

Università degli Studi di Padova

Padua Research Archive - Institutional Repository

Stable, low-error, and calibration-free polarization encoder for free-space quantum communication

Original Citation:

Availability:

This version is available at: 11577/3349084 since: 2021-01-21T15:55:46Z

Publisher:

Published version:

DOI: 10.1364/OL.396412

Terms of use:

Open Access

This article is made available under terms and conditions applicable to Open Access Guidelines, as described at <http://www.unipd.it/download/file/fid/55401> (Italian only)

(Article begins on next page)

Stable, low-error and calibration-free polarization encoder for free-space quantum communication

Marco Avesani,^{1,*} Costantino Agnesi,^{1,*} Andrea Stanco,¹ Giuseppe Vallone,^{1,2,3} and Paolo Villoresi^{1,3}

¹*Dipartimento di Ingegneria dell'Informazione, Università degli Studi di Padova, Via Gradenigo 6B - 35131 Padova, Italia*

²*Dipartimento di Fisica e Astronomia, Università degli Studi di Padova, via Marzolo 8, 35131 Padova, Italy*

³*Istituto di Fotonica e Nanotecnologie - CNR, Via Trasea 7 - 35131 Padova, Italia*

Polarization-encoded free-space Quantum Communication requires a quantum state source featuring fast polarization modulation, long-term stability and a low intrinsic error rate. Here we present a source based on a Sagnac interferometer and composed of polarization maintaining fibers, a fiber polarization beam splitter and an electro-optic phase modulator. The system generates predetermined polarization states with a fixed reference frame in free-space that does not require calibration neither at the transmitter nor at the receiver. In this way we achieve long-term stability and low error rates. A proof-of-concept experiment is also reported, demonstrating a Quantum Bit Error Rate lower than 0.2% for several hours without any active recalibration of the devices.

I. INTRODUCTION

Quantum key distribution (QKD) allows two spatially distant parties to generate, through the exchange of qubits encoded into single photons, a secure and private cryptographic key. The security and privacy of the keys generated by QKD is guaranteed by the principles of quantum mechanics.

Practical implementations of QKD require rapid modulation of the degrees of freedom of the photons used to encode the qubits. One of the most exploited encoding, in particular for free-space application, is represented by polarization. A quantum source featuring long-term stability and a low intrinsic Quantum Bit Error rate (QBER) is crucial for free-space [1, 2], and in particular satellite [3, 4] QKD application. Nonetheless, most of the methods used so far to modulate the photon's polarization were characterized by a low temporal stability and a limited contrast in the modulation due to source imperfections. Moreover, some implementation could lead to side-channel attacks, undermining the security of the QKD protocol.

The simplest solution is the use of different lasers, one for each state required by the QKD protocol. This approach has been used in several works [5–7] and in particular in the recent satellite-to-ground demonstration [3]. This solution could be demanding from the economic and energetic point of view as it requires four independent lasers, temperature controllers and current generators. More importantly, if the lasers are not properly calibrated and controlled, the generated states can be distinguished and the implementation could be vulnerable to attacks such as those described recently in [8].

In order to prevent the above attacks a single laser source with an active polarization modulator is typically used. A common technique is based on the use of

birefringent phase modulators in an in-line configuration [9, 10]. In this scheme, the photons are injected in the phase modulator (typically based on LiNbO₃ crystals) with a polarization state that is diagonal with respect to the optical axis of the modulator's crystal. By applying a V_{RF} voltage, the ordinary and extraordinary refractive indices of the crystal vary independently, allowing to control the relative phase between the $|H\rangle$ and $|V\rangle$ polarization.

This solution presents several disadvantages. First of all, the polarization modulation is highly sensible to temperature and bias voltage drift and requires active stabilization. A second issue is related to the polarization mode dispersion (PMD) induced by the birefringence, which reduces the degree of polarization for short pulses, decreasing the modulation performance. Thirdly, high voltages are required to modules to induce the required polarization modulation. Lastly, modulators able to support both polarization are not always commercially available, especially outside the C band.

