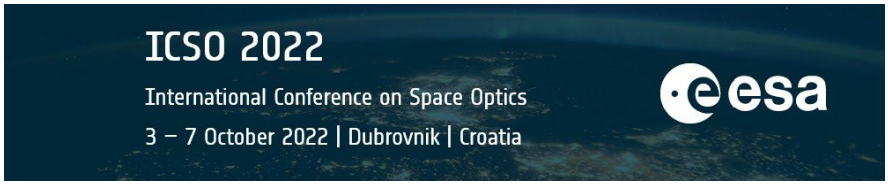
International Conference on Space Optics—ICSO 2022

Dubrovnik, Croatia

3–7 October 2022

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



High-performance 1560 nm Entangled Photon Source for high secure key rates QKD satellite-based communications

International Conference on Space Optics — ICSO 2022, edited by Kyriaki Minoglou, Nikos Karafolas, Bruno Cugny, Proc. of SPIE Vol. 12777, 1277725 · © 2023 ESA and CNES · 0277-786X · doi: 10.1117/12.2689969

High-performance 1560 nm Entangled Photon Source for high secure key rates QKD satellite-based communications

Jean-Marc Merolla*[a], Benjamin Pages[b], Johann Cussey[b], Romain Martinenghi[b], Valentin Parra[b], Emmanuel Fretel[b], Jérôme Prieur[b], Jorge Piris[c]
[a]Institut FEMTO-ST, 15B Avenue des Montboucons, Besançon, FRANCE;
[b]AUREA Technology SAS, 18 rue Alain Savary, Besançon, FRANCE;
[c]ESTEC, Keplerlaan 1, 2200 AG Noordwijk, NETHERLAND.

ABSTRACT

In the frame of the Secure And cryptoGrAphic (SAGA) project under ESA ARTES 4.0 program, we report the design and the test of a High-Performance Entangled Photon Source (HP-EPS) dedicated to QKD satellite-based communication, by using the Conventional-band optical fiber telecom components. We developed an asynchronous time binning higher than 10 bits/sec and 5 bits/sec for respectively a 60 dB (LEO) and a 65 dB (GEO) transmission loss budgets (both downlinks combined). The compactness and simplicity of the optical design, the low electrical consumption and the low mass combined with the robustness of the all-fibered design to the space environment (mechanical vibrations, shock, and radiations) make the HP-EPS a valuable and serious candidate for the satellite-based QKD quest.

Keywords: Entangled photon source, quantum key distribution, satellite communication,

1. INTRODUCTION

The optical telecommunications networks and their associated technologies have experienced a fast past evolution due to the ever-increasing issue of rapid user growth and increasing digital traffic demand. Indeed, optical communications components achieve high-speed, long-distance and high-reliability necessary to implement high-speed and heavy traffic telecommunication networks. In addition, optical communications can potentially offer a global service in so-called Integrated Satellite-Terrestrial Network (ISTN)[1] which combines the global coverage, mobility and scalability of the satellite networks with transmission capacity and low latency of the terrestrial networks. Because such networks carry critical data, or are used by critical infrastructures such as financial, healthcare, energy and governmental organizations, the communications security becomes of high importance to secure information against the growth of cyber-criminal activities. Conventional encryption methods are mainly based on symmetric cryptographic algorithms. In these methods, the message is mixed with a key (a random bit stream in case of digital communication) and the security relies mainly on the difficulty to retrieve the original message without knowing the key. The so-called one-time pad encryption invented by Vernam[2] which uses a symmetric random secret key shared between legitim users have been proven unbreakable by Shannon[3], if the key is used one time and if its length is as long as the message. However, these methods suffer from the problem of key sharing. Public key exchange protocols have been proposed[4] to provide a solution of the problem of keys exchange based on mathematical complexity. The method is based on the use of a couple of public and private keys. The secret shared key is build using the public keys which are mutually exchange. The security of the public key algorithm is based on the assumption that the problem to retrieve the secret shared key without knowing one of the private keys is challenging to solve, but not proven impossible. Therefore, such schemes cannot ensure information-theoretic security because they are exposed to advances in hardware and algorithms, including upcoming quantum computers[5]. Quantum Key Distribution (QKD) offers in theory unconditional security based on the laws of physics ensuring a perennial confidentiality. Since pioneer works numerous advances[6] in terms of protocols than implementations have been realized to proposed operational systems operating in different networks[6] including satellite networks. Among the QKD methods, one of the most promising is those based on entangled photon source. Indeed, entanglement is in the heart of numerous quantum applications and is a key resource for the development of Quantum Information Networks (QIN)[7]. Combining with quantum memories, high-performance entangled photon sources (HP_EPS) will enable quantum communications at very long distance[8]. In QKD applications, entanglement-based protocols can be used to implement device-independent QKD[9]. In addition, entanglement-based protocols do not require any random generator unlike prepare-and-measure

