npj | quantum information

Published in partnership with The University of New South Wales

Article

https://doi.org/10.1038/s41534-025-00991-5

Frequency-bin entanglement-based Quantum Key Distribution

Noemi Tagliavacche[1], Massimo Borghi[1] ✉, Giulia Guarda[2,3], Domenico Ribezzo[3,4], Marco Liscidini[1], Davide Bacco[5,6], Matteo Galli[1] & Daniele Bajoni[7]

Entanglement is an essential ingredient in many quantum communication protocols. In particular, entanglement can be exploited in quantum key distribution (QKD) to generate two correlated random bit strings whose randomness is guaranteed by the nonlocal property of quantum mechanics. Most of QKD protocols tested to date rely on polarization and/or time-bin encoding. Despite compatibility with existing fiber-optic infrastructure and ease of manipulation with standard components, frequency-bin QKD have not yet been fully explored. Here we report a demonstration of entanglement-based QKD using frequency-bin encoding. We implement the BBM92 protocol using photon pairs generated by two independent, high-finesse, ring resonators on a silicon photonic chip. We perform a passive basis selection scheme and simultaneously record sixteen projective measurements. A key finding is that frequency-bin encoding is sensitive to the random phase noise induced by thermal fluctuations of the environment. To correct for this effect, we developed a real-time adaptive phase rotation of the measurement basis, achieving stable transmission over a 26 km fiber spool with a secure key rate ≥ 4.5 bit/s. Our work introduces a new degree of freedom for the realization of entangled based QKD protocols in telecom networks.

The generation and distribution of entanglement at large distances is pivotal to the development of large-scale architectures for distributed quantum computing, metrology and communication[1]. One of the most successful implementations is quantum key distribution, which enables two remote parties to establish a shared string of bits (key) with unconditional security[2]. The security of entanglement-based QKD comes from the non-local correlations between entangled particles and is guaranteed by the Bell's theorem[3]. Under these assumptions, a secret key can be exchanged between two users even if their hardware is partially or completely untrusted[4,5]. Additionally, employing entanglement relaxes the bounds in security proofs[5,6]. In recent years, much progress has been made to close loopholes[3,7], increase the data rate[8,9], the communication distance[10,11] and the network size[12–14]. Most of the experiments use entangled photon pairs generated by spontaneous parametric down conversion (SPDC) in nonlinear crystals because they have high rates, broadband emission, and great versatility[12,15,16]. Depending on crystal engineering and pump configuration, entangled photon pairs can be created in different degrees of freedom, of which the most exploited are energy[12], time-bin[16] and polarization[17]. Time and polarization are easily manipulated with table-top solutions such as waveplates and beamsplitters, which can be made cost-effective at telecommunication wavelengths using the widely deployed fiber-optic components.

In parallel, chip-based quantum key distribution has emerged as a promising direction for making QKD more practical and scalable[18]. By integrating most of the components onto a compact photonic chip, chip-based QKD allows for the miniaturization of quantum communication systems, significantly improving their stability and speed of operation, reducing their cost and energy consumption. To date, most of the work focused on the realization of transceiver modules for polarization or time-bin encoding using attenuated laser pulses[19,20]. However, the ever-growing demonstrations of integrated photon pair sources of ultra-high brightness[21], wide bandwidth of emission[22], and the generation of entangled photons over multiple degrees of freedom[23] and in multiple dimensions[24], motivate the integration of on–chip entanglement-based QKD solutions. For example, recent experiments have demonstrated the transmission of secure keys by using photon pairs generated by SPDC in an AlGaAs nanowire using polarization encoding[25], or by spontaneous four-wave mixing (SFWM) in an AlGaAs resonator by exploiting energy-time entanglement[26]. A wide-

