Optics Letters

All-fiber self-compensating polarization encoder for quantum key distribution

Costantino Agnesi,[1,†] Marco Avesani,[1,†] Andrea Stanco,[1] Paolo Villoresi,[1,2] and Giuseppe Vallone[1,2,*]

[1]Dipartimento di Ingegneria dell'Informazione, Università degli Studi di Padova, Via Gradenigo 6B—35131 Padova, Italy
[2]Istituto di Fotonica e Nanotecnologie—CNR, Via Trasea 7—35131 Padova, Italy
*Corresponding author: vallone@dei.unipd.it

Received 4 March 2019; revised 26 March 2019; accepted 4 April 2019; posted 5 April 2019 (Doc. ID 361423); published 6 May 2019

Quantum key distribution (QKD) allows distant parties to exchange cryptographic keys with unconditional security by encoding information on the degrees of freedom of photons. Polarization encoding has been extensively used for QKD along free-space, optical fiber, and satellite links. However, the polarization encoders used in such implementations are unstable, expensive, and complex and can even exhibit side channels that undermine the security of the protocol. Here we propose a self-compensating polarization encoder based on a lithium niobate phase modulator inside a Sagnac interferometer and implement it using only commercial off-the-shelf (COTS) components. Our polarization encoder combines a simple design and high stability reaching an intrinsic quantum bit error rate as low as 0.2%. Since realization is possible from the 800 to the 1550 nm band using COTS devices, our polarization modulator is a promising solution for free-space, fiber, and satellite-based QKD.

https://doi.org/10.1364/OL.44.002398

Quantum key distribution (QKD) is an emerging quantum technology that allows two distant parties to distill a secret key with unconditional security by leveraging on the quantum mechanical nature of light [1]. As several standard encryption schemes have been proven insecure and major steps have been made towards the development of the quantum computer [2], QKD has gained vast recognition. Indeed, the keys generated in different scenarios may be used for symmetric key cryptography, when high levels of privacy and long-term secrecy are required. Several implementations of QKD systems have been reported in recent years, demonstrating the possibility of exploiting photonic degrees of freedom, such as polarization, time-bin, and orbital angular momentum, in free-space, optical fiber, or even satellite links [3–9]. However, in-field adoption of QKD alongside the current telecommunication infrastructures requires all components of the system to be simple and stable.

Widespread efforts have been made to simplify the requirements of QKD systems and to enhance the stability of the practical implementations. Recently, for example, a three-state and two-decoy state version of the BB84 protocol [10] has been proposed [11] and demonstrated to be secure [12,13], notably simplifying the requirements of the quantum state encoder and increasing the performances in the finite-key regime. Likewise, a stable intensity modulator for decoy-state preparation [14] and a stable phase modulator for time-bin encoding [15] have been demonstrated at repetition rates above GHz, both based on Sagnac interferometric configurations.

Despite polarization encoding being the predilected choice for free-space and satellite-based QKD experiments, few steps have been made to develop a simple and stable polarization state encoder. The use of inline lithium niobate ($LiNbO_3$) modulators has been an adopted solution [11,16], where the birefringence of the crystal is controlled by an external RF field. The applied voltage changes the index of refraction of both polarization modes differently, introducing a relative phase between each polarization, thereby modulating the polarization state. However, high $\tilde{V}_\pi$ voltage is needed to introduce a relative π shift between orthogonal polarizations, usually a factor 1.5 higher when compared to V_π of standard phase modulators. Moreover, the stability of this inline configuration is critical, as the temperature variations caused by the environment or by the RF internal power dissipation induce drifts in the resulting polarization state.

To address this problem, a double-pass autocompensating configuration with a Faraday mirror has been proposed in [17], which significantly improved long-term stability. However, this approach has important drawbacks such as the use of nonstandard products [the polarization-maintaining (PM) fiber has to be oriented at 45° with respect to the optical axis of the $LiNbO_3$ crystal], high $\tilde{V}_\pi$ voltages, the required use of high birefringence fibers to compensate for polarization mode dispersion, and the need of titanium-diffused phase modulators (TD-PM) able to guide two orthogonal polarizations that are hardly available at wavelengths outside the C band. Moreover, any misalignment of the PM fiber with respect to the optical axis of the $LiNbO_3$ crystal will impact the possibility to generate orthogonal states.