protocols, making simple and robust the implementation of such systems. These advantages are essential for the development of satellite based QKD, which has recently attracted a lot of attention in Asia and in Europe. Indeed, in the race of global-scale quantum communications, satellite-based QKD offers real alternative to the quantum repeater to unlock the distance issue in terrestrial networks. After the success of the Micius satellite[10] in 2016, many satellite-based QKD initiatives have been launched[10]. In 2019, the European Quantum Communication Infrastructure (Euro-QCI) launched the development of a secure quantum communication infrastructure (both spatial and terrestrial) with pan-European reach. In this context, we report the investigations we performed in the frame of the ESA ARTES 4.0 program, concerning the development of a High-Performances Entangled Photon Sources (HP-EPS) operating at 1560 nm telecom wavelength for satellite-based QKD. By using C-band optical fiber telecom components, the HP-EPS features outstanding compactness and brightness performances enabling high Secure Key Rates (SKR) and LEO and GEO distances compliant with satellite-based communications. Operating at 1560 nm potentially overcomes the main drawbacks of the more traditional 800 nm satellite based QKD. Compared to 800 nm, the telecom C-band wavelength[11] has the atmospheric transmission slightly higher and lower Rayleigh scattering. In addition, the sunlight intensity at 1550 nm is 5 times weaker than at 800 nm, which enable daylight operation. Notice that finally the use of commercially available off-the-shelf (COTS) Telcordia-qualified optical fiber telecom components associated with a smart design architecture accelerates the deployment of the HP-EPS sources.

The paper is divided into two main parts. We first describe the HP-EPS entangled photon source developed, and the method used to the implementation of a QKD experiment using a BBM92 protocol. In the second part we present our main experimental results including the source performances as well as the QKD test results.

2. PHOTON SOURCE AND TIME ENCODING BBM92 PROTOCOL

2.1 Entangled Photon Source

The figure 1 represents the simplified architecture of our HP-EPS.

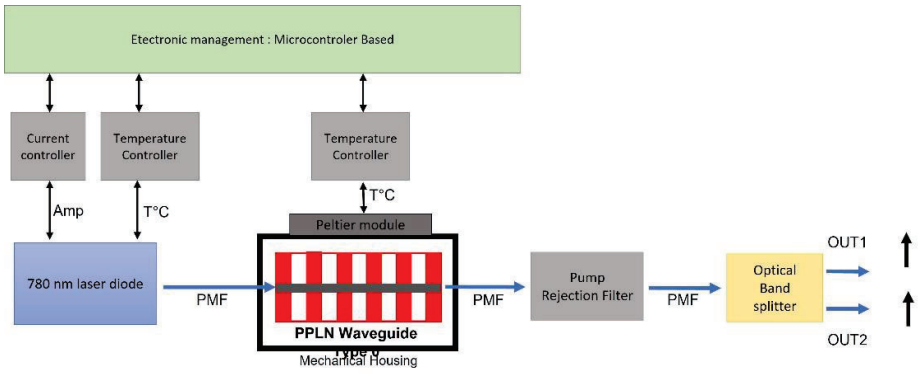


Figure 1. Schematic of the HP-EPS.

The HP-EPS is composed by a pump laser diode emitting at 780 nm, pigtailed Periodically Poled Lithium Niobate waveguide (PPLN-WG), a pump rejection filter and optical splitters. All optical components are off-the-shelf optical components pigtailed with Polarization Maintaining Fibers (PMF). The entangled photons are generated by high-efficiency type 0 Spontaneous Parametric Down Conversion (SPDC) based on the χ^2second-order nonlinearity in waveguides. The waveguide and poling are designed to allow phase matched SPDC for a laser pump around 780 nm generating the twin photons around 1560 nm. Neglecting the vacuum, we can describe the output state of a parametric down converted entangled source as:

$$|\psi\rangle = N \iint_{-\infty}^{+\infty} d\omega_i \, d\omega_s A(\omega_i, \omega_s)|\omega_i\rangle|\omega_s\rangle \tag{1}$$

N is a constant related to the probability of the spontaneous process, $A(\omega_i, \omega_s)$ represents the Joint Spectral Amplitude (JSA). The JSA is the product of the pump envelop function and the phase matching function. If the width of the pump bandwidth is narrow compared to the spectral bandwidths of the signal and the idler, then JSA can be approximated by:

$$A(\omega_i, \omega_s) = e^{\left[-\frac{(\omega_S+\omega_i+2\omega_0)^2}{2\Omega_p^2}\right]} e^{\left[-\frac{(\omega_S-\omega_i)^2}{2\Omega_F^2}\right]} \tag{2}$$

where (ω_s, ω_{si}) represent the frequencies of the signal and the idler, respectively, around the center frequency, ω_0. Ω_p is the bandwidth of the downconversion pump, whereas Ω_F is the phase-matching frequency. It is convenient to rewrite the state generated by a type 0 source in time domain:

$$|\psi\rangle = N \iint_{-\infty}^{+\infty} dt_i \, dt_s \tilde{A}(t_i, t_s)|t_i\rangle|t_s\rangle \tag{3}$$

$\tilde{A}(t_i, t_s)$ is the Joint Temporal Amplitude which is the Fourier transform of the JSA. $\tilde{A}(t_i, t_s)$ being non-vanishing only for $|t_s - t_i| < \tau$, a coincidence can be only observed in a time window (or time bin) of a duration of ~ τ. When the pumping signal is continuous, the "coincidence time" τ is mainly limited by the detection jitter (and not the source), which includes both the detectors jitters and the post processing electronic jitters. Hence, we can discretize the state considering the photons are equally likely to be found in any of the time bins of duration τ. The two-photons state is then:

$$|\psi\rangle = N \frac{1}{\sqrt{M}} \sum_{k=0}^{M-1} |k_i\rangle|k_s\rangle, \tag{4}$$

$$\text{with } |k\rangle_i|k\rangle_s = \int_{k\tau}^{(k+1)\tau} \int_{k\tau}^{(k+1)\tau} dt_i dt_s |t_i\rangle|t_s\rangle. \tag{5}$$