To avoid temperature and bias voltage stabilization, it is possible to use the birefringent modulator in a two-pass scheme using a Faraday mirror [11]. However, this scheme still requires non-standard components and high voltages to induce the necessary modulation. Moreover, PMD is also not completely compensated, allowing only modest modulation performances [11].

To solve the problems of the polarization modulators mentioned above, we have recently proposed the POGNAC [12] and exploited it in a complete QKD experiment featuring the lowest intrinsic QBER reported to date [13]. The POGNAC uses an optical circulator and a single mode fiber (SMF) to guide the photons into a fiber Polarization Beam Splitter (PBS) that represents the beginning of a Sagnac interferometer that includes a standard phase modulator (ϕ -mod). A polarization controller (PC) is used to obtain at the input of the fiber PBS a balanced overlap of the horizontal $|H\rangle$ and vertical $|V\rangle$ polarization modes. The photons

* These authors contributed equally to this work.

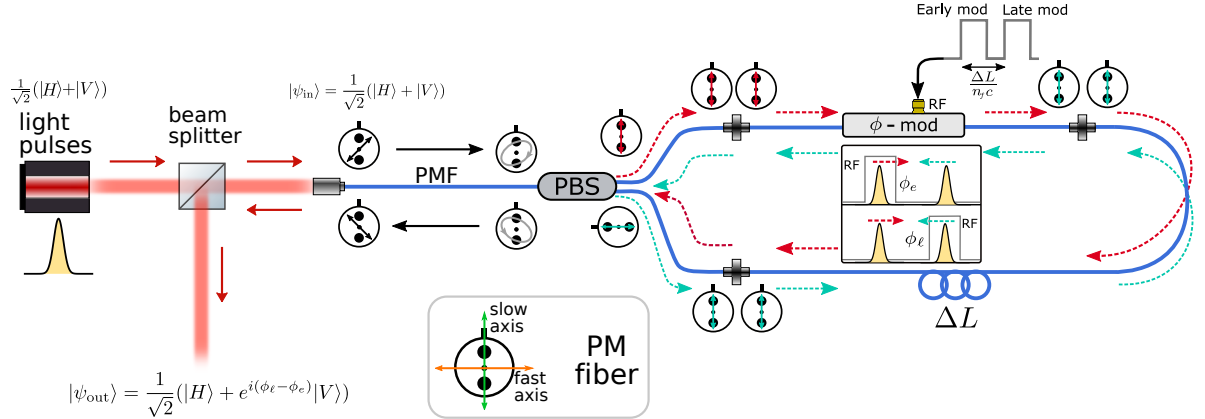


Figure 1. Scheme of the proposed polarization modulator. The free-space beam-splitter is used to separate incoming from outgoing light. A Sagnac interferometer including a fiber polarizing beam splitter, a phase modulator and polarization Maintaining fibers (indicated in blue) is used to modulate the polarization state. We always consider a left-handed reference frame whose z axis is directed toward the photon's propagation direction.

exit back from the fiber PBS with a polarization state given by $|\psi\rangle = \frac{1}{\sqrt{2}}(|H\rangle + e^{i\phi}|V\rangle)$, with ϕ determined by the ϕ -mod, and then are directed toward the exit port of the circulator. Some similar schemes require the introduction of a Faraday rotator in the Sagnac loop [14, 15]. The Sagnac loop geometry has also been exploited for polarization-independent phase modulation [16] as well as intensity modulation [17].

