EPJ Quantum Technology
a SpringerOpen Journal

EPJ.org

RESEARCH Open Access

# A Sagnac-based arbitrary time-bin state encoder for quantum communication applications

Kannan Vijayadharan[1*†], Matías Rubén Bolaños[1†], Marco Avesani[1,2], Giuseppe Vallone[1,2], Paolo Villoresi[1,2] and Costantino Agnesi[1,2*]

*Correspondence:
costantino.agnesi@unipd.it
[1]Dipartimento di Ingegneria dell'Informazione, Università degli Studi di Padova, Via Gradenigo 6B, Padova, 35131, Padova, Italy
[2]Padua Quantum Technologies Research Center, Università degli Studi di Padova, via Gradenigo 6B, Padova, 35131, Padova, Italy
[†]Equal contributors

**Abstract**

Time-bin encoding of quantum information is highly advantageous for long-distance quantum communication protocols over optical fibres due to its inherent robustness in the channel and the possibility of generating high-dimensional quantum states. The most common implementation of time-bin quantum states using unbalanced interferometers presents challenges in terms of stability and flexibility of operation. In particular, a limited number of states can be generated without modifying the optical scheme. Here we present the implementation of a fully controllable arbitrary time-bin quantum state encoder, which is easily scalable to arbitrary dimensions and time-bin separations. The encoder presents high stability and low quantum bit error rate (QBER) for all the tested repetition rates and time-bin separations, without requiring hardware modifications. We further demonstrate phase randomisation and phase encoding without the need for additional resources.

**Keywords:** Quantum communication; Quantum key distribution; Entanglement generation; Time-bin encoding; High-dimensional encoding

## 1 Introduction

The realisation of a large-scale quantum network requires the transfer of quantum information and the generation of entanglement between the end nodes. In this regard, different photonic degrees of freedom, such as polarisation, frequency, transverse spatial modes, or time-bins, are utilised to encode and transmit quantum information [1–3]. The choice of the photonic degree of freedom is highly dependent on the characteristics of the quantum channel employed to connect the different nodes. For example, optical fibres are often used for metropolitan and suburban links. This allows us to scale quantum networks using existing telecommunication infrastructure [4–7]. Although polarisation encoding has been successfully used for Quantum Key Distribution (QKD) in such scenarios [8–11], the presence of aerial fibres renders its implementation quite cumbersome [12]. For this reason, time-bin is a common choice for such scenarios. Furthermore, time-bin encoding can support higher-dimensional protocols [13, 14], which allow higher



Springer

channel capacities and can be advantageous, particularly in highly noisy channels [15]. From a more fundamental perspective, high-dimensional entanglement exhibits stronger non-classical correlations [16].

In time-bin encoding, quantum information is encoded in the photon's arrival time and the relative phase between temporal modes. For time-bin qubits, the two eigenstates of the computational basis are defined by two well-separated arrival times, commonly referred to as the *early* and *late* bins, $|E\rangle$ and $|L\rangle$ respectively, and a general state takes the form $|\Psi\rangle = \alpha\,|E\rangle + e^{i\phi}\beta\,|L\rangle$ (where $\alpha^2 + \beta^2 = 1$). Typically, time-bin states are created by using a pulsed laser and an unbalanced interferometer [4, 17, 18], or by carving pulses from a continuous wave laser using an intensity modulator driven by electrical signals [13, 19–23]. The specific requirements and features of a time-bin encoder depend on its intended use case.

For QKD applications, precise state encoding is required, while also maintaining a controlled phase relation between the bins. Moreover, different receivers might require different time-bin separations. When using the unbalanced interferometer approach, achieving the first point implies the addition of extra intensity modulators to both encode states and implement decoy-state protocols, as well as extra phase modulators for phase encoding. Not only that, but the requirement for a Mach-Zehnder interferometer (MZI) at both the source and receiver sides makes the phase stabilisation process considerably more challenging, which can in turn have detrimental effects on the quantum bit error rate (QBER) over time. Finally, modifying the time-bin separation proves difficult due to optical delay lines allowing for only fine-tuning. On the other hand, the pulse carving approach exploits MZIs that require dedicated stabilisation modules for their correct functioning. Although such modules can be purchased or developed in-house [24], the use of these devices increases the overall complexity and cost of the system. While recent work by Kim et al. [25] demonstrates the creation of a time-bin qubit with full control over the probability amplitudes, for complete generality the dimensionality also needs to be controlled. When using the carving approach for QKD, phase randomisation has to be carefully implemented, since non-randomised qubits can lead to quantum hacking attacks [26], however, not all proof-of-principle QKD experiments take this into account [6].

For entanglement generation applications, a stable phase relation between the early and late states is also required, while several applications, such as the violation of Bell inequalities beyond CHSH, require the creation of a non-maximally entangled state [27]. Using only an unbalanced interferometer allows for the creation of only maximally entangled states, such as the Bell state $|\Phi^+\rangle$, unless additional intensity and phase modulators are added. Moreover, as in the case for QKD, pulse carving approaches also require MZI stabilisation schemes.

In this paper, we propose the architecture for an arbitrary time-bin quantum state encoder using commercial off-the-shelf fibre components. Our scheme provides all the advantages of the carving approach, while also tackling the issue of active stabilisation for Mach-Zehnder modulators by exploiting a modulation scheme based on Sagnac interferometers and taking advantage of its intrinsic stability [28–33]. We then provide experimental results and performance analysis of the proposed encoder, highlighting its capabilities of generating arbitrary time-bin states.

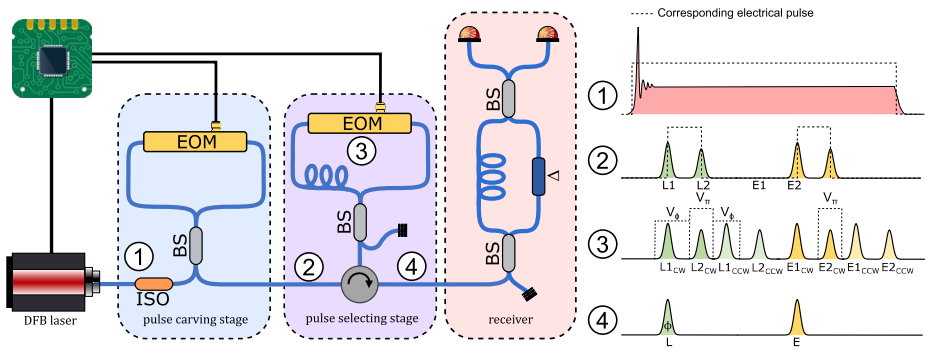


**Figure 1** Experimental design (left) and qualitative explanation of its working principle (right). **(1)** In a first stage, if phase randomisation between subsequent time-bin states is required, the laser can be gain-switched past its settling time until it reaches the steady state. If instead phase randomisation is not required, the laser is switched on in continuous wave mode. **(2)** The laser output is sent through a symmetric Sagnac interferometer with an electro-optic modulator from which two optical pulses are created for every electrical one. **(3)** Each pair of pulses is sent through another Sagnac interferometer where one of the two is extinguished, while an arbitrary phase can be applied to the non-extinguished one. **(4)** The final output of the encoder is now an arbitrary time-bin state with phase encoding. ISO: Isolator, BS: beamsplitter, EOM: electro-optic phase modulator, $\Delta$: fibre stretcher

## 2 Methods

We propose a time-bin state encoder consisting of three components: a distributed feedback (DFB) laser and two Sagnac interferometer-based intensity-phase modulation stages (Fig. 1). In the first step, if phase randomisation is a requirement, we gain-switch a laser by sending sufficiently long electrical current pulses such that it reaches a steady-state emission [34], from where pulses will be carved (see Fig. 1(1)). By gain-switching this way and carving pulses from the steady state, we guarantee that the phase relation between carved pulses is constant, thus creating a coherent superposition between them, while also having phase randomisation between different pairs of gain-switched pulses, a necessary requirement for QKD applications.

