ADVANCED QUANTUM TECHNOLOGIES
www.advquantumtech.com

Scalable Implementation of Temporal and Phase Encoding QKD with Phase-Randomized States

*Saverio Francesconi, Claudia De Lazzari, Domenico Ribezzo, Ilaria Vagniluca, Nicola Biagi, Tommaso Occhipinti, Alessandro Zavatta, and Davide Bacco**

Quantum key distribution (QKD), that is, exchanging cryptographic keys encoded in quantum particles exploiting the laws of quantum physics, is already a reality in our society. Current implementations are based on attenuated laser technique, a practical replacement of single photons which requires a random phase for each quantum state in order to achieve the highest level of security. In particular, the time-bin and phase encoding techniques are mainly exploiting laser in gain-switching modes combined with asymmetric interferometers or multiple laser sources in a master–slave configuration, which present limitations in terms of stability and scalability. In this work, a novel scheme for implementing a reconfigurable and scalable QKD transmitter based on the time-bin encoding protocol with a decoy-state method employing phase-randomized weak coherent states is proposed and demonstrated. The scheme is tested and validated up to 26 dB-attenuation channel using standard single-photon detectors working in the telecom wavelength range.

1. Introduction

Quantum key distribution (QKD) allows sharing of symmetric encryption keys between two or more remote parties, in an unconditionally secure way.[1–3] These symmetric keys are then used by ciphers (either hardware or software-based) to protect the transmission of the shared data. Today, we are experiencing a great enhancement in the number of QKD companies around the world and multiple test beds have been demonstrated so far,[4–6] from medical data protection to video calls between three European countries enabled by quantum keys,[7] just to give a few examples.

Current quantum systems can be categorized into two main groups: discrete variable (DV)-based systems, which exploit discrete degrees of freedom of light for encoding the quantum states, for example, polarization, time of arrival and phase, space encoding, and scheme based on continuous variable (CV), where the quantum information is encoded in the amplitude and phase quadrature of the optical field. The security proof of DV protocols, including the well-established BB84[1] (with its multiple variants), relies on the no-cloning theorem and the indistinguishability of non-orthogonal states, holding as long as the quantum states are made by single photons. Using attenuated laser pulses instead of single photons is practically convenient, however, it opens the way to powerful eavesdropping attacks, taking advantage of the fraction of pulses that, inevitably, contain two or more photons.[8] The introduction of decoy-state method[9–11] has boosted the experimental advancement of DV protocols with attenuated laser sources, paving the way toward many record-breaking implementations of QKD.[12–19] However, all these experiments assume that the quantum signals are completely phase randomized at the QKD transmitter. Indeed, the security proof requires that the quantum states (prepared by Alice) must be represented with a diagonal density matrix (mixture states) in the photon-number basis.[20,21] In this way, each quantum state exhibits a random, uniformly distributed global phase, and the information leakage resulting from phase correlation is successfully avoided. One way to achieve a random global phase is to use active phase randomization, which can be implemented by adding a discrete phase modulation of the quantum signals, considering that around ≈10 phase levels provide an output very close to the continuous phase randomization.[22,23] However, to implement such multiple levels of phase modulation, a proper digital-to-analog converter driving an extra optical modulator has to be included in the QKD setup, and extra random bits have to be consumed in the process. Alternatively, continuous phase

S. Francesconi, C. De Lazzari, I. Vagniluca, N. Biagi, T. Occhipinti, A. Zavatta, D. Bacco
QTI S.r.l.
50125 Firenze, Italy
E-mail: davide.bacco@unifi.it

D. Ribezzo, A. Zavatta
Istituto Nazionale di Ottica del Consiglio Nazionale delle Ricerche (CNR-INO)
50125 Firenze, Italy

D. Ribezzo
Università degli Studi di Napoli Federico II
Napoli Italy

D. Bacco
Department of Physics and Astronomy
University of Florence
50019 Sesto Fiorentino, Italy

The ORCID identification number(s) for the author(s) of this article can be found under https://doi.org/10.1002/qute.202300224

DOI: 10.1002/qute.202300224

randomization can be achieved directly at the laser source, using a pulsed laser diode operating above and below the threshold, with the laser current driven above and below the threshold level. Here, every pulse originates from a new spontaneous emission process, where the seed photons exhibit an intrinsically random phase.[24] This technique has been demonstrated up to ≈10 GHz frequencies of repetition rate, but it carefully requires that the remaining photons from previous lasing have vanished from the laser cavity before starting a new stimulated emission.[25]

