

ARTICLE

Open Access

Gigahertz-rate thin-film lithium niobate receiver for time-bin quantum communication

Andrea Bernardi^{1,2✉}, Marco Clementi³, Marcello Bacchi³, Matías Rubén Bolaños⁴, Sara Congia^{3,5}, Francesco Garrisi², Andrea Martellosio², Marco Passoni², Alexander Wrobel², Costantino Agnesi^{4,6}, Giuseppe Vallone^{4,6}, Paolo Villoresi⁴, Federico Andrea Sabattoli², Matteo Galli³ and Daniele Bajoni¹

Abstract

Time-bin encoded quantum states of light are crucial for quantum technology applications. The integration of manipulation functionalities into chip-scale devices is essential for deploying scalable, high-performance, and cost-effective quantum networks. Here we develop a fully integrated, high-throughput quantum receiver based on the thin-film lithium niobate (TFLN) platform, capable of high-speed electro-optic manipulation of time-bin encoded quantum states. The device's novel architecture enables active switching of time-bin quantum states with an electro-optic bandwidth exceeding 30 GHz, while supporting real-time arbitrary projective measurements with a bandwidth of over 1 GHz. We showcase its versatility and performance through several applications, including the certification of entanglement with Bell's inequality violation by 38 standard deviations and with >95% visibility. We then apply it to a fiber-based quantum communication scenario, where we experimentally demonstrate an entanglement-based quantum key distribution (QKD) protocol, achieving stable finite-size secure key rates exceeding 25 kbit/s over 12 h of continuous operation. By leveraging a high-speed active switching scheme, the system overcomes the need for temporal post-selection, eliminating a fundamental loophole that compromises the security of time-bin entanglement-based QKD protocols and relaxes the temporal resolution requirements of single-photon detectors. Moreover, it enables active selection of the projection basis, increasing the flexibility for communication parties. This approach establishes a versatile and scalable architecture for time-bin encoded quantum communication, enabling practical protocols on industry-grade photonic technology.

Introduction

Entanglement is a fundamental physical resource¹ that, by the laws of quantum mechanics, enables functionalities that are impossible to achieve with classical systems². It plays a central role in a wide range of quantum information applications, including quantum communication, computing, and sensing. Among these, the development of quantum networks has attracted substantial interest in recent years. Such networks facilitate the long-range transfer of quantum information, often leveraging existing

telecommunication infrastructure³, and enable the distribution of cryptographic keys via entanglement-based QKD protocols^{4–7}, which provide stronger security than traditional “prepare-and-measure” schemes. Specifically, they allow for secure communication even in the presence of untrusted network components^{4,5} and offer enhanced robustness over long distances⁸. In the realm of quantum photonics, entanglement can be implemented using different degrees of freedom of the electromagnetic field, such as path, polarization, frequency, and time — the latter either in a continuous (“time-energy”) ^{9,10} or discrete (“time-bin”) basis^{11,12}. Each encoding scheme offers specific advantages and trade-offs depending on the application and hardware constraints. Among them, time-bin entanglement stands out in quantum communication applications for its compatibility with existing fiber-optic

Correspondence: Andrea Bernardi (andrea.bernardi01@universitadipavia.it)

¹Dipartimento di Ingegneria Industriale e dell'Informazione, Università di Pavia, Via A. Ferrata 5, 27100 Pavia, Italy

²Advanced Fiber Resources Milan s.r.l., Via Fellini 4, 20097 San Donato Milanese, Italy

Full list of author information is available at the end of the article

© The Author(s) 2026



Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.



infrastructure and resilience to environmental perturbations, making it ideal for long-distance QKD implementations^{13,14}. Time-bin entanglement is relatively easy to generate and manipulate, and supports advanced functionalities such as high-dimensional encoding¹⁵ and hyper-entanglement involving other degrees of freedom^{16,17}. More generally, time-bin encoding entails a natural way to achieve temporal synchronization among users, automatically establishing a common frame of reference between two or more communication parties¹⁸.

Recently, great research interest has been devoted to the development of quantum technological applications based on time-bin entanglement. On the one hand, efforts have focused on enhancing clock rates — and more in general secure key rates (SKR) — in QKD protocols^{19,20}. Other studies have investigated the combination of such an encoding scheme with dense wavelength division multiplexing (DWDM), aiming at parallelizing multiple quantum channels in star-topology architectures to increase network capacity^{21–23}. Further attention has been devoted to the implementation of time-bin entanglement in integrated photonic devices. Recently, the programmable generation and the tomography of time-bin-entangled states have been demonstrated on a single thin-film lithium niobate (TFLN) photonic chip^{24,25}. The generation of high-dimensional entangled states, or *qudits*, has also been shown through a chip-based interferometer cascade and subsequently exploited to demonstrate high-dimensional entanglement-based QKD¹⁵.

Despite such great progress, several limitations still hinder the widespread deployment of quantum communication systems based on time-bin entanglement. First of all, projections on the time-bin basis require high temporal resolution single-photon detectors, which should be able to unambiguously discriminate between the “early” and “late” time of arrival of the associated wavepackets, typically limiting the separation of time bins to at least hundreds of picoseconds. Even more critically, time-bin entanglement-based applications are affected by the post-selection loophole (PSL)²⁶. This arises from the necessity to discard non-interfering detection events associated with time-bin wavepackets that do not temporally overlap at the measurement stage. Such discarding compromises the security of QKD implementations^{27,28}, as it allows local hidden variable models to reproduce the observed correlations even in the absence of entanglement by exploiting detector blinding attacks²⁶. Identifying these events requires observers to exchange timing information via classical communication and also necessitates discriminating detection times with a temporal resolution on the order of the time-bin separation. Thus, overcoming the need for high temporal resolution and closing the PSL are essential objectives, especially from the perspective of using photonic integrated technologies for QKD

applications, where low time-bin separation times are sought to minimize the footprint of integrated delay lines and to maximize the SKRs.

Overall, photonic chips would allow scalability, cost-effectiveness, high throughput, reduced size, and high phase stability compared to their bulk optics and fiber-based counterparts, and it would therefore be desirable to foster their deployment in the development of time-bin entanglement-based quantum applications. To enable this, it is essential to overcome the limitations imposed by the PSL, improve system integration, and support high-speed operation without increasing demands on detection hardware.

In this work, we address these limitations by developing a fully integrated quantum receiver designed for general time-bin quantum applications. We resolve the PSL by implementing an ultrafast active switching scheme²⁹ exhibiting a 30 GHz electro-optic (EO) modulation bandwidth, made possible by TFLN technology. This allows for the deterministic superposition of all time-bin wavepacket states with picosecond-range separation. Consequently, this eliminates the need for post-selection and, in the case of measurements in the interferometric bases, relaxes the time resolution constraints on the detection system, here ultimately limited only by the clock rate (i.e., by the repetition rate of the pump laser).

The device presented here is a general-purpose time-bin universal projector that can be used for a variety of applications. It can operate either as a phase-stable state preparation stage, used to tailor a pump pulse shape, or as a receiver, capable of performing real-time arbitrary projective measurements in the time-bin basis, enabled by an EO bandwidth exceeding 1 GHz. Fully packaged in a standard telecom casing, it is compact and stable, which makes it suitable for a wide range of quantum applications. We demonstrate the potential of our device through several key quantum information applications. First, we generate a time-bin entangled state by combining one of the realized integrated devices with an integrated silicon waveguide used as a nonlinear source, enabling the generation of arbitrary time-bin quantum states. We certify entanglement by violating Bell’s inequality by 38 standard deviations and achieving interference fringe visibility of over 95% using the other two separate quantum receivers. Second, we perform quantum state tomography, enabled by the capability of our device to implement arbitrary time-bin projective measurements on two independent users. Finally, we implement two versions of an entanglement-based QKD protocol, both in a PSL-free fashion: we first show QKD using a “standard” passive-basis selection scheme, where fiber beam splitters are used to choose Alice’s and Bob’s projection bases. In these demonstrations, we achieve finite-size SKRs exceeding 25.4 kbit/s — the highest reported for any time-bin



entanglement-based QKD system — with sustained stability over several hours and with a total channel loss of 0.5 dB. We then fully leverage the potential of the device as a quantum receiver, showing how active basis selection can be straightforwardly implemented using a second input port and pseudorandom bit sequence (PRBS) from the perspective of providing full and real-time arbitrariness in the choice of the projection basis. Crucially, this performance is achieved with picosecond-scale time-bin separation, yet without requiring detectors capable of resolving it. By closing the PSL, our system's timing requirements are relaxed entirely to the clock rate of the source laser, paving the way for high-speed, secure, and truly integrated quantum communication.

Results

Device description and operating principle

A conceptual device layout is shown in Fig. 1a. It consists of two main stages, arranged in a cascaded configuration. The first stage is a high-speed balanced Mach-Zehnder modulator (MZM), realized by long and efficient EO phase modulators included in each arm of the interferometer, and exhibiting a broad modulation bandwidth (3-dB bandwidth exceeding 30 GHz; see Fig. 2b). It also includes two thermal phase shifters (TPS), one on each arm of the interferometer, to control the bias operating point while ensuring optical symmetry and extended phase tuning range. The second stage is an unbalanced Mach-Zehnder interferometer (MZI), where the relative temporal path delay is set to 100 ps, obtained by a geometrical path unbalance of 1.31 cm. It includes a broad-band EO phase modulator and a TPS, both placed in the longer arm of the interferometer, while the shorter arm incorporates a 2% power-splitter monitor. This component allows for bias monitoring of the MZM and serves to partially compensate for the propagation loss in the longer arm.

The device is designed to operate on a generic qubit encoded in the time-bin basis, schematically depicted on the Bloch sphere in Fig. 1b, and mathematically described as:

$$|\phi\rangle = \alpha|0\rangle + \beta e^{i\theta_s}|1\rangle \quad (1)$$

where $|0\rangle$ corresponds to the photon state in the early time-bin, $|1\rangle$ to the photon state in the late time-bin, θ_s is the relative phase between the two bins, and α, β are real-valued probability amplitudes.

As illustrated in Fig. 1a.i, when the MZM is biased at the quadrature point (*mode 1*), it acts as a 50:50 beam splitter. In this configuration, injecting a generic optical field that encodes the time-bin state $|\phi\rangle$ into the device results, heuristically, in a superposition of photons traveling through either the longer or shorter arms of the

unbalanced interferometer. Photons taking the longer path experience a delay of 100 ps relative to those in the shorter path, resulting in a three-peak detection pattern as a function of arrival time after recombination. Interference arises only in the central peak, where there is the temporal overlap between the early and late time bins that travel relatively along the longer and shorter paths. More rigorously, this configuration implements the positive operator-valued measurement (POVM):

$$\hat{\Pi}_{\pm}(\theta) = \frac{1}{4} \hat{\mathbb{I}} + \frac{1}{2} \hat{P}_{\pm}(\theta) \quad (2)$$

where $\hat{\mathbb{I}} = |0\rangle\langle 0| + |1\rangle\langle 1|$ is the identity operator representing non-interfering paths (outer peaks), and:

$$\hat{P}_{\pm}(\theta) = \frac{1}{2} (|0\rangle \pm e^{i\theta}|1\rangle)(\langle 0| \pm e^{-i\theta}\langle 1|) \quad (3)$$

is the projector describing the interferometric contribution, associated with the central peak and controlled by the phase θ applied in the unbalanced MZI. The signs $\pm$ account for the dependence on the two output ports of the unbalanced MZI stage, which exhibit a relative phase shift of π .