---

[1]Dipartimento di Fisica, Università di Pavia, Via Bassi 6, Pavia, Italy. [2]European Laboratory for Non-Linear Spectroscopy (LENS), Sesto Fiorentino, Italy. [3]CNR-National Institute of Optics (CNR-INO), Florence, Italy. [4]University of L' Aquila, Department of Physical and Chemical Sciences, L' Aquila, Italy. [5]QTI S.r.l., Firenze, Italy. [6]University of Florence, Department of Physics and Astronomy, Sesto Fiorentino, Italy. [7]Dipartimento di Ingegneria Industriale e dell'Informazione, Università di Pavia, Via Ferrata 5, Pavia, Italy. ✉e-mail: massimo.borghi@unipv.it

bandwidth photon pair source from a silicon nanowire has been used in a fully connected network of 40 users, realized by a combination of beamsplitters and wavelength multiplexing[13]. Similarly, a silicon nitride resonator was used as the source of nonclassical light of a four-user quantum network[22]. Chip-to-chip entanglement distribution has been demonstrated using path-encoding[27] and path-to-polarization conversion in a optical fiber[28]. Entanglement has also been distributed by using time-bin qudits, harnessing the intrinsic phase stability of on-chip interferometers in silica[29] and thin-film lithium niobate[9].

Much less explored is frequency-bin encoding, i.e. the possibility to encode and manipulate qubits in the frequency degree of freedom[30]. This strategy has great potential because it is compatible with the existing fiber-optic infrastructure, it is a good candidate for high-dimensional encoding and can be easily manipulated with standard components for telecommunication[31]. However, despite progresses in quantum state engineering[32,33], entanglement distribution, and advancements in the implementation of single and multiple qubit gates[34], the use of frequency-bin encoding for QKD has not yet been fully explored. At the moment of writing, only a feasibility study of entanglement based QKD with frequency bin qubits has been reported, which implements photon pairs generated by a large silicon micro-resonator with a free spectral range of 21 GHz[35]. However, the demonstration still has some missing parts, such as random basis selection, simultaneous detection of all the possible measurement outcomes and radio-frequency (RF) clock distribution between the remote users. In addition, the robustness of frequency-bin encoding to both phase noise and bit-flip errors in real-field transmission tests has not been studied systematically. Here we address these missing points and report the a demonstration of entanglement based QKD using frequency-bin encoding. Entangled photon pairs are generated by two ring resonators of high-finesse on a silicon photonic chip. The use of independent resonators driven by two mutually coherent pumps[32,33] allows us to simultaneously achieve a high pair generation rate of 27 MHz/mW^2 and a small frequency-bin spacing of 15 GHz, suitable for frequency mixing by electro-optic modulation using commercial devices. We implement passive basis selection and simultaneously record all sixteen projective measurements using six superconducting detectors. A key finding is that the random phase noise induced by thermal fluctuations of the environment impairs transmission after few km of fiber, thus we implement a real-time phase compensation system that keeps the quantum bit error rate (QBER) low and stable over the time. A systematic investigation of phase noise is performed by correlating the phase drift between frequency-bins, the variation of optical path in the fiber and its temperature. Stable transmission is demonstrated in fiber spools of different lengths up to 26 km. Overall, our work incorporates all the elements to realize frequency-bin QKD with entangled photons in telecom networks.