For practical DV-QKD based on optical links made by conventional single-mode optical fiber, time-bin, and phase encoding methods are often preferred over polarization encoding, as the compensation of polarization drifts in the fiber channel is not required.[2] Moreover, the polarization degree of freedom is limited to a 2D Hilbert space, while multiple time bins can be exploited to prepare qudits for high-dimensional QKD with temporal and phase encoding.[16,26] Notably, employing high-dimensional states improves the key generation rate up to the medium-loss regime, as in typical metropolitan links, thanks to the larger information gain per photon.[27]

The conventional method to prepare time-bin or phase-encoded qubits, with continuous randomization of phase, utilizes a delay line interferometer (DLI) like an asymmetric Michelson[19,28] or an asymmetric Mach–Zehnder[29] after the laser source. In this way, each phase-randomized pulse is split into a pair of pulses, coherent with each other, with a controllable phase relation. The subsequent optical setup encodes a quantum state on each pair of pulses, depending on the basis choice and decoy protocol. This approach requires active stabilization of the QKD transmitter, which has to match the phase drifts of the receiver. Moreover, while working in two dimensions, it is not suitable for high-dimensional encoding in time and phase, which requires more than two time-bins per state. A different solution, that does not need the interferometer, is the so-called pulsed laser seeding (PLS),[30–32] where phase-randomized pulses are generated using two gain-switched lasers. The lasing action of the first laser (master) is used to stimulate the emission of the second laser (slave). The photons emitted by the slave inherit the phase of the master's photons that triggered the emission, resulting in the generation of phase-randomized pulses. Additionally, the pulses emitted by the slave laser will be narrower and less affected by timing jitter compared to those emitted by the master, because stimulated emission is a narrower process compared to spontaneous emission. This method is particularly suitable for generating ready-to-use pulses but, despite a more complex setup, it does not provide significant advantages if further modulation of the generated pulses is desired. Conversely, optical band-pass filters are required to reduce spurious emissions, and Bragg fiber gratings are needed to pre-compensate for chromatic dispersion in fiber communications.[30–32]

In this work, we introduce an alternative approach to generate sequences of quantum states, with time-bin and phase encoding, that exhibit a random global phase. We present the method in a completely general setting since it allows the generation of phase-randomized coherent states of arbitrary dimension. The approach is scalable, enabling the implementation of the high-dimensional generalization of many DV protocols, as proposed in ref. [33]. We experimentally demonstrate it in the case of qubits preparation as we test the bi-dimensional BB84 protocol with decoy method.

2. Laser Source and Random Phase

Spontaneous emission has been identified as a means to produce quantum randomness. Indeed, when a laser is turned on the phase of the emitted wave-packet is derived from the vacuum fluctuations of the optical field. Driving the laser above and below the lasing threshold allows the production of a train of phase-randomized pulses, given that the laser cavity prior to lasing is in the vacuum state and thus the lasing is entirely prompt by spontaneous emission.[34]

In order to produce phase-randomized pulses, a gain-switched laser can be employed in two different regimes:[24] short pulses and steady state. If the electric driving signal is short, photon emission is extinguished after the emission of a short Gaussian-shaped pulse, having a duration of tens of picoseconds. Due to the abrupt change in the carrier density and in the refractive index of the laser cavity, the emitted pulses present a frequency chirp and a broadened spectrum. On the other hand, if the driving current is kept longer the intensity relaxes into a steady state, in which cavity gain approximately balances loss. In this condition of equilibrium the refractive index of the laser cavity is more stable and therefore the spectrum is narrower, being less chirped.

Gain-switched short pulses are commonly employed as light source of QKD systems.[19,28] As we said before, this approach requires active stabilization of the QKD transmitter and it cannot be easily scaled up for high-dimensional encoding. In this paper, we demonstrate the usage and advantage of steady-state pulses for QKD transmitters.

A distributed-feedback (DFB) laser (G&H AA0701), with a 10 GHz-modulation bandwidth, is periodically driven above and below the lasing threshold with a 1.2 ns-long squared electrical signal at 600 MHz frequency. This repetition rate is sufficiently low not to violate the empty cavity condition, necessary to the phase randomization. The driving signal has an AC peak-to-peak current $I_{pp} = 38$ mA and a DC adjustable offset I_{DC}. We define the minimum drive current as $I_{min} = I_{pp}/2 - I_{DC}$, which refers to the drive current at the bottom of the AC current. In the following, we use the normalized minimum excitation, defined by ref. [25].

$$\Lambda = \frac{I_{min} - I_{th}}{I_{th}} \tag{1}$$

where I_{th} is the laser threshold current ($I_{th} = 14$ mA). When $\Lambda > 0$ the laser is always turned on, while when $\Lambda < 0$ the laser is turned off when the AC current is low. In particular, when $\Lambda < -1$ no current is injected at the minimum and the laser is reverse biased.