The device's innovative aspect arises from its ability to operate the MZM to act as a fast optical switch (*mode 2*): photons in the early (late) time-bin can be deterministically routed into the longer (shorter) arm of the unbalanced interferometer (Fig. 1a.ii). In this way, the input photons belonging to the two time-bin slots are temporally overlapped at the output of the second interferometer. This leads to a single interference peak in the detection pattern over time, whereas all photons contribute coherently to the interference pattern. In these conditions, the implemented POVM is $\hat{P}_{\pm}(\theta)$, as defined in Eq. (3). Indeed, by varying the phase θ in the longer arm of the unbalanced MZI, either via the TPS or the EO modulator, it is possible to project the time-bin state into any equatorial state of the Bloch sphere (Fig. 1b) without any temporal post-selection on the detected events, i.e., discarding contributions from the lateral peaks. Moreover, the projections can be executed with a high degree of precision from static conditions (tens of hours) with the TPS, and up to GHz speeds with the EO phase modulator.

A third operating condition (*mode 3*) is possible when the modulation signal applied to the optical switch is phase-shifted by 180° , thus reversing the photon routing (Fig. 1a.iii). In this configuration, at the output of the device, it is possible to perform a measurement in the computational basis by post-selecting events in the early or late time bins, as now the POVM is $\hat{\mathbb{I}}/2$. In this configuration, the time-bin separation at the output doubles from 100 ps to 200 ps due to the propagation of the late



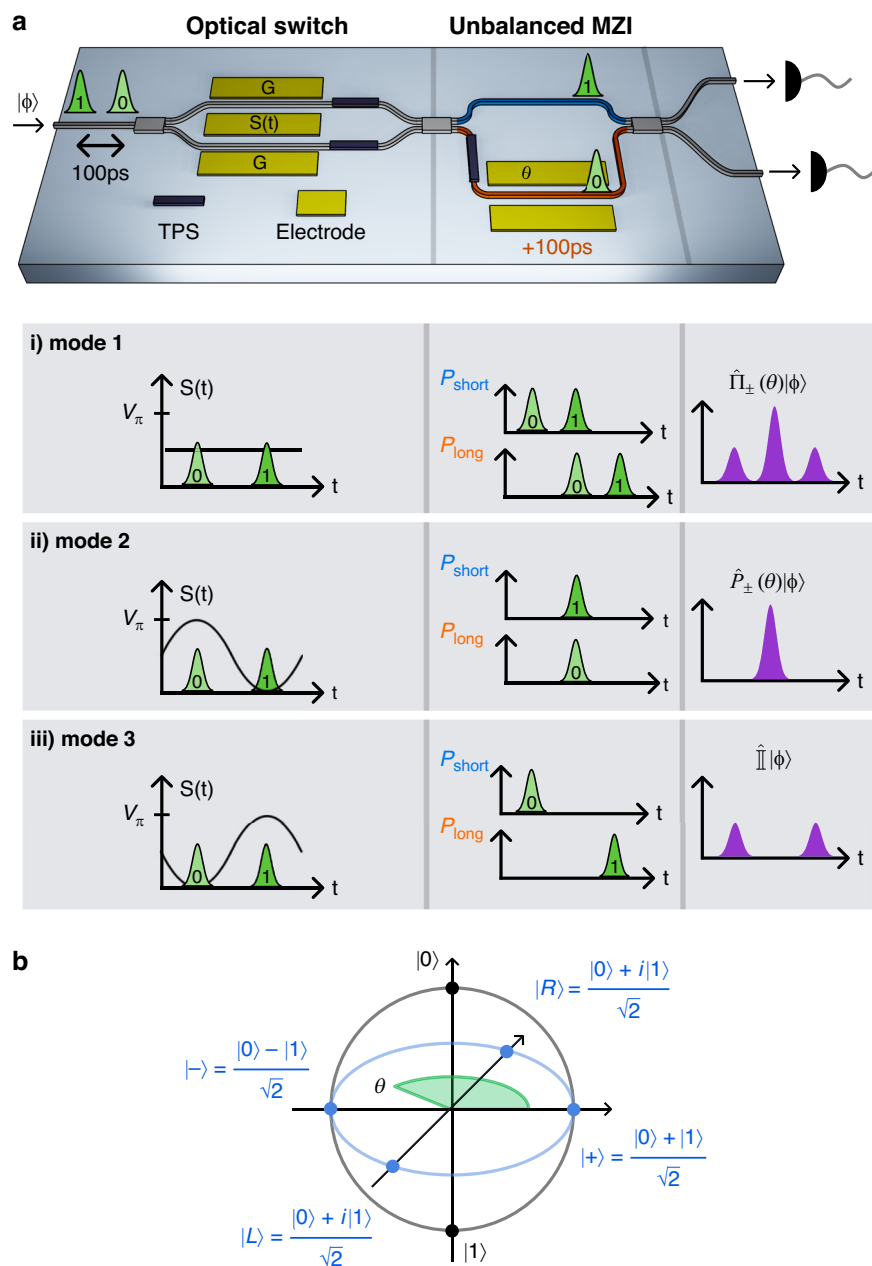
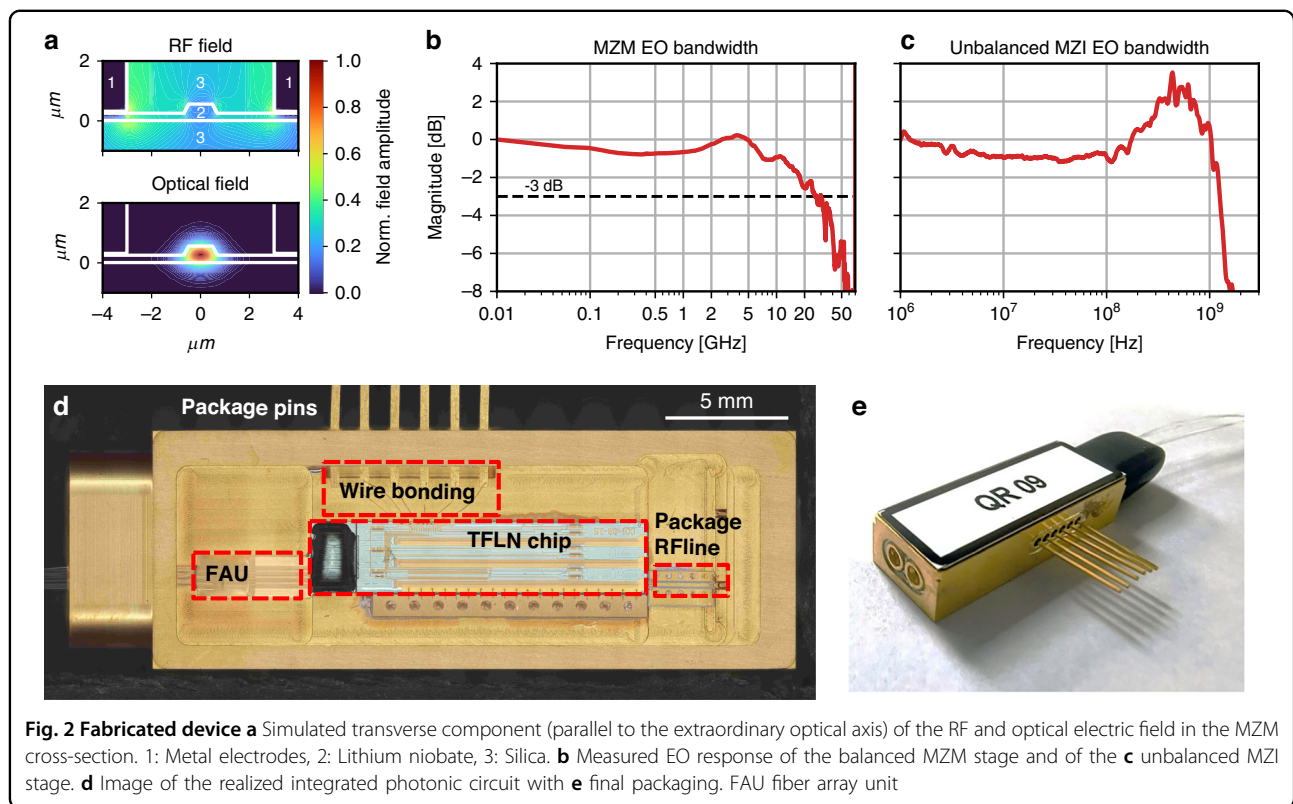


Fig. 1 Conceptual schematic **a** Schematic of the integrated optical circuit. The evolution of the input photon state is illustrated for the three configurations: (i) the first-stage MZM is biased at quadrature with no RF modulation; (ii) the MZM is driven such that early (late) time-bin photons are routed into the longer (shorter) path of the unbalanced MZI; (iii) the RF modulation is inverted, routing early (late) photons into the shorter (longer) path. **b** The integrated quantum receiver can implement an arbitrary time-bin state projector. When operated in configuration a.ii, it projects into the equator of the Bloch sphere (blue); when operated in a.iii, it projects into the poles of the Bloch sphere

(early) pulse through the longer (shorter) interferometer path. The doubled temporal separation relaxes the requirements on the temporal resolution of the detection system, improving compatibility with detectors exhibiting moderate timing jitter.