The Sagnac-based polarization modulators described above have some limitations related to the presence of the single-mode fiber for optical input and output. Indeed, the fiber requires that the device is manually calibrated via the PC to obtain a balanced overlap of the horizontal and vertical polarization modes at the input of the PBS. This is a disadvantage in the development of autonomous systems. Moreover, temperature drifts require (slow) recalibration of the device. Moreover, at the exit of the Sagnac interferometer the single mode fiber that guides the light from the PBS to the circulator introduces a unitary transformation of the polarization state that is not known a priori. This complicates the implementation of QKD protocols in free-space (and in particular in satellite-to-ground QKD) as it introduces a further calibration phase at the receiver. Furthermore, temperature variations and mechanical stress of the fiber slowly change the corresponding unitary transformation.

The issue related to the polarization calibration at the input has been solved in [18] where a polarization maintaining fiber (PMF) with optical axis oriented at 45° is used at the input of the Sagnac loop. However, the use of SMF at the output still requires a calibration phase at the receiver since the emitted state are generated up to an unknown unitary transformation.

In this manuscript we present iPOGNAC, a polarization encoder that solves all the previously mentioned issues with a simple scheme. The iPOGNAC, generates predetermined polarization states with a fixed reference frame in free-space that does not require calibration neither at the transmitter nor at the receiver, featuring a long-term stability and a low intrinsic QBER. We think that this polarization encoder provides a simple and effective solution for free-space quantum communication.

II. PROPOSED SCHEME

The scheme of the iPOGNAC can be seen in Fig. 1. Collimated laser pulses propagating in free-space with diagonal polarization $|D\rangle = (|H\rangle + |V\rangle)/\sqrt{2}$ (considering a left-handed reference frame whose z axis is directed toward the photon's propagation direction) enter the setup. This polarization state can be generated in several ways, for example by using a polarizer, by using a Half Wave Plate (HWP), or by physically rotating the collimator if the light is delivered by a laser emitting light coupled to the slow (or fast) axis of a PMF. It is important to note that any state that is a balanced superposition of $|H\rangle$ and $|V\rangle$, i.e., laying in the equator of the Bloch sphere, is equally suitable.

The light pulses then impinge a free-space Beam Splitter (BS). The reflected light is discarded, while the transmitted pulses encounter a collimating lens that couples the light into a PMF with slow axis aligned to the vertical direction. Since PMFs are designed to be birefringent, the polarization modes $|H\rangle$ and $|V\rangle$ experience different indexes of refraction and the polarization state at the end of the PMF is changed to an

elliptical polarization $|\psi_1\rangle = (|H\rangle + e^{i\delta}|V\rangle)/\sqrt{2}$. The phase δ depends on the length of the fibre, the difference between the fast and slow indexes of refraction of the PMF, temperature and mechanical strain applied to the PMF. Interestingly enough, for laser pulses with short coherence times the phase δ can be large enough to effectively depolarize the light.

After propagating in the PMF, the light encounters a fiber-based Polarization Beam Splitter (PBS). From this point the setup is identical to the original POGNAC [12], which allows us to inherit its high intrinsic stability and the capability of modulating polarization exploiting a ϕ -mod. The light is split into orthogonal linear polarizations by the fiber PBS. It is important to note that each of the polarized beams exiting from the PBS is aligned to the slow axis of a PM fiber. This effectively maps the polarization degree of freedom onto the optical path of the photons, with the polarized light traveling along only the slow axis of the PM fibers of both PBS exit ports. This is the standard behavior of fiber-based polarization beam combiners and splitters.

This PBS marks the beginning of the Sagnac interferometer, fully implemented with PM fibers. The vertically polarized component travels in the clockwise direction (CW) while the horizontally polarized component travels in the counter-clockwise direction (CCW). In the CW direction a ϕ -mod is first encountered introducing an "Early" phase ϕ_e to the CW propagating light pulse. A PMF delay line is then encountered, after which the CW light pulse impinges once again on the PBS. The CW propagating light exits the Sagnac interferometer with horizontal polarization. In the reverse direction, the CCW first encounters the PMF delay line such that it arrives on the modulator later than the CW pulse. Then, the ϕ -mod introduces a "Late" phase ϕ_ℓ to the CCW propagating light pulse. Lastly, the CCW light pulse impinges once again on the PBS, exiting the Sagnac interferometer with vertical polarization.