We first verify the phase randomization by observing the interference of adjacent pulses in an unbalanced and fiber-based Michelson interferometer. **Figure 1** shows a sketch of the measurement setup. Indeed, the phases of adjacent pulses are more correlated than those between more temporally separated pulses. The unbalanced interferometer introduces a time delay equal to the pulse period (1.67 ns). A phase shifter (piezoelectric fiber stretcher), located in one of the interferometer arms, is employed

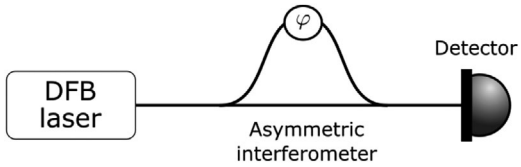

Figure 1. Sketch of the setup for phase correlation measurement. The delay line in one arm of the interferometer is equal to the pulse period. The relative phase φ between the two arms is scanned with a piezoelectric actuator.

to modulate the phase of the interference φ which was measured with a 5-GHz telecom photodetector. If the interfering pulses are coherent with each other (fixed relative phase), then the output signal of the photodetector depends on the phase difference between the two arms of the interferometer. When the phase φ is scanned with the piezo actuator, a clear interference fringe is observed.

On the other hand, if the phase between the pulses is random, the interference output varies over time, and the interference fringe will disappear with temporal averaging.

The visibility of the interference is defined as

$$V = \frac{I_{\max} - I_{\min}}{I_{\max} + I_{\min}} \tag{2}$$

where $I_{\max}$ ($I_{\min}$) is the maximum (minimum) of the interference fringe. We employ this quantity to evaluate the degree of phase correlation: as the correlation becomes higher the visibility gets closer to 1.

Figure 2 reports the visibility V of the interference fringes as a function of the normalized minimum driving voltage Λ. As expected, if the laser is always turned on ($\Lambda > 0$) the visibility is higher than 50% and the pulses are not phase randomized. For $\Lambda < -0.30$, the observed visibility is lower than 0.004.

Since visibility can be impacted by several experimental factors (e.g., polarization, laser coherence time, and so on), we now analyze more in detail the case in which $\Lambda = -0.30$ to demonstrate the phase randomization of the pulses. By using a fast photodiode as detector, we measure the interference of each pulse with the adjacent one. By sorting the data we obtain the intensity distribution, which are reported in **Figure 3a**. When two coherent pulses of constant phase difference $\Delta\phi$ interfere, the output intensity I_0 is proportional to $(1 + \cos\Delta\phi)$. If the pulses have a uniform phase distribution, then the intensity distribution would produce two lateral peaks at both ends. The experimental results are in good agreement with the expected distribution.The observed differences, in particular the peaks height, is mainly due to the time jitter.

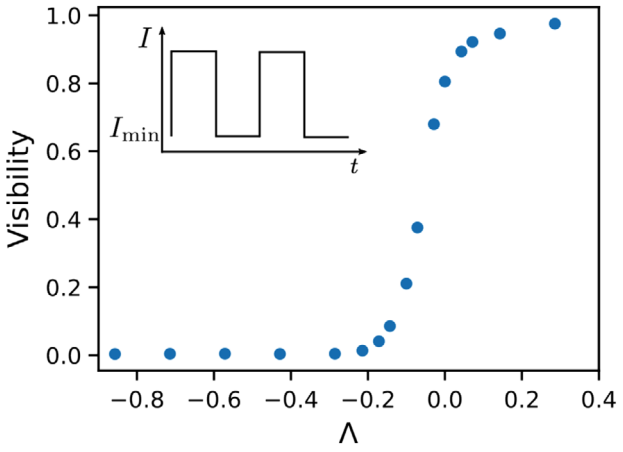

Figure 2. Visibility of the interference as a function of the normalized minimum driving current (Λ). The inset shows the laser driving signal: $I_{\min}$ is the minimum current value.