By comparing the operating conditions of *mode 1* and *mode 2*, we can see that there is a fundamental difference

in the achievable interference visibility if no post-selection is applied to the detected photons. When a generic time-bin encoded pure state $|\phi\rangle$ is injected into the device, the maximum interference visibility at the output increases from a maximum of 50% in *mode 1* to 100% in *mode 2* thanks to the optical switching configuration. This distinction becomes even more relevant in the context of



time-bin entangled photon pairs. Considering a maximally entangled Φ -type Bell state:

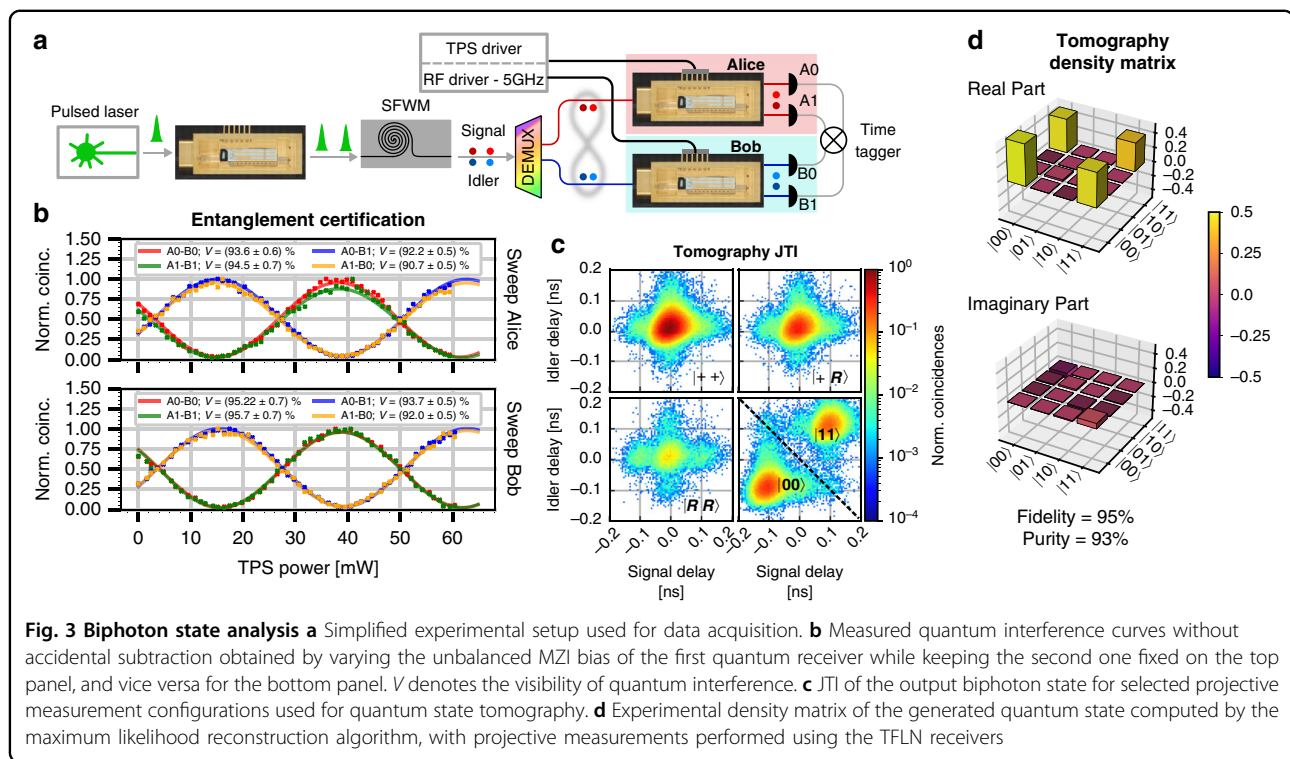
$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \quad (4)$$

If each photon of the pair is sent to two separate devices operating in *mode 1* and no temporal post-selection is applied, the resulting two-photon interference visibility is limited to 25%²⁹. With this low visibility, the Bell and Clauser–Horne–Shimony–Holt (CHSH) inequalities cannot be violated³⁰, opening a PSL that affects local-realistic tests of quantum mechanics, and thus hindering the security of QKD protocols²⁶. Even in the presence of high-resolution single-photon detectors, by performing temporal post-selection, the number of coincidence events contributing to quantum interference is reduced to 1/4 of the total, reducing the SKR potentially achievable. In contrast, when both devices operate in *mode 2*, the time-bin components are deterministically overlapped, enabling maximum quantum interference. This configuration closes the PSL and produces a single interference peak in the time-resolved coincidence histogram, with visibility up to 100%, while increasing throughput due to the lack of discarded events. As a result, it becomes possible to certify entanglement and support secure QKD with a four-fold increase in the SKR.

Fabrication and classical characterization

The integrated device was fabricated on an X-cut lithium niobate on insulator (LNOI) wafer. The single-mode optical waveguide (propagation loss around 0.2 dB cm^{-1}) is combined with radio-frequency (RF) traveling-wave coplanar waveguides for EO modulation (Fig. 2a). The optical and RF field profiles are engineered to maximize the modulation efficiency, with a measured $V_\pi L_\pi \approx 3.37 \text{ V cm}$ (at 1 MHz). Figure 2b shows the EO modulation spectrum for the MZM (optimized for high-frequency operation) and Fig. 2c for the unbalanced MZI stage, with a 3 dB bandwidth as high as 30 GHz and 1 GHz, respectively. The reduced bandwidth of the second-stage interferometer reflects the fact that this stage was not optimized for high-frequency operation. In particular, compared to the MZM, few differences account for the limited bandwidth performance: it does not include the integrated 50Ω termination, leaving the electrodes open, and it is not connectorized with a high-speed RF connector. The combined effect of the electrodes' capacitance and the long wire bonds introduces inductive and capacitive parasitic effects that result in peaking around 500 MHz and a limited bandwidth. Comparable performance can be achieved in future iterations by adopting the same design and packaging solution for the MZI as for the MZM. Further details are provided in the “Materials and methods” section.





The fabricated photonic chips were packaged for ease of handling, as illustrated in Fig. 2d, e, and connectorized with optical, RF, and low-frequency interconnections for the respective components.

The final device has a footprint of 9.6×26 mm. We stress that a key advantage of the TFLN platform lies in the exceptional EO properties of lithium niobate, combined with the high spatial mode confinement of both the optical and electrical fields (see Fig. 2a), enabled by the integrated photonic design. Additional details on the device design, fabrication, and linear characterization are provided in the “Materials and methods” section. For the experimental demonstrations described in the following sections, one or more devices (all exhibiting comparable performances) were combined in complex experimental setups, where they were employed either as quantum receivers, for projection on the time-bin basis, or as pump tailoring stages at the input of an entangled photon source. Each one was only stabilized in temperature via thermo-electric coolers (TEC), without the need for further active feedback to compensate for interferometers’ bias phase drift, already minimized through the thermal stabilization and the isolation provided by the package.

Entanglement certification

We now investigate the suitability of the device, designed as a building block for complex systems involving multipartite states, to manipulate a biphoton time-bin entangled state. As a first demonstration of its

functionality, we certify entanglement by violating both Bell^{9,11} and CHSH³¹ inequalities using two spatially separated devices acting as analyzer interferometers while closing the PSL. The simplified experimental setup is illustrated in Fig. 3a. Optical pulses emitted by an actively mode-locked laser are coupled to one of the fabricated devices, used for pump tailoring. By tuning the bias operating point of the balanced MZM, it is possible to generate a pair of twin pulses separated by 100 ps, with arbitrary relative amplitudes. These pulses are injected into a 16 mm long integrated silicon waveguide and, under appropriate pump power conditions (see Supplementary Note 4), time-bin entangled photon pairs are generated via spontaneous four-wave mixing (SFWM)³². The resulting quantum state can be expressed as $|\phi\rangle = \alpha|00\rangle + \beta e^{i\theta_s}|11\rangle$, where all the parameters can be freely tuned through the device settings: the probability amplitudes α and β by tuning the bias of the first-stage MZM, and the relative phase θ_s by tuning the phase applied in the second-stage MZI. In the following, we set $\alpha = \beta = 1/\sqrt{2}$ and $\theta_s = 0$, which prepares the Bell state $|\Phi^+\rangle$, defined by Eq. (4). The output photons are demultiplexed using commercial 100 GHz DWDM filters (ITU channel 28-1554.94 nm for the signal and channel 38-1546.92 nm for the idler) and routed to two of the developed devices, hereafter referred to as Alice and Bob. Each quantum receiver operates in active switching (*mode 2*), as shown in Fig. 1a.ii, ensuring that all of the input photons contribute to quantum interference. The two complementary



outputs of each interferometer are routed to superconducting nanowire single-photon detectors (SNSPDs), where detection events are recorded using a digital time tagger.

The quantum interference curves retrieved from the coincidence detection patterns for all four detector combinations are shown in Fig. 3b. In the top panel, the phase θ_A on Alice's device is scanned while Bob's phase θ_B is kept fixed. In the bottom panel, θ_B is scanned while θ_A remains constant. This measurement effectively implements a Franson-type test of the Bell inequality, mathematically corresponding to a projective measurement operated on the state $|\Phi^+\rangle$. The expected coincidence rate for outputs at the same side of the second MZI is given by:

$$R \propto \text{Tr}[(\hat{P}_\pm(\theta_A) \otimes \hat{P}_\pm(\theta_B))|\Phi^+\rangle\langle\Phi^+|] = \frac{1 + \cos(\theta_A + \theta_B)}{2} \quad (5)$$

A π shift is applied to the above expression in the case of detections at opposite output ports of the two MZIs. By fitting the number of accumulated coincidence counts as a function of the applied MZI TPS power with a sinusoidal function, we extract high-visibility two-photon interference fringes, defined as $V = \frac{\max(R) - \min(R)}{\max(R) + \min(R)}$, which is $(93.5 \pm 0.6)\%$ on average across all four detector combinations without accidental subtraction. For all cases, the fitted visibility exceeds the $1/\sqrt{2}$ threshold required to violate the Bell inequality by at least 38 standard deviations, thus certifying entanglement without any temporal post-selection on the detection events. We also performed the CHSH inequality test by evaluating coincidences at the specific phase settings that maximize the S -parameter ($\theta_A = \{-\pi/4, \pi/4\}$, $\theta_B = \{0, \pi/2\}$ for all 4 possible combinations). We recorded a value of $S = 2.54 \pm 0.04$, exceeding the classical bound ($S = 2$) by more than 13 standard deviations. We stress that the experiment so performed serves at the same time as a test of entanglement, given the violation of the classical bound, and of quantum nonlocality, given the use of two distinct devices, albeit not space-like in the present demonstration. Moreover, both proofs are free of the PSL. The close match between the experimental data and fits, the similar π -phase shift powers, and the high fringe visibility across the two devices confirm their stability and reliability.