M represents the maximal number of temporal mode excited by the pump. The state is entangled in time and frequency (or energy), hence enables the use of protocol based on frequency bin or time bin entanglement which will be use to estimate the performances of the source in a QKD experiment. At the output of the PPLN-WG a rejection filter ensures pump signal isolation higher than 100 dB and a deterministic splitting of the entangled photons. All the active controls, i.e the current driver of the laser diode, the temperature controller of the laser diode and the temperature controller of the PPLN-WG are designed on a compact electronic card. A second card, mainly a microcontroller, is devoted to the management of the different set-points of the first electronic card. An accurate temperature control of the PPLN-WG using a Peltier module is designed to provide precise operating wavelength selection and very high stability. All the optical fiber components and electronics boards are packaged in an aluminum housing (see figure 2).

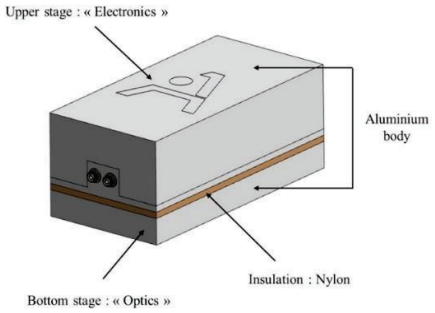


Figure 2: HP-EPS 3D housing.

The dimension of the housing is equivalent to 2U CubeSat format, i.e 10 cm x 10 cm x 20 cm and its total weight is lower than 2 kg, including the complete electronics. The thermal dissipation of the source is passive and doesn't require any additional thermal management module. The electrical power consummation is as low as 15 W. The figure 3 is a picture of the HP_EPS prototype.

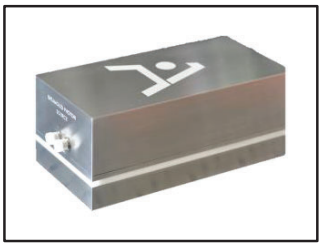


Figure 3. picture of the HP-EPS prototype.

A Graphical User Interface (see figure 4) allows the monitoring and the control of the current and the power intensity of the laser diode as well as the temperature of PPLN-WG.

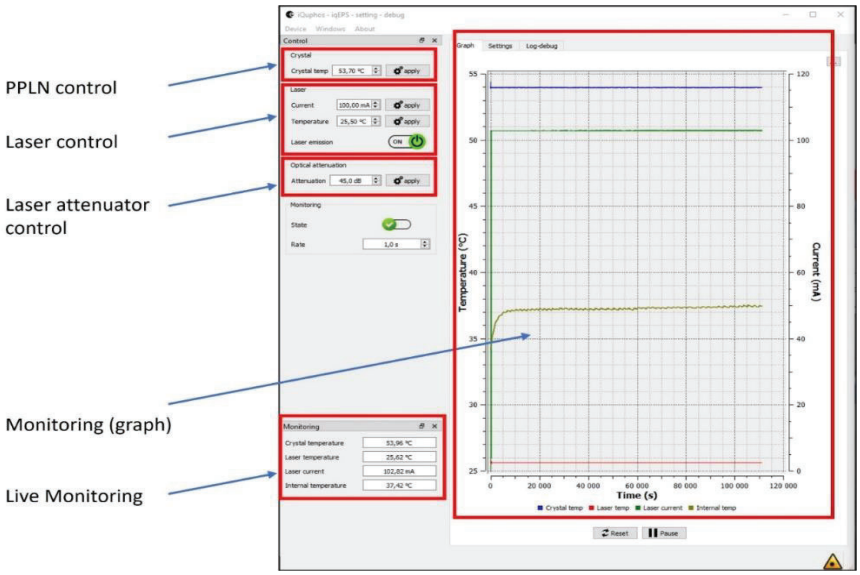


Figure 4. Graphical User Interface of the HP-EPS.

2.2 Implementing a BBM92 protocol using the HP-EPS

Quantum key distribution protocols follow standard steps enabling legitim users to share common secret keys. The main steps can be summarized as follow. The first step consists in transmitting the entangled photons to the legitim users which perform a local measurement of the photon state. Following the BBM92 protocol, the measurement is a projection of the state on a particular basis. Two unbiased bases are used. If the users use the same basis, then they share the same information (the bit value linked to the observed detection). If the basis used are different, then no information can be shared. The sifting, then consist in removing the measurements performed in different basis or the undetected signals. To implement these two first steps with our source, we have proposed a scheme based on those depicted in ref [Takesus]. The figure 5 represents the schematic of the set-up.

