation

The intensity modulator introduced in this work, depicted in Fig. 1, is based on the iPOGNAC polarization modulator [23]. This design choice results in our intensity modulator inheriting all of the key performance characteristics of the iPOGNAC. In particular, its self-compensating design leads to long-term stability without the need for any feedback mechanism. This has been thoroughly tested in previous works [23, 25], even in an urban field trail [26]. Furthermore, compared to other polarization encoders, the iPOGNAC is capable of producing fixed, stable, and well-defined polarization states without any need for calibration. This fact is exploited in the construction of the intensity modulator.

To achieve these characteristics, the iPOGNAC combines a hybrid free-space and fiber-optical scheme, obtaining the polarization stability of free-space optics as well as the flexibility and technological maturity of fiber-based optical components. The iPOGNAC begins with a free-space segment composed of a half-wave plate (HWP) and a beamsplitter (BS). The HWP is used to convert the input linearly polarized light pulses to a diagonal state of polarization (SOP) $|D\rangle = (|H\rangle + |V\rangle)/\sqrt{2}$. Instead, the BS is used to separate the input beam from the output. The light is then coupled into a polarization-maintaining (PM) optical fiber and sent to an unbalanced Sagnac interferometer containing a high-bandwidth phase modulator. Here, however, the BS is replaced by a fiber-based polarization beamsplitter (PBS) with a PM optical fiber input and outputs. The asymmetry of the interferometer allows us to control the SOP exiting the device. Indeed by suitably choosing

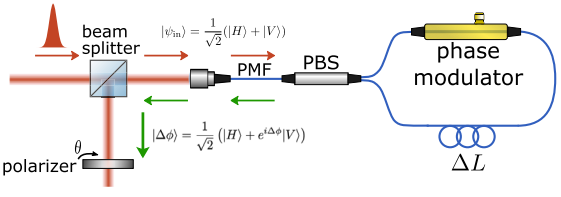

Figure 1 Intensity modulator scheme. Scheme of the proposed intensity modulator composed of an iPOGNAC polarization modulator followed by a polarizer rotated at an angle θ

the voltages and the arrival time of the pulses driving the phase modulator, the polarization state changes as follows:

$$|\Delta\phi\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle + e^{i\Delta\phi}|V\rangle\right), \tag{1}$$

where $\Delta\phi = \phi_{\mathrm{CW}} - \phi_{\mathrm{CCW}}$, and ϕ_{CW} and ϕ_{CCW} are the phases applied by the phase modulator to the pulses that travel the Sagnac loop clockwise (CW) and counter-clockwise (CCW) respectively. In particular, if we apply a voltage pulse that induces a π phase shift to either the CW or the CCW light pulses, the iPOGNAC generates the antidiagonal SOP $|A\rangle = (|H\rangle - |V\rangle)/\sqrt{2}$. Instead, if no phase shifts are applied, the SOP remains $|D\rangle$. These two states are fundamental in the operation of our iPOGNAC-based intensity modulator, since we target modulating between two mean photon number levels, as required for the 1-decoy state QKD protocol [27]. This decoy-state scheme is chosen as it simplifies the requirements of the quantum state encoder and can provide higher rates in the finite-key scenario [27]. Alternatively, this scheme can be used to implement the two-decoy state protocol with the vacuum state generated by not emitting any laser pulse, as done in Refs. [11, 12]. The light pulses then travel back through the PM fiber and are emitted onto the free-space once again, where the BS directs the light toward the free-space output port.

What distinguishes our intensity modulator from a standard iPOGNAC polarization modulator is that we place a polarizer, with a rotation angle θ, at the output port.

The polarizer rotated at an angle θ results in a projection onto the state $|\theta\rangle = \cos(\theta)|H\rangle + \sin(\theta)|V\rangle$ which can be rewritten as $|\theta\rangle = \cos(\theta - \frac{\pi}{4})|D\rangle + \sin(\theta - \frac{\pi}{4})|A\rangle$ to simplify calculations. When the $|D\rangle$ SOP encounters the polarizer, its transmission probability is given by $|\langle\theta|D\rangle|^2 = \cos^2(\theta - \pi/4)$,whereas the transmission probability for the $|A\rangle$ state is given by $|\langle\theta|A\rangle|^2 = \sin^2(\theta - \pi/4)$. From this, we obtain the intensity ratio value between these two possible states is given by:

$$\mathrm{IR}(\theta) = \frac{|\langle\theta|A\rangle|^2}{|\langle\theta|D\rangle|^2} = \tan^2\left(\theta - \frac{\pi}{4}\right). \tag{2}$$

From Eq. (2), it is clear that the intensity ratio between the two states can be easily tuned to any value by changing the polarizer angle θ, with physical device imperfections representing the only limit. This feature makes our iPOGNAC-based intensity modulator more flexible than other self-compensating intensity modulators such as the one introduced by Roberts *et al.* [22], which has an intensity ratio that is fixed at construction by the transmissivity and reflectivity of the beam splitter used in their Sagnac interferometer. Tuning this ratio can be crucial to obtain the best performance of the QKD system since a change to the operational scenario could lead to a different optimal setting for the decoy states [27]. Furthermore, this feature simplifies the construction and industrialization of the intensity modulator since its performance is not dependent on the fabrication tolerances of the optical components, leading to higher standards of quality and performance repeatability. It is worth noting that the polarizer can be replaced with a polarization-dependent isolator to avoid loopholes caused by back-propagating light.