In the first intensity modulation stage, the *pulse carving stage*, we use a Sagnac-based intensity modulator in the regime in which the width of the electrical pulse ($\Delta t_{\text{carving}}$) is much larger than the asymmetry in the Sagnac interferometer ($\delta t_{\text{asymm}}$), which for our case corresponds to the intrinsic asymmetries due to the length of the $LiNbO_3$ waveguide in the electro-optic phase modulator (EOM). In this regime, the output interferes constructively only when there is a phase difference $\phi$ between the CW (clockwise) and CCW (counterclockwise) components, thus creating two optical pulses of width $\delta t_{\text{asymm}}$ separated by $\Delta t_{\text{carving}}$ and with amplitude $\propto \sin^2(\phi)$, as represented in Fig. 1(2). Therefore, by modifying the asymmetry in the first stage Sagnac interferometer $\delta t_{\text{asymm}}$, it is also possible to control the output optical pulse width. When taking into account more realistic electrical pulses, where the rising and falling edge are not instantaneous, the width of the optical pulse will be further broadened, with the rising edge shape only affecting the first optical pulse, and the falling edge only affecting the second (Fig. 2). A detailed model is provided in Berra et al. [35]. Although this stage alone could be used to create a 2-dimensional time-bin state, discrepancies in the rising and falling edges of the electrical pulse would be reflected in the shape of the generated optical pulses, increasing distinguishability between the two. This behaviour is unacceptable for any entanglement application, since distinguishability between the time-bin states decreases the visibility of the entire system.

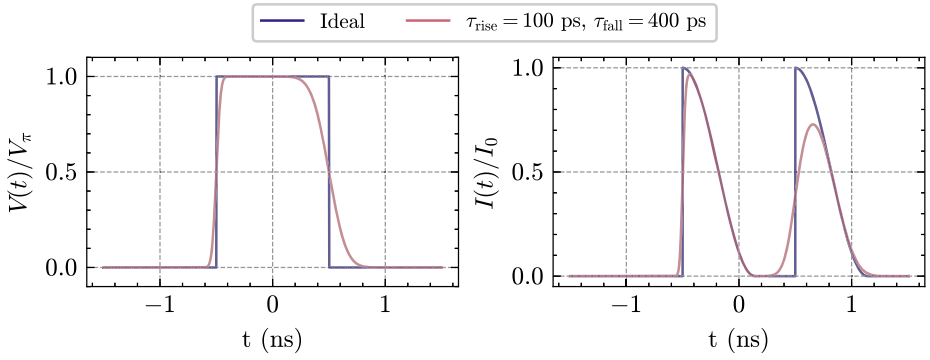


**Figure 2** (Left) Ideal rectangular voltage pulse (in blue) and a non-ideal one with non-zero rising/falling edges (in red) used to drive the pulse carving stage. (Right) Optical pulses obtained with both electrical pulses at the output of the pulse carving stage. For visualisation purposes, the falling edge of the non-ideal pulse was deliberately increased

To remove the distinguishability from the pulse carving stage, we added a second intensity modulation stage, the *pulse selecting stage*, in which one of the two optical pulses generated by a single electrical pulse is extinguished. To do so, we use an intentionally unbalanced Sagnac interferometer by adding a fixed-length optical fibre (equivalent to an optical delay of $\delta t_{\text{asymm}_2}$) to one of the branches, after which we apply a $\pi$ phase shift to either the CW or the CCW component, as shown in Fig. 1(3) [28]. Following a similar logic to the pulse carving stage, since the output pulse amplitude is $\propto \sin^2(\phi)$, by applying a relative phase shift of $\pi$, the pulse is effectively extinguished, up to an extinction ratio that is given by

$$ER(T) = 10\log_{10}\left|\frac{1}{2T-1}\right|^2, \tag{1}$$

with $T$ the transmittance of the beamsplitter [28]. It is worth noting that at least 30 dB of extinction ratio is achievable for $T \in [0.484, 0.516]$, showing that good quality of pulse selection can be achieved even taking into account manufacturing errors in the beamsplitter.

With both stages, any $d$-dimensional time-bin state can be created by sending $d$ pulses of width $\Delta t_{\text{carving}}$ separated by $\Delta t$ to the pulse carving stage, followed by extinguishing one of the two optical pulses created by each electrical pulse in the pulse selecting stage, as shown in Fig. 1(4). Assuming a train of rectangular pulses in the pulse carving stage defined by

$$V(t) = \sum_i^d V_i \Pi\left(\frac{t - i\cdot\Delta t}{\Delta t_{\text{carving}}} - t_0\right), \tag{2}$$

with $\Pi\left(\frac{t}{\Delta t}\right)$ a rectangular pulse of width $\Delta t$ and unit amplitude centred at $t = 0$, each pulse will create two optical pulses of width $\delta t_{\text{asymm}}$ separated by $\Delta t_{\text{carving}}$ with amplitude $\propto sin^2\left(\frac{V_i}{V_\pi}\pi\right)$, where $V_\pi$ corresponds to the voltage necessary to apply a phase shift of $\pi$ on the electro-optic modulator. Then, after pulse selecting one of the two generated

optical pulses per electrical pulse sent, the resulting quantum state corresponds to

$$|\Psi\rangle = \sum_{i}^{d} \alpha_i \, |t_0 + i \cdot \Delta t\rangle = \sum_{i}^{d} \alpha_i \, |t_i\rangle \,, \tag{3}$$

where the state $|t_i\rangle$ corresponds to a weak coherent state centred at time $t_i$ and $\alpha_i$ is such that $\alpha_i^2 = \frac{a_i^2}{\sum_j a_j^2}$, where $a_i^2 = \sin^2\left(\frac{V_i}{V_\pi}\pi\right)$. Moreover, we have that $\sum_i a_i^2 \propto \langle n \rangle$, with $\langle n \rangle$ the average number of photons of the output state, allowing the encoding of different mean number of photons by controlling the values of $V_i$. Lastly, by applying $V_\phi$ to both the CW and the CCW components of the non-extinguished pulse on the pulse selecting stage, the resulting quantum state becomes

$$|\Psi\rangle = \sum_{i}^{d} e^{-i\phi_i} \alpha_i \, |t_i\rangle \,, \tag{4}$$

making our design capable of creating any arbitrary time-bin encoded qudit, including arbitrary dimension, time-bin separation, and phase encoding, all while requiring only two EOMs.

Moreover, for QKD applications where decoy state protocols are required, whereas current systems have to include extra intensity modulators, our encoder is capable of adding decoy states by tuning the value of $\sum_i a_i^2 \propto \langle n \rangle$ on the pulse carving stage.