Results

Device and experimental setup

A simplified version of the experimental setup is shown in Fig. 1a. A tunable and continuous wave pump laser at 1543.69 nm is sent through an electro-optic phase modulator (PM) driven by a sinusoidal RF signal at a frequency of 15 GHz. The process of phase modulation creates several frequency-sidebands that are mutually coherent with the input pump laser and equally spaced in frequency by the modulation frequency[32,33]. The amplitude of the RF driving signal is adjusted to equalize the intensity of the baseband comb line with that of the first-order sidebands. After amplification, we used a bandpass filter to isolate approximately three coherent comb lines of equal amplitude and to remove background noise. A narrowband fiber Bragg grating (FBG) is then employed to eliminate one of the three comb lines. The pump, now consisting of two mutually coherent comb-lines separated by 15 GHz, is then coupled to a silicon chip by using a lensed fiber. An on-chip inverse taper with a 160 nm tip allows us to achieve a coupling loss of 3.5 dB/facet. The pump excites two nominally identical microring resonators (labelled as R0 and R1 in Fig. 1a), which are coupled to the same bus waveguide. Metallic heaters are placed on the top of the rings and allows one to thermally tune the resonance wavelength. More details on the sample geometry and fabrication are provided in[32,33]. The spectral response of the device is shown in Fig. 1b, which highlights the set of resonances used to generate the signal and the idler entangled photon pairs by SFWM. Metallic heaters were used to tune all the resonances of R0 and R1 to a frequency-bin spacing of 15 GHz, matching the frequency separation between the two comb lines of the pump laser. The resonators have a free spectral range of ~524 GHz and a loaded quality factor of 10^5. Each ring is actively locked to a different comb line of the pump laser using a Field Programmable Gate Array (FPGA) that controls the heater currents. A distinct dither tone is applied to each ring and revealed by homodyne detection to minimize the pump transmission. The locking allows one to maximize the pair generation rate and to keep it stable over time. The two pumps trigger photon-pair generation from R0 and R1 in a coherent superposition of the corresponding set of resonances ($|0\rangle_s|0\rangle_i$ for R0, $|1\rangle_s|1\rangle_i$ for R1, see Fig. 1)[32,33]. We adjusted the relative intensity and phase of the comb lines of the pump laser

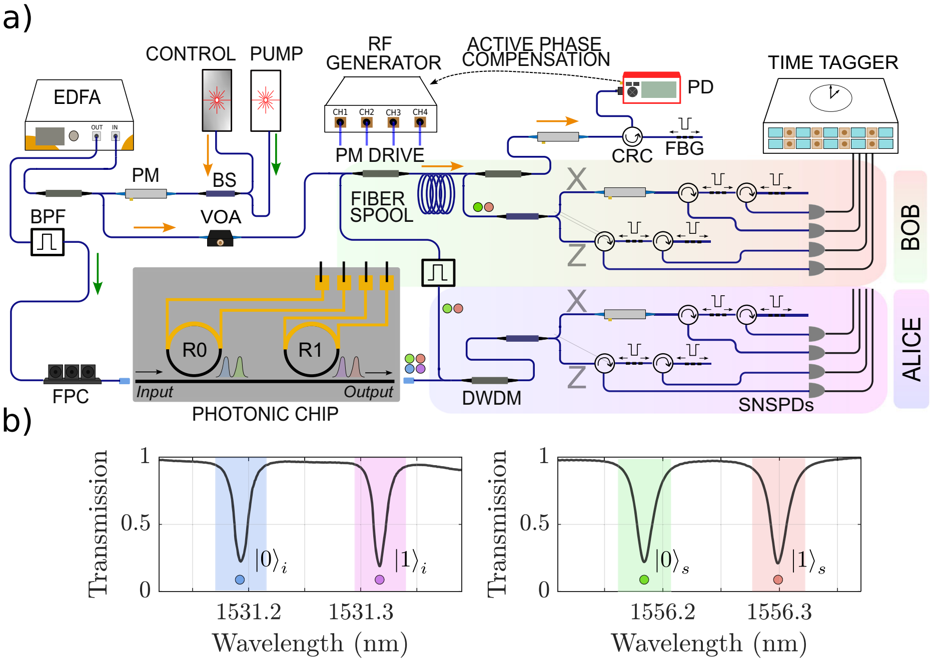

Fig. 1 | Experimental setup and device spectra. **a** Simplified sketch of the experimental setup. The direction of the pump(control) laser is indicated with a green(orange) arrow. Optical connections are shown in blue. The frequency-bins of the Alice's photon (idler) are indicated by a blue and a violet filled circle, while those directed to Bob (signal) by a green and a red filled circle. BS beamsplitter, EDFA Erbium Doped Fiber Amplifier, VOA Variable Optical Attenuator, FPC Fiber Polarization Controller, BPF bandpass filter, DWDM Dense Wavelength Division Multiplexing, PM electro-optic phase modulator, CRC circulator, FBG fiber Bragg grating, SNSPD superconducting nanowire single photon detector, PD photodiode. The layout of the chip shows the two resonators R0 and R1 (black), and the placement of the metallic heaters (yellow). **b** Spectral response of the device at the idler (left) and signal (right) wavelengths. The encoding of the signal and idler qubits is shown with the same colors used in panel (**a**).