Another key feature of our intensity modulator is that it is passively free from the patterning effect. This effect arises when the intensity of a pulse emitted by the transmitter

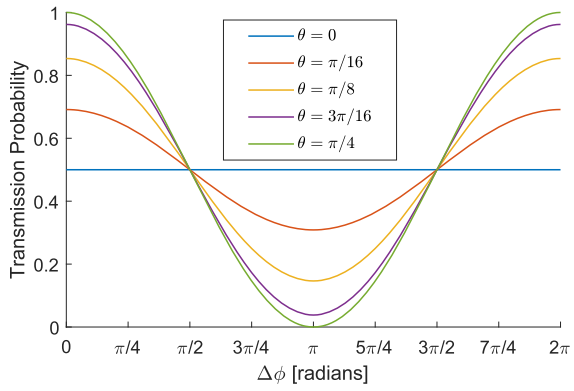

Figure 2 Theoretical intensity ratio response. Theoretical optical response of the system as a function of the iPOGNAC polarization phase modulation $\Delta\phi$ (see Eq. (1)) for different polarizer rotation angles θ

depends on the previous pulse intensity. This is a security concern for the implementation of the decoy-state method and results in a significant drop in the achievable secure rate when taken into account [19, 20]. The patterning effect can be mitigated in two ways: (i) by removing any dependence on the DC voltage level, which we achieved by exploiting a Sagnac loop configuration, and (ii) by working at the points with vanishing derivative of the optical response function since in the latter points, small deviations caused by imperfections and the finite modulation bandwidth of the system cause only small variations in the intensity ratio [22]. In our design, the latter is guaranteed by using orthogonal SOPs $|D\rangle$ ($\Delta\phi = 0$) and $|A\rangle$ ($\Delta\phi = \pi$), which always correspond to the peak and trough points of the optical response function for all values of the polarizer angle θ, as inferred from Fig. 2. Similar patterning-effect mitigation could have been obtained by applying $\pi/2$ radians phase shifts and obtaining the orthogonal circular left $|L\rangle = (|H\rangle + i|V\rangle)/\sqrt{2}$ and circular right $|R\rangle = (|H\rangle - i|V\rangle)/\sqrt{2}$ SOPs. However, this would have increased the complexity of the setup since a quarter-wave plate (QWP) would have been introduced to perform the required projection and coordinated rotation of the QWP and the polarizer would have been necessary. We also note that at a fixed polarizer angle, by changing the value of $\Delta\phi$ any intensity ratio between 0 and the value predicted by Eq. (2) can be obtained. Therefore, different intensity levels can be generated by using different values of $\Delta\phi$, but a patterning effect might emerge.

2.2 Modular QKD source

We developed a QKD source capable of implementing efficient three-states one-decoy BB84 protocol [28] working in the NIR optical band. The light source used at the transmitter is a gain-switched PM fiber-coupled distributed-feedback laser (Eagleyard EYP-DFB-0795), emitting 795 nm light pulses with 575 ps FWHM at a repetition rate of $R = 50$ MHz and driven by a laser pulser (Highland Technology T165). A PM fiber-based polarizer is then encountered to guarantee a stable and fixed SOP as the input for the iPOGNAC-based intensity modulator, described in detail in Sect. 2.1. For convenience, instead of rotating the intensity modulator's polarizer, we decided to keep it at a fixed angle and inserted a HWP before it to emulate the polarization rotation angle. This allowed us to have a fixed output polarization state $|D\rangle$ at the output of the intensity modulator without changing the characteristics of the device and simplifying the interface with the following