The use of two stages of Sagnac modulators limits the maximum achievable repetition rate of the system. From the pulse carving stage, encoding a $d$-dimensional time-bin state requires $d$ electrical pulses of width $\Delta t_{\text{carving}}$ with their rising edges separated by $\Delta t$, where $\Delta t_{\text{carving}} < \Delta t$, which sets the maximum achievable repetition rate at $R = \left[(d-1)\Delta t + \Delta t_{\text{carving}} + \delta t_{\text{asymm}}\right]^{-1}$. Then, the pulse selection stage works for arbitrary states as long as electrical pulses can be applied to a single optical pulse without affecting the rest. This condition is easily applied when

$$\delta t_{\text{asymm}_2} > (d-1)\Delta t + \Delta t_{\text{carving}+\delta t_{\text{asymm}}} \tag{5}$$

(i.e., all counter-clockwise components are after the clockwise ones),

$$\delta t_{\text{asymm}_2} < \Delta t - \Delta t_{\text{carving}} \tag{6}$$

(i.e. the counter-clockwise component of the early pulses are between the clockwise component of the early and late pulses), or

$$\delta t_{\text{asymm}_2} < \Delta t_{\text{carving}} \tag{7}$$

(i.e. the counter-clockwise component of each pulse is placed before the clockwise component of the next pulse.), all of which give an upper bound on the achievable repetition rate for the states given by

$$R \leq \frac{1}{(d-1)\Delta t + \Delta t_{\text{carving}} + \delta t_{\text{asymm}_2} + \delta t_{\text{asymm}}},$$

**Table 1** Examples for achievable repetition rates assuming $\Delta t = 2$ ns, $\Delta t_{\text{carving}} = 1$ ns and $\delta t_{\text{asymm}} = 0.32$ ns. For the configurations associated to Eq. (6) and (7), a single valid value was chosen for simplicity

| Configuration | $\delta t_{\text{asymm}_2}$ | $R$ |
|---|---|---|
| Eq. (5) | 6.64 ns | ≈ 150 MHz |
| Eq. (6) | 1.5 ns | ≈ 207 MHz |
| Eq. (7) | 0.5 ns | ≈ 260 MHz |

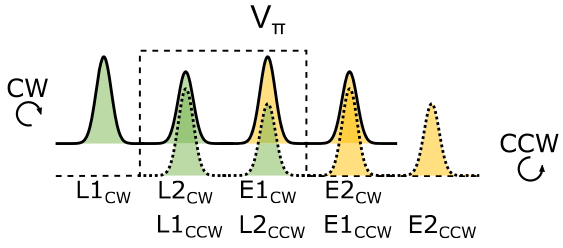


**Figure 3** Pulse selecting scheme to create the $|-\rangle$ state at a higher repetition rate. This figure is analogous to the one represented in Fig. 1(3)

which is maximized for the third configuration. However, this requires very short electrical pulses and precise alignment both of optical and electrical pulses, making the first and second configurations easier to implement, albeit at a loss on the maximum achievable repetition rate (see Table 1).

Nevertheless, for QKD applications, it is enough to create three states to obtain a secure BB84 protocol [36], which is possible with a slightly different hardware condition in which the second stage asymmetry

$$\delta t_{\text{asymm}_2} \sim \delta t_{\text{asymm}} \sim \Delta t_{\text{carving}}. \tag{8}$$

In this way, it is possible to create the $|-\rangle$ state simply by applying a single pulse during the pulse selecting stage (Fig. 3). This method allows for the three-state encoding for repetition rates $R < \frac{1}{5\delta t_{\text{asymm}}}$, while otherwise it would be upper bounded by $R < \frac{1}{\Delta t + \Delta t_{\text{carving}} + \delta t_{\text{asymm}_2} + \delta t_{\text{asymm}}}$. Moreover, if phase encoding is not required, it is possible to take the destructive port on the pulse selecting stage to relax the $V_\pi$ requirement for the EOM while also reducing the intrinsic QBER of the system.

*Experimental implementation* The encoder was implemented at 1550 nm and 780 nm, two relevant wavelengths in several quantum communication applications, particularly for QKD implementations in both free-space and fibre channels, since telecommunication wavelengths allow the use of fibre already deployed in the metropolitan area, while 780 nm is useful for both free-space satellite channels [37, 38], and to generate telecommunications wavelength entangled photons [39]. For both the 1550 nm and 780 nm encoders, we used a DFB laser as source and two EOMs inside the Sagnac loops for both modulation stages. For the first Sagnac modulator configuration, the EOM was placed symmetrically in the loop, exploiting the inherent fabrication imperfections of both fibre paths, leading to an estimated $\delta t_{\text{asymm}} \approx 320$ ps For both cases, to feed the electrical signals, we used an FPGA UltraScale+ development board by Xilinx, from which we used its balun-free

DAC channels, each coupled to an RF amplifier placed before each EOM. For all cases with $\Delta t > 1$ ns, we chose $\Delta t_{\text{carving}} = 1$ ns, otherwise reducing it to $\Delta t_{\text{carving}} = 500$ ps for the cases with $\Delta t = 1$ ns.

## 3 Results and discussion

The performance of the proposed time-bin encoder scheme is characterised by a series of tests, including both time-of-arrival measurements with the detector placed directly after the encoder output and interferometric measurements with time-bin receivers. From these measurements, it is possible to retrieve the relevant information on a time-bin qubit. From time-of-arrival measurements, the probability amplitudes of any $d$-dimensional state, i.e. $|\alpha_i|^2$ from equation (4), can be directly measured. On the other hand, by using the Franson interferometer, which is an unbalanced Mach-Zehnder interferometer (uMZI), and controlling the relative phase between both arms of the interferometer, it is possible to measure the relative phases on the state, i.e., $\phi_i$ from equation (4). In the first instance, to control the relative phase in the receiver, a software-controlled piezoelectric fibre stretcher was used (see receiver in Fig. 1).

### 3.1 Phase stability

The phase stability of the encoder is characterised by measuring the phase drift of the generated time-bin superposition over an extended measurement period. To do this, we first create a time-bin superposition state (the $|-\rangle$ state in this case) using the encoder and compare the phase drift against the same state created using an uMZI. For a fair comparison, in the latter case, a single pulse carved by the encoder is used to create the superposition state using the uMZI.

Due to phase instabilities, the measured state at the receiver is

$$|\psi\rangle_j = \frac{1}{\sqrt{2}}(|E\rangle - e^{i\phi_s}|L\rangle), \tag{9}$$

where $\phi_s$ is the phase drift of the source (ideally $\phi_s = 0$). The phase $\phi_s$ is estimated from the receiver measurements for both cases, and the phase stability is estimated. Even though the measurements for both cases were taken at different times, they were done one immediately after the other under the same conditions. For both cases, the uMZIs in the receiver side were properly passively stabilised in a closed isolated container and left to stabilise for $\sim 1$ hour. To quantify the phase stability over time, the Allan deviation $\sigma$, defined such that

$$\sigma^2(\tau) = \frac{1}{2\tau^2}\left\langle (x_{n+2} - 2x_{n+1} + x_n)^2 \right\rangle \tag{10}$$

where $x_i$ is the $i$-th of the phase values spaced by the measurement interval $\tau$ (Fig. 4). The results show significant phase stability using the encoder, highlighting its advantage over an unbalanced interferometer to create time-bin states. It should be noted that the unbalanced interferometer at the source could be further stabilised to improve its stability over time, but doing so implies extra resources and complexity of the system [40]. The purpose of this characterisation is to highlight the fact that, when little to no stabilisation scheme is used on the source side (be it with the encoder or uMZI), the encoder presents higher intrinsic stability.

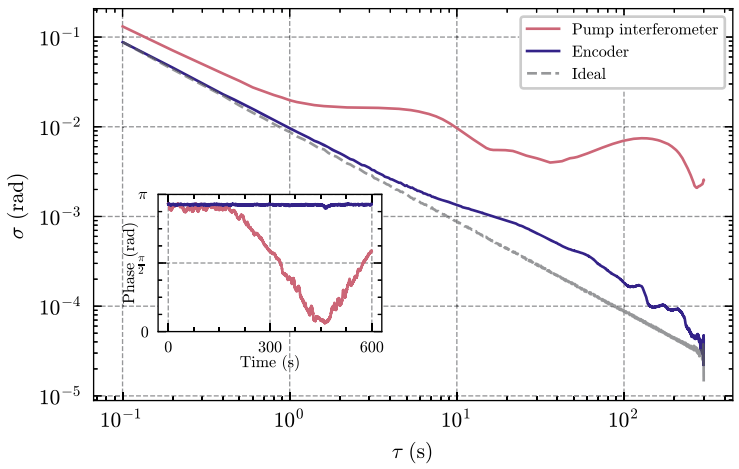


**Figure 4** Allan deviation plot obtained at the receiver for a time-bin state generated with our encoder (in blue) and with an unbalanced interferometer (in red), both compared with the deviation obtained for a random walk signal sampled every 100 ms with 5 mrad phase diffusion. Inset: Measured phase as a function of time from which the Allan deviation was obtained

### 3.2 QKD experiment

To demonstrate the capabilities of our encoder while highlighting its versatility for different time-bin receivers, we used the proposed time-bin encoder to generate a fixed pseudo-random sequence of 512 symbols to simulate a BB84 QKD implementation with decoy state. To simulate a QKD system as faithfully as possible, the system was prepared with typical values of decoy state BB84 experiments [41]. With this in mind, we chose $\nu/\mu \sim 0.3$, with $\nu = 0.2$ and $\mu = 0.6$ the mean number of photons for decoy and signal pulses respectively, and we generated the 512-symbol sequence with $p_Z = 87\%$ and $p_X = 13\%$ with $p_{Z(X)}$ the probability to generate a state on the key (check) basis.