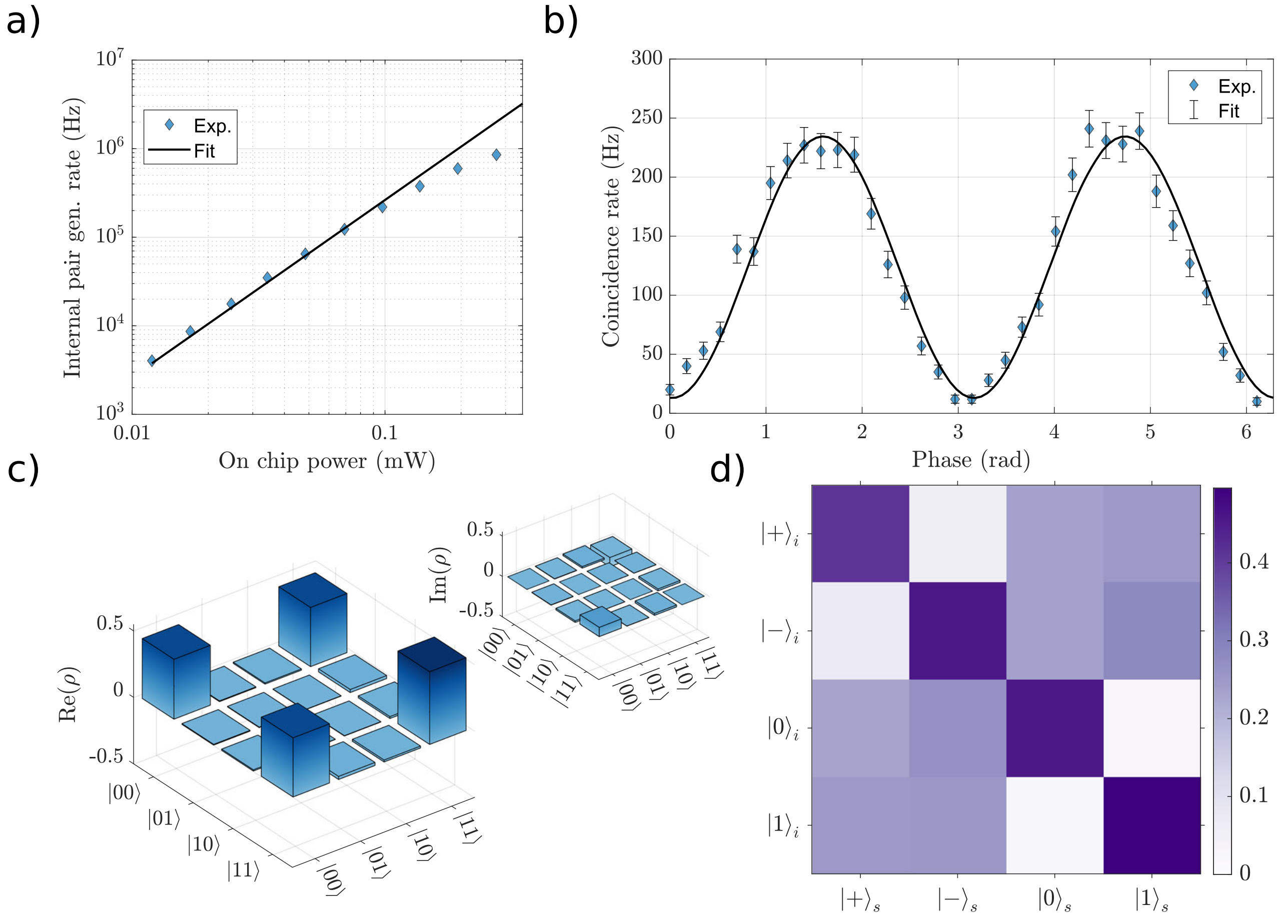

Fig. 2 | Characterization of the photon pair sources. a On-chip pair generation rate of ring R0 for different pump powers P. The data is fit with the model aP^2 (solid black line) for $P < 100\,\mu W$. **b** Bell fringe without any fiber spool applied to Bob's arm. Accidental counts are not subtracted. The solid black line is a sinusoidal fit of the data. **c** Reconstructed real and imaginary (top-right inset) part of the density matrix of the state at the output of the chip. **d** Correlation matrix of the probability outcomes on the two mutually unbiased basis sets $X_{s(i)} = \{|+\rangle_{s(i)}, |-\rangle_{s(i)}\}$ and $Z = \{|0\rangle_{s(i)}, |1\rangle_{s(i)}\}$ for the signal(idler) photon.

to generate the maximally entangled Bell state $|\Psi^+\rangle = (1/\sqrt{2})(|0\rangle_s|0\rangle_i + |1\rangle_s|1\rangle_i)$[33]. We stress that coherence between the terms $|0\rangle_s|0\rangle_i$ and the $|1\rangle_s|1\rangle_i$ is inherited from the coherence between the two comb lines of the pump laser. The phase between the two terms in the Bell state is defined at the input of the phase modulators used for the X-basis measurement, and is controlled by adjusting the phase of the sinusoidal RF signal which drives the PM of the pump. A lensed fiber is used to couple light out of the chip, and a DWDM filter splits the signal and the idler photon into different paths. From now on, we will refer to the idler at ~1531.3 nm as the Alice's photon, while to the signal photon at ~1556.3 nm as the Bob's photon. The residual pump is removed in both paths using bandpass filters with high-extinction ratio. A fiber spool is then introduced into Bob's path. The length of the spool is varied in the transmission tests until a maximum of 26 km. We exploited 50/50 beamsplitters to execute passive basis selection among the $Z = \{|0\rangle, |1\rangle\}$ and $X = \{|+\rangle = (1/\sqrt{2})(|0\rangle + |1\rangle), |-\rangle = (1/\sqrt{2})(|0\rangle - |1\rangle)\}$-basis. The measurement in the Z-basis is performed by using two fiber Bragg gratings (FBG, 12.5 GHz of bandwidth) to reflect the $|0\rangle_{s(i)}$ and