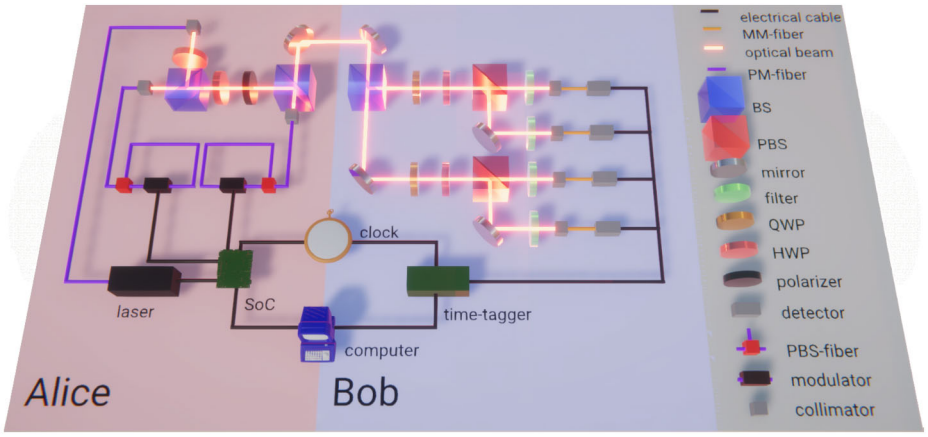

Figure 3 Full-setup scheme. A rendered version of the modular source and receiver for near-infrared quantum communications

module. In a satellite mission, the HWP can be replaced by a liquid crystal device which minimizes power and space requirements and eliminates undesirable torques. This solution has been implemented in a past nanosatellite mission described in Refs. [29, 30]. The HWP was set at an equivalent polarizer angle $\theta \approx 0.50$ rad, tuned to guarantee a signal and decoy ratio of $\nu/\mu \approx 0.30$ which is near optimal for the three-state and one-decoy efficient BB84 protocol for a wide range of total losses (30 dB to 60 dB) of interest for satellite-based QKD [27]. Interestingly enough, in recent satellite QKD experiment losses of about 20 dB have also been reported [31].

The light then encountered a second iPOGNAC encoder, responsible for modulating the degree of freedom of polarization of the qubit. In this case, the amplitude of the driving electric pulse was set to induce a $\pi/2$ phase shift, allowing the iPOGNAC to generate circular left $|L\rangle$, circular right $|R\rangle$, or diagonal $|D\rangle$ polarized light. In this way, we generate the three states required by the simplified three-polarization state version of BB84, with the key generation basis $\mathcal{Z} = \{|0\rangle, |1\rangle\}$ where $|0\rangle := |L\rangle$, $|1\rangle := |R\rangle$, and the control state $|+\rangle$ of the $\mathcal{X} = \{|+\rangle, |-\rangle\}$ control basis where $|+\rangle := |D\rangle$ and $|-\rangle := |A\rangle$. As discussed in the previous section, the iPOGNAC can also generate the $|A\rangle$ by inducing π shifts and therefore is capable of implementing the standard four-state BB84 protocol. However this would not come with any advantage since, as demonstrated by Tamaki *et al.* [32], the BB84 QKD protocol can be fully secured using only one control state and the resulting secret key rate is the same as the original. A Variable Optical Attenuator (VOA) then sets an appropriate intensity for signal ($\mu \approx 0.6$) and decoy ($\nu \approx 0.2$) pulses. The light was then sent to the quantum receiver via a free-space channel.

The electronic signals that trigger the laser pulser and drive the modulators are controlled by a system-on-a-chip (SoC) that includes a field-programmable gate array (FPGA) and a CPU [33] and is integrated on a dedicated board (Zedboard by Avnet).

2.3 QKD receiver

The quantum state receiver is based on a well-tested and fully free-space design that has been used even in satellite-based QKD experiments [11]. The measurement basis choice is performed passively using a 60:40 BS. At each output port of the BS, QWPs, HWPs, and

PBSs are placed to perform projective measurements. In particular, the transmitted light (60%) is measured in the key-generation basis $\mathcal{Z}$, whereas the reflected light (40%) is measured in the $\mathcal{X}$ control basis. After projection, light is filtered by 10 nm FWHM passband filters and collected by multimode fibers (NA = 0.22 and 105 μm core size) which guide light toward silicon-based single-photon avalanche diodes (SPAD) with 68% quantum efficiency and about 1000 dark counts per second. A time-to-digital converter was used to record the detection events that were then processed by a computer.

In our setup, synchronization between the transmitter and the receiver can be performed via a direct RF cable link, exploiting a clock-data-recovery routine performed on a co-propagating classical optical link [34], or via Qubit4Sync qubit-based synchronization [35]. However, for experimental simplicity, a direct RF cable link was preferred.

3 Results and discussion

3.1 Tunability of the intensity

As mentioned in Sect. 2.1, the first key feature of the iPOGNAC-based intensity modulator is its capability of tuning the optimal ratio between the two intensity levels μ, ν simply by rotating the polarizer at the end of the intensity modulator.

We tested this behavior using the setup described in the previous section, shown in Fig. 3, by sending a pseudorandom sequence of intensities and tacking a 60 s acquisition for each equivalent polarizer angle obtained by rotating an HWP. As reported in Fig. 4, a total of 12 different equivalent polarizer angles were tested in the range around 0 and $\pi/4$, all in good correspondence with the theoretical values obtained from Eq. (2).