Another approach is the use of four independent lasers, which are then combined with polarization beam splitters (PBSs), polarization controllers (PCs), and a beam splitter (BS) [5,6,18,19]. This approach surely simplifies the electronic

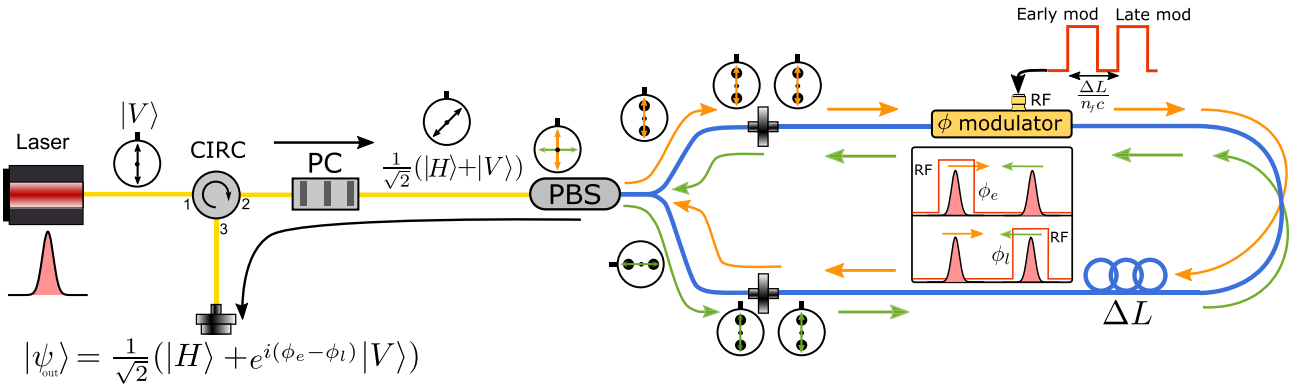

Fig. 1. Schematic representation of the working principle of the POGNAC. SM fibers are drawn in yellow while PM fibers are in blue.

control of the QKD transmitter, but is expensive and power inefficient since it requires 4 times as many lasers, laser current drivers, and temperature controllers. Furthermore, the use of independent lasers could open side channels that undermine the security of the implementation in the presence of an eavesdropper. In fact, differences in the temporal shape and frequency spectrum of the independent laser pulses could be exploited to infer the polarization state without requiring a direct measurement [16,20].

In this Letter, we propose the POGNAC, a polarization modulator based on a $LiNbO_3$ phase modulator inside a Sagnac interferometer. We implement and test it using commercial off-the-shelf (COTS) components. The POGNAC exhibits a high degree of simplicity and stability, low intrinsic quantum bit error rate (QBER), and can be implemented for operation on both the 800 nm band and the 1550 nm band, rendering it compatible with free-space, optical fiber, and satellite-based QKD.

Our proposed polarization modulator based on a Sagnac interferometer (POGNAC) can be seen in Fig. 1. A linearly polarized laser pulse enters the optical circulator (CIRC) in port 1 and exits in port 2. A PC is then encountered, which transforms the polarization state into $|\psi\rangle = \frac{1}{\sqrt{2}}(|H\rangle + e^{i\varphi_0}|V\rangle)$, a balanced superposition of horizontal and vertical polarization with arbitrary relative phase, i.e., any state on the equator of the Bloch sphere with $|H\rangle$ ($|V\rangle$) at the north (south) pole. The light is split into orthogonal linear polarizations by a fiber PBS. It is important to note that each of the polarized beams exiting from the PBS are 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 only along the slow axis of the PM fibers of both PBS exit ports. This is the standard behavior of COTS fiber-based PBSs.

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 counterclockwise direction (CCW). In the CW direction, a $LiNbO_3$ phase modulator is first encountered introducing a phase ϕ_e to the light pulse. A PM fiber 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 PM fiber delay line. Then, the $LiNbO_3$ phase modulator introduces a 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 PM fiber 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 phase modulator. This ensures that both CW and CCW pulses exit the Sagnac interferometer at the same time, perfectly recombining the two orthogonal polarization states after the PBS. The emerging polarization state is thus given by

$$|\psi_{\text{out}}^{\phi_e,\phi_\ell}\rangle = \frac{1}{\sqrt{2}}(|H\rangle + e^{i(\phi_e-\phi_\ell-\varphi_0)}|V\rangle). \quad (1)$$

Since the polarization state depends only on the phase difference $\phi_e - \phi_\ell$, any phase drift that introduces a common phase to both counterpropagating pulses is self-compensated, rendering the design immune to thermal and bias drifts.