the $|1\rangle_{s(i)}$ frequency-bin into two superconducting nanowire single-photon detectors (SNSPD) (85% of detection efficiency). The measurement in the X basis is performed by mixing the $|0\rangle_{s(i)}$ and $|1\rangle_{s(i)}$ frequency-bins by using two PM[32]. A time tagging electronics is used to detect and record the arrival times of the signal and idler photons. The post-processing of the timestamps allows us to unambiguously identify the events of all the sixteen mutually exclusive outcomes, corresponding to the different Alice's and Bob's states combinations. It is worth to note that, while the setup in Fig. 1a shows the use of eight SNSPDs, in the actual experiment we implemented only six detectors (see supplemental document). The two schemes are equivalent but we adopted the sketch in Fig. 1a for ease of understanding. The detailed scheme of the actual experimental setup and the analysis of timestamps is reported in detail in the supplemental document.

Characterization of the photon pair sources

We characterized the brightness of both photon pair sources and the level of background noise, which will impact the secure key rate and the QBER. The brightness is extracted by measuring the coincidence rate at the detector for different input pump powers, and by exciting only one source at a time. Coincidences are recorded within a window of 700 ps. This is shown in Fig. 2a for ring R0 (results for R1 are very similar and not shown). The on-chip generation rate is obtained from the raw coincidence rate at the detectors by correcting for the total losses from generation to detection. The coincidences are fit with a quadratic function of the pump power up to $100\,\mu W$, from which a brightness of 27(1) $\mathrm{MHz} \cdot \mathrm{mW}^{-2}$ is extracted. The deviation from a quadratic behavior for input powers $> 100\,\mu W$ is due to two-photon absorption and induced free-carrier absorption in silicon[36]. From now on, in all the experiments we set the pump power of each comb line to $200\,\mu W$, corresponding to a on-chip pair generation rate of ~0.7 MHz and a measured coincidence to accidental ratio (CAR) of ~20[36].