Quantum state tomography

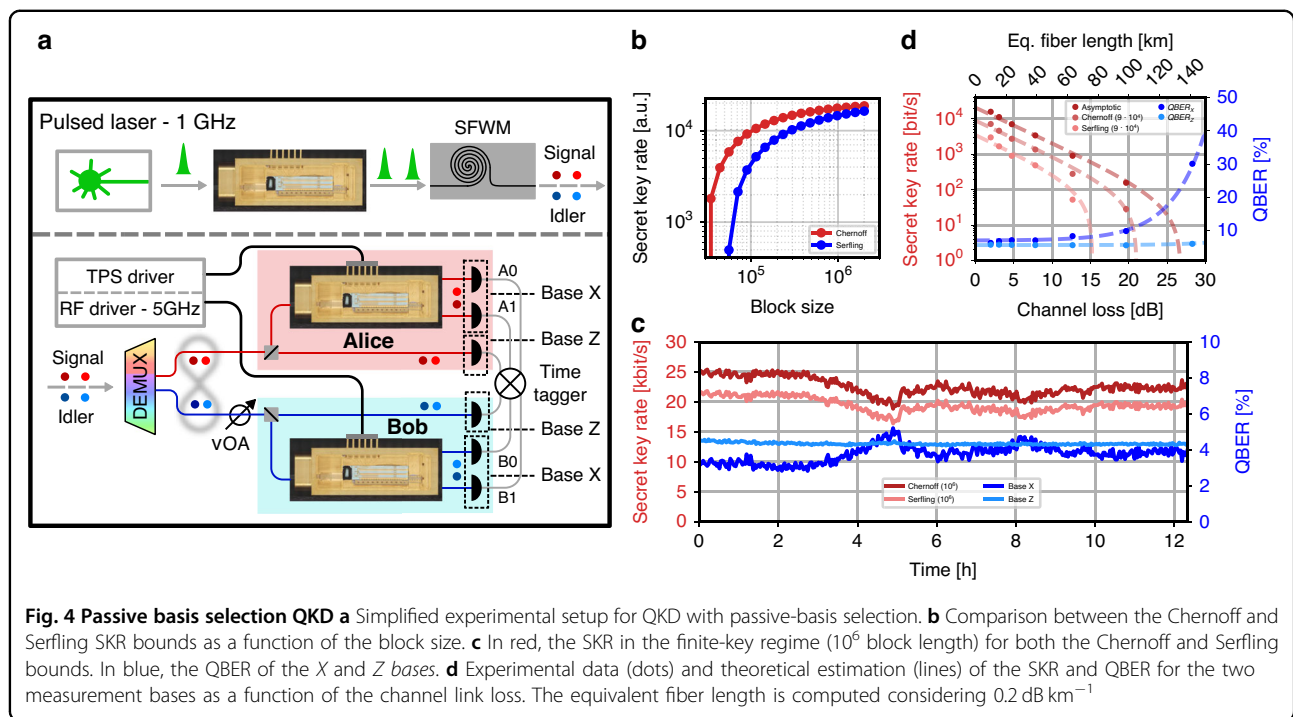
A full tomography of the generated state at the output of the integrated silicon waveguide can be performed by setting the appropriate phase conditions on both integrated quantum receivers simultaneously over a sequence of steps. A complete quantum state characterization requires projective measurements on the three orthogonal bases for each qubit³³. In this work, since each quantum receiver can measure the two orthogonal states of a

selected basis simultaneously within a single configuration, three measurement configurations were used per device. Permuting the settings between Alice and Bob resulted in a total of 9 combinations, allowing the complete set of 36 projective measurements required for full two-qubit quantum state tomography to be acquired. In particular, projections onto the equatorial bases $X = \{|+\rangle, |-\rangle\}$ and $Y = \{|R\rangle, |L\rangle\}$ are performed by operating the MZM to overlap the time bins into a single time slot (*mode 2*, Fig. 1a.ii) and by adjusting the phase of the unbalanced MZI according to Eq. (5), with $\theta_{A,B} = 0$ and $\pi/2$, respectively. In the computational basis $Z = \{|0\rangle, |1\rangle\}$, the projection is implemented by operating the device optical switch reversely (*mode 3*, Fig. 1a.iii).

The unitary evolution imparted by the receivers to the biphoton state for such operational modes can be effectively visualized through a measurement of the joint temporal intensity (JTI)^{34–36} at the output of the devices. Figure 3c shows the measured JTI of four projective measurements out of a total of nine, for one possible pair of detectors (A0-B0) out of a total of four. In the three projective measurements $|++\rangle\langle++|$, $|+R\rangle\langle+R|$, and $|RR\rangle\langle RR|$, we observe a strong suppression of coincidence counts in the outer time bins (i.e., when photons are detected in the earlier or later arrival time slot windows at Alice or Bob), resulting in a well-localized overlap in the central time-bin where interference occurs. Compared with Eq. (5), the first and third projectors correspond respectively to the maximum and minimum of the two-photon interference pattern. In the fourth JTI plot, the projections onto the $|00\rangle$ and $|11\rangle$ states are represented according to which of the two areas, delimited by the dashed lines, the coincidence events belong to. Note that, while this measurement requires higher temporal resolution to discriminate the outcome, here the separation of the coincidence peaks is increased by 100 ps, leading to a total temporal separation of 200 ps and thus relaxing the requirement of detector resolution by a factor of 2.

From the experimental data, we reconstructed the density matrix of the biphoton entangled state through a maximum likelihood estimation algorithm³³. The result, shown in Fig. 3d, exhibits a purity of 93% and a fidelity of 95% with respect to the Bell state $|\Phi^+\rangle$. A closer analysis of the density matrix reveals that the generated state deviates slightly from the ideal one. Specifically, the probability amplitude of the $|00\rangle$ component is greater than that of $|11\rangle$, and the imaginary part suggests a slight phase shift relative to the Bell state $|\Phi^+\rangle$. From the reconstructed density matrix, we provide a further characterization of entanglement beyond the Bell-curve visibility and the S -parameter reported in the previous section. First, we evaluate the entanglement of formation³⁷ to be as high as 87%. Then, we assess the von Neumann entropy of the reduced subsystems, defined as





$E(\rho_{A,B}) = -\text{Tr}[\rho_{A,B} \log_2(\rho_{A,B})]$. This yields values of $E(\rho_A) = 0.976$ and $E(\rho_B) = 0.978$ for Alice and Bob, respectively, approaching the theoretical maximum of 1, expected for a maximally mixed qubit state. These high entropy values indicate a strong degree of mixedness in the reduced states, which, when combined with the high purity of the two-qubit state, represent a clear signature of bipartite entanglement².

Quantum key distribution: passive-basis selection

The integrated TFLN device can serve as a receiver stage for implementing the Bennett-Brassard-Mermin (BBM92) entanglement-based QKD (EBQKD) protocol⁵. This is achieved using the same photon-pair source configuration used for entanglement certification and quantum state tomography, with a slight modification introduced at the user stations, as shown in Fig. 4a. Specifically, once the photons are demultiplexed and routed toward Alice and Bob, a passive fiber 50:50 beam splitter is placed. At one output port, the incoming photons are sent directly to an SNSPD; at the other port, photons are routed to the input of a TFLN device. Here, the device is configured with the optical switching activated (*mode 2*), such that the early and late time bins are temporally overlapped at the output (Fig. 1a.ii). The unbalanced MZI is held at a fixed phase $\theta_{A,B} = 0$, enabling projective measurements in the X basis. In this configuration, coincidence detection events are maximized between specific detector pairs (e.g., A0-B0 and A1-B1) when the input state is the maximally entangled Bell state $|\Phi^+\rangle$ (Eq. (4)).

For photons routed directly to the SNSPDs (bypassing the quantum receiver), a time of arrival analysis distinguishes early ($|00\rangle$) and late ($|11\rangle$) time-bin events, corresponding to projective measurements on the Z basis. This configuration enables the implementation of the BBM92 protocol, where both users perform measurements in two mutually unbiased bases, X and Z. The basis choice is intrinsically random due to the passive beam splitter, and the randomness of the measurement outcomes is ensured by the entangled photon-pair source, as demonstrated in the previous section. For a comprehensive review of quantum cryptography and the various steps involved in QKD protocols, we refer the reader to ref.³⁸.

In this QKD configuration, there is an asymmetry in detection rates between the X and Z bases due to the additional optical losses caused by the presence of the device in the measurement path of the X basis. The maximum measured coincidence rate is 959 Hz for the X basis and 62 kHz for the Z basis, with respective optical losses of 13.3 dB (15.3 dB) and 5.9 dB (6.3 dB) for the signal (idler) photons from the entangled photon pairs source to SNSPDs input. Despite this asymmetry, the QKD protocol can still be successfully implemented by adopting an efficient information reconciliation scheme³⁹. Under these conditions, the sifting factor q — defined as the probability that both users perform projections in the same basis — is significantly improved, approaching unity. This maximizes the key rate by minimizing the number of discarded events during the



sifting process. Such an asymmetric basis choice is advantageous, provided that a minimum number of measurements are still performed in the less probable basis (the X basis), to ensure sufficient statistics for detecting potential eavesdropping attempts and thereby guaranteeing the security of the protocol.

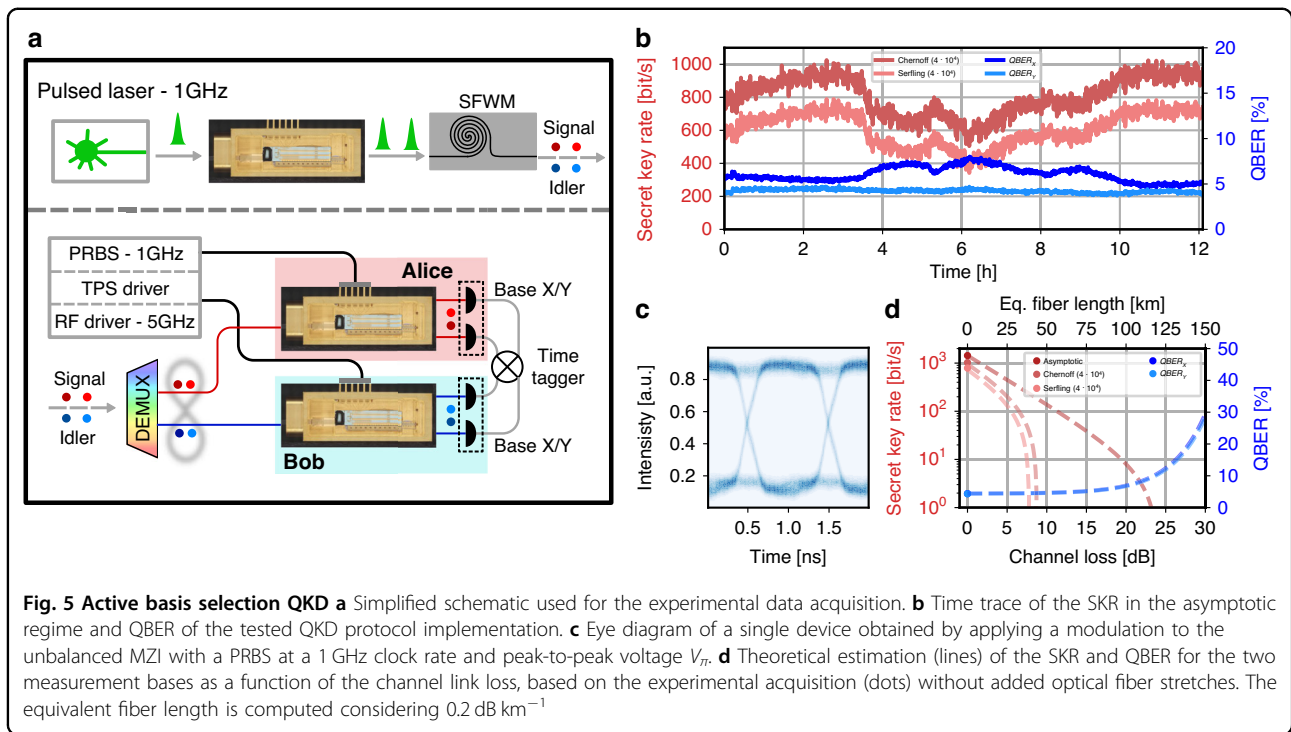
To estimate the finite-size SKR, it is required to find an upper bound on the probability of failure on the parameter estimation (PE) step. To do so, we resorted to two different statistical bounds: one based on the Serfling inequality, presented by Tomamichel et al.⁴⁰ and from here on referred to as the *Serfling bound*, and a more recent one based on the Chernoff inequality, presented by Mannalath et al.⁴¹ and from here on referred to as the *Chernoff bound* (see Supplementary Note 1). Since this work represents the first experimental implementation of the BBM92 protocol using the Chernoff bounds, we opted to show the SKR analysis done with both bounds to further showcase the advantage of using this new bound with respect to the Serfling one, widely used in literature. The resulting experimental finite-size SKR as a function of the sifted bit block length is shown in Fig. 4b. Compared to the Serfling bound, the Chernoff bound requires considerably smaller sample sizes for its statistical test to be considered relevant. This allows Alice and Bob to generate a secret key at much smaller block lengths, which is especially beneficial for EBQKD, where coincidence rates are usually low.