3.2 Patterning effect mitigation

The second key feature of the intensity modulator, as explained in Sect. 2.1, is the fact that it mitigates patterning effects by operating at the peak of the optical response function where the derivate is smaller. This guarantees that fluctuation of the driving electric signal produces small deviations in the final intensities.

As before, we tested this behavior using the setup described shown in Fig. 3 by sending a 1024-bit pseudorandom sequence of intensities and tacking a 120 s acquisition for a polarizer angle of $\theta \approx 0.50$ rad, tuned to guarantee a signal and decoy ratio of $\nu/\mu \approx 0.30$. The detection histogram for a subset of 50 intensities can be seen in Fig. 5.

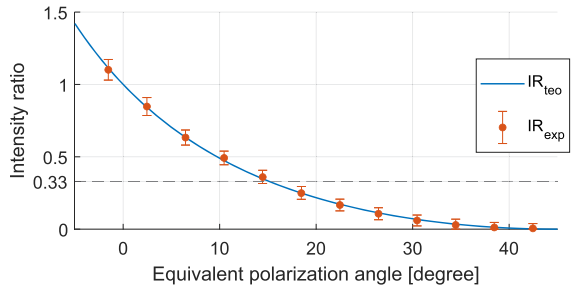

Figure 4 Intensity ratio. Ratio between ν and μ intensities: the dots represent the experimental data with associated error bars, whereas the continuous line is derived from Eq. (2). The typical value of the intensity ratio for the protocol [27] is approximately 0.33, as represented by the horizontal dashed line

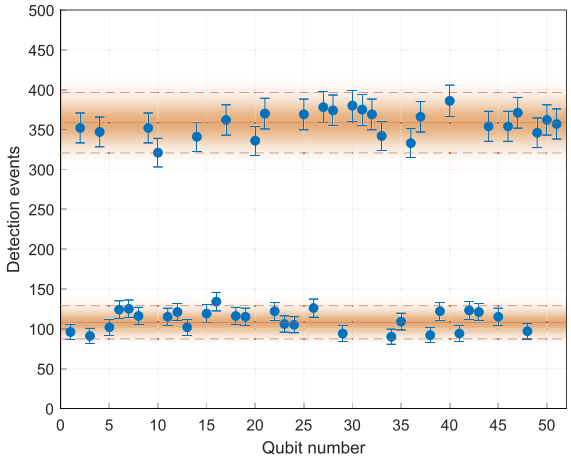

Figure 5 Patterning statistics. Single photon detection statistics (blue) for a 50-symbol portion of a random μ, ν intensity pattern: the dots represent the experimental data with associated error bars, instead, the solid line represents the average value whereas the dashed lines represent the $\pm 2\sigma$ confidence interval

Table 1 Average pulse intensities of μ and ν when preceded by either μ or ν. The average pulse intensity for the μ intensity is normalized to unity

Pattern	$c_{i\to i'}$	$d_{i\to i'}$ (%)
$\mu \to \mu$	1.00 ± 0.04	0.001
$\nu \to \mu$	1.00 ± 0.04	−0.001
$\nu \to \nu$	0.30 ± 0.02	−0.001
$\mu \to \nu$	0.30 ± 0.02	0.001

For each intensity, we computed the normalized average intensity of its subsequent pulse:

$$c_{i\to i'} = \frac{\langle s_{i\to i'} \rangle}{\langle \mu \rangle} \tag{3}$$

and the deviation from the average:

$$d_{i\to i'} = \frac{\langle s_{i\to i'} - \langle i' \rangle \rangle}{\langle i' \rangle}, \tag{4}$$

where $s_{i\to i'}$ is the click's count for the symbol i' with preceding symbol i, and $\langle i' \rangle$ is the average between all the same symbols. The results reported in Table 1 show that all the fluctuations are within the experimental uncertainty and confirm that there is no patterning. This result is a substantial improvement compared to the best-case scenario of around 18.2% deviations observed by Yoshino *et al.*. [19] when producing decoy states using a commercial Mach-Zehnder intensity modulator at the quadrature point, and is in line with the results obtained by Roberts *et al.* [22]. We would like to note that even though our experimental demonstration is limited to a repetition rate of 50 MHz, the patterning effect mitigation of Sagnac loop-based intensity modulators have been demonstrated up to a repetition rate of 2 GHz [22].