Since inside the PMF Sagnac interferometer, both the CW and CCW travel along the fast axis of the PM fiber, no polarization mode dispersion is observed and a single polarization mode propagates in the ϕ -mod.

The polarization state emerging from the PBS is thus given by

$$|\psi_2^{\phi_e, \phi_\ell}\rangle = \frac{1}{\sqrt{2}} \left(|H\rangle - e^{i(\phi_\ell - \phi_e - \delta)} |V\rangle \right). \quad (1)$$

It is important to note that the light that entered the Sagnac loop with $|H\rangle$ polarization emerge with $|V\rangle$ polarization, and vice versa. This has the effect of changing the sign of the phase δ and introducing an extra π shift. Indeed, by using a left-handed reference frame whose z axis that is always directed toward the photon's propagation direction, the PBS and the Sagnac loop without modulation implement an $i\sigma_y$ operation,

namely $|H\rangle \rightarrow -|V\rangle$ and $|V\rangle \rightarrow |H\rangle$.

After exiting the fiber PBS that closes the Sagnac loop, the light propagates backwards through the PMF, which adds an additional phase δ between the propagating polarization modes. Interestingly enough this additional δ phase compensates the phase accumulated by the forward propagation in the PMF. It is worth noting that such phase δ is compensated also for laser pulses with short coherence times, even when the delay between the two modes is larger than the coherence length. This can be easily understood since the $|H\rangle$ ($|V\rangle$) polarized light that first traveled along the fast (slow) axis, emerges as $|V\rangle$ ($|H\rangle$) after the Sagnac loop and travels back along the slow (fast) axis.

The collimating lens then emits the light back into free space. The light then impinges once more the free-space BS and the transmitted light is discarded. On the other hand, the exit on the reflection port of the free-space BS represents the output of the iPOGNAC polarization modulator. Due to an extra π shift due to the reflection, the polarization state of light at the output is described by

$$|\psi_{\text{out}}^{\phi_e, \phi_\ell}\rangle = \frac{1}{\sqrt{2}} \left(|H\rangle + e^{i(\phi_\ell - \phi_e)} |V\rangle \right). \quad (2)$$

Since inside the Sagnac loop the CW pulse anticipates the arrival of the CCW pulse on the ϕ -mod by a factor $\frac{\Delta L}{n_f c}$ (where n_f is the index of refraction of the slow axis of the PMF and c the velocity of light), by carefully timing the applied voltage on the ϕ -mod, the polarization state $|\psi_{\text{out}}\rangle$ can be modulated.

Indeed, by changing the phases ϕ_e and ϕ_ℓ any state lying on the equator of the Bloch sphere can be generated. For QKD application, a single voltage level $V_{\pi/2}$ (corresponding to the voltage required to introduce a phase shift of $\pi/2$ in the ϕ -mod) and different timing are sufficient to generate the states $|D\rangle$, $|L\rangle = \frac{1}{\sqrt{2}}(|H\rangle + i|V\rangle)$ and $|R\rangle = \frac{1}{\sqrt{2}}(|H\rangle - i|V\rangle)$, allowing the implementation of the 3-state version of the BB84 protocol [10]. In particular, if no voltage (or equal voltage) is applied to the CW and CCW pulses, the polarization state remains unchanged, i.e. $|\psi_{\text{out}}^{0,0}\rangle = |D\rangle$. If $V_{\pi/2}$ voltage is applied to the CW pulse and no voltage is applied to the CCW pulse, the output state becomes $|\psi_{\text{out}}^{\frac{\pi}{2},0}\rangle = |L\rangle$. Alternatively, if no voltage is applied to the CW pulse and $V_{\pi/2}$ voltage is applied to the CCW pulse, the output state becomes $|\psi_{\text{out}}^{0,\frac{\pi}{2}}\rangle = |R\rangle$. We note that, by using a generic input state of the form $\alpha|H\rangle + \beta|V\rangle$, the output states $\beta|H\rangle + \alpha e^{i(\phi_\ell - \phi_e)}|V\rangle$ can be generated.