A long-duration measurement, exceeding 12 h, was performed running our QKD setup, at 0.5 dB channel losses. The SKR always exceeds 18.8 kbit s^{-1} , with a maximum value of 25.4 kbit s^{-1} in the finite-size regime using the Chernoff bound, with its asymptotic limit value being $\sim 14\%$ higher, and its finite-size regime using the Serfling bound $\sim 13.5\%$ lower. The quantum bit error rate (QBER) for the two measurement bases and the SKR are reported in Fig. 4c. The QBER in the Z basis is mainly limited by the timing jitter of the SNSPDs, which is ~ 50 ps full width half maximum (FWHM), compared to a time-bin separation of 100 ps. The detection time window used to distinguish between early and late time bins was optimized to maximize the SKR in the Z basis (see Supplementary Note 2). The QBER in the X basis depends on the interferometric performance of the projection implemented by the device. Here, an average QBER of 3.76% was recorded, consistent with the measured visibility reported in the entanglement certification section, according to the relation $\text{QBER} = (1 - V)/2$ ³⁸. The small variations observed in the QBER in the interferometric basis are mainly attributed to phase drift in the interferometer, which causes deviations of the applied projection from the ideal one. These fluctuations are reflected in the temporal evolution of the SKR and can be mitigated in practical implementations by standard interferometric

stabilization techniques or by periodic protocol interruption and realignment procedures. Note that other contributions to noise, such as accidental and dark detections, are negligible in the present experimental conditions.

Measurements simulating a variable-length fiber link were performed by adjusting the attenuation in Bob's fiber link through a variable optical attenuator (VOA). A more realistic proof-of-principle was then performed with fiber spools of different lengths, and could be further extended to a metropolitan-area field test. We note that in these scenarios, appropriate dispersion compensation strategies should be put in place to mitigate the effect of chirp for link lengths exceeding 8 km (see Supplementary Note 3). Indeed, group velocity dispersion in standard telecom fibers broadens the time-bin wavepackets, thereby degrading the temporal confinement required for proper device switching and reducing the distinguishability between early and late time bins. Figure 4d shows the measured (dots) and theoretical SKR (dashed line) in the asymptotic regime and for a finite block size of 9×10^4 . The corresponding QBER values for the two measurement bases are also shown. Note that QKD is feasible for equivalent fiber lengths exceeding 100 km (0.2 dB km^{-1} loss). The main limitation in this configuration arises from the signal-to-noise ratio (SNR) of the coincidence counts in the X basis: at high channel attenuation, detector dark counts significantly reduce the visibility of the interference, thus increasing the QBER. In contrast, the associated Z basis QBER is almost unaffected by dark counts in the attenuation sweep, due to a higher SNR. An additional important consideration for real-world implementations involving physically separated stations is the requirement for precise timing synchronization between the users and the pulsed source. Such synchronization is crucial to accurately discriminate the received time-bin slots and to correctly align the modulation and switching signals for proper routing within the receivers. Efficient synchronization techniques achieving picosecond-level precision have been demonstrated up to 50 km link length, even without the need for additional communication channels^{42–44}. We note that this synchronization requirement only concerns the technical implementation and does not, in itself, limit or compromise the security of the QKD protocol, whose security relies on entanglement. However, the security of the present implementation is not device-independent, since the detection loophole remains open⁴⁵. Closing this loophole is a well-known experimental challenge that goes beyond the scope of this work. Nevertheless, the proposed overcoming of the temporal PSL represents a necessary step toward the deployment of loophole-free time-bin architectures.





Quantum key distribution: active basis selection

The BBM92 QKD protocol can also be implemented using an alternative user receiver setup whose schematic configuration is shown in Fig. 5a. Compared to the previous configuration, which relied on passive-basis selection, this configuration removes the beam splitter and directs all the photons toward the device, where measurements are performed by actively selecting the applied projector. Precisely, the projective measurements are performed in the two mutually unbiased X and Y bases, both of which exhibit quantum interference for all incoming photons without post-selection due to the active time-bin switching (*mode 2*) operated by the first-stage MZM.

The device applies the POVM defined in Eq. (3), corresponding to either $\hat{P}_+(\theta)$ or $\hat{P}_-(\theta)$, depending on the device output port. The phase θ determines the measurement basis and is physically implemented by the unbalanced MZI as a combination of two contributions:

$$\theta = \theta_{\text{TPS}} + \theta_{\text{RF}} \quad (6)$$

where θ_{TPS} is a phase set by the TPS, and θ_{RF} is the phase modulation applied by the EO modulator.

The basis choice for each user is applied at the repetition rate of the pulsed pump laser (1 GHz) to ensure a random and independent selection for every entangled photon pair. In our setup, the EO modulator of the unbalanced MZI is driven by an arbitrary waveform generator (AWG) programmed with a PRBS. To improve

the security of the protocol, these could, in principle, be replaced by quantum random number generators (QRNG), even integrated on the same chip^{46,47}. Alice and Bob use PRBS sequences of lengths $2^7 - 1$ and $2^9 - 1$, respectively, both operating at a 1 GHz bit rate. This configuration ensures that the joint basis-choice pattern repeats every $127 \times 511 = 64,897$ clock periods, effectively emulating a non-repeating sequence. The modulation signals have a peak-to-peak voltage of $V_{\text{pp}} = V_{\pi}/2$. To ensure the switching between desired X and Y measurement bases, the TPS is statically set to apply a phase $\theta_{\text{TPS}} = \pi/4$ when no voltage is applied to the EO modulator. This ensures toggling the total phase θ between 0 and $\pi/2$ every clock cycle. An eye diagram showing the continuous-wave light modulation of the unbalanced MZI, driven by the PRBS sequence, is shown in Fig. 5c.

As for the previous case, we conducted a long-duration measurement exceeding 12 h continuously without any interruption and without the use of active stabilization, apart from maintaining the device package at a constant temperature. Once again, both Serfling and Chernoff bounds were used to obtain and compare the secret key rates. The time traces of the SKR for both bounds, along with the QBER values for the X and Y bases, are shown in Fig. 5b. A maximum SKR of $1.024 \text{ kbit s}^{-1}$ was recorded, with an average of $0.805 \text{ kbit s}^{-1}$ over the measurement period. The average QBER value for the Y basis over time is 4.02%, while the X basis exhibits a higher value of 6.1%. For the Y basis, the marginal increase in QBER compared to the previous configuration is primarily attributed to



non-ideal AWG modulation, as the basis projection is switched every nanosecond. The increased QBER observed in the X basis—beyond the limitation affecting the Y basis—is additionally attributed to an initial offset in the operating point, for which the initial QBER was 5.5%, together with larger phase-drift variations over time. Nevertheless, given the high modulation speed, the observed QBER values confirm the excellent device performance under fast, active operation. Compared to the passive QKD system, the SKR is reduced since both measurement bases are now implemented passing through the device, and thus the total optical losses are higher: 12.15 dB for Alice and 10.1 dB for Bob from the entangled photon pairs source to the SNSPDs input. Additionally, the sifting factor q is no longer close to 1, but reduced to 0.5, due to the equal probability of selecting each basis. This high-loss scenario better showcases the difference between the two bounds used to estimate the SKR, as block lengths are smaller.

An estimation of the SKR as a function of channel loss is reported in Fig. 5d for both the asymptotic regime and finite block size of 4×10^4 , where using the Chernoff bound provides an increase of 33.2% on the secret key generation when compared with the Serfling bound generation. At the measured coincidence rate, a block of key is generated approximately every 25 s. If fast key generation is required, we note that an average of 450 bit s^{-1} of secret key was generated even using a block length of 10^4 , where the secret key generated using the Chernoff bound becomes 122.3% higher with respect to the Serfling bound. At high channel loss, the QBER is primarily limited by detector dark counts. In this configuration, compared to the passive one, the QBER degradation for the interferometric bases is expected to occur at slightly longer fiber length, as the receiver coincidence rate increases due to the removal of the beam splitter, which in the previous setup introduced an additional 3 dB loss.

Overall, we emphasize that this configuration, although the SKR is reduced due to the additional optical losses introduced by the quantum receiver and the slight QBER increase arising from the added complexity of the phase modulation, not only removes the PSL as in the passive QKD case, but also eliminates the need to resolve the separation between individual time bins. Indeed, only the separation between successive time-bin states must be distinguished. This relaxed detection requirement makes it possible to increase the SKR by simply raising the pump laser repetition rate and reducing the time-bin separation.

Discussion

In this work, we have engineered and demonstrated a fully packaged integrated photonic circuit capable of supporting multiple quantum applications, achieving state-of-the-art performance. The main purpose of our

device is to overcome the problem of PSL, and the need for temporal post-selection in general, which arises from the nature of Franson-like unbalanced interferometers, and limits both the security and efficiency of QKD protocols based on time-bin entangled states. We address this issue by implementing an active switching solution²⁹, of which, to the best of our knowledge, our device represents the first realization on an integrated photonic platform. Another integrated solution, proposed by Santangustina et al.⁴⁸, also addresses the PSL issue through a “hug” scheme, which passively discards photons that do not temporally overlap, resulting in a 50% reduction in usable photon pairs. More problematically, this approach has interlinked interferometers that extend along the optical link between Alice and Bob, which hinders the practical deployment of QKD applications in the field.

Our PSL-free architecture can be generally used as an arbitrary time-bin projector and, owing to the combination of TPSs and broadband TFLN modulators, the integrated quantum receiver enables fast switching, in the tens of gigahertz range, of time-bin encoded states. This allows the use of closely spaced time-bin states, and therefore high clock (repetition) rates and SKR throughputs, and makes it possible to operate projective measurements at tunable timescales, ranging from sub-nanosecond speeds to stable operation over several hours.