Another relevant metric that we extracted is the visibility of two-photon interference from the pairs generated by R0 and R1. The sources are simultaneously excited and their pair generation rate is equalized by regulating the relative intensity of the comb lines of the pump laser. We used the Alice and Bob PM to project their respective photons along the equator of their Bloch sphere, i.e. we performed the local projector $(1/\sqrt{2})(\langle 0|_{s(i)} + e^{i\theta_{s(i)}}\langle 1|_{s(i)})$, with $\theta_s = \theta_i = \theta$. We swept θ by changing the

RF phase driving both PM, and recorded the two-photon interference fringe shown in Fig. 2b. The raw visibility (without background subtraction) is 89.5(2)%, which increases to 93.3(2)% by correcting for the accidental counts. The visibility is limited by the distinguishability between photons generated by R0 and R1[33]. To fully characterize the state, we also performed quantum state tomography using a complete set of projectors (the tensor product of the eigenvectors of three Pauli operators Z, X and Y of the signal/idler qubits), and reconstructed the density matrix of the state using a standard maximum likelihood approach[33]. The density matrix, shown in Fig. 2c, has an Ulhman fidelity of 0.941(2) with the target $|\Psi^+\rangle\langle\Psi^+|$.

The performance of the Alice and Bob receiver is assessed by performing correlation measurements in the Z and X-basis. Ideally, the measurement outcomes should be perfectly correlated when the two parties choose the same basis (XX and ZZ correlation subspaces), and completely random when they choose different basis (XZ and ZX correlation subspaces). Randomness in the outcome is ensured by the fact that the two basis are mutually unbiased. The measured correlation matrix T_{exp} is shown in Fig. 2d. The probabilities are normalized in each of the four (XX, XZ, ZX, ZZ) 2×2 subspaces. We evaluated the fidelity $\mathcal{F}$ with the ideal correlation matrix T_{th} as

$$\mathcal{F} = \frac{\mathrm{Tr}(T^{\dagger}_{\text{exp}} T_{\text{th}})\mathrm{Tr}(T^{\dagger}_{\text{th}} T_{\text{exp}})}{\mathrm{Tr}(T^{\dagger}_{\text{exp}} T_{\text{exp}})\mathrm{Tr}(T^{\dagger}_{\text{th}} T_{\text{th}})}, \tag{1}$$

where $T^{\dagger}$ is the matrix transpose. The fidelity between T_{exp} and T_{th} is 0.987(1), while the fidelities $\mathcal{F}_{ij}(i = \{X, Z\}, j = \{X, Z\})$ of the four subspaces are $\mathcal{F}_{XX} = 0.975(2)$, $\mathcal{F}_{ZZ} = 0.995(2)$, $\mathcal{F}_{XZ} = 0.994(2)$ and $\mathcal{F}_{ZX} = 0.997(2)$.

Secure key rate analysis for different lengths of fiber spool

We adopt the BBM92 protocol for secure key exchange, a variation of the BB84 protocol that employs entangled photons[37], and calculate the lower bound for the secure key rate initially under the infinite key approximation, which is given by[38]

$$\mathrm{SKR} \geq [1 - H_2(\varepsilon_Z)f - H_2(\varepsilon_X)]S\,R_r\,\alpha\,\eta. \tag{2}$$

Here, $H_2(x)$ is the entropy of the binary variable x, $\varepsilon_Z(\varepsilon_X)$ is the QBER in the Z (X) basis, and $f > 1$ is the error reconciliation efficiency. The term $H_2(\varepsilon_Z)f$ represents the number of bits disclosed during the error correction protocol, so discarded from the total key length estimation. The term $H_2(\varepsilon_X)$ keeps into account the bits lost during the privacy amplification, necessary to minimize the correlation between Alice's and Bob's keys with the key owned by a potential eavesdropped (Eve). S represents the sifting ratio, i.e., the amount of bits discarded during the basis reconciliation process, R_r is the qubit generation rate, α is the channel attenuation and η is the detectors' efficiency.