Considering that the CW pulse anticipates the arrival of the CCW pulse on the $LiNbO_3$ crystal by a factor $\frac{\Delta L}{n_f c}$ (where n_f is the index of refraction of the PM fiber and c is the velocity of light), by carefully timing the applied voltage on the phase modulator, the polarization state $|\psi_{\text{out}}\rangle$ can be modulated. For the sake of simplicity, let's suppose that $\varphi_0 = 0$. If no voltage (or equal voltage) is applied to the CW and CCW pulses, the polarization state remains unchanged, i.e.,

$$|\psi_{\text{out}}^{0,0}\rangle = |D\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle). \quad (2)$$

Instead, if $V_{\pi/2}$ voltage is applied to the CW pulse and no voltage is applied to the CCW pulse, the output state becomes

$$|\psi_{\text{out}}^{\frac{\pi}{2},0}\rangle = |L\rangle = \frac{1}{\sqrt{2}}(|H\rangle + i|V\rangle). \quad (3)$$

Alternatively, if no voltage is applied to the CW pulse and $V_{\pi/2}$ voltage is applied to the CCW pulse,

$$|\psi_{\text{out}}^{0,\frac{\pi}{2}}\rangle = |R\rangle = \frac{1}{\sqrt{2}}(|H\rangle - i|V\rangle). \quad (4)$$

Finally, if V_π is applied to the CW (or CCW pulse) and no voltage is applied to the other, the output state becomes

$$|\psi_{\text{out}}^{\pi,0}\rangle = |A\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle). \quad (5)$$

The modulated light pulses then exit through port 3 of the CIRC.

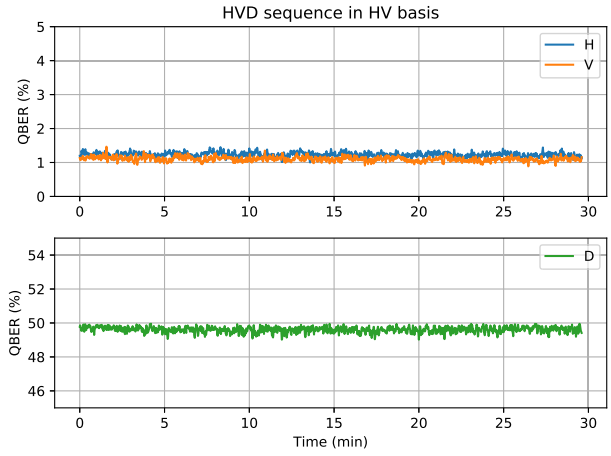

Fig. 2. QBER as a function of time for the pseudorandom $\{|H\rangle, |V\rangle, |D\rangle\}$ sequence ($V_{\pi/2}$ modulation) measured in the $\{|H\rangle, |V\rangle\}$ basis.

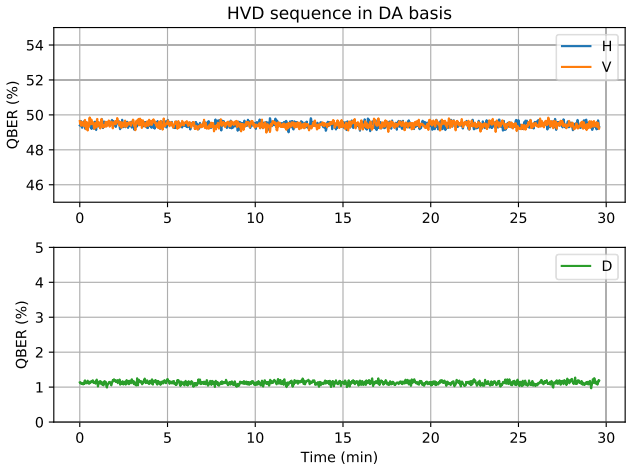

Fig. 3. QBER as a function of time for the pseudorandom $\{|H\rangle, |V\rangle, |D\rangle\}$ sequence ($V_{\pi/2}$ modulation) measured in the $\{|D\rangle, |A\rangle\}$ basis.