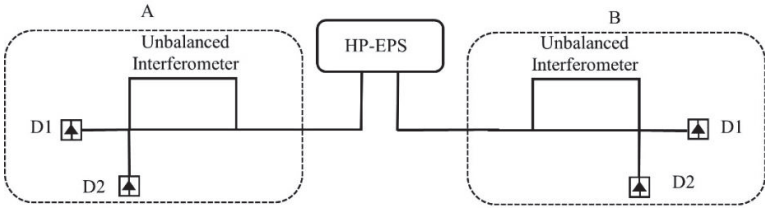


Figure 5 : BBM92 set-up

The basic set-up is composed by the HP-EPS source, two receivers composed by unbalanced interferometer and four single photon detectors. It is convenient to rewrite the output time entangled state as:

$$|\psi\rangle = N\frac{1}{\sqrt{M}}\sum_{k=0}^{M-1}|k\rangle_i|k\rangle_s = N\frac{1}{\sqrt{\frac{M}{2}}}\sum_{m=nk}^{m=\frac{M-1}{2}}\frac{1}{\sqrt{2}}\left(|m\rangle_i|m\rangle_s + |m+1\rangle_i|m+1\rangle_s\right) \quad (6)$$

In this representation, m corresponds to the time unbalanced (in number of bins of τ duration) of the interferometer arms. The term in the square root of the first factor is related to the average number of photons per bin and it is chosen to keep low the probability to detect more than single event per time bin. The summation over m is the number of temporal modes, equivalent in the pulse implementation of number of pump pulses that are coherent. Because the number of modes is high, we can consider that the probability of detect a given number of photons pairs per time bin follows a Poisonian law and depends on the average number of pairs per bin. For the sake of simplicity, the description of the protocol will be performed only using a single m equivalently to the description of the pulsed implementation proposed in [TAK06 Hiroki Takesue, Long-distance distribution of time-bin entanglement generated in a cooled fiber, Optics express, Vol. 14, No. 8, 3454-3460, 2006]. At each receiver, each photon is passed through an unbalanced interferometer, correlation can occur into three time slots t_1, $t_1 + m$, $t_1 + 2m$. In the 2nd time slot, there is an interference issued from the superposition of an initial state $|m\rangle_i|m\rangle_s$ following the long arm at each receiver, with an initial state $|m+1\rangle_i|m+1\rangle_s$ following the short arm at each receiver. Hence the interfering state is described by:

$$\frac{1}{4\sqrt{2}}\left(|m,D1\rangle_A|m,D1\rangle_B - |m,D2\rangle_A|m,D2\rangle_B + i|m,D1\rangle_A|m,D2\rangle_B + i|m,D2\rangle_A|m,D1\rangle_B - \left(1 + e^{i(\phi_A+\phi_B)}\right)\left\{|m+1,D1\rangle_A|m+1,D1\rangle_B + |m+1,D2\rangle_A|m+1,D2\rangle_B\right\} + i\left(e^{i(\phi_A+\phi_B)} - 1\right)\left\{|m+1,D1\rangle_A|m+1,D2\rangle_B - |m+1,D2\rangle_A|m+1,D1\rangle_B\right\} + e^{i(\phi_A+\phi_B)}\left\{|m+2,D1\rangle_A|m+2,D1\rangle_B - |m+2,D2\rangle_A|m+2,D2\rangle_B - i|m+2,D1\rangle_A|m+2,D2\rangle_B - i|m+2,D2\rangle_A|m+2,D1\rangle_B\right\}\right) \quad (7)$$

where $|m,D1\rangle_A$represents a state in which a photon is detected at time slot m and detector $D1$ on side A, and $\phi_{A/B}$represents the phase difference of the interferometer on side A/B. In Eq. (6), correlation occurring in the 1st (m slot) and the 3rd time slots (m slot) correspond to a detection in a time-basis and correlations occurring in the 2nd time slot (m+1)) correspond to a detection in energy-basis. Setting the sum $\phi_A + \phi_B$ of the phase differences, at 0 allows perfect correlation on detectors D1 or D2. Selection on the above basis is made spontaneously with no active selection procedure. When Alice and Bob detect photons, they record the detection time and which detector clicked. After the detection, they disclose their measurement basis through the classical channel but not the result. If they detect photons in the same basis, they can generate a key bit from the above correlations. Otherwise, they simply discard the events. By repeating this sequence, Alice and Bob can generate a sifted key which correspond to the second step of the generic protocol of QKD.
The last two steps correspond to the error correction and privacy amplification which allow the generation of the final secret key.

3. RESULTS

3.1 HP-EPS Spectrum

We have developed different test-benches to estimate the main performances of our source. The first characterization concerns the measure of the optical spectrum of the source. The figure 6 represents the test bench devoted to the spectrum bandwidth measurement.

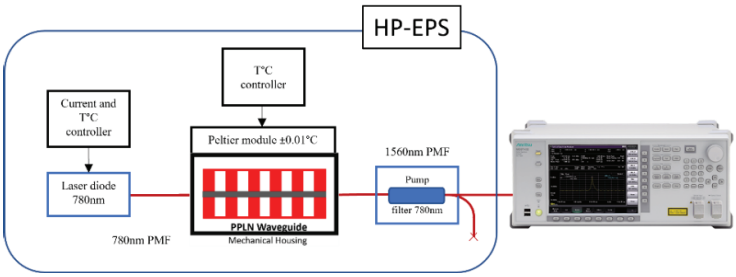


Figure 6: EPS spectrum measurement set-up before photon splitting.