We have demonstrated its versatility across different tasks: certification of genuine time-bin entanglement by more than 38 standard deviations without the need for temporal post-selection, quantum state tomography of time-bin encoded states, and preparation stage by modulating the pump pulses demonstrating its ability to generate high-fidelity (95%) and high-purity (93%) arbitrary time-bin entangled states when combined, as in this case, with a nonclassical light source. Furthermore, we have also demonstrated that the developed device can effectively implement the BBM92 entanglement-based QKD protocol in both passive and active basis selection modes, proving its versatility and reconfigurability. The BBM92 is a well-established^{5,49} and widely used QKD protocol based on entanglement. Recent works include high-rate^{20,21,23,50,51} and high-dimensionality¹⁵ demonstrations. However, the Post-Selection Loophole was always open in these previous works. To the best of our knowledge, the present work reports the first realizations of time-bin QKD closing the Post-Selection Loophole, achieved at the same time with long-term operational stability (more than 12 h), and notably, with the highest SKR (exceeding 25 kbit s^{-1}) demonstrated so far in time-bin entanglement-based systems, as summarized in Table 1.

In the active basis selection QKD configuration, compared to the passive one, the requirement on the minimum time resolution of the detection system is relaxed: now it is sufficient to resolve the time-bin repetition rate,



Table 1 Comparison among entanglement-based QKD demonstrations using different degrees of freedom (DoF)

User implementation	DoF	SKR per channel	Link length	Clock rate	Bin separation	Protocol
Silica-based ⁵⁰	Time	0.14 bit s ⁻¹	100 km	0.333 GHz	1 ns	BBM92 ⁵
Fiber-based ²¹	Time	42 bit s ⁻¹ (29 bit s ⁻¹)	47 km (60.5 km)	220 MHz	3 ns	BBM92 ⁵
Fiber-based ²²	Time	5.1 bit s ⁻¹	0 km	18 MHz	3.6 ns	E91 ⁶¹
PIC ¹⁵	Time	2.04 kbit s ⁻¹ (37 bit s ⁻¹)	0 km (60 km)	250 MHz	64 ps	BBM92 ⁵
Free space ²³	Time	5.1 kbit s ⁻¹	0 km	80 MHz	1 ns	BBM92 ⁵
Fiber-based ⁶²	Pol.	223 bit s ⁻¹	201 km	CW	—	Modified BBM92 ⁶³
Fiber-based ⁶⁴	Time + Pol.	700 bit s ^{-1a}	0 km	50 MHz	5 ns	Custom ⁶⁵
Fiber-based ⁵¹	Time-Energy	7 kbit s ⁻¹	50 km	CW	1.6 ns	Modified BBM92 ⁶⁶
TFLN (this work)	Time	25.4 kbit s⁻¹	0 km	1 GHz	100 ps	BBM92⁵

All implementations employ fiber-based channels, with channel losses scaling approximately as ~0.2 dB/km attenuation in standard single-mode fiber for the reported distances

PIC photonic integrated circuit

^aValues extracted from published plots

rather than the time-bin separation as in the passive-basis setup. This was made possible by the unique device’s capability to temporally overlap the two time bins through active switching and simultaneously apply a gigahertz-rate modulation in the Franson-like interferometer. The fast and accurate control of these modulations enables high visibility of quantum interference, as also confirmed by the low QBER values. In both QKD demonstrations, we report more than 12 h of continuous QKD operation without any interruption, drift, and the need for active stabilization of the interferometers’ bias, apart from standard temperature control of the device package following the initial calibration of the required operational phase settings.

Our results demonstrate that TFLN can be effectively adapted for quantum technologies, enabled by industrial- and commercial-grade fabrication processes. Indeed, the TFLN platform is an emerging technology originally developed for telecommunications, valued for its high-speed EO modulation. We tailored a complete compact device that integrates multiple high-quality optical components originally thought for classical telecom applications – including edge couplers, beam splitters, EO modulators, thermal phase shifters, and low-loss waveguides – on a single packaged chip, and we combine them to prove their suitability for quantum applications. Moreover, we prove the technology reliability by repeatable excellent performances even across different fabricated devices. We also demonstrate the first experimental implementation of the BBM92 protocol, taking advantage of the recently found Chernoff⁴¹ bound for SKR estimation, proving its advantage with respect to the previously-used Serfling⁴⁰ bound when small block lengths are used, as is commonly the case for EBQKD protocols.

The present integrated optical circuit can also be extended to other quantum applications. For instance, recently developed integrated interferometers for multi-dimensional time-bin states (up to 8 levels)¹⁵ could be combined with our switching approach to overcome the PSL. This would require multi-port interferometers with path delays in multiples of the time-bin spacing and multi-port switching via cascaded high-speed modulators. The realized device can also be directly employed for the implementation of entanglement swapping⁵². Furthermore, it can be combined with the processing of other degrees of freedom, such as frequency and polarization, by exploiting relatively fast EO modulators⁵³ and polarization filters⁵⁴. This integration could enable hyper-entangled quantum applications, including quantum secure direct communication (QSDC)^{55,56}, entanglement purification⁵⁷ and improve channel capacity.

Perspective device improvements primarily entail increasing the SKR. This could be first pursued by operating the protocol at higher clock rates. In the case of the active basis selection configuration, it is currently limited to 1 GHz for practical reasons (the limited bandwidth of the unbalanced MZI modulation stage, not optimized for broadband operation, as discussed in the “Materials and methods” section), but potentially compatible with up to 5 GHz, the maximum repetition rate set by the MZI unbalance delay. Conversely, in the case of passive-basis selection configuration for the investigated channel losses in this work, particularly in the low-loss regime, the achievable SKR is limited by the maximum detection rate of the SNSPDs (~1.5 MHz). If this limitation is overcome, the repetition rate could also reach 5 GHz without further hardware constraints. We stress that in our approach, when combined with state-of-the-art low-jitter SNSPDs⁵⁸ and a reduced unbalanced interferometer delay, the



maximum clock rate achievable is ultimately limited by the pulse duration, which in turn determines the minimum time-bin separation required to preserve orthogonality of the states. In particular, by employing broader-bandwidth optical pulses with picosecond-scale duration, this approach could potentially reach clock rates up to a hundred gigahertz, and a proportional increase in the SKR. A second aspect affecting the SKR, particularly severe in EBQKD protocols, is the overall setup losses. The optimization of the whole setup, including the design of the fabricated devices, will allow for a direct increase in the coincidence rates, and hence in the overall SKR.

To improve the security of the protocol in the active basis selection configuration and in real application scenarios, the PRBS modulation could be substituted by a QRNG⁴⁷, potentially realized through compact hybrid-integrated circuits⁴⁶, in order to guarantee certified randomness of the basis choice.

Further improvements concern the visibility of the interference fringes, where we achieve approximately 93.5% on average. This causes an increase in QBER, which ultimately limits the maximum range achievable for QKD. The primary limitation is attributed to polarization-mode mixing, namely, the coupling between TE and TM modes in the devices. This can be mitigated by integrating a polarization filter⁵⁴, which we have found to improve the extinction ratio from a tested median value of 19.3 dB to 34.2 dB in interferometric performance (see Supplementary Note 5); and using Euler bends⁵⁹ in future design improvements. Another suitable pathway may consist in the use of materials characterized by less severe birefringence, such as the emerging thin-film Lithium Tantalate (LiTaO₃) platform, exhibiting comparable Pockels coefficient⁶⁰. Other minor limiting factors for the reduced visibility are the CAR value, which is around ~100 for the presented experimental demonstrations, the residual unbalanced losses in the MZI stage, which can be mitigated with the adoption of variable attenuators²⁴, the non-ideal sinusoidal photon-switching modulation, and uncertainties in the applied bias and V_{pp} modulation signal.

From the perspective of scaling to large and multi-party optical networks, all the experimental implementations here reported were carried out using the standard ITU 100 GHz bandwidth allocation for each of the two user channels, which also matches the transform-limited photon bandwidth and optimizes spectral density. The quantum receiver platform also relies on components designed for C+L band operation, ensuring compatibility with DWDM systems and paving the way for scalable quantum networking over existing telecom infrastructure^{20–23}. By adopting quantum information density as a figure of merit, proposed by ref.¹⁵, defined as $d^N/(\Delta t \cdot \Delta \nu)$, our implementation achieves a value of $2^2/[100 \text{ ps} \cdot 2 \cdot (100 \text{ GHz} \cdot 2)] = 0.1$. This value is among the best

results reported in the literature, underlining the efficiency of our integrated solution in terms of both spectral and temporal resource utilization.

In summary, our work demonstrates a versatile and high-performance integrated photonic circuit based on the TFLN platform that allows the tailoring of pump pulse for the generation of time-bin states and overcoming the PSL limitation, certifies genuine time-bin entanglement, and enables stable, high-rate EBQKD, paving the way toward scalable quantum communication networks.

Materials and methods

Device fabrication and characterization

The integrated photonic devices were fabricated by Advanced Fiber Resources Milan s.r.l. on a 4-inch X-cut LNOI wafer. Optical waveguides featuring *rib* geometry are patterned by a deep UV (248 nm) stepper lithography (ASML PAS 5500/350C), on a 550 nm-thick LN layer with a 275 nm-deep etching, and are embedded in a silica cladding, supporting single-mode operation across the standard C+L telecom bands, with typical propagation losses of 0.2 dB cm^{-1} . The cladding thickness ensures full confinement of the optical mode within the LN layer and the surrounding glass matrix.

A schematic of the fabricated chip is shown in Fig. 1a. Input photons are coupled into the circuit via one of four edge couplers and initially pass through a 50:50 multimode interferometer (MMI) that forms the first-stage MZM, which functions as an optical switch. The MZM comprises two geometrically balanced optical arms, each equipped with a TPS for precise bias control. EO modulation is applied through 1 cm-long ground-signal-ground RF electrodes that drive the waveguides in push-pull configuration, enabling high-speed modulation.

The second stage of the device consists of a 2×2 MMI that connects to an unbalanced interferometer with a fixed delay of 100 ps between its two arms. The phase in the longer arm can be tuned using either a TPS or an EO phase modulator. The interferometer is closed by a third 2×2 MMI, which routes the outputs to two edge couplers for off-chip optical collection. The EO bandwidth of this second-stage interferometer is limited to approximately 1 GHz. This limitation arises primarily from packaging-related constraints, namely the lateral pins and long wire bonds, which feature a relatively low RF bandwidth as they are intended for driving components such as TPSs, since the package provides a high-speed RF connection to only one modulator. Secondly, the electrodes in the MZI are non-terminated. Both of these effects limit the overall bandwidth and lead to the peaking at ~500 MHz in Fig. 2c. While a push-pull configuration was not adopted in this iteration to keep the shorter arm as compact as possible (hundreds of microns), extending the interferometer arms to accommodate such an architecture—



while maintaining the necessary path-length imbalance—would improve by a factor of 2 the modulation efficiency ($V_\pi L$). We highlight that these limitations are mainly due to packaging constraints, but do not compromise the overall functionalities of the device. Adopting similar design solutions as used for the high-speed optical switch, a comparable performance for the unbalanced MZI could be achieved.

The devices used for the experimental demonstration exhibited an average insertion loss of approximately 6.5 dB due to both coupling and on-chip losses.