As a first instance, to demonstrate the best achievable performance for our encoder, we performed the 4-state version of the BB84 protocol at a fixed 100 MHz repetition rate with a more limiting, but better performing, hardware configuration, corresponding to equation (5). We measured QBER on both the time-of-arrival basis (i.e. the key basis) and on the superposition basis (i.e. the check basis) for an hour to evaluate the performance and long-term stability of the device (Fig. 5). From this measurement, the secret key rate was estimated throughout the duration, obtaining an average SKR = 101.66 ± 5.31 kb/s at 25 dB of total losses. To estimate the secret key rate, decoy state bounds were applied, taking into account finite-key effects [41]. Moreover, by performing the measurement in a long pseudo-random sequence, we can evaluate possible crosstalk or patterning effects. It was observed that the QBER values for both bases were kept under the 1% threshold for most of its runtime, even with a non-fully optimised active phase stabilisation scheme on the receiver. By performing a first-neighbour patterning analysis (Fig. 6), we concluded that there is no complete distinguishability by changing the preceding symbol in the sequence. It is worth noting that the standard deviation of 0 for the $|+\rangle$, $|-\rangle$ and $|-\rangle$, $|+\rangle$ sequences is due to that combination appearing only once in the 512-symbol sequence, while the $|+\rangle$, $|+\rangle$ sequence does not appear at all, thus not having an associated QBER value. Then, as a second instance, we performed a 3-state version of the BB84 protocol using both states of the key basis ($|E\rangle$ and $|L\rangle$) and only one state for the check basis ($|-\rangle$).

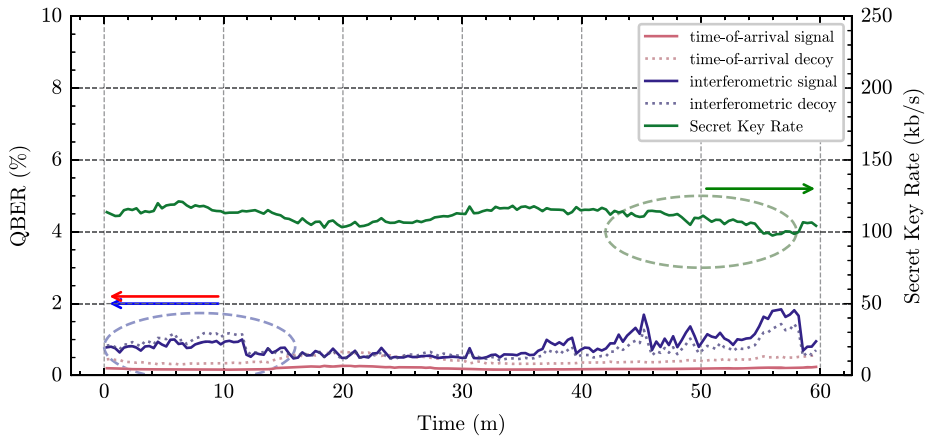


**Figure 5** QBER on the *Z* and *X* basis for a 512-symbol sequence over time. In green, associated with the right axis, the SKR obtained over time

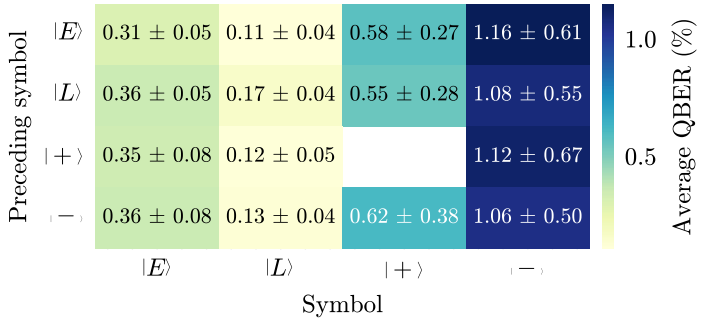


**Figure 6** Average QBER obtained for each symbol type for all possible preceding symbols. Due to low statistics of |+⟩ and |−⟩ symbols, combination of those two symbols are either not present or have considerably large relative error

The measurements were done with different repetition rates $R = 100, 125, 200$ MHz for a fixed time-bin separation of $\Delta t = 2$ ns (Fig. 7b), and for different $\Delta t = 1, 2, 4$ ns (and the corresponding receivers) for a fixed repetition rate of 100 MHz (Fig. 7a). We observed that on average the QBER value was kept mostly under 1% for the *Z* basis, while under 2% for the *X* basis. By increasing $\Delta t$, we observed an overall improvement over the measured QBER, due to larger time-bins making alignment of the electrical signal less challenging. It was also observed that changing the repetition rate of the system does not significantly affect QBER.

### *3.2.1 Phase randomisation*

Phase randomisation between consecutive time-bin states is a requirement for QKD applications, with a non-optimal phase randomisation negatively affecting secret key generation [42]. The phase randomisation of the time-bin states is obtained by carefully gain-switching the laser and fully depleting the cavity before carving the next state to ensure that the phase is uncorrelated with the preceding one. From a direct measurement of the gain-switched laser pulse, we estimated the settling time $t_{ss}$ (i.e. the time required for the laser to reach the steady-state after gain-switching) and the off time $t_{off}$ (i.e. the time re-

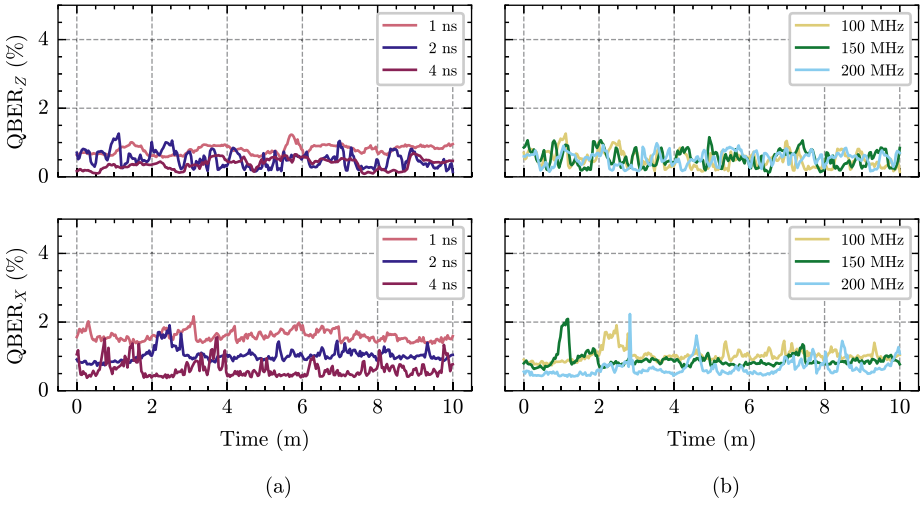


**Figure 7** QBER on the $Z$ and $X$ basis for a 512-symbol sequence over time: (a) for different time-bin separation $\Delta t$ with a fixed repetition rate $R = 100$ MHz, and (b) for different repetition rate $R$ with a fixed time-bin separation $\Delta t = 2$ ns

quired for the laser to fully deplete the cavity). These parameters provide an upper bound for the repetition rate of the system, such that $R < (t_{ss} + t_{off})^{-1}$, so we characterised it with the minimum $t_{off}$ possible such that phase randomisation occurred.