By noting that $\{|D\rangle, |A\rangle\}$ and $\{|L\rangle, |R\rangle\}$ form two mutually unbiased basis (MUBs), we can conclude that our proposed polarization modulator can generate the necessary polarization states to perform the standard BB84 QKD protocol [10]. We note that when $\varphi_0 \neq 0$, the same scheme allows the generation of two MUBs lying on the equator of the Bloch sphere. Furthermore, by choosing $\{|L\rangle, |R\rangle\}$ as the key generation states and $|D\rangle$ as the control state, the simplified three-polarization-state version of BB84 [11] can be implemented requiring only two voltage levels, i.e., 0 and $V_{\pi/2}$, and fine positioning of the RF electrical pulse, which can be done using digital outputs of a field-programmable gate array (FPGA). It can be useful to note that the four polarization states can also be generating by applying four different voltage levels, i.e., zero, $V_{\pi/2}$, V_{π}, and $V_{3\pi/2}$, only to the CW or CCW pulse, always applying zero voltage to the other.

We used a World Star Tech laser-diode-emitting light at 850 nm and an Hewlett-Packard 8013B pulse generator (PG) to generate laser pulses with 1.2 ns FWHM duration and 100 kHz repetition rate due to laser source limitation. No performance degradation is expected up to the 100 MHz rate [14]. The light pulses first traversed a Glan–Thompson polarizer, and was then coupled into a single-mode (SM) fiber. In our implementation, the CIRC was replaced with a 50:50 BS. This replacement introduced additional 6 dB of losses, which did not represent a problem since the light pulses were attenuated to the single-photon level after the polarization modulator. A PC then transformed the polarization state into $|\psi\rangle = \frac{1}{\sqrt{2}}(|H\rangle + e^{i\varphi_0}|V\rangle)$. The light pulses then impinged a fiber-based PBS. A $\Delta L = 1$ m PM fiber was used as the delay line inside the Sagnac interferometer. The RF signal used to drive the $LiNbO_3$ phase modulator was generated by an Avnet Zedboard FPGA board, which was triggered by the PG. The FPGA generated squared pulses with 3 ns duration that could be arbitrarily delayed with respect to the trigger pulses with approximately 100 ps precision. This allowed us to send an electrical pulse that modulated either the CW propagating or the CCW propagating pulse, or not to send any electrical pulse according to a previously established pseudorandom sequence. The electrical pulses were then amplified to $V_{\pi/2}$ by an RF amplifier and then sent to the phase modulator. In this manner, we simulated the polarization state transmission required by the simplified version of BB84 [11]. To test the generation of the $|A\rangle$ state, we replaced the FPGA with the Agilent 33521A arbitrary function generator that produced electrical pulses with 20 ns duration, allowing us to generate a $|D\rangle$, $|A\rangle$ sequence. This replacement was necessary to reach V_{π} necessary to obtain the $|A\rangle$ state.

The light exited the polarization modulator through the 50:50 BS and then encountered an optical attenuator (OA) that attenuated to the single-photon level. Then, a further PC (not shown in Fig. 1) compensated the unitary transformation due to the SM fibers outside the POGNAC and transformed the generated states into $|H\rangle$, $|V\rangle$, $|D\rangle$, and $|A\rangle$. The light pulses were then launched into free space using a fiber collimator. A free-space polarization analyzer was then used to evaluate the performances of the polarization modulator. The analyzer was composed by a half-wave plate (HWP) and a PBS. This allowed us to measure in the $\{|H\rangle, |V\rangle\}$ or in the $\{|D\rangle, |A\rangle\}$ basis by simply rotating the HWP. The single-photon detection was performed using Excelitas SPCM-AQRH single-photon avalanche diode and the quTAU Time-Tagger. A computer was then used to analyze the results.