The balanced MZM is the key element of the device as it acts as a high-speed optical switch, deterministically routing early (late) time-bin photons to the longer (shorter) path of the interferometer. This configuration eliminates the need for temporal post-selection, enabling direct projection measurements. To achieve this, the switch must apply a π phase shift within a 100 ps time window, corresponding to a modulation frequency of 5 GHz. Thus, the RF line geometry must be carefully optimized to ensure efficient switching performance. The main design criteria include:

- Impedance matching between the RF line and the 50 Ω signal source to maximize power transfer.
- Velocity matching between the RF phase velocity and the optical group velocity to enhance EO bandwidth.
- Field overlap optimization between the RF and optical modes to minimize the modulation voltage (V_π).

At low frequency (1 MHz), the device exhibits $V_\pi = 3.37$ V, an estimated $V_\pi = 4.35$ V at 5 GHz, and a tested 3 dB EO bandwidth of approximately 30 GHz. The ultimate switching frequency of the MZM is estimated to be ~ 60 GHz when modulated with a sinusoidal signal for switching, and is primarily limited by the maximum allowable power dissipation in the integrated 50 Ω RF termination. Figure 6 shows a linear device characterization, displaying the interference pattern of the unbalanced MZI. In this case, when a continuous-wave (CW) laser is injected, the first balanced MZM is set in quadrature, and the output powers of the two outputs are recorded by sweeping the TPSs, registering an extinction ratio of approximately 20 dB. The relatively limited extinction ratio of the second-stage interferometer, which bounds the maximum achievable quantum interference visibility, is mainly attributed to polarization-mode mixing and differential losses between the two interferometer arms, rather than to any splitting imbalance of the 2×2 MMI (see Supplementary Note 5). The average thermal power required to achieve a π phase shift using the TPSs is $P_\pi = 23.5$ mW among the realized devices.

To ensure robustness and portability, the TFLN chip is fully integrated into a metal package, as shown in Fig. 1e. The optical interface consists of a pigtailed 4-channel

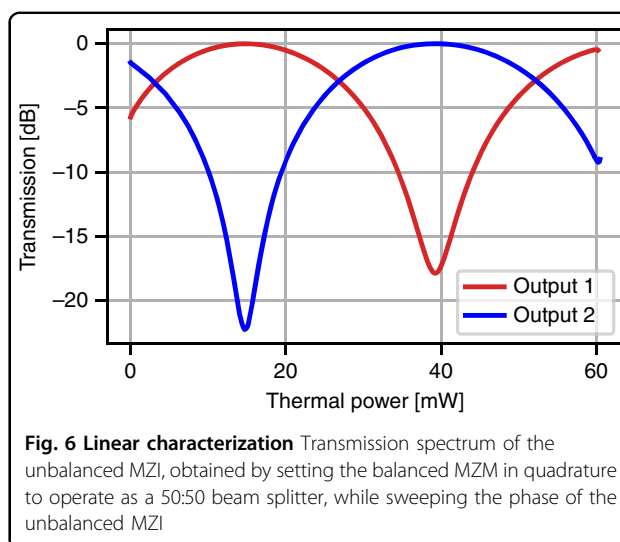


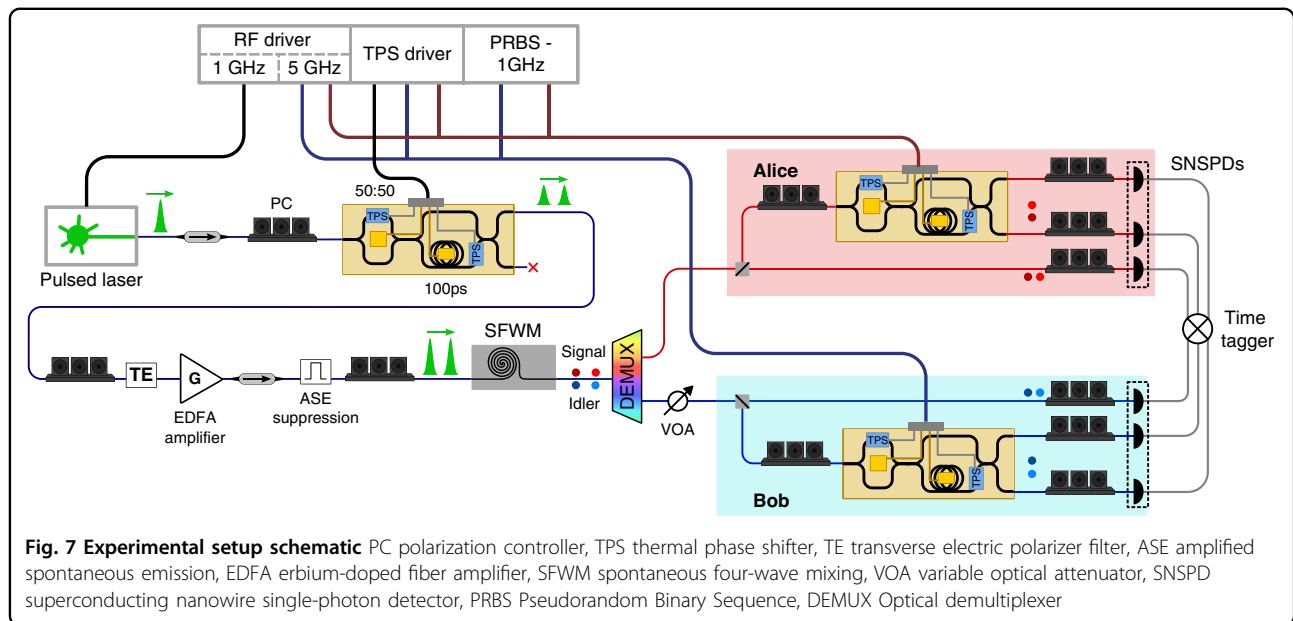
Fig. 6 Linear characterization Transmission spectrum of the unbalanced MZI, obtained by setting the balanced MZM in quadrature to operate as a 50:50 beam splitter, while sweeping the phase of the unbalanced MZI

fiber array unit (FAU) with Nufern UHNA7 fibers spliced to standard single-mode and polarization-maintaining fibers. The chip is mounted in the metal package using thermally conductive glue, improving heat dissipation and thermal stabilization. A standard G3PO RF connector is used to feed high-speed modulation signals to the MZM electrodes via precision wire bonding. All TPSs and the unbalanced MZI EO phase modulator are connected to external drivers through lateral package pins, which are wire-bonded to the corresponding chip contact pads.

Experimental setup

The experimental setup used for the experimental demonstration is shown in Fig. 7. For the generation of entangled states, it includes an actively mode-locked laser operating at a 1 GHz repetition rate, with a spectral bandwidth of 0.42 nm FWHM corresponding to 9.2 ps pulse duration centered at ITU channel 33 (1550.92 nm). The laser pulses pass through an optical isolator, and the polarization is adjusted to match the transverse electric (TE) mode of the fabricated TFLN photonic circuit. These pulses are then injected into the TFLN device, where the MZM is operated as a 50:50 beam splitter by tuning the TPS, generating two balanced time-bin pump pulses.

After exiting the device, the twin pulses are amplified using an erbium-doped fiber amplifier (EDFA), which also allows tunability of the pump power. The ASE noise from both the laser and the amplifier is effectively suppressed by several bandpass filters centered at the laser frequency. The filtered twin pulses are coupled via grating couplers into a 16 mm long silicon waveguide, realized on a 310 nm SOI layer thickness by the CEA-Leti pilot line, where pairs of entangled photons are generated by SFWM. At the output, the photon pairs are spectrally separated with two bandpass filters centered at ITU channels 28 and 38 (1554.94 nm and 1546.92 nm, respectively). This separates



the signal and idler photons, which are then forwarded to Alice and Bob's receivers.

The receiver configuration changes slightly depending on the performed application. In all configurations, polarization controllers are used before and after the device to match the TE polarization and maximize the SNSPD's efficiency. All three TFLN devices (one for pulse tailoring and two at the receivers) are connected to an external power supply to control the bias. For the balanced MZM, power is applied to only one of the two integrated TPSs while the second is grounded, as a single-phase shifter provides a sufficient tuning range for quadrature biasing. The TPS of the unbalanced MZI is controlled in a similar manner. We emphasize that no active feedback control system was required for any of the experimental measurements to compensate for bias drift. The device packaging, combined with temperature stabilization via a TEC system, is sufficiently stable against phase drifts. This approach simplifies the operating architecture by eliminating the need for complex auxiliary bias-tracking systems. The two receiver devices are also connected to an RF signal generator, which applies a sinusoidal voltage at 5 GHz with 4.35 V peak-to-peak amplitude, enabling operation of the optical switch. The RF source also drives the pulsed laser, ensuring synchronization among the two receiver users and the entangled photon source. The output signals from the SNSPDs are analyzed using a time tagger that records the detection events. The described setup is used for entanglement certification and quantum state tomography.

In QKD with passive-basis selection, a fiber-based 50:50 beam splitter is placed before the device in order to perform measurements in the computational basis Z . To perform the QKD implementation while varying the channel link

losses, a VOA is placed before Bob's beam splitter, which has 2 dB insertion loss at minimum attenuation. In the QKD with active basis selection, the beam splitter is removed, and the EO modulator in the unbalanced MZI is driven by an AWG (synchronized with the RF signal generator) to actively control the projective measurements.

Acknowledgements

A.B. acknowledges PNRR MUR project F13C22000920005. M.B. and M.C. acknowledge support of the Italian Ministry of Education (MUR) PNRR project PE0000023-NQSTI. M.G. acknowledges the PNRR MUR project CN00000013-HPC. S.C. acknowledges European Union funding from the STARLight project (project ID: 101194170). D.B. acknowledges the HyperSpace project (project ID 101070168). M.C. acknowledges funding from the European Union under the MSCA Postdoctoral Fellowship grant 101211100 (project GLINT). M.R.B. acknowledges support from the European Union's Horizon Europe Framework Programme under the Marie Skłodowska Curie Grant No. 101072637, Project Quantum-Safe Internet (QSI). The authors acknowledge CEA-Leti, Grenoble, for providing the silicon photonic chip used as a source of photon pairs.

Author details

¹Dipartimento di Ingegneria Industriale e dell'Informazione, Università di Pavia, Via A. Ferrata 5, 27100 Pavia, Italy. ²Advanced Fiber Resources Milan s.r.l., Via Fellini 4, 20097 San Donato Milanese, Italy. ³Dipartimento di Fisica "A. Volta", Università di Pavia, Via A. Bassi 6, 27100 Pavia, Italy. ⁴Dipartimento di Ingegneria dell'Informazione, Università degli Studi di Padova, Via Gradenigo 6B, 35131 Padua, Italy. ⁵CEA LETI and University Grenoble Alpes, MINATEC Campus, F-38054 Grenoble Cedex, France. ⁶Quantum Technologies Research Center, Università degli Studi di Padova, Via Gradenigo 6B, 35131 Padua, Italy

Author contributions

D.B. and M.G. conceived the conceptual idea. A.B., F.G., A.M., M.P., A.W., and F.A.S. engineered and fabricated the device. S.C. realized and optimized the Silicon source. A.B. and M.B. performed the experimental measurements under the coordination of M.C., M.G., and D.B. A.B. performed the data analysis, with support from M.R.B., C.A., G.V., and P.V. A.B. and M.C. wrote the manuscript, with support from M.R.B. All authors have proofread the manuscript.