To characterise phase randomisation using the same time-bin receiver as in the QKD experiment, the electrical pulses were carefully aligned such that the early pulse is carved close to the laser turning off, while the late pulse is carved from the consecutive laser pulse, guaranteeing that $\Delta t > t_{ss} + t_{off}$. On the other hand, to study the non-phase randomised scenario, we first carved the time-bin state from a single gain-switched laser pulse and, in a later stage, carved it from a continuous wave laser. We then verified the phase randomisation of the pulses by performing interferometric measurements using the time-bin receiver and sending states at a repetition rate of 100 MHz.

When a phase scan is performed on two phase randomised pulses by inducing a relative phase between them, there is a low visibility of the interference fringe $V_{pr} = 0.8\%$, while the visibility of the non-phase randomised pulses when carving from a single gain-switched pulse was obtained to be $V_{npr} = 92.4\%$. As this visibility value was considerably lower than expected, the same analysis was performed when carving the time-bin states from the same laser in continuous wave operation, for which the visibility was obtained to be $V_{npr} = 98.7\%$ (Fig. 8). We attributed this discrepancy in visibilities to the fact that the laser spectrum is modified when gain-switching, increasing the linewidth of the laser and, as such, reducing phase stability. To verify this behaviour, we obtained the spectrum of the DFB laser both with and without gain switching it using an AQ6370D Optical Spectrum Analyser by Yokogawa (Fig. 9). Nevertheless, using our device's phase encoding scheme, with the addition of a Quantum Random Number Generator (QRNG), it is possible to perform phase randomisation on the states without gain-switching techniques and without requiring an additional phase modulator. Due to the embedded system nature of the FPGA development board, QRNG-based phase encoding to perform phase randomisation is fairly straightforward to implement [43, 44].

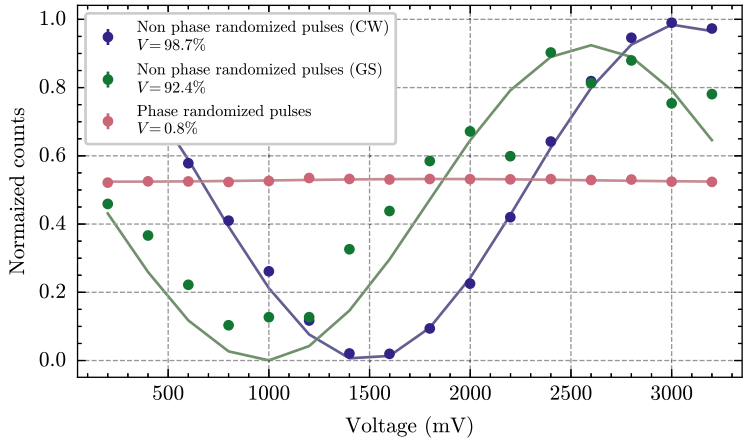


**Figure 8** Phase scan applied to: phase randomised pulses (in red), non-phase randomised pulses when carving from a continuous wave laser (in blue), and non-phase randomised pulses when carving from a gain-switched laser after reaching the steady state (in green)

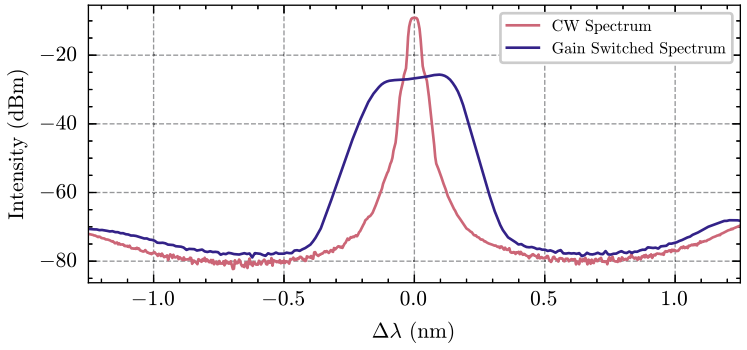


**Figure 9** Comparison of the spectra of the DFB laser in gain-switched mode (in red) and continuous-wave mode (in blue). The x-axis is the relative shift around the central wavelength

As shown by Currás-Lorenzo et al. in [42], a non-zero degree of phase correlation reduces the maximum achievable key rate. Following the method in [45], by estimating the visibility for both scenarios, we obtained a degree of phase correlation $p_c^* = 0.008$, implying a *source quality* $q = 0.97$. We attribute this non-optimal source quality to the fact that we set the $t_{\text{off}}$ as short as possible, and we expect the source quality to improve for lower repetition rates and longer $t_{\text{off}}$.

### 3.3 High-dimensional state encoding

To demonstrate the capability to create arbitrary high-dimensional states described by Eq. (4), a sequence of four-dimensional time-bin states composed of

$$|\psi_0^4\rangle = \frac{|t_0\rangle + |t_1\rangle + |t_2\rangle + |t_3\rangle}{2},$$

$$|\psi_1^4\rangle = \frac{|t_0\rangle + e^{-\pi i/3}|t_1\rangle + e^{-2\pi i/3}|t_2\rangle + e^{-\pi i}|t_3\rangle}{2},$$

was prepared and measured at a repetition rate of 40 MHz with $\Delta t = 3$ ns.

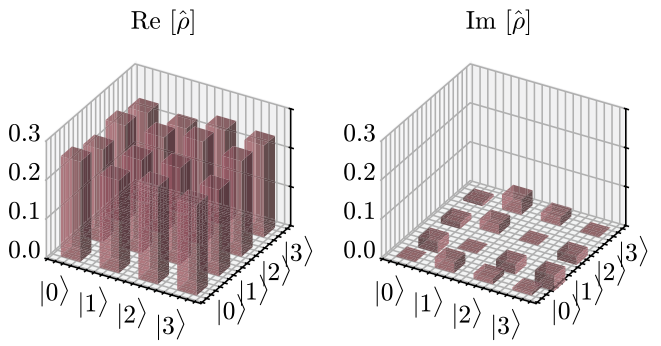


**Figure 10** Reconstructed density matrix for $|\psi_0^4\rangle$

To perform quantum state tomography, we measured the time-bin state using cascaded MZIs with delays of $\Delta t$ and $2\Delta t$, and phase differences $\phi_1$ and $\phi_2$. To reconstruct the complete density matrix, measurements corresponding to the 4-dimensional Pauli matrices $\sigma_X$, $\sigma_Y$ and $\sigma_Z$ are required [46]. By placing a 90:10 beamsplitter before the interferometer and measuring the direct time of arrival of the input state, the time-bin basis or $\sigma_Z$ can be measured. The interference measurements from the cascaded uMZI correspond to $\sigma_X$ or $\sigma_Y$ depending on the phases $\phi_1$ and $\phi_2$ being 0 or $\frac{\pi}{2}$ respectively.

As demonstrated in [19], only two detectors are required to perform a full state tomography on a four-dimensional time-bin state using cascaded MZIs. Additionally, in order to mitigate the experimental challenge of fluctuation of the photon count rate and phase drift between different measurements, we implemented a simultaneous measurement of the three bases using a single high-speed EOM external to the uMZI and synchronised with the source. By applying a four-symbol phase sequence to the state at a rate one-fourth that of the source generation rate, the measurement settings are effectively changed between subsequent time-bins.