3.3 QKD experiment

To evaluate the overall performances of our modular quantum source, we performed a proof-of-principle 15-minute long QKD experiment. Such a duration was targeted since it represents the typical duration of a Low Earth Orbit satellite passage [11]. The test was performed using a quantum channel consisting of a free-space segment and attenuating neutral density filters to simulate losses caused by geometrical losses and atmospheric absorption typical of satellite links. Two pseudorandom sequences are used to set the polarization state and the intensity values respectively. Based on the above sequences, the signal and decoy state are sent with probabilities $P_\mu = 0.7$ and $P_\nu = 0.3$, while the two polarization basis are sent with probabilities $P_\mathcal{Z} = 0.9$ and $P_\mathcal{X} = 0.1$ respectively.

The mean detection rate R_{det} was of $\approx 2.7 \cdot 10^5$ events per seconds. Considering that the source emits on average $(\mu P_\mu + \nu P_\nu) \cdot R = 2.4 \cdot 10^7$ photons per second, we estimate that the total losses were approximately 19 dB. The channel contribution to these losses is about 15 dB, while the remaining 4 dB can be attributed to the detectors' efficiencies and other receiver losses. These losses were chosen to test the intrinsic behavior of the source while avoiding detector saturation.

We report the quantum bit error rate (QBER) and the secret key rate (SKR) obtained in Fig. 6. The QBER was calculated independently for the key generation basis $\mathcal{Z}$ and the control basis $\mathcal{X}$. We can see that both QBERs are lower than the ≈ 11 % upper limit for secure key generation, with $\mathrm{Q}_\mathcal{Z} = 0.62 \pm 0.05\%$ and $\mathrm{Q}_\mathcal{X} = 1.15 \pm 0.01\%$. The SKR was calculated following the finite-size analysis of Ref. [27]:

$$\mathrm{SKR} = \frac{1}{t}\left[s_0 + s_1\left(1 - h(\phi_\mathcal{Z})\right) - \lambda_{\mathrm{EC}} - \lambda_{\mathrm{c}} - \lambda_{\mathrm{sec}}\right], \tag{5}$$

where terms s_0 and s_1 are the lower bounds on the number of vacuum and single-photon detection events in the key generating $\mathcal{Z}$ basis, $\phi_\mathcal{Z}$ is the upper bound on the phase error rate in the $\mathcal{Z}$ basis corresponding to single-photon pulses, $h(\cdot)$ is the binary entropy, λ_{EC} and λ_{c} are the number of bits published during the error correction and confirmation of correctness steps, $\lambda_{\mathrm{sec}} = 6\log_2(\frac{19}{\epsilon_{\mathrm{sec}}})$ with $\epsilon_{\mathrm{sec}} = 10^{-10}$ is the security parameter associated

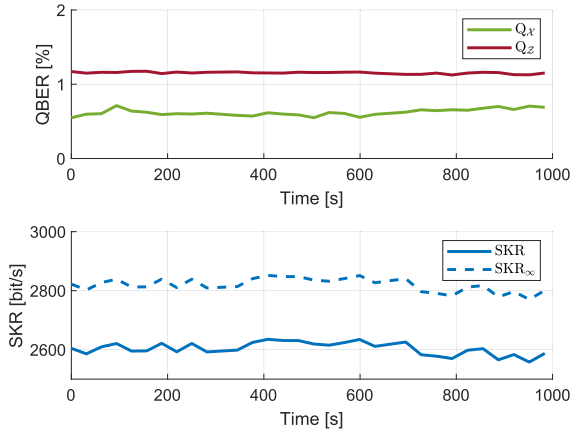

Figure 6 QBER and SKR. The Quantum Bit Error Rate and the Secure Key Rate obtained with our modular QKD source. An average $\mathrm{Q}_\mathcal{Z} = 0.62 \pm 0.05$ and $\mathrm{Q}_\mathcal{X} = 1.15 \pm 0.01$ were observed whereas a finite-key $\mathrm{SKR} = 2603 \pm 21$ ($\mathrm{SKR}_\infty = 2819 \pm 23$) bits per second was obtained

to the secrecy analysis, and finally t is the duration of the quantum transmission phase. Equation (5) is applied to $6.59 \cdot 10^6$-bit-long key blocks. This resulted in a finite-key analysis SKR or around SKR = 2603 ± 21 bits per second whereas the asymptotic SKR is around $\mathrm{SKR}_\infty = 2819 \pm 23$ bits per second.

4 Conclusions

In this manuscript, we have proposed a novel QKD source based on a modular design exploiting the iPOGNAC encoder [23] for both intensity and polarization modulation. In this way, our QKD source is immune to side-channel [16] and Trojan Horse attacks [17] targeting sources using multiple lasers, and passively mitigates the intensity pattering effect [19] without sacrificing the tunability of the decoy state ratio and maintaining all benefits deriving from the iPOGNAC. The source was experimentally tested at the NIR optical band around 800 nm, representing the first implementation of the iPOGNAC scheme at this wavelength and confirming the key features of the source.