The pseudorandom $\{|H\rangle, |V\rangle, |D\rangle\}$ sequence was continuously sent by our polarization encoder and measured by the free-space polarization analyzer in the $\{|H\rangle, |V\rangle\}$ basis. Every 3 s, the QBER was calculated. The results can be seen in Fig. 2. An average QBER of $1.23 \pm 0.07\%$ was measured for $|H\rangle$ and $1.10 \pm 0.07\%$ for $|V\rangle$. Instead, for $|D\rangle$, a $49.6 \pm 0.2\%$ QBER was measured, as expected for a MUB state.

After approximately 30 min, the HWP of the free-space polarization analyzer was rotated to measure in the $\{|D\rangle, |A\rangle\}$ basis, without modifying the polarization encoder. As before, every 3 s, the QBER was calculated. The results can be seen in Fig. 3. An average QBER of $1.12 \pm 0.04\%$ was measured for $|D\rangle$. Instead, for $|H\rangle$ and $|V\rangle$, a $49.4 \pm 0.1\%$ QBER was measured, as expected for MUB states.

Similarly, to test the generation of the $|A\rangle$ state, a $\{|D\rangle, |A\rangle\}$ sequence was sent, and the HWP of the free-space polarization analyzer was rotated to measure in the $\{|D\rangle, |A\rangle\}$ basis. As before, every 3 s, the QBER was calculated. The results can be seen in

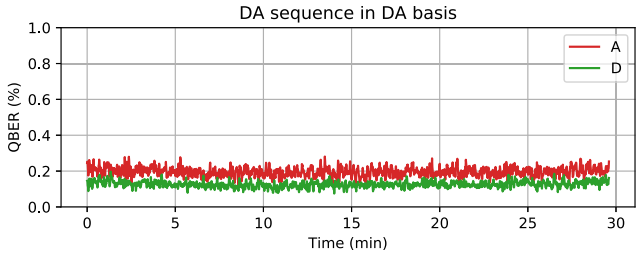

Fig. 4. QBER as a function of time for the $\{|D\rangle, |A\rangle\}$ sequence (V_π modulation) measured in the $\{|D\rangle, |A\rangle\}$ basis.

Fig. 4. An average QBER of $0.20 \pm 0.02\%$ was measured for $|A\rangle$ and $0.13 \pm 0.01\%$ for $|D\rangle$. The lower QBER in this configuration can be attributed to the cleaner electrical RF pulses generated by the function generator respect to the ones generated by the FPGA.

Since no active (i.e., varying with time) polarization compensation was present in any case, the results shown in Figs. 2–4 demonstrate the high stability of the POGNAC.

In conclusion, we proposed and experimentally tested the POGNAC, a novel polarization encoder system for free-space, fiber, and satellite-based QKD. Compared to the previously proposed solutions, our approach offers several key advantages. The Sagnac design renders the modulation sensible only to phase differences between CW and CCW propagating pulses, making the POGNAC insensible to temperature and bias drifts, greatly improving long-term stability over inline implementations [11,16,17].

Compared to the self-compensating solution proposed in [17], the POGNAC does not need a custom phase modulator. In fact, inside the Sagnac, only one polarization is guided and standard proton-exchange phase modulators (PE-PM) can be used. The Faraday mirror solution instead requires TD-PMs that are able to support both polarizations. TD-PMs are commercially available only from few manufacturers, while PE-PMs are COTS devices available at different wavelengths, including the 800 nm band, relevant for free-space QKD.

Moreover, to the best of our knowledge, the modulation voltages required by our solution are considerably lower than previous proposals. In the POGNAC, the phase modulation is directly converted in a polarization modulation. Instead in [11,16,17], the applied voltage changes the index of refraction of both polarization modes differently, introducing a relative phase between each polarization, thereby modulating the polarization state. Usually, these implementations require a $\tilde{V}_\pi$ 1.5 times higher than our proposal.

Our experimental results show that low QBER can be obtained stably overtime without the need of an additional feedback system, greatly simplifying the design of a polarization QKD source. Such simplicity renders our source suitable for CubeSat missions, where a small footprint and low energy consumption are of critical importance [21]. Furthermore, the temporal stability of the source attests the compatibility with QKD links with satellites even in middle Earth orbit [22], or part of a global navigation satellite system [23], where visibility times between the ground station and satellite can exceed the hour.