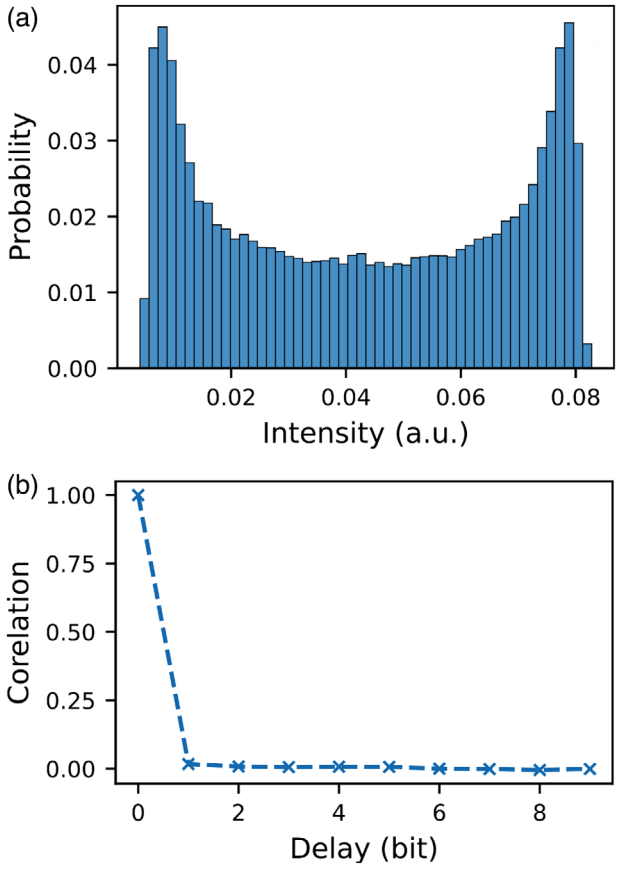

Figure 3. a) Experimental intensity distribution for the interference of 60000 optical pulses and b) their intensity correlation as a function of the delay in bit unit (each bit corresponds to about 1.67 ns.).

We would like to point out, as observed also by reference,[24] that only the steady-state regime produces the sharp peaks at the ends of the sampling range, which indicate a high quality of the interference. On the contrary, short-pulse emission, due to frequency chirp and additional time jitter, produce a rather uniform distribution without the two peaks.

To further verify the quality of the phase randomization, we take the same experimental data of Figure 3a) and we derive the intensity correlation as a function of the delay in bit unit (where one bit corresponds to about 1.68 ns). The result, reported in Figure 3b, shows that the correlation probability p_{phc} drops to less than 2% already between one pulse and the adjacent. These values are compatible with measurements of same kind found in the literature, where phase-randomized pulses are employed as a

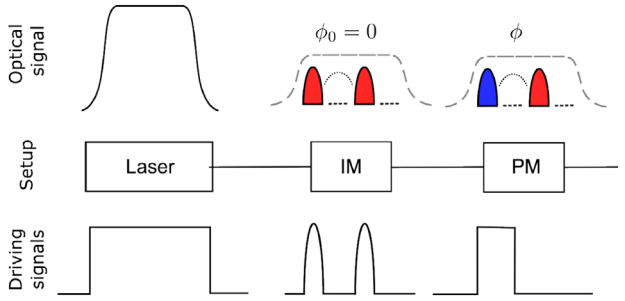

Figure 4. Schematic picture of the preparation method for $p = 4$. The phase-randomized pulse generated by the laser source is modulated by the intensity modulator (IM) in $p = 4$ sub-pulses, two of which are empty. The two non-empty sub-pulses have zero-relative phase $\phi_0 = 0$. The phase modulator (PM) finally sets the relative phase to ϕ. The lower row reports the driving electrical signals that are applied to the laser and the modulators. The pulses' color represent their optical phase.

quantum random number generator (QRNG).[24,35] In that case the correlation is further reduced by applying post-processing algorithm, while in our case we are only interested in generating phase-randomized optical pulses for time-bin QKD.

In the next sections we employ the phase-randomized pulses to prepare the quantum states for QKD protocols, considering the effect of the residual degree of phase correlation p_{phc}.

3. Quantum States Preparation

The phase-randomized optical pulse goes through an intensity modulator (IM) that divides the pulse into p sub-pulses (some of them can be empty). After this step, each global pulse can be identified with a state in a p-dimensional Hilbert space. In time encoding, the conventional Z basis is defined by p orthogonal quantum states, $\{|j\rangle\}_{j=0,1,\dots,p-1}$, prepared accordingly to the time-bin occupation of the photon, that are distinguished by the time of arrival at the detector. The mutually unbiased basis used in the BB84 protocol and denoted by X, is given by p quantum states that are the superposition states of the Z basis; precisely

$$|f_m\rangle = \frac{1}{\sqrt{p}} \sum_{j=0}^{p-1} e^{i\frac{2\pi m}{p} j} |j\rangle\,, \quad m = 0, \dots, p-1 \tag{3}$$

In order to prepare these states, a phase modulator (PM) is placed after the IM to set the relative phase between the sub-pulses of each pulse. **Figure 4** illustrates the experimental steps to obtain quantum states having $p = 4$. In general, with this setup it is possible to prepare different choices of mutually unbiased bases, composed by superposition states, as suggested in ref. [26].