The modularity of the scheme is advantageous in the development, testing and qualification of the entire QKD system. This is mainly because a single base element, *i.e.* the iPOGNAC, is responsible for two key tasks in QKD implementation. This allows the system developer to concentrate in optimizing and hardening a single device, without dissipating resources for others. This is particularly propitious for satellite missions since space-qualification is an expensive and time-consuming process. Furthermore, the design is compatible both at telecom wavelengths and, as demonstrated here, at the NIR optical band, which are of interest for satellite-based quantum communications. In fact, the results here presented can be considered a consolidation of the Technology Readiness Level to TRL 4 (breadboard demonstration in the laboratory). Future developments will focus on increasing the TRL level by optimizing, hardening and miniaturizing the design and validating it in a relevant environment which includes vibrations, temperature fluctuation, and vacuum. For these reasons, we believe that our work paves the way for the development of a second generation of QKD satellites that can guarantee excellent performances at the highest security levels.

Funding
This work was supported by the European Union's Horizon 2020 research and innovation programme, project QUANGO (grant agreement No 101004341) and by MIUR (Italian Minister for Education) under the initiative "Departments of Excellence" (Law 232/2016).

Availability of data and materials
The data that support the findings of this study are available from the corresponding author, G.V., upon reasonable request.

Declarations

Ethics approval and consent to participate
Not applicable.

Consent for publication
All authors have approved the publication. The research in this work did not involve any human, animal or other participants.

Competing interests
The authors declare no competing interests.

Author contributions
C.A., M.A., G.V., P.V. designed the experiment. A.S., M.A., F.B., C.A. developed the control electronics. F.B., C.A. developed the transmitter and receiver control software and the post-processing software. F.B., S.C. performed the experiment. All authors discussed the results. C.A., F.B. wrote the manuscript with inputs from all the authors.

Author details
[1]Dipartimento di Ingegneria dell'Informazione, Università degli Studi di Padova, via Gradenigo 6B, 35131 Padova, Italy.
[2]Padua Quantum Technologies Research Center, Università degli Studi di Padova, via Gradenigo 6B, 35131 Padova, Italy.
[3]Dipartimento di Fisica e Astronomia, Università degli Studi di Padova, via Marzolo 8, 35131 Padova, Italy.