This measurement has been performed preliminary to the integration of the Optical Band Splitter allowing the deterministic splitting of the entangled photons. Notice that the brightness of the PPLN-WG is high enough to realize a classical measurement of the spontaneous parametric down conversion (SPDC) spectrum of the source by using a standard optical spectrum analyser (OSA) and a laser pump power of 10 mW and at 780.5 nm. The figure 7 shows the spontaneous spectrum of the source.

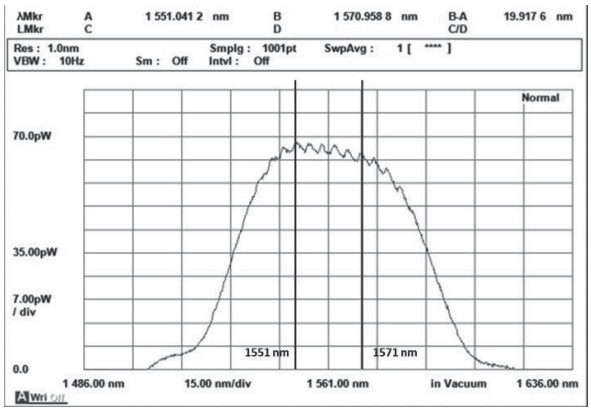


Figure 7*:* SPDC spectrum before wavelength splitting (10 mW pump power).

The crystal temperature has been chosen such as the HP-EPS operates at the degeneracy, where the entangled photons are indistinguishables. The spontaneous parametric down conversion spectrum features a 3dB bandwidth higher than 60 nm centred at 1561 nm.
A second measurement is performed including a combination of standard telecommunication filters, centred respectively at 1571nm and 1551 nm. To observe the spectrum, the two outputs of the filters are combined and the signal is injected in the OSA. The figure 8 shows the spontaneous spectrum at the ouput of the CWDM filter.

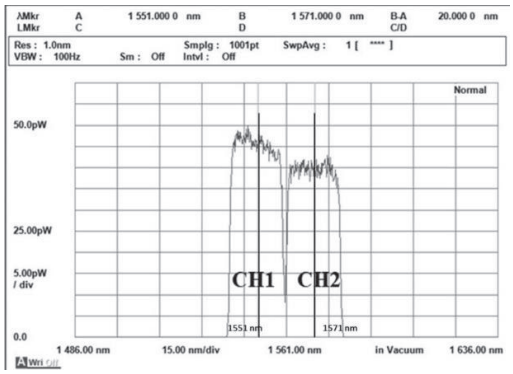


Figure 8*:* SPDC spectrum after wavelength splitting (10 mW pump power).

As expected, we observe two separated spectra, respectively centered at 1551 nm and 1571 nm, but with a slight asymmetry in term in amplitude. This small difference is due to the losses asymmetries of the filters in a cascade configuration.

3.2 HP-EPS Brightness and Coincidence-to- Accidental Ratio (CAR)

The second test bench implemented is shown in figure 9. The bench is composed by two variable optical attenuators, two very-low noise single photon detectors and a time correlator (time tagger electronics device) allowing the detection of

quantum correlations. The single photon detectors provide detection quantum efficiencies of around 80% at a dark count rate of 30 counts per second. The time jitter of the detectors is below 15 ps.

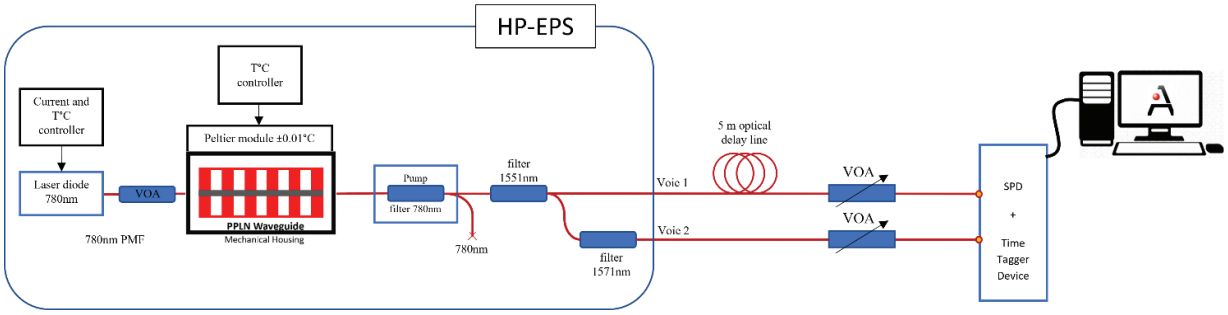


Figure 9: HP-EPS Brightness Test bench.

This test bench is devoted to the measure of two important specifications of the HP-EPS: the brightness and the coincidence-to-Accidental Ration (CAR). The brightness indicates the number of photon pairs per second generated by the source for a given laser pump power and a given spectral bandwidth. The second parameter is the ratio between the signal and the noise emitted by the source. The higher the CAR the better the quality of the emitted signal. Both parameters are estimated relatively by varying the laser pump power. The figure 10.a and 10.b respectively show the brightness and the CAR as a function of the pump power.