Furthermore, to consider a scenario as realistic as possible, we subtract from the calculated rate the term associated with the finite-size effect. This effect arises because estimating variables from a finite data sample introduces errors, potentially leading to an overestimation of the key rate[5,10]. Figure 3a illustrates the key rate as a function of increasing block sizes n_Z. The block size represents a set of collected states used for executing post-processing algorithms. For the key rate in the finite-size key regime we have[5]:

$$\mathrm{SKR}_{fin} = \mathrm{SKR} - \Delta(n_Z, \epsilon_{sec}) - \lambda_{EV}. \tag{3}$$

Here, $\Delta(n_Z, \epsilon_{sec}) = \sqrt{\log(1/\epsilon_{sec})/n_Z}$ is derived directly from the Hoeffding inequality. It guarantees that the probability of the secret key rate being less than $\mathrm{SKR} - \Delta(n_Z, \epsilon_{sec})$ is at most ϵ_{sec}. The term $\lambda_{EV} = \log_2(2/\epsilon_{cor})/\tau_{n_Z}$, with τ_{n_Z} being the time necessary to exchange a block size, must be subtracted to account for the error verification stage. This ensures that the probability of Alice's and Bob's keys differing is at most ϵ_{cor}.

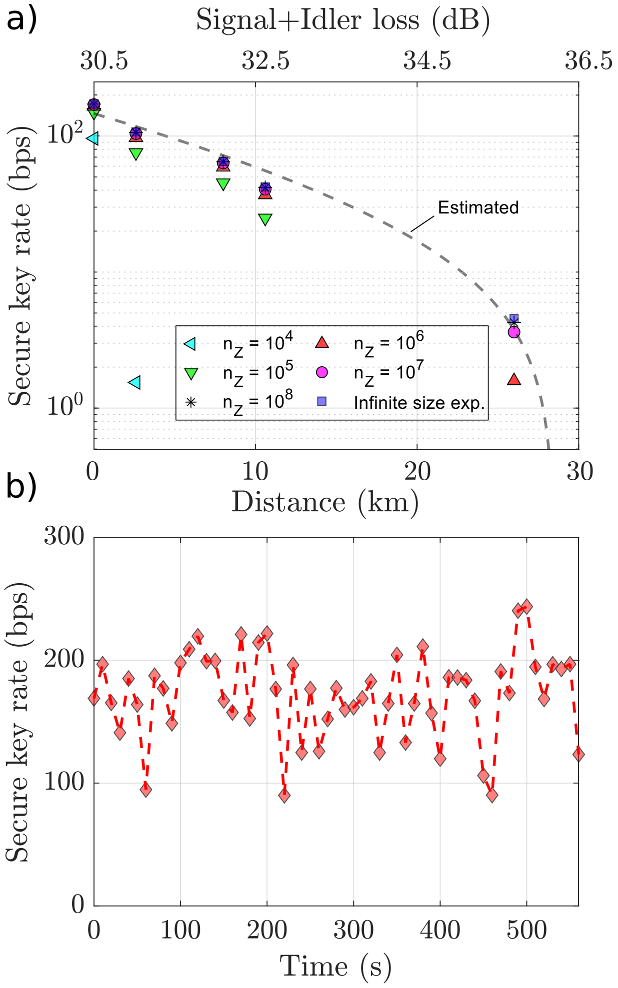

Fig. 3 | Secure key rate analysis. a Secure Key rate as a function of distance (length of the fiber spool). The points represent the experimental data. The dotted line represents the estimated SKR using Eq. (2). Different symbols are used to show finite-size effect for different block sizes n_Z The total loss include that related to the fiber spool and the loss from the chip to the detectors (averaged over all the possible signal-idler paths leading to a coincidence event). **b** Secure key rate in the infinite-key approximation as