It is important to stress that the proposed scheme requires only standard components, reducing construction costs and allowing the scheme to be used at different wavelengths, such as 800nm, 1064nm or 1550nm.

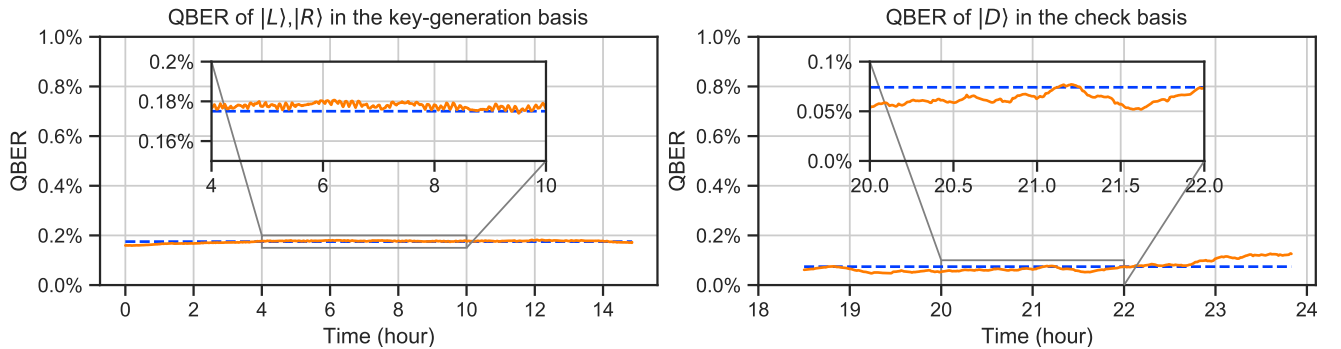


Figure 2. Experimental QBER as a function of time measured from $t_0=18:30$ of 12 Sept. 2019. The left panel shows the QBER in key-generation basis, where an average value of $Q_{\mathcal{K}} = 0.175\% \pm 0.005\%$ was obtained. The right panel shows the QBER in check basis, where an average value of $Q_{\mathcal{C}} = 0.07\% \pm 0.02\%$ was obtained. The time between 14.5 and 18.5 hour was needed for the helium cycle of the SNSPD detectors. During this time, no operation on the source was performed.

III. PROOF-OF-CONCEPT EXPERIMENT

We performed a proof-of-concept experiment of the iPOGNAC. As a light source we used a gain-switched distributed feedback (DFB) laser which emitted a 50 MHz stream of phase-randomized pulses with 270 ps full-width-at-half-maximum duration at 1550 nm. To generate the the $|D\rangle$ polarization state a Glan-Thompson polarizer was used. The iPOGNAC was assembled using standard Commercial Off-The-Shelf (COTS) components exclusively. The electronic signals used to drive the iPOGNAC were generated by a Field Programmable Gate Array (FPGA) (Zynq-7020) mounted on a dedicated board (ZedBoard by Avnet). The FPGA was capable of triggering the DFB laser and to produce the "Early" and "Late" modulation pulses with specific time delays in order to address the ϕ_e and ϕ_ℓ phases (all the signals were properly amplified by RF amplifiers). The output of the iPOGNAC was then attenuated to the single-photon level using attenuators and directed to a free-space polarization analyzer comprised of a Quarter Wave Plate (QWP), a HWP and a PBS. The output ports of the polarization analyzer were then coupled to single-mode fibers which directed the light to two superconductive nanowire single-photon detectors (SNSPD) with detection efficiencies around 85%.