Received: 21 March 2023 Accepted: 26 June 2023 Published online: 12 July 2023

References

1. Gisin N, Ribordy G, Tittel W, Zbinden H. Quantum cryptography. Rev Mod Phys. 2002;74:145–95. https://doi.org/10.1103/RevModPhys.74.145.
2. Pirandola S, Andersen UL, Banchi L, Berta M, Bunandar D, Colbeck R, Englund D, Gehring T, Lupo C, Ottaviani C, Pereira JL, Razavi M, Shamsul Shaari J, Tomamichel M, Usenko VC, Vallone G, Villoresi P, Wallden P. Advances in quantum cryptography. Adv Opt Photonics. 2020;12(4):1012. https://doi.org/10.1364/AOP.361502.
3. Scarani V, Bechmann-Pasquinucci H, Cerf NJ, Du šek M, Lütkenhaus N, Peev M. The security of practical quantum key distribution. Rev Mod Phys. 2009;81:1301–50. https://doi.org/10.1103/RevModPhys.81.1301.
4. Agnesi C, Vedovato F, Schiavon M, Dequal D, Calderaro L, Tomasin M, Marangon DG, Stanco A, Luceri V, Bianco G, Vallone G, Villoresi P. Exploring the boundaries of quantum mechanics: advances in satellite quantum communications. Philos Trans R Soc, A. 2018;376(2123):20170461. https://doi.org/10.1098/rsta.2017.0461.
5. Kaltenbaek R, Acin A, Bacsardi L, Bianco P, Bouyer P, Diamanti E, Marquardt C, Omar Y, Pruneri V, Rasel E, Sang B, Seidel S, Ulbricht H, Ursin R, Villoresi P, van den Bossche M, von Klitzing W, Zbinden H, Paternostro M, Bassi A. Quantum technologies in space. Exp Astron. 2021;51(3):1677–94. https://doi.org/10.1007/s10686-021-09731-x.
6. Sidhu JS, Joshi SK, Gündoğan M, Brougham T, Lowndes D, Mazzarella L, Krutzik M, Mohapatra S, Dequal D, Vallone G, Villoresi P, Ling A, Jennewein T, Mohageg M, Rarity JG, Fuentes I, Pirandola S, Oi DKL. Advances in space quantum communications. IET Quantum Commun. 2021;2(4):182–217. https://doi.org/10.1049/qtc2.12015.
7. Boaron A, Boso G, Rusca D, Vulliez C, Autebert C, Caloz M, Perrenoud M, Gras G, Bussières F, Li M-J, Nolan D, Martin A, Zbinden H. Secure quantum key distribution over 421 km of optical fiber. Phys Rev Lett. 2018;121:190502. https://doi.org/10.1103/PhysRevLett.121.190502.
8. Villoresi P, Jennewein T, Tamburini F, Aspelmeyer M, Bonato C, Ursin R, Pernechele C, Luceri V, Bianco G, Zeilinger A, Barbieri C. Experimental verification of the feasibility of a quantum channel between space and Earth. New J Phys. 2008;10(3):033038. https://doi.org/10.1088/1367-2630/10/3/033038.
9. Vallone G, Bacco D, Dequal D, Gaiarin S, Luceri V, Bianco G, Villoresi P. Experimental satellite quantum communications. Phys Rev Lett. 2015;115:040502. https://doi.org/10.1103/PhysRevLett.115.040502.
10. Vallone G, Dequal D, Tomasin M, Vedovato F, Schiavon M, Luceri V, Bianco G, Villoresi P. Interference at the single photon level along satellite-ground channels. Phys Rev Lett. 2016;116:253601. https://doi.org/10.1103/PhysRevLett.116.253601.
11. Liao S-K, Cai W-Q, Liu W-Y, Zhang L, Li Y, Ren J-G, Yin J, Shen Q, Cao Y, Li Z-P, Li F-Z, Chen X-W, Sun L-H, Jia J-J, Wu J-C, Jiang X-J, Wang J-F, Huang Y-M, Wang Q, Zhou Y-L, Deng L, Xi T, Ma L, Hu T, Zhang Q, Chen Y-A, Liu N-L, Wang X-B, Zhu Z-C, Lu C-Y, Shu R, Peng C-Z, Wang J-Y, Pan J-W. Satellite-to-ground quantum key distribution. Nature. 2017;549(7670):43–7. https://doi.org/10.1038/nature23655.
12. Liao S-K, Cai W-Q, Handsteiner J, Liu B, Yin J, Zhang L, Rauch D, Fink M, Ren J-G, Liu W-Y, Li Y, Shen Q, Cao Y, Li F-Z, Wang J-F, Huang Y-M, Deng L, Xi T, Ma L, Hu T, Li L, Liu N-L, Koidl F, Wang P, Chen Y-A, Wang X-B, Steindorfer M, Kirchner G, Lu C-Y, Shu R, Ursin R, Scheidl T, Peng C-Z, Wang J-Y, Zeilinger A, Pan J-W. Satellite-relayed intercontinental quantum network. Phys Rev Lett. 2018;120(3):030501. https://doi.org/10.1103/physrevlett.120.030501.
13. Bennett CH, Brassard G. Quantum cryptography: public key distribution and coin tossing. Theor Comput Sci. 2014;560(P1):7–11. https://doi.org/10.1016/j.tcs.2014.05.025.
14. Hwang W-Y. Quantum key distribution with high loss: toward global secure communication. Phys Rev Lett. 2003;91:057901. https://doi.org/10.1103/PhysRevLett.91.057901.
15. Lo H-K, Curty M, Tamaki K. Secure quantum key distribution. Nat Photonics. 2014;8(8):595–604. https://doi.org/10.1038/nphoton.2014.149.
16. Nauerth S, Fürst M, Schmitt-Manderbach T, Weier H, Weinfurter H. Information leakage via side channels in freespace BB84 quantum cryptography. New J Phys. 2009;11(6):065001. https://doi.org/10.1088/1367-2630/11/6/065001.
17. Lee MS, Woo MK, Kim Y-S, Cho Y-W, Han S-W, Moon S. Quantum hacking on a free-space quantum key distribution system without measuring quantum signals. J Opt Soc Am B. 2019;36(3):77–82. https://doi.org/10.1364/JOSAB.36.000B77.
18. Wang X-B, Yang L, Peng C-Z, Pan J-W. Decoy-state quantum key distribution with both source errors and statistical fluctuations. New J Phys. 2009;11(7):075006. https://doi.org/10.1088/1367-2630/11/7/075006.
19. Yoshino K-I, Fujiwara M, Nakata K, Sumiya T, Sasaki T, Takeoka M, Sasaki M, Tajima A, Koashi M, Tomita A. Quantum key distribution with an efficient countermeasure against correlated intensity fluctuations in optical pulses. npj Quantum Inf. 2018;4(1):8. https://doi.org/10.1038/s41534-017-0057-8.
20. Zapatero V, Navarrete Á, Tamaki K, Curty M. Security of quantum key distribution with intensity correlations. Quantum. 2021;5:602. https://doi.org/10.22331/q-2021-12-07-602. arXiv:2105.11165v2.
21. Gao Y, Yuan Z. Suppression of patterning effect using IQ modulator for high-speed quantum key distribution systems. Opt Lett. 2023;48(4):1068–71. https://doi.org/10.1364/OL.481374.
22. Roberts GL, Pittaluga M, Minder M, Lucamarini M, Dynes JF, Yuan ZL, Shields AJ. Patterning-effect mitigating intensity modulator for secure decoy-state quantum key distribution. Opt Lett. 2018;43(20):5110–3. https://doi.org/10.1364/OL.43.005110.
23. Avesani M, Agnesi C, Stanco A, Vallone G, Villoresi P. Stable, low-error, and calibration-free polarization encoder for free-space quantum communication. Opt Lett. 2020;45(17):4706–9. https://doi.org/10.1364/OL.396412.
24. Dvorak F, Maschke J, Vlcek C. The response of polarization maintaining fibers upon temperature field disturbance. Adv Electr Electron Eng. 2014;12(2):168–76. https://doi.org/10.15598/aeee.v12i2.1084.
25. Scalcon D, Agnesi C, Avesani M, Calderaro L, Foletto G, Stanco A, Vallone G, Villoresi P. Cross-encoded quantum key distribution exploiting time-bin and polarization states with qubit-based synchronization. Adv Quantum Technol. 2022;5(12):2200051. https://doi.org/10.1002/qute.202200051.