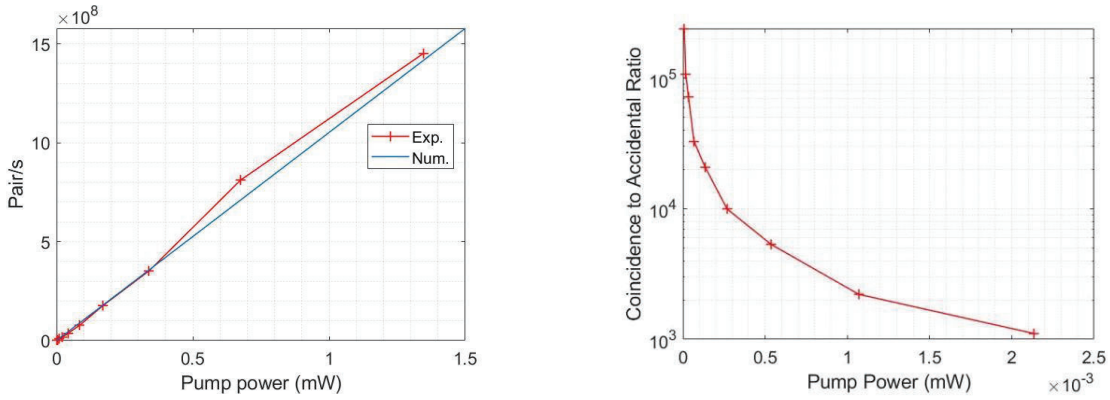


Figure 10: a) Brightness as a function of the laser pump power, b) CAR as a function of the laser pump power.

The HP-EPS brightness has been measured to be as high as 1 Gpair/s at 1 mW laser pump power.

This result drastically reduces the constraints on the laser source power requirements for a future implementation in a satellite. Moreover, using low laser pump power goes in the direction of energy saving and size reduction, two important factors for space integration.

3.3 QKD test bench

The HP-EPS source is tested in a QKD proof-of-concept experiment to estimate the secure key rate and the distance which can be achieve using this source. As explain in the previous section, the protocol used is based on time entanglement. The experimental set-up is shown in the figure 11.

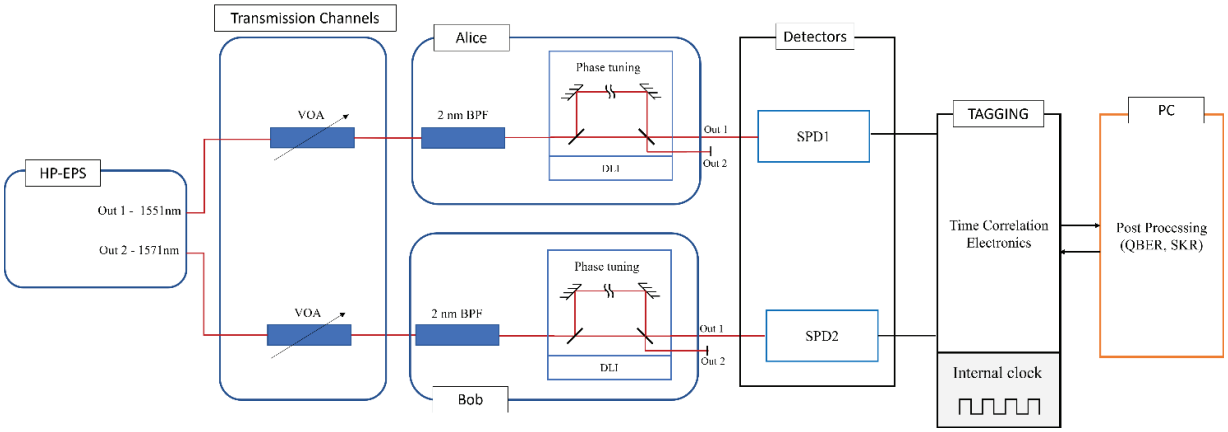


Figure 11: QKD test bench.

In this set-up, two tunable voltage attenuators are used to simulate the losses of a transmission channel. Losses up to 70 dB can be introduced to estimate the variation of the secure key rate SKR as a function of the attenuation. Two GHz free spectral range (FSR) delay line interferometers (DLI) are devoted to the state manipulation (Alice and Bob). The relative delay can be tuned by using temperature control. Notice that ultra-narrow bandpass filters are placed front of the input of the delay line interferometers to ensure an intrinsic low quantum bit error (QBER). Two single photon detectors (SPD) connected to one of the outputs generate an electrical signal corresponding to the detection of a photon. A time tagger (TAGGING) collects the signal and measures the arrival time of the photons. All the post processing (QBER and SKR estimation, set points control, etc…) is performed using a proprietary software. The figure 12 shows a picture of the experimental set-up.

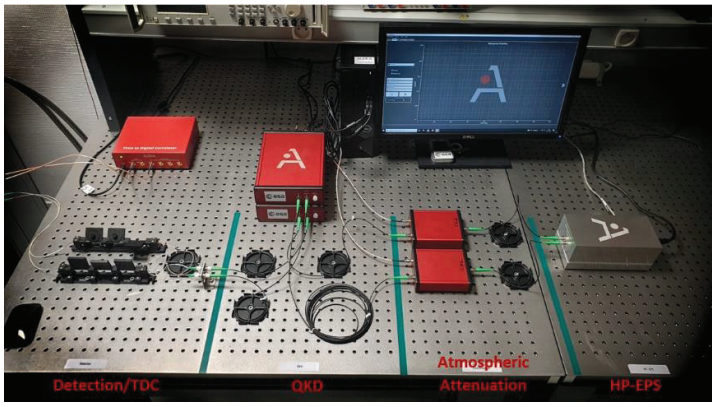


Figure 12: Experimental set-up.