In order to test the long-term stability of our system, a fixed sequence composed by the three polarization states $\{|L\rangle, |R\rangle, |D\rangle\}$ is prepared by the iPOGNAC. We note that those three states are sufficient to realize the three-state BB84 protocol presented in [19]. The states are then measured by a free-space measurement station projecting the states in the key-generation basis $\mathcal{K} = \{|L\rangle, |R\rangle\}$ or in the check basis $\mathcal{C} = \{|D\rangle, |A\rangle\}$ with $|A\rangle = 1/\sqrt{2}(|H\rangle - |V\rangle)$. The selection of the basis is performed by acting on the QWP placed before the PBS of the measurement station. The timestamps of the

photo-detection events are digitized by time-to-digital converted and then streamed to the PC for the post-processing analysis. We performed two acquisitions: the first one, lasting almost 15 hours and acquired during the night, measures the QBER in the key-generation basis $\{|L\rangle, |R\rangle\}$ and is presented in the left panel of Fig 2. In this configuration we measured an average QBER for the $|L\rangle, |R\rangle$ states $Q_{\mathcal{K}}$ of $0.175\% \pm 0.07\%$.

After that, the helium cycle of the SNSPD was performed in order to keep the detectors at the operating temperature. The cycle lasted 4 hours and during this time no operation on the source was performed. Then, by acting on the QWP at the measurement station, we aligned the measurement station along the check-basis \mathcal{C} and we performed another acquisition lasting 5 hours and half, during the day. The data are presented in the right panel of Fig 2. We measured an average QBER for the $|D\rangle$ state of $Q_{\mathcal{C}} = 0.07\% \pm 0.02\%$.

In both cases, the data shown in Fig. 2 confirm the excellent performances of the iPOGNAC in terms of QBER and long-term stability, making it optimal solution as polarization encoder for classical and quantum free-space communications.

The small and slow residual drifts visible in Fig 2 can be attributed to the temperature variations of the measurement apparatus. In fact, the lab was not temperature stabilized and experiences variation of several degrees during the day. These variations can induce small polarization rotations to the photons travelling in the single mode fibers connected to the SNSPD. Since the efficiency of the SNSPD is polarization-dependent, these rotations can induce small drifts in the measured QBER.

IV. CONCLUSIONS

In conclusion, we proposed and tested a novel polarization encoder, called iPOGNAC, characterized by a low intrinsic error and high temporal stability. Moreover, the encoder can generate predetermined polarization states with a fixed reference frame in free-space.

We experimentally implemented the proposed protocol, using only COTS components, obtaining a low intrinsic QBER $< 0.2\%$ and long-term stability measured over 24 hours. Indeed, these performances are well-suited for practical QKD systems.

In particular, the iPOGNAC is a promising solution for quantum communication with satellites or moving objects for at least two reasons. Firstly, its ability of generating polarization states that are fixed with respect to the transmitter's reference frame eliminates the need of calibration between the transmitter and the receiver. Secondly, given its free-space output, it can be easily interfaced with a telescope. Moreover, the proposed source, further miniaturized with micro-optic

technology, can be also exploited in fiber-based QKD with the requirement of a receiver calibration. Finally, the iPOGNAC could be also used at the receiver side in a QKD application, to rapidly switch between measurement basis, or for classical communication exploiting polarization modulation [20].

The device here presented is object of the Italian Patent Application No. 102019000019373 filed on 21.10.2019 [21].

Note added - After the completion of the present manuscript we became aware of a similar proposal presented in [22].