The four-symbol phase sequence was engineered to be able to reconstruct all relevant $\langle\sigma_i\rangle$ with $i = X, Y, Z$. The first symbol does not apply phase to the state, allowing the extraction of $\langle\sigma_X\rangle$ from the interference fringes of the cascaded interferometers. Meanwhile, the following 3 symbols apply a $\phi = \pi/2$ phase over the pulses corresponding to $|t_0\rangle$ and $|t_k\rangle$ with $k = 1, 2, 3$ for each symbol, respectively. By measuring the amplitudes of a particular subset of the interference fringes, all expectation values $\langle\sigma_Y\rangle$ can be reconstructed.

From the detection probabilities corresponding to the measurement settings applied, the density matrix $\rho$ of the measured state was reconstructed by maximum likelihood estimation (Fig. 10). The fidelity of the measured state was calculated by $\mathcal{F} = \langle\psi_{\text{ideal}}|\rho|\psi_{\text{ideal}}\rangle$ to be 0.969 with respect to $|\psi_0^4\rangle$. We attribute the infidelity to a slight mismatch in the applied phase $\phi$ from the desired value of $\pi/2$ and phase drift in the measurement interferometer, as is evident from the imaginary part of $\rho$ in Fig. 10.

A different approach was used to characterise the measured state for $|\psi_1^4\rangle$. Instead of the complete set of 16 measurements required for state tomography, a reduced subset was used, measuring only the overlap with the ideal state to calculate the fidelity as $\mathcal{F} = |\langle\psi|\psi_{\text{ideal}}\rangle|^2$, resulting in $\mathcal{F} = 0.989 \pm 0.011$. It is to be noted that in an adversarial scenario or without prior knowledge of the prepared state, a full tomography is required since this assumes purity of the state.

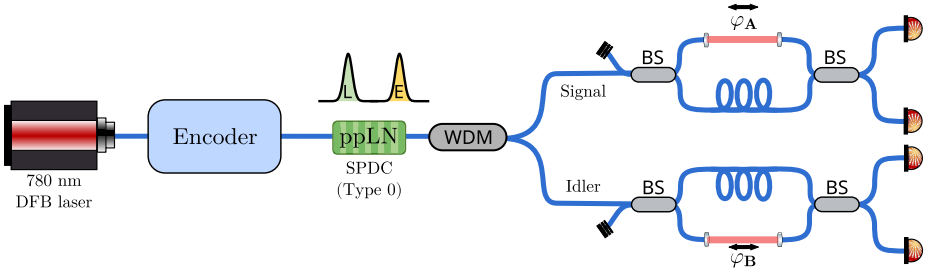


**Figure 11** Simplified experimental design for the time-bin entanglement scheme. WDM: Wavelength Division Multiplexing filter, BS: beamsplitter

### 3.4 Time-bin entanglement

A time-bin entangled state is created by pumping a nonlinear crystal with a time-bin qubit to generate a pair of entangled photons by spontaneous parametric downconversion (SPDC) process.

Here, we start with an equal superposition state created by the encoder as the pump photon with the state

$$|\psi\rangle_{\text{pump}} = \frac{1}{\sqrt{2}}(|E\rangle + e^{i\phi}|L\rangle), \tag{11}$$

to then generate the maximally entangled $|\Phi^+\rangle$ state (Fig. 11). The repetition rate and bin separation were 200 MHz and 2 ns, respectively. A periodically poled lithium niobate waveguide is used for Type-0 SPDC process, producing the state

$$|\psi\rangle_{\text{PDC}} = |\Phi^+\rangle = \frac{1}{\sqrt{2}}(|E\rangle_1|E\rangle_2 + e^{i\phi}|L\rangle_1|L\rangle_2). \tag{12}$$

The entangled photon pairs are separated by wavelength filtering and sent to the two state analysers to perform projective measurements on the state. The state analysers are identical unbalanced interferometers with a delay equal to the bin separation of 2 ns. By post-selecting on the middle peak in the detection histogram, measurements are performed on the two photons in the superposition basis with the coincidence probability given by $\frac{1}{4}(1 + \cos(\phi_A + \phi_B))$, where $\phi_A$ and $\phi_B$ correspond to the local phase shift introduced by each state analyser. By performing a phase scan on one of the receiver interferometers using a nanometric translation stage, we observe a visibility of up to 96% in the coincidence count rate (Fig. 12), certifying the entanglement and corresponding to a CHSH violation with $S = 2.72 \pm 0.037$.

For certifying the entanglement, only the detection events exhibiting quantum interference were postselected. This opens up the postselection loophole in Bell tests [47], which can be circumvented by using fast optical switches [48] or specialised interferometric geometries [39], but this is beyond the scope of this paper. Furthermore, while we have only shown the scenario of a maximally entangled state, the encoder is capable of creating non-maximally entangled states as well using unequal arbitrary superposition states to pump the downconversion process. However, measurement of such states requires more complex receiver architectures that involve high-speed optical switches and reconfigurable beamsplitters.

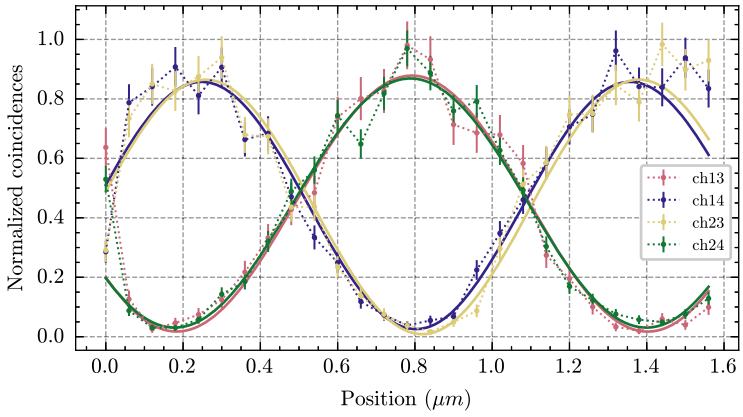


**Figure 12** Modulation of the rate of postselected coincidences between the signal and idler photons with respect to the relative phase introduced in the receiver interferometer. Measured data from the four detector channels plotted along with a cosine fit

## 4 Conclusion

We have demonstrated a novel arbitrary time-bin state encoder with a low bit error rate and high long-term stability. Our device shows higher stability over time compared with an unbalanced interferometer to create time-bin states, even without any active stabilisation methods. The pulses carved from a continuous-wave laser allowed for higher spectral purity and low-chirp operation compared to directly modulated lasers, and tunability in pulse duration compared to mode-locked lasers. The inherent stability of the Sagnac interferometer also leads to stable long-term operation that mitigates the bias drift problem in Mach-Zehnder modulator-based approaches for carving pulses.

We have shown the capability of the encoder to create arbitrary time-bin qudits, including phase encoding, without increasing the design complexity and number of optical components. The validity of the generated qubits was confirmed by efficient high-dimensional tomographic measurements using two cascaded interferometers and a single external EOM capable of performing measurements on all the required bases.

Moreover, the ability to encode relative phases in the time-bin state would allow, by including an extra QRNG, to phase-randomise subsequent states without affecting the source spectrum, as would happen for gain-switching regimes. The capability to not affect the spectrum has a direct impact, for example, on the quantum bit error rate (QBER) of the source for QKD applications, as it depends on the interference visibility, which we have shown is lower for gain-switching regimes, implying a higher intrinsic QBER.

We demonstrated the applicability of the encoder for quantum communication applications, in particular for entanglement generation and QKD, with reconfigurability of parameters while maintaining a low error rate. We have shown that the encoder scheme can be implemented at different wavelengths, enabling its usage as a pump source for entanglement generation. Furthermore, operations at different repetition rates and with different time-bin separations $\Delta t$ have been demonstrated for QKD without requiring any hardware modification in the source. This shows the flexibility of the system to conform to the requirements of different time-bin receivers, some of which might already be deployed. Thus, the arbitrary time-bin state preparation we have demonstrated here allows for adaptability to existing/deployed time-bin quantum communication systems.