3.4 Visibility

The visibility can be interpreted as an estimator of the minimal intrinsic QBER that can be achieved with the test bench. It is assessed for the whole transmission systems. It corresponds to an interference measurement. In our set-up, 2 x 2 nm bandpass filters are implemented to reduce the external noise. In addition the pump power is selected to ensure that the CAR is high enough to allow the measurement of the visibility. The pump power is then set at 30 nW. Pratically, the visibility is measured by computing the extinction ratio in the energy-basis (central peak) by using the following formula

$$Visibility\ (\%) = \frac{Counts_{max} - Counts_{min}}{Counts_{max} + Counts_{min}} . 100 \quad (8)$$

The “Counts” corresponds to the number of photons included in the central peak. Tuning the relative phase between 0 and π of the DLIs arms enables the counts variation of the central peak between a minimum and maximum (see figure 13).

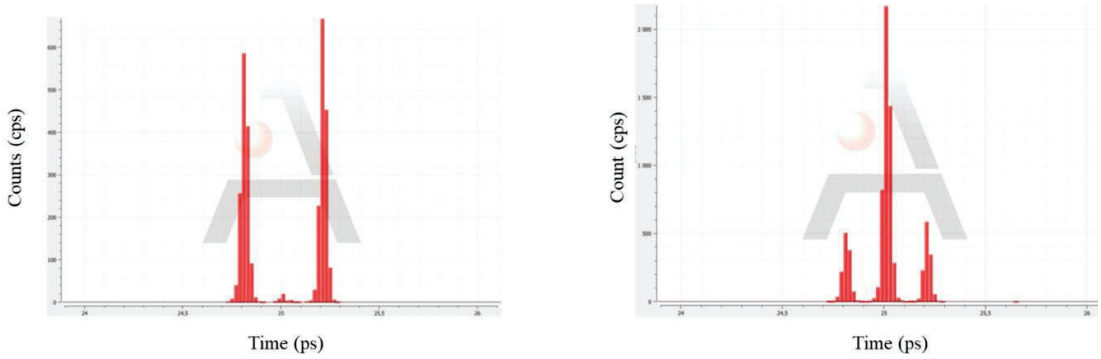


Figure 13: Coincidence measurement with the DLIs as a function of the phase difference, Left: Maximum extinction of the central peak, Right: Minimum extinction of the central peak.

The different output configuration (out1-out1, out2-out2, out1-out2 and out2-out1) of the delay line interferometers are tested to estimate the worst visibility achieved. In this case for 3 min of acquisition and 30 nW of pump power, we observe a maximal count in the central peak of 4915 counts and a minimal counts of 25 counts. The minimal visibility thus achieve with our system is then 99%.

3.5 SKR and QBER estimates

The SKR and the QBER are estimated using The BBM92 protocol described in the previous section. The collected data are post-processed automatically thanks to a dedicated software we have developed which provides the value of the QBER and of the SKR.

Because we intend to demonstrate reasonable key rate generation over high attenuation, we first optimize the number pairs by detection windows generates by the source. The detection windows is 100 ps and the selected attenuation such as the global attenuation is 64 dB. This attenuation includes the intrinsic attenuation of the optical components and the efficiency of the very low noise single photon detectors. The figure 14 shows the SKR and QBER variation as the function on average number of pairs per detection windows.

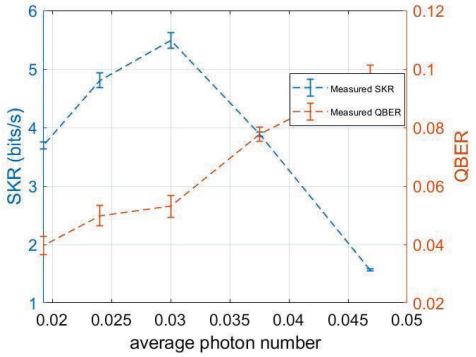


figure 14: SKR & QBER versus average photon number per detection window at 64dB of attenuation.

The experimental measurements show that the maximum SKR is reached for an average photon number per detection window of 0.03 and a QBER of approximately 6%. This average photon number corresponds to a pumping power of 340 μW, i.e., 350 Mpairs/sec. Under theses conditions, we have performed tests that simulate the atmospheric losses in satellite to ground transmission. For the QBER and SKR measurements campaign, we realized 10 measurements to have a representative statistic and compute the error bars. The figure 15.a and 15.b show respectively the SKR and the QBER variation as the function of attenuation. Concerning the SKR, 3 curves has been computed i) Raw corresponding to the raw Signal detected on the receiver side before the post-processing, ii) Effective SKR without authentication, corresponding to the SKR after the privacy amplification process but without authentication processing, and iii) Effective SKR with authentication corresponding to the SKR after the privacy amplification process but with authentication processing.