Data availability

Data underlying the results presented in this paper are not publicly available at this time but may be obtained from the authors upon reasonable request.



Conflict of interest

The authors declare no competing interests.

Supplementary information The online version contains supplementary material available at <https://doi.org/10.1038/s41377-026-02306-5>.

Received: 10 October 2025 Revised: 25 March 2026 Accepted: 9 April 2026
Published online: 18 May 2026

References

- Schrödinger, E. Probability relations between separated systems. *Math. Proc. Camb. Philos. Soc.* **32**, 446–452 (1936).
- Nielsen, M. A. & Chuang, I. L. *Quantum Computation and Quantum Information* (Cambridge Univ. Press, Cambridge, 2010).
- Pittaluga, M. et al. Long-distance coherent quantum communications in deployed telecom networks. *Nature* **640**, 911–917 (2025).
- Ekert, A. K. et al. Practical quantum cryptography based on two-photon interferometry. *Phys. Rev. Lett.* **69**, 1293–1295 (1992).
- Bennett, C. H., Brassard, G. & Mermin, N. D. Quantum cryptography without Bell's theorem. *Phys. Rev. Lett.* **68**, 557–559 (1992).
- Bennett, C. H. & Brassard, G. Quantum cryptography: public key distribution and coin tossing. *Theor. Comput. Sci.* **560**, 7–11 (2014).
- Lo, H. K., Curty, M. & Tamaki, K. Secure quantum key distribution. *Nat. Photon.* **8**, 595–604 (2014).
- Ma, X. F., Fung, C. H. F. & Lo, H. K. Quantum key distribution with entangled photon sources. *Phys. Rev. A* **76**, 012307 (2007).
- Franson, J. D. Bell inequality for position and time. *Phys. Rev. Lett.* **62**, 2205–2208 (1989).
- Tittel, W. et al. Violation of bell inequalities by photons more than 10 km apart. *Phys. Rev. Lett.* **81**, 3563–3566 (1998).
- Brendel, J. et al. Pulsed energy-time entangled twin-photon source for quantum communication. *Phys. Rev. Lett.* **82**, 2594–2597 (1999).
- Marcikic, I. et al. Time-bin entangled qubits for quantum communication created by femtosecond pulses. *Phys. Rev. A* **66**, 062308 (2002).
- Montaut, N. et al. Progress in integrated and fiber optics for time-bin based quantum information processing. *Adv. Opt. Technol.* **14**, 1560084 (2025).
- Singh, A. et al. Photonic quantum information with time-bins: principles and applications. Preprint at <https://arxiv.org/abs/2507.08102> (2025).
- Yu, H. et al. Quantum key distribution implemented with d-level time-bin entangled photons. *Nat. Commun.* **16**, 171 (2025).
- Chapman, J. C., Lim, C. C. W. & Kwiat, P. G. Hyperentangled time-bin and polarization quantum key distribution. *Phys. Rev. Appl.* **18**, 044027 (2022).
- Congia, S. et al. Generation of hyperentangled photon pairs in the time and frequency domain on a silicon photonic chip. *Opt. Lett.* **50**, 5117 (2025).
- Patel, K. A. et al. Coexistence of high-bit-rate quantum key distribution and data on optical fiber. *Phys. Rev. X* **2**, 041010 (2012).
- Zhang, Q. et al. Generation of 10-GHz clock sequential time-bin entanglement. *Opt. Express* **16**, 3293–3298 (2008).
- Mueller, A. et al. High-rate multiplexed entanglement source based on time-bin qubits for advanced quantum networks. *Opt. Quantum* **2**, 64–71 (2024).
- Fitzke, E. et al. Scalable network for simultaneous pairwise quantum key distribution via entanglement-based time-bin coding. *PRX Quantum* **3**, 020341 (2022).
- Kim, J. H. et al. Quantum communication with time-bin entanglement over a wavelength-multiplexed fiber network. *APL Photon.* **7**, 016106 (2022).
- Huang, Y. W. et al. A sixteen-user time-bin entangled quantum communication network with fully connected topology. *Laser Photon. Rev.* **19**, 2301026 (2025).
- Finco, G. et al. Time-bin entangled bell state generation and tomography on thin-film lithium niobate. *npj Quantum Inf.* **10**, 135 (2024).
- Maeder, A. et al. Programmable bell state generation in an integrated thin film lithium niobate circuit. *Light Sci. Appl.* **15**, 43 (2026).
- Aerts, S. et al. Two-photon Franson-type experiments and local realism. *Phys. Rev. Lett.* **83**, 2872–2875 (1999).
- Jogenfors, J. et al. Hacking the Bell test using classical light in energy-time entanglement-based quantum key distribution. *Sci. Adv.* **1**, e1500793 (2015).
- Xavier, G. B. et al. Energy-time and time-bin entanglement: past, present and future. *npj Quantum Inf.* **11**, 129 (2025).
- Vedovato, F. et al. Postselection-loophole-free Bell violation with genuine time-bin entanglement. *Phys. Rev. Lett.* **121**, 190401 (2018).
- Verstraete, F. & Wolf, M. M. Entanglement versus Bell violations and their behavior under local filtering operations. *Phys. Rev. Lett.* **89**, 170401 (2002).
- Clauser, J. F. et al. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.* **23**, 880–884 (1969).
- Takesue, H. et al. Entanglement generation using silicon wire waveguide. *Appl. Phys. Lett.* **91**, 201108 (2007).
- Altepeter, J. B., Jeffrey, E. R. & Kwiat, P. G. Photonic state tomography. *Adv. At. Mol. Opt. Phys.* **52**, 105–159 (2005).
- Kuzucu, O. et al. Joint temporal density measurements for two-photon state characterization. *Phys. Rev. Lett.* **101**, 153602 (2008).
- Drago, C. & Sipe, J. E. Deconstructing squeezed light: Schmidt decomposition versus the whittaker-shannon interpolation. *Phys. Rev. A* **110**, 023710 (2024).
- Borghini, M. et al. Uncorrelated photon pair generation from an integrated silicon nitride resonator measured by time-resolved coincidence detection. *Opt. Lett.* **49**, 3966 (2024).
- Wootters, W. K. Entanglement of formation of an arbitrary state of two qubits. *Phys. Rev. Lett.* **80**, 2245–2248 (1998).
- Gisin, N. et al. Quantum cryptography. *Rev. Mod. Phys.* **74**, 145–195 (2002).
- Lo, H.-K., Chau, H. F. & Ardehali, M. Efficient quantum key distribution scheme and a proof of its unconditional security. *J. Cryptol.* **18**, 133–165 (2005).
- Tomamichel, M. et al. Tight finite-key analysis for quantum cryptography. *Nat. Commun.* **3**, 634 (2012).
- Mannalath, V., Zapatero, V. & Curty, M. Sharp finite statistics for quantum key distribution. *Phys. Rev. Lett.* **135**, 020803 (2025).
- Pelet, Y. et al. Entanglement-based clock syntonization for quantum key distribution networks: demonstration over a 50 km-long link. *Appl. Phys. Lett.* **126**, 174003 (2025).
- Williams, J. et al. Implementation of quantum key distribution and quantum clock synchronization via time bin encoding. In *Proc. SPIE 11699, Quantum Computing, Communication, and Simulation* 16–25 (SPIE, 2021).
- Calderaro, L. et al. Fast and simple qubit-based synchronization for quantum key distribution. *Phys. Rev. Appl.* **13**, 054041 (2020).
- Acin, A. et al. Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.* **98**, 230501 (2007).
- Peri, A. et al. High-performance heterodyne receiver for quantum information processing in a laser-written integrated photonic platform. *Adv. Photon.* **8**, 016009–016009 (2026).
- Bertapelle, T. et al. High-speed source-device-independent quantum random number generator on a chip. *Opt. Quantum* **3**, 111–118 (2025).
- Santagiustina, F. B. L. et al. Experimental post-selection loophole-free time-bin and energy-time nonlocality with integrated photonics. *Optica* **11**, 498–511 (2024).
- Marcikic, I. et al. Distribution of time-bin entangled qubits over 50 km of optical fiber. *Phys. Rev. Lett.* **93**, 180502 (2004).
- Honjo, T. et al. Long-distance entanglement-based quantum key distribution over optical fiber. *Opt. Express* **16**, 19118–19126 (2008).
- Pelet, Y. et al. Operational entanglement-based quantum key distribution over 50 km of field-deployed optical fibers. *Phys. Rev. Appl.* **20**, 044006 (2023).
- de Riedmatten, H. et al. Long-distance entanglement swapping with photons from separated sources. *Phys. Rev. A* **71**, 050302 (2005).
- Tagliavacche, N. et al. Frequency-bin entanglement-based quantum key distribution. *npj Quantum Inf.* **11**, 60 (2025).
- Zhang, J. et al. Compact polarization splitter-rotator based on lithium niobate-on-insulator platform. *J. Appl. Phys.* **136**, 164503 (2024).
- Sheng, Y.-B., Zhou, L. & Long, G.-L. One-step quantum secure direct communication. *Sci. Bull.* **67**, 367–374 (2022).
- Yang, Y. L. et al. A 300-km fully-connected quantum secure direct communication network. *Sci. Bull.* **70**, 1445–1451 (2025).
- Sheng, Y.-B. & Deng, F.-G. Deterministic entanglement purification and complete nonlocal Bell-state analysis with hyperentanglement. *Phys. Rev. A* **81**, 032307 (2010).
- Korzh, B. et al. Demonstration of sub-3 ps temporal resolution with a superconducting nanowire single-photon detector. *Nat. Photon.* **14**, 250–255 (2020).
- Jiang, X. H., Wu, H. & Dai, D. X. Low-loss and low-crosstalk multimode waveguide bend on silicon. *Opt. express* **26**, 17680–17689 (2018).
- Wang, C. L. et al. Lithium tantalate photonic integrated circuits for volume manufacturing. *Nature* **629**, 784–790 (2024).



61. Ekert, A. K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67**, 661–663 (1991).
62. Zhuang, S.-C. et al. Ultrabright entanglement based quantum key distribution over a 404 km optical fiber. *Phys. Rev. Lett.* **134**, 230801 (2025).
63. Lim, C. C. W. et al. Security analysis of quantum key distribution with small block length and its application to quantum space communications. *Phys. Rev. Lett.* **126**, 100501 (2021).
64. Zhong, Z.-Q. et al. Hyperentanglement quantum communication over a 50 km noisy fiber channel. *Optica* **11**, 1056–1061 (2024).
65. Doda, M. et al. Quantum key distribution overcoming extreme noise: Simultaneous subspace coding using high-dimensional entanglement. *Phys. Rev. Appl.* **15**, 034003 (2021).
66. Neumann, S. P. et al. Continuous entanglement distribution over a transnational 248 km fiber link. *Nat. Commun.* **13**, 6134 (2022).