**Acknowledgements**
The authors would like to thank Davide G. Marangon for fruitful discussions. The authors would like to thank Marco Calabrese and Matteo Buffolo for lending us the Optical Spectrum Analyser.

**Author contributions**
K.V. and M.A. conceived the original idea for the encoder. K.V., M.R.B. and C.A. designed the system and the experiments. M.R.B. designed the control electronics. K.V., M.R.B. and C.A. performed the measurements and analysed the data. M.A., G.V., P.V. and C.A. supervised the experiments. All authors discussed the results. C.A., K.V. and M.R.B wrote the manuscript with inputs from all authors.

**Funding information**
This work was supported by the European Union's Horizon Europe Framework Programme under the Marie Sklodowska Curie Grant No. 956071, Project AppQInfo; Grant No. 101070168, Project HyperSpace; and Grant No. 101072637, Project Quantum-Safe Internet (QSI).

**Data availability**
No datasets were generated or analysed during the current study.

## Declarations

**Ethics approval and consent to participate**
Not applicable.

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

**Competing interests**
The authors declare no competing interests.

Received: 11 July 2025 Accepted: 8 October 2025 Published online: 10 November 2025

**References**

1. Pirandola S, Andersen UL, Banchi L, Berta M, Bunandar D, Colbeck R, Englund D, Gehring T, Lupo C, Ottaviani C, Pereira JL, Razavi M, Shaari JS, Tomamichel M, Usenko VC, Vallone G, Villoresi P, Wallden P. Advances in quantum cryptography. Adv Opt Photonics. 2020;12(4):1012–236. https://doi.org/10.1364/AOP.361502.
2. Jiang Y-F, Wei K, Huang L, Xu K, Sun Q-C, Zhang Y-Z, Zhang W, Li H, You L, Wang Z, Lo H-K, Xu F, Zhang Q, Pan J-W. Remote blind state preparation with weak coherent pulses in the field. Phys Rev Lett. 2019;123:100503. https://doi.org/10.1103/PhysRevLett.123.100503.
3. Cao X-Y, Li B-H, Wang Y, Fu Y, Yin H-L, Chen Z-B. Experimental quantum e-commerce. Sci Adv. 2024;10(2):3258. https://doi.org/10.1126/sciadv.adk3258.
4. Boaron A, Boso G, Rusca D, Vulliez C, Autebert C, Caloz M, Perrenoud M, Gras G, Bussières F, Li M-J, Nolan D, Martin A, Zbinden H. Secure quantum key distribution over 421 km of optical fiber. Phys Rev Lett. 2018;121:190502. https://doi.org/10.1103/PhysRevLett.121.190502.
5. Dynes J, Wonfor A, Tam W-S, Sharpe A, Takahashi R, Lucamarini M, Plews A, Yuan Z, Dixon A, Cho J, et al. Cambridge quantum network. npj Quantum Inf. 2019;5(1):101. https://doi.org/10.1038/s41534-019-0221-4.
6. Ribezzo D, Zahidy M, Vagniluca I, Biagi N, Francesconi S, Occhipinti T, Oxenløwe LK, et al. Deploying an inter-European quantum network. Adv Quantum Technol. 2022;6(2):2200061. https://doi.org/10.1002/qute.202200061.
7. Martin V, Brito JP, Ortíz L, Mendez R, Buruaga J, Vicente R, Sebastian-Lombrana A, Rincon D, Perez F, Sanchez C, et al. Madqci: a heterogeneous and scalable sdn-qkd network deployed in production facilities. npj Quantum Inf. 2024;10(1):80. https://doi.org/10.1038/s41534-024-00873-2.
8. Avesani M, Calderaro L, Foletto G, Agnesi C, Picciariello F, Santagiustina FBL, Scriminich A, Stanco A, Vedovato F, Zahidy M, Vallone G, Villoresi P. Resource-effective quantum key distribution: a field trial in Padua city center. Opt Lett. 2021;46(12):2848–51. https://doi.org/10.1364/OL.422890.
9. Agnesi C, Giacomin M, Sartorato D, Artuso S, Vallone G, Villoresi P. In-field comparison between G.652 and G.655 optical fibres for polarisation-based quantum key distribution. IET Quantum Commun. 2024;5(4):567–74. https://doi.org/10.1049/qtc2.12095.
10. Du Y, Zhu X, Hua X, Zhao Z, Hu X, Qian Y, Xiao X, Wei K. Silicon-based decoder for polarization-encoding quantum key distribution. Chip. 2023;2(1):100039. https://doi.org/10.1016/j.chip.2023.100039.
11. Wei K, Hu X, Du Y, Hua X, Zhao Z, Chen Y, Huang C, Xiao X. Resource-efficient quantum key distribution with integrated silicon photonics. Photon Res. 2023;11(8):1364–72. https://doi.org/10.1364/PRJ.482942.
12. Li D-D, Gao S, Li G-C, Xue L, Wang L-W, Lu C-B, Xiang Y, Zhao Z-Y, Yan L-C, Chen Z-Y, Yu G, Liu J-H. Field implementation of long-distance quantum key distribution over aerial fiber with fast polarization feedback. Opt Express. 2018;26(18):22793–800. https://doi.org/10.1364/OE.26.022793.
13. Islam NT, Lim CCW, Cahall C, Kim J, Gauthier DJ. Provably secure and high-rate quantum key distribution with time-bin qudits. Sci Adv. 2017;3(11):1701491. https://doi.org/10.1126/sciadv.1701491.
14. Ecker S, Bouchard F, Bulla L, Brandt F, Kohout O, Steinlechner F, Fickler R, Malik M, Guryanova Y, Ursin R, Huber M. Overcoming noise in entanglement distribution. Phys Rev X. 2019;9:041042. https://doi.org/10.1103/PhysRevX.9.041042.
15. Sheridan L, Scarani V. Security proof for quantum key distribution using qudit systems. Phys Rev A. 2010;82:030301. https://doi.org/10.1103/PhysRevA.82.030301.