26. Avesani M, Calderaro L, Foletto G, Agnesi C, Picciariello F, Santagiustina FBL, Scriminich A, Stanco A, Vedovato F, Zahidy M, Vallone G, Villoresi P. Resource-effective quantum key distribution: a field trial in Padua city center. Opt Lett. 2021;46(12):2848–51. https://doi.org/10.1364/OL.422890.
27. Rusca D, Boaron A, Grünenfelder F, Martin A, Zbinden H. Finite-key analysis for the 1-decoy state QKD protocol. Appl Phys Lett. 2018;112(17):171104. https://doi.org/10.1063/1.5023340.
28. Grünenfelder F, Boaron A, Rusca D, Martin A, Zbinden H. Simple and high-speed polarization-based QKD. Appl Phys Lett. 2018;112(5):051108. https://doi.org/10.1063/1.5016931.
29. Tang Z, Chandrasekara R, Tan YC, Cheng C, Sha L, Hiang GC, Oi DKL, Ling A. Generation and analysis of correlated pairs of photons aboard a nanosatellite. Phys Rev Appl. 2016;5:054022. https://doi.org/10.1103/PhysRevApplied.5.054022.
30. Villar A, Lohrmann A, Bai X, Vergoossen T, Bedington R, Perumangatt C, Lim HY, Islam T, Reezwana A, Tang Z, Chandrasekara R, Sachidananda S, Durak K, Wildfeuer CF, Griffin D, Oi DKL, Ling A. Entanglement demonstration on board a nano-satellite. Optica. 2020;7(7):734–7. https://doi.org/10.1364/OPTICA.387306.
31. Chen Y-A, Zhang Q, Chen T-Y, Cai W-Q, Liao S-K, Zhang J, Chen K, Yin J, Ren J-G, Chen Z, Han S-L, Yu Q, Liang K, Zhou F, Yuan X, Zhao M-S, Wang T-Y, Jiang X, Zhang L, Liu W-Y, Li Y, Shen Q, Cao Y, Lu C-Y, Shu R, Wang J-Y, Li L, Liu N-L, Xu F, Wang X-B, Peng C-Z, Pan J-W. An integrated space-to-ground quantum communication network over 4,600 kilometres. Nature. 2021;589(7841):214–9. https://doi.org/10.1038/s41586-020-03093-8.
32. Tamaki K, Curty M, Kato G, Lo H-K, Azuma K. Loss-tolerant quantum cryptography with imperfect sources. Phys Rev A. 2014;90:052314. https://doi.org/10.1103/PhysRevA.90.052314.
33. Stanco A, Santagiustina FBL, Calderaro L, Avesani M, Bertapelle T, Dequal D, Vallone G, Villoresi P. Versatile and concurrent fpga-based architecture for practical quantum communication systems. IEEE Trans Quantum Eng. 2022;3:6000108. https://doi.org/10.1109/TQE.2022.3143997.
34. Berra F, Agnesi C, Stanco A, Avesani M, Kuklewski M, Matter D, Vallone G, Villoresi P. Synchronization of quantum communication over an optical classical communication channel. arXiv:2306.17603. 2022. https://doi.org/10.48550/arXiv.2306.17603.
35. Calderaro L, Stanco A, Agnesi C, Avesani M, Dequal D, Villoresi P, Vallone G. Fast and simple qubit-based synchronization for quantum key distribution. Phys Rev Appl. 2020;13:054041. https://doi.org/10.1103/PhysRevApplied.13.054041.

Publisher's Note