Lastly, the configuration based on a Sagnac interferometer could allow for high repetition rates, up to few GHz, as recently demonstrated with an intensity modulator for decoy-state preparation [14], as well as a stable phase modulator for time-bin encoding [15].

Funding. Ministero dell'Istruzione, dell'Università e della Ricerca (MIUR) (Fondo dipartimenti universitari di eccellenza); Agenzia Spaziale Italiana (ASI) (E16J16001490001).

[†]These authors contributed equally to this Letter.

REFERENCES

1. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
2. G. Wendin, Rep. Prog. Phys. **80**, 106001 (2017).
3. G. Vallone, V. D'Ambrosio, A. Sponselli, S. Slussarenko, L. Marrucci, F. Sciarrino, and P. Villoresi, Phys. Rev. Lett. **113**, 060503 (2014).
4. G. Vallone, D. Dequal, M. Tomasin, F. Vedovato, M. Schiavon, V. Luceri, G. Bianco, and P. Villoresi, Phys. Rev. Lett. **116**, 253601 (2016).
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, Nat. Photonics **11**, 509 (2017).
6. 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, Nature **549**, 43 (2017).
7. N. T. Islam, C. C. W. Lim, C. Cahall, J. Kim, and D. J. Gauthier, Sci. Adv. **3**, e1701491 (2017).
8. D. Cozzolino, D. Bacco, B. Da Lio, K. Ingerslev, Y. Ding, K. Dalgaard, P. Kristensen, M. Galili, K. Rottwitt, S. Ramachandran, and L. K. Oxenløwe, "Fiber based high-dimensional quantum communication with twisted photons," arXiv:1803.10138 (2018).
9. A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, Phys. Rev. Lett. **121**, 190502 (2018).
10. C. H. Bennett and G. Brassard, Theor. Comput. Sci. **560**, 7 (2014).
11. F. Grünenfelder, A. Boaron, D. Rusca, A. Martin, and H. Zbinden, Appl. Phys. Lett. **112**, 051108 (2018).
12. D. Rusca, A. Boaron, F. Grünenfelder, A. Martin, and H. Zbinden, Appl. Phys. Lett. **112**, 171104 (2018).
13. D. Rusca, A. Boaron, M. Curty, A. Martin, and H. Zbinden, Phys. Rev. A **98**, 052336 (2018).
14. G. L. Roberts, M. Pittaluga, M. Minder, M. Lucamarini, J. F. Dynes, Z. L. Yuan, and A. J. Shields, Opt. Lett. **43**, 5110 (2018).
15. 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, Opt. Lett. **43**, 2030 (2018).
16. M. Jofre, A. Gardelein, G. Anzolin, G. Molina-Terriza, J. P. Torres, M. W. Mitchell, and V. Pruneri, J. Lightwave Technol. **28**, 2572 (2010).
17. I. Lucio-Martinez, P. Chan, X. Mo, S. Hosier, and W. Tittel, New J. Phys. **11**, 095001 (2009).
18. D. Bacco, M. Canale, N. Laurenti, G. Vallone, and P. Villoresi, Nat. Commun. **4**, 2363 (2013).
19. G. Vest, M. Rau, L. Fuchs, G. Corrielli, H. Weier, S. Nauerth, A. Crespi, R. Osellame, and H. Weinfurter, IEEE J. Sel. Top. Quantum Electron. **21**, 131 (2015).
20. M. S. Lee, M. K. Woo, Y.-S. Kim, Y.-W. Cho, S.-W. Han, and S. Moon, J. Opt. Soc. Am. B **36**, B77 (2019).
21. D. K. Oi, A. Ling, G. Vallone, P. Villoresi, S. Greenland, E. Kerr, M. Macdonald, H. Weinfurter, H. Kuiper, E. Charbon, and R. Ursin, EPJ Quantum Technol. **4**, 6 (2017).
22. D. Dequal, G. Vallone, D. Bacco, S. Gaiarin, V. Luceri, G. Bianco, and P. Villoresi, Phys. Rev. A **93**, 010301 (2016).
23. L. Calderaro, C. Agnesi, D. Dequal, F. Vedovato, M. Schiavon, A. Santamato, V. Luceri, G. Bianco, G. Vallone, and P. Villoresi, Quantum Sci. Technol. **4**, 015012 (2018).