ACKNOWLEDGMENTS

Part of this work was supported by MIUR (Italian Minister for Education) under the initiative "Departments of Excellence" (Law 232/2016)

-
- [1] M. Avesani, L. Calderaro, M. Schiavon, A. Stanco, C. Agnesi, A. Santamato, M. Zahidy, A. Scriminich, G. Foletto, G. Contestabile, M. Chiesa, D. Rotta, M. Artiglia, A. Montanaro, M. Romagnoli, V. Soriano, F. Vedovato, G. Vallone, and P. Villoresi, "Full daylight quantum-key-distribution at 1550 nm enabled by integrated silicon photonics," (2019), [arXiv:1907.10039 \[quant-ph\]](https://arxiv.org/abs/1907.10039).
- [2] S.-K. Liao, H.-L. Yong, C. Liu, G.-L. Shentu, D.-D. Li, J. Lin, H. Dai, S.-Q. Zhao, B. Li, J.-Y. Guan, W. Chen, Y.-H. Gong, Y. Li, Z.-H. Lin, G.-S. Pan, J. S. Pelc, M. M. Fejer, W.-Z. Zhang, W.-Y. Liu, J. Yin, J.-G. Ren, X.-B. Wang, Q. Zhang, C.-Z. Peng, and J.-W. Pan, "Long-distance free-space quantum key distribution in daylight towards inter-satellite communication," *Nat. Photonics* **11**, 509–514 (2017).
- [3] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, F.-Z. Li, X.-W. Chen, L.-H. Sun, J.-J. Jia, J.-C. Wu, X.-J. Jiang, J.-F. Wang, Y.-M. Huang, Q. Wang, Y.-L. Zhou, L. Deng, T. Xi, L. Ma, T. Hu, Q. Zhang, Y.-A. Chen, N.-L. Liu, X.-B. Wang, Z.-C. Zhu, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, "Satellite-to-ground quantum key distribution," *Nature* **549**, 43–47 (2017).
- [4] G. Vallone, D. Bacco, D. Dequal, S. Gaiarin, V. Luceri, G. Bianco, and P. Villoresi, "Experimental satellite quantum communications," *Phys. Rev. Lett.* **115**, 040502 (2015).
- [5] S.-K. Liao, H.-L. Yong, C. Liu, G.-L. Shentu, D.-D. Li, J. Lin, H. Dai, S.-Q. Zhao, B. Li, J.-Y. Guan, W. Chen, Y.-H. Gong, Y. Li, Z.-H. Lin, G.-S. Pan, J. S. Pelc, M. M. Fejer, W.-Z. Zhang, W.-Y. Liu, J. Yin, J.-G. Ren, X.-B. Wang, Q. Zhang, C.-Z. Peng, and J.-W. Pan, "Long-distance free-space quantum key distribution in daylight towards inter-satellite communication," *Nat. Photonics* **11**, 509–513 (2017).
- [6] D. Bacco, M. Canale, N. Laurenti, G. Vallone, and P. Villoresi, "Experimental quantum key distribution with finite-key security analysis for noisy channels," *Nat. Commun.* **4**, 2363 (2013).
- [7] G. Vest, M. Rau, L. Fuchs, G. Corrielli, H. Weier, S. Nauerth, A. Crespi, R. Osellame, and H. Weinfurter, "Design and Evaluation of a Handheld Quantum Key Distribution Sender module," *IEEE J. Sel. Top. Quantum Electron.* **21**, 131–137 (2015).
- [8] M. S. Lee, M. K. Woo, Y.-S. Kim, Y.-W. Cho, S.-W. Han, and S. Moon, "Quantum hacking on a free-space quantum key distribution system without measuring quantum signals," *J. Opt. Soc. Am. B* **36**, B77 (2019).
- [9] M. Jofre, A. Gardelein, G. Anzolin, G. Molina-Terriza, J. P. Torres, M. W. Mitchell, and V. Pruneri, "100 MHz Amplitude and Polarization Modulated Optical Source for Free-Space Quantum Key Distribution at 850 nm," *J. Light. Technol.* **28**, 2572–2578 (2010).
- [10] F. Grünenfelder, A. Boaron, D. Rusca, A. Martin, and H. Zbinden, "Simple and high-speed polarization-based QKD," *Appl. Phys. Lett.* **112**, 051108 (2018).
- [11] I. Lucio-Martinez, P. Chan, X. Mo, S. Hosier, and W. Tittel, "Proof-of-concept of real-world quantum key distribution with quantum frames," *New J. Phys.* **11**, 095001 (2009), 0901.0612.
- [12] C. Agnesi, M. Avesani, A. Stanco, P. Villoresi, and G. Vallone, "All-fiber self-compensating polarization encoder for quantum key distribution," *Opt. Lett.* **44**, 2398–2401 (2019).