Compared to previously demonstrated approaches,[19] this scheme does not require any interferometer, simplifying its operation and scalability to high-dimensional protocols. Indeed, the use of steady-state emission instead of short pulses allows to generate optical pulses with an arbitrary time duration, given that the laser driving signal has a sufficient low repetition rate. From these pulses it is possible to prepare quantum states having a high dimensionality (i.e., $p > 2$) without any hardware modifications with respect to the case $p = 2$. It is only necessary to modify the electrical signals that drive the laser and the modulators,

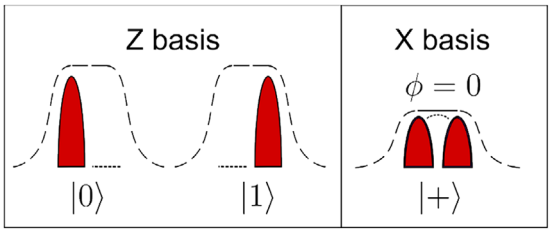

Figure 5. Quantum states of the case $p = 2$ for the implementation of the three-state BB84 protocol in time-bin encoding. States early ($|0\rangle$) and late ($|1\rangle$)) of the Z basis, and the superposition state ($|+\rangle$) with zero-relative phase of the X basis. The phase is represented by the pulse color.

which can be easily done via software. On the contrary, when exploiting the short-pulse regime, the pulses time duration cannot be extended and to generate high-dimensional quantum states it is necessary to employ a nested interferometer, which complicates the transmitter hardware and its operation.

4. Implementation of 2D BB84

The quantum state source has been integrated into our time-bin QKD system to determine its performance. We implement the three-states time-bin encoding BB84 protocol with 1-decoy method, in the finite-key regime.[19,36,37] In time-bin encoding, the Z basis is identified with the time-of-arrival basis. The two states $|0\rangle$ and $|1\rangle$ of the Z basis are therefore defined by the photon's occupation of one over two time bins and they are usually called "early" and "late." In this version of BB84, only one state of the X basis, denoted by $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$, is prepared and sent, which consists in the superposition of the states of the Z basis with zero-relative phase. **Figure 5** reports a sketch of the employed states. Compared to the general setup shown in Figure 4, this implemented protocol does not require the phase modulator.

At the transmitter side, states of the two mutually unbiased bases (Z and X) are randomly selected, prepared, and sent through the quantum channel. Accordingly to Section 2, the states in the two bases of the time-bin QKD protocol are prepared from the optical pulses generated by the DFB laser and carved out by an intensity modulator controlled by a field programmable gate array (FPGA).[38]

At the receiver side, before the measurements, a 50:50 beam splitter acts as a passive basis choice. The Z-basis output brings the photons directly to a single-photon detector (SPD), while the X-basis output lets the photons pass through a DLI that introduces a time delay equal to one time bin and reaches the detection stage. The detectors are InGaAs single-photon avalanche photodiodes (SPAD). **Figure 6** resumes the setup of the system.[38]

The secure key is distilled from the Z-basis detections, while the X-basis detections are used for the security analysis. For 1-decoy three-state BB84 protocol, in the finite-key regime, the secure key length l is bounded by[19]

$$l \leq s^l_{Z,0} + s^l_{Z,1}(1 - h(\phi^u_Z)) - \lambda_{\text{EC}} - 6\log_2\left(\frac{19}{\epsilon_{\text{sec}}}\right) - \log_2\left(\frac{2}{\epsilon_{\text{corr}}}\right) \tag{4}$$

with $s^l_{Z,0}$ and $s^l_{Z,1}$ being the lower bounds for the vacuum and the single-photon events, ϕ^u_Z the upper bound of the phase error

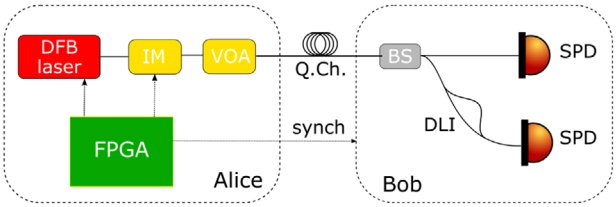

Figure 6. Schematics of the experimental setup. DFB laser, distributed feedback laser; FPGA, field programmable gate array; IM, intensity modulators; Q. Ch., quantum channel; BS, beam-splitter; DLI, delay line interferometer; SPD, single-photon detector.

Table 1. Experimental parameters and results for different channel attenuation.

Attenuation [dB]	μ_1	$QBER_Z$ [%]	ϕ^u_Z [%]	SKR [kbit s^{-1}]
6	0.013	1.4	4	2.4
11	0.04	1.5	3	2.2
16	0.11	1.5	3.9	1.7
21	0.23	2.8	8.3	0.911
26	0.28	2.2	10	0.280

μ_1, signal mean photon number; $QBER_Z$, quantum bit error rate of Z basis; ϕ^u_Z, upper bound of the phase-error rate of the Z basis; SKR: secret key rate.

rate, λ_{EC} the number of disclosed bits in the error correction stage, $h(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ the binary entropy and $\epsilon_{sec} = 10^{-15}$ and $\epsilon_{corr} = 2^{-127}$ the secrecy and correctness parameters.

In order to consider in our analysis the small residual phase correlation, we employ the correlation probability of adjacent pulses p_{phc}, which have been measured previously. We therefore reduce the secure key length to $l \leq (1 - p_{phc})l$ before the privacy amplification stage.

5. Results

The QKD system has been tested to distribute secret keys at different channel attenuation, from 6 to 26 dB. In order to maximize the secret key rate (SKR), for each attenuation value we have optimized the mean photon numbers of the signal (μ_1) and the decoy (μ_2), the block size and the deadtime of the SPDs. **Table 1** summarizes the used values of the experimental parameters and the obtained results for each attenuation. **Figure 7** reports the SKR as a function of the attenuation and the optimized values for signal and decoy intensities.

To demonstrate the long-term stability and operation of our system, we have run it continuously for a period of 63.8 h at a channel attenuation of 11 dB. The system is automatically tuned and stabilized by the control software and electronics.[38] **Figure 8** reports the SKR as a function of time.

As the last step, in order to prove the scalability of the proposed method, we have extended the implementation to high-dimensional QKD protocols. Quantum states having $p > 2$ are carved out from the same phase-randomized optical pulses which have been employed for the $p = 2$. Therefore, the impact of the correlation between adjacent pulses on the performances of a 2D or a 4D QKD protocol is the same.

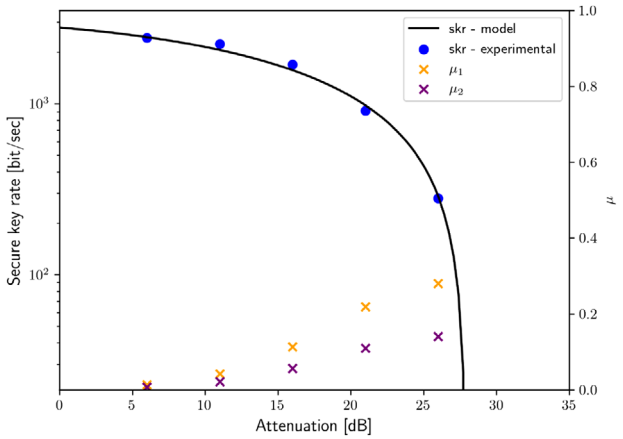

Figure 7. Secure key rate curve (black curve) as a function of the attenuation loss. Blue dots are experimental points acquired at 6, 11, 16, 21, and 26 dB, respectively. Optimized values for signal and decoy intensities are reported in yellow and purple (crosses) as a function of the attenuation value.

Table 2. Contribution to the QBER observed for quantum states in $p = 4$.

Channel loss	6 dB
QBER (phase errors)	2.6 %
QBER (time errors)	0.45 %
QBER (both phase and time errors)	0.43 %

In particular, we have measured the QBER for the 4D states of the Z basis ($z1, z2, z3, z4$) reported in ref. [26]. Table 2 shows the different contributions to the QBER: phase errors, time errors, both phase and time errors). The main contribution is the phase error, that is when $z1$ is detected as $z2$ and $z3$ is detected as $z4$. In conclusion, the reported results are compatible with those already published in ref. [26], where the quantum states were not phase randomized.

6. Conclusions

We have demonstrated a new principle for generating phase-randomized weak coherent states at telecom wavelength, exploiting off-the-shelf fiber-based components and achieving excellent

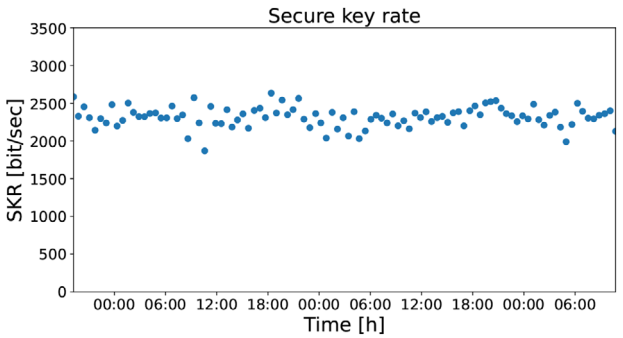

Figure 8. Secret key rate at 11 dB of channel loss attenuation continuously acquired for a duration of 63.8 h.

results in terms of visibility and secret key generation rate. Our results pave the way toward an easier and more secure implementation of a scalable transmitter for QKD systems, which can also be employed for high-dimensional encoding both in fiber and free space.

Acknowledgements

This work was funded by the European Union (ERC, QOMUNE, 101077917, by the Project EQUO (European QUan- tum ecOsystems) which is funded by the European Commis- sion in the Digital Europe Programme under the grant agreement No 101091561, the Project SERICS (PE00000014) un- der the MUR National Recovery and Resilience Plan funded by the European Union – NextGenerationEU, the Project QuONTENT under the it Progetti di Ricerca, CNR program funded by the Consiglio Nazionale delle Ricerche (CNR) and by the European Union – PON Ricerca e Innovazione 2014- 2020 FESR – Project ARS01/00734 QUANCOM, the Project QUID (Quantum Italy Deployment) funded by the European Commission in the Digital Europe Programme under the grant agreement No 101091408.

Conflict of Interest

The authors declare no conflict of interest.

Data Availability Statement

The data that support the findings of this study are available from the corresponding author upon reasonable request.

Keywords

phase randomization, quantum communication, quantum Key Distribution, quantum photonics, security of QKD

Received: July 17, 2023
Revised: November 13, 2023
Published online: December 15, 2023

[1] C. H. Bennett, G. Brassard, in Quantum Cryptography: Public Key Distribution and Coin Tossing. *Proc. IEEE Int. Conf. Computers Systems and Signal Processing*. Bangalore, 10-12 December **1984**, pp. 175–179.
[2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, M. Peev, *Rev. Mod. Phys.* **2009**, *81*, 1301.
[3] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, *Adv. Opt. Photonics* **2020**, *12*, 1012.
[4] J. Qiu, *Nature* **2014**, *508*, 441.
[5] A. De Touzalin, C. Marcus, F. Heijman, I. Cirac, R. Murray, T. Calarco, *European Comission* **2016**, 1 https://ec.europa.eu/futurium/en/content/quantum-manifesto-quantum-technologies.html
[6] G. Lenhart, QKD standardization at ETSI *AIP Conf. Proc.* **2012**, *1469*, 50.
[7] D. Ribezzo, M. Zahidy, I. Vagniluca, N. Biagi, S. Francesconi, T. Occhipinti, L. K. Oxenløwe, M. Lončarić, I. Cvitić, M. Stipčević, Ž. Pušavec, R. Kaltenbaek, A. Ramšak, F. Cesa, G. Giorgetti, F. Scazza, A. Bassi, P. De Natale, F. S. Cataliotti, M. Inguscio, D. Bacco, A. Zavatta, *Adv. Quantum Technol.* **2023**, *6*, 2200061.
[8] G. Brassard, N. Lütkenhaus, T. Mor, B. C. Sanders, *Phys. Rev. Lett.* **2000**, *85*, 1330.
[9] W.-Y. Hwang, *Phys. Rev. Lett.* **2003**, *91*, 057901.
[10] H.-K. Lo, X. Ma, K. Chen, *Phys. Rev. Lett.* **2005**, *94*, 230504.
[11] X.-B. Wang, *Phys. Rev. Lett.* **2005**, *94*, 230503.
[12] M. Lucamarini, K. Patel, J. Dynes, B. Fröhlich, A. Sharpe, A. Dixon, Z. Yuan, R. Penty, A. Shields, *Opt. Express* **2013**, *21*, 24550.
[13] J. F. Dynes, W. W. Tam, A. Plews, B. Fröhlich, A. W. Sharpe, M. Lucamarini, Z. Yuan, C. Radig, A. Straw, T. Edwards, A. J. Shields, *Sci. Rep.* **2016**, *6*, 35149.
[14] B. Fröhlich, M. Lucamarini, J. F. Dynes, L. C. Comandar, W. W.-S. Tam, A. Plews, A. W. Sharpe, Z. Yuan, A. J. Shields, *Optica* **2017**, *4*, 163.
[15] 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, J.-W. Pan, *Nature* **2017**, *549*, 43.