16. Kaszlikowski D, Gnaciński P, Żukowski M, Miklaszewski W, Zeilinger A. Violations of local realism by two entangled *N*-dimensional systems are stronger than for two qubits. Phys Rev Lett. 2000;85:4418–21. https://doi.org/10.1103/PhysRevLett.85.4418.
17. Marcikic I, Riedmatten H, Tittel W, Scarani V, Zbinden H, Gisin N. Time-bin entangled qubits for quantum communication created by femtosecond pulses. Phys Rev A. 2002;66:062308. https://doi.org/10.1103/PhysRevA.66.062308.
18. Sax R, Boaron A, Boso G, Atzeni S, Crespi A, Grünenfelder F, Rusca D, Al-Saadi A, Bronzi D, Kupijai S, Rhee H, Osellame R, Zbinden H. High-speed integrated qkd system. Photon Res. 2023;11(6):1007–14. https://doi.org/10.1364/PRJ.481475.
19. Takesue H, Noguchi Y. Implementation of quantum state tomography for time-bin entangled photon pairs. Opt Express. 2009;17(13):10976–89. https://doi.org/10.1364/OE.17.010976.
20. Vagniluca I, Da Lio B, Rusca D, Cozzolino D, Ding Y, Zbinden H, Zavatta A, Oxenløwe LK, Bacco D. Efficient time-bin encoding for practical high-dimensional quantum key distribution. Phys Rev Appl. 2020;14:014051. https://doi.org/10.1103/PhysRevApplied.14.014051.
21. Shao S-F, Zhou L, Lin J, Minder M, Ge C, Xie Y-M, Shen A, Yan Z, Yin H-L, Yuan Z. High-rate measurement-device-independent quantum communication without optical reference light. Phys Rev X. 2025;15:021066. https://doi.org/10.1103/PhysRevX.15.021066.
22. Zhu H-T, Huang Y, Liu H, Zeng P, Zou M, Dai Y, Tang S, Li H, You L, Wang Z, Chen Y-A, Ma X, Chen T-Y, Pan J-W. Experimental mode-pairing measurement-device-independent quantum key distribution without global phase locking. Phys Rev Lett. 2023;130:030801. https://doi.org/10.1103/PhysRevLett.130.030801.
23. Lu Y-S, Yin H-L, Xie Y-M, Fu Y, Chen Z-B. Repeater-like asynchronous measurement-device-independent quantum conference key agreement. Rep Prog Phys. 2025;88(6):067901. https://doi.org/10.1088/1361-6633/addeec.
24. Iskander G, Sinclair N, Peña C, Xie S, Spiropulu M. Stabilization of an electro-optic modulator for quantum communication using a low-cost microcontroller. Caltech Undergrad Res J. 2019.
25. Kim J, Park J, Kim H-S, Kim G, Kim JT, Park J, Moon K, Kwak S-C, Kim M-s, Ju JJ. Fully controllable time-bin entangled states distributed over 100-km single-mode fibers. EPJ Quantum Technol. 2024;11(1):53. https://doi.org/10.1140/epjqt/s40507-024-00267-5.
26. Tang Y-L, Yin H-L, Ma X, Fung C-HF, Liu Y, Yong H-L, Chen T-Y, Peng C-Z, Chen Z-B, Pan J-W. Source attack of decoy-state quantum key distribution using phase information. Phys Rev A. 2013;88:022308. https://doi.org/10.1103/PhysRevA.88.022308.
27. Acín A, Massar S, Pironio S. Randomness versus nonlocality and entanglement. Phys Rev Lett. 2012;108:100402. https://doi.org/10.1103/PhysRevLett.108.100402.
28. Roberts GL, Pittaluga M, Minder M, Lucamarini M, Dynes JF, Yuan ZL, Shields AJ. Patterning-effect mitigating intensity modulator for secure decoy-state quantum key distribution. Opt Lett. 2018;43(20):5110–3. https://doi.org/10.1364/OL.43.005110.
29. Agnesi C, Avesani M, Stanco A, Villoresi P, Vallone G. All-fiber self-compensating polarization encoder for quantum key distribution. Opt Lett. 2019;44(10):2398–401. https://doi.org/10.1364/OL.44.002398.
30. Li Y, Li Y-H, Xie H-B, Li Z-P, Jiang X, Cai W-Q, Ren J-G, Yin J, Liao S-K, Peng C-Z. High-speed robust polarization modulation for quantum key distribution. Opt Lett. 2019;44(21):5262–5. https://doi.org/10.1364/OL.44.005262.
31. Avesani M, Agnesi C, Stanco A, Vallone G, Villoresi P. Stable, low-error, and calibration-free polarization encoder for free-space quantum communication. Opt Lett. 2020;45(17):4706–9. https://doi.org/10.1364/OL.396412.
32. Agnesi C, Avesani M, Calderaro L, Stanco A, Foletto G, Zahidy M, Scriminich A, Vedovato F, Vallone G, Villoresi P. Simple quantum key distribution with qubit-based synchronization and a self-compensating polarization encoder. Optica. 2020;7(4):284–90. https://doi.org/10.1364/OPTICA.381013.
33. Ma D, Liu X, Huang C, Chen H, Lin H, Wei K. Simple quantum key distribution using a stable transmitter-receiver scheme. Opt Lett. 2021;46(9):2152–5. https://doi.org/10.1364/OL.418851.
34. Paraïso TK, Woodward RI, Marangon DG, Lovic V, Yuan Z, Shields AJ. Advanced laser technology for quantum communications (tutorial review). Adv Quantum Technol. 2021;4(10):2100062. https://doi.org/10.1002/qute.202100062.
35. Berra F, Bolaños MR, De Toni A, Vijayadharan K, Agnesi C, Avesani M, Stanco A, Villoresi P, Vallone G. General model and modulation strategies for Sagnac-based encoders. 2025. https://doi.org/10.48550/arXiv.2510.11873.
36. Rusca D, Boaron A, Curty M, Martin A, Zbinden H. Security proof for a simplified Bennett-Brassard 1984 quantum-key-distribution protocol. Phys Rev A. 2018;98:052336. https://doi.org/10.1103/PhysRevA.98.052336.
37. Lu C-Y, Cao Y, Peng C-Z, Pan J-W. Micius quantum experiments in space. Rev Mod Phys. 2022;94:035001. https://doi.org/10.1103/RevModPhys.94.035001.
38. Li Y, Cai W-Q, Ren J-G, Wang C-Z, Yang M, Zhang L, Wu H-Y, Chang L, Wu J-C, Jin B, et al. Microsatellite-based real-time quantum key distribution. Nature. 2025;640(8057):47–54. https://doi.org/10.1038/s41586-025-08739-z.
39. Santagiustina FBL, Agnesi C, Alarcón A, Cabello A, Xavier GB, Villoresi P, Vallone G. Experimental post-selection loophole-free time-bin and energy-time nonlocality with integrated photonics. Optica. 2024;11(4):498–511. https://doi.org/10.1364/OPTICA.499247.
40. Švarc V, Nováková M, Dudka M, Ježek M. Sub-0.1 degree phase locking of a single-photon interferometer. Opt Express. 2023;31(8):12562–71. https://doi.org/10.1364/OE.480569.
41. Rusca D, Boaron A, Grünenfelder F, Martin A, Zbinden H. Finite-key analysis for the 1-decoy state qkd protocol. Appl Phys Lett. 2018;112(17):171104. https://doi.org/10.1063/1.5023340.
42. Currás-Lorenzo G, Nahar S, Lütkenhaus N, Tamaki K, Curty M. Security of quantum key distribution with imperfect phase randomisation. Quantum Sci Technol. 2023;9(1):015025. https://doi.org/10.1088/2058-9565/ad141c.
43. Stanco A, Santagiustina FBL, Calderaro L, Avesani M, Bertapelle T, Dequal D, Vallone G, Villoresi P. Versatile and concurrent FPGA-based architecture for practical quantum communication systems. IEEE Trans Quantum Eng. 2022;3:1–8. https://doi.org/10.1109/TQE.2022.3143997.
44. Francesconi S, De Lazzari C, Ribezzo D, Vagniluca I, Biagi N, Occhipinti T, Zavatta A, Bacco D. Scalable implementation of temporal and phase encoding qkd with phase-randomized states. Adv Quantum Technol. 2024;7(2):2300224. https://doi.org/10.1002/qute.202300224.

45. Grünenfelder F, Boaron A, Rusca D, Martin A, Zbinden H. Performance and security of 5 GHz repetition rate polarization-based quantum key distribution. Appl Phys Lett. 2020;117(14):144003. https://doi.org/10.1063/5.0021468.
46. Thew RT, Nemoto K, White AG, Munro WJ. Qudit quantum-state tomography. Phys Rev A. 2002;66:012303. https://doi.org/10.1103/PhysRevA.66.012303.
47. Jogenfors J, Larsson J-Å. Energy-time entanglement, elements of reality, and local realism. J Phys A, Math Theor. 2014;47(42):424032. https://doi.org/10.1088/1751-8113/47/42/424032.
48. Vedovato F, Agnesi C, Tomasin M, Avesani M, Larsson J-Å, Vallone G, Villoresi P. Postselection-loophole-free Bell violation with genuine time-bin entanglement. Phys Rev Lett. 2018;121:190401. https://doi.org/10.1103/PhysRevLett.121.190401.

## Publisher's note