- [13] C. Agnesi, M. Avesani, L. Calderaro, A. Stanco, G. Folletto, M. Zahidy, A. Scriminich, F. Vedovato, G. Vallone, and P. Villoresi, “Simple quantum key distribution with qubit-based synchronization and a self-compensating polarization encoder,” *Optica* **7**, 284 (2020), 1909.12703.
- [14] Y. F. Jiang, K. Wei, L. Huang, K. Xu, Q. C. Sun, Y. Z. Zhang, W. Zhang, H. Li, L. You, Z. Wang, H. K. Lo, F. Xu, Q. Zhang, and J. W. Pan, “Remote Blind State Preparation with Weak Coherent Pulses in the Field,” *Phys. Rev. Lett.* **123** (2019), 10.1103/PhysRevLett.123.100503.
- [15] Y.-P. Li, W. Chen, F.-X. Wang, Z.-Q. Yin, L. Zhang, H. Liu, S. Wang, D.-Y. He, Z. Zhou, G.-C. Guo, and Z.-F. Han, “Experimental realization of a reference-frame-independent decoy BB84 quantum key distribution based on Sagnac interferometer,” *Opt. Lett.* **44**, 4523 (2019).
- [16] S. Wang, W. Chen, Z.-Q. Yin, D.-Y. He, C. Hui, P.-L. Hao, G.-J. Fan-Yuan, C. Wang, L.-J. Zhang, J. Kuang, S.-F. Liu, Z. Zhou, Y.-G. Wang, G.-C. Guo, and Z.-F. Han, “Practical gigahertz quantum key distribution robust against channel disturbance,” *Opt. Lett.* **43**, 2030–2033 (2018).
- [17] G. L. Roberts, M. Pittaluga, M. Minder, M. Lucamarini, J. F. Dynes, Z. L. Yuan, and A. J. Shields, “Patterning-effect mitigating intensity modulator for secure decoy-state quantum key distribution,” *Opt. Lett.* **43**, 5110–5113 (2018).
- [18] Y. Li, Y.-H. Li, H.-B. Xie, Z.-P. Li, X. Jiang, W.-Q. Cai, J.-G. Ren, J. Yin, S.-K. Liao, and C.-Z. Peng, “High-speed robust polarization modulation for quantum key distribution,” *Opt. Lett.* **44**, 5262 (2019).
- [19] D. Rusca, A. Boaron, F. Grünenfelder, A. Martin, and H. Zbinden, “Finite-key analysis for the 1-decoy state qkd protocol,” *Appl. Phys. Lett.* **112**, 171104 (2018).
- [20] S. Benedetto and P. Poggiolini, “Theory of Polarization Shift Keying Modulation,” *IEEE Trans. Commun.* **40**, 708–721 (1992).
- [21] G. Vallone, C. Agnesi, M. Avesani, and P. Villoresi, “Metodo di modulazione della polarizzazione di impulsi fotonici per la generazione di chiavi crittografiche quantistiche, e relativo modulatore di polarizzazione,” Italian Patent application n. 102019000019373, Deposit date 21 October 2019.
- [22] H. Xu and S. Wang, “An intrinsic-stabilization polarization encoder for quantum key distribution,” in *Sixth Symposium on Novel Optoelectronic Detection Technology and Applications* (SPIE, 2020).