[16] N. T. Islam, C. C. W. Lim, C. Cahall, J. Kim, D. J. Gauthier, *Sci. Adv.* **2017**, *3*, e1701491.
[17] Z. Yuan, A. Plews, R. Takahashi, K. Doi, W. Tam, A. Sharpe, A. Dixon, E. Lavelle, J. Dynes, A. Murakami, M. Kujiraoka, M. Lucamarini, Y. Tanizawa, H. Sato, A. J. Shields, *J. Lightwave Technol.* **2018**, *36*, 3427.
[18] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, F.-Z. Li, J.-F. Wang, Y.-M. Huang, L. Deng, T. Xi, L. Ma, T. Hu, L. Li, N.-L. Liu, F. Koidl, P. Wang, Y.-A. Chen, X.-B. Wang, M. Steindorfer, G. Kirchner, C.-Y. Lu, R. Shu, *et al. Phys. Rev. Lett.* **2018**, *120*, 030501.
[19] 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, H. Zbinden, *Phys. Rev. Lett.* **2018**, *121*, 190502.
[20] D. Gottesman, H.-K. Lo, N. Lutkenhaus, J. Preskill, in *Proc. Int. Symp. Information Theory, 2004. ISIT 2004.* IEEE, Chicago, Illinois, USA **2004**, pp. 136.
[21] Y.-L. Tang, H.-L. Yin, X. Ma, C.-H. F. Fung, Y. Liu, H.-L. Yong, T.-Y. Chen, C.-Z. Peng, Z.-B. Chen, J.-W. Pan, *Phys. Rev. A* **2013**, *88*, 022308.
[22] Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, H.-K. Lo, *Phys. Rev. Lett.* **2014**, *112*, 190503.
[23] Z. Cao, Z. Zhang, H.-K. Lo, X. Ma, *New J. Phys.* **2015**, *17*, 053014.
[24] Z. Yuan, M. Lucamarini, J. Dynes, B. Fröhlich, A. Plews, A. Shields, *Appl. Phys. Lett.* **2014**, *104*, 26.
[25] T. Kobayashi, A. Tomita, A. Okamoto, *Phys. Rev. A* **2014**, *90*, 032320.
[26] I. Vagniluca, B. Da Lio, D. Rusca, D. Cozzolino, Y. Ding, H. Zbinden, A. Zavatta, L. K. Oxenløwe, D. Bacco, *Phys. Rev. Appl.* **2020**, *14*, 014051.
[27] D. Cozzolino, B. Da Lio, D. Bacco, L. K. Oxenløwe, *Adv. Quantum Technol.* **2019**, *2*, 1900038.
[28] A. Boaron, B. Korzh, R. Houlmann, G. Boso, D. Rusca, S. Gray, M.-J. Li, D. Nolan, A. Martin, H. Zbinden, *Appl. Phys. Lett.* **2018**, *112*, 171108.
[29] K.-i. Yoshino, M. Fujiwara, K. Nakata, T. Sumiya, T. Sasaki, M. Takeoka, M. Sasaki, A. Tajima, M. Koashi, A. Tomita, *npj Quantum Inf.* **2018**, *4*, 8.
[30] Z. Yuan, B. Fröhlich, M. Lucamarini, G. Roberts, J. Dynes, A. Shields, *Phys. Rev. X* **2016**, *6*, 031044.
[31] M. Minder, M. Pittaluga, G. L. Roberts, M. Lucamarini, J. F. Dynes, Z. Yuan, A. J. Shields, *Nat. Photonics* **2019**, *13*, 334.
[32] Y. S. Lo, R. I. Woodward, N. Walk, M. Lucamarini, I. De Marco, T. K. Paraïso, M. Pittaluga, T. Roger, M. Sanzaro, Z. L. Yuan, A. J. Shields, *APL Photonics* **2023**, *8*, 036111.
[33] D. Bacco, F. S. Cataliotti, P. De Natale, T. Occhipinti, I. Vagniluca, A. Zavatta, *International Patent WO2022189523A1*, **2022**.

[34] T. K. Paraïso, R. I. Woodward, D. G. Marangon, V. Lovic, Z. Yuan, A. J. Shields, *Adv. Quantum Technol.* **2021**, *4*, 2100062.
[35] C. R. S. Williams, J. C. Salevan, X. Li, R. Roy, T. E. Murphy, *Opt. Express* **2010**, *18*, 23584.
[36] D. Rusca, A. Boaron, F. Grünenfelder, A. Martin, H. Zbinden, *Appl. Phys. Lett.* **2018**, *112*, 171104.
[37] D. Rusca, A. Boaron, M. Curty, A. Martin, H. Zbinden, *Phys. Rev. A* **2018**, *98*, 052336.
[38] D. Bacco, I. Vagniluca, B. Da Lio, N. Biagi, A. Della Frera, D. Calonico, C. Toninelli, F. S. Cataliotti, M. Bellini, L. K. Oxenløwe, A. Zavatta, *EPJ Quantum Technol.* **2019**, *6*, 5.