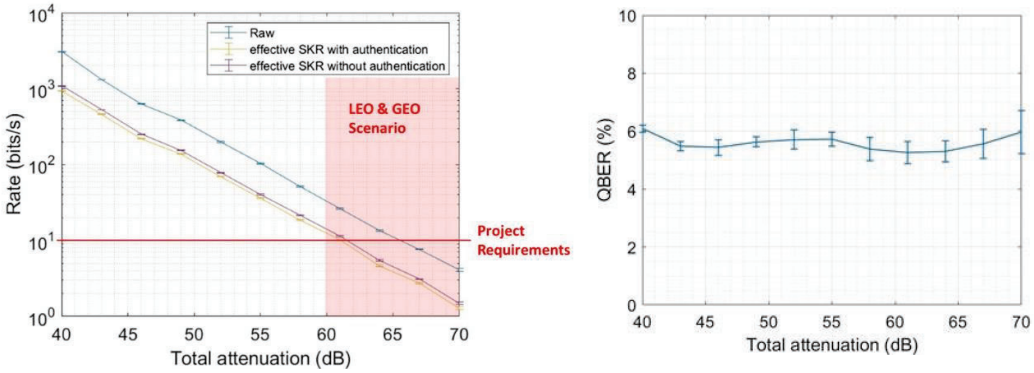


figure 15: a) SKR variation as the function of attenuation, b) QBER variation as the function of attenuation.

Notice that the acquisition time progressively increases with the attenuation from 1 min to 16 due to the low photon flow. The initial 1 min acquisition time was selected to correspond approximately to a satellite transit in a LEO scenario, and the increase in time was chosen to obtain the minimum number of raw bits required to build a Secret Key. Indeed the SKR cannot be estimated on flight but only after a minimum acquisition time. The post treatment algorithm uses the raw bits to identify and discard the errors and build the key. Thus, on the total number of events detected, only few of them will be used as a Secret Key. Most of the signal is in fact lost (~80%) in the process. In this project, we considered minimum raw keys lengths of 5 000 bits to run the algorithm. The Key Rate is then computed using the ratio of the Key (Raw or Secret) Length with the acquisition time. This work confirms that it is possible to reach a SKR = 10 bits/s at 60dB (LEO scenario) attenuation.

Acknowledgement

The authors thanks ESA for the funding of the IQUPHOS (Improved QUantum PHoton Source) project (ESA Contract 4000133673/20/NL/MM) in the frame of the SAGA project

4. CONCLUSION

We have designed a high-performance entangled photon source dedicated to satellite communication based on off-the-shelve components. The brightness of the source has been measured to be higher than 1 Gpairs/sec at a mW cw (continuous wave) pumping power and the coincident-to-accidental ratio (CAR) obtained exceeds 10,000 for a pair rate generation of 250 kpairs/s.

Exploiting the time bin entanglement of the HP-EPS, we have implemented a fiber-based QKD set-up using standard fibered unbalanced compact Mach-Zehnder interferometer with a GHz Free Spectral Range. The atmospheric free-space transmission losses have been simulated using voltage-controlled attenuators. SKR of the order of 300 bits/sec, 10 bits/sec and 5 bits/sec has been measured respectively for a 45 dB, 60 dB (LEO) and 65 dB (GEO) transmission loss budget (both downlinks combined).

In addition, a first study of the spatialization (not described in the text) has shown no major difficulty for satellite integration making the HP-EPS a valuable and serious candidate for the satellite-based QKD missions.

REFERENCES

[1] Guo, Q. et al., "SDN-Based End-to-End Fragment-Aware Routing for Elastic Data Flows in LEO Satellite-Terrestrial Network," IEEE Access, 7, 396-410 (2019).
[2] Vernam,G. S., "Cypher Printing Telegraph System", J. Am. Inst. Elec. Eng., 55, 109-115 (1926).
[3] Shannon,C. E., "Communication Theory of Secrecy Systems", Bell Syst. Tech. J., 28, 656- 715 (1949).
[4] Diffie,W. Hellman, M. E., "New Directions in Cryptography", IEEE Trans. on Inf. Theory, 22 (6), 644–654 (1976).
[5] Shor, P. W. "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer", SIAM Rev., 41(2), 303-332 (1999).
[6] Pirandola, S. et al., "Advances in Quantum Cryptography",Adv. in Opt. and Photonics, 12 (4), 1012-1236 (2020).
[7] De Parny, L. F. et al, "Satellite-based Quantum Information Networks: Use cases, Architecture, and Roadmap," arXiv:quantph \2202.01817 (2022).
[8] Singh, M. K., Jiang, L., Awschalom, D. D., Guha, S. "Key Device and Materials Specifications for a Repeater Enabled Quantum Internet," IEEE Trans. Quant. Eng., 2, 1-9 (2021).
[9] Acin,A., Brunner, N., Gisin, N., Massar, S., Pironio, S., Scarani, V., "Device-Independent Security of Quantum Cryptography against Collective Attacks", Phys. Rev. Lett. 98, 230501 (2007).
[10] Chao-Yang Lu, Yuan Cao, Cheng-Zhi Peng, and Jian-Wei Pan, "Micius quantum experiments in space", arXiv:quantph\2208.10236 (2022).
[11] Liao, S.-K. and al., "Long-distance free-space quantum key distribution in daylight towards inter-satellite communication ", Nat. Phot. 11, 509-514 (2017).
[12] Takesue, H., " Long-distance distribution of time-bin entanglement generated in a cooled fiber ", Opt. Exp. 14(8), 3453-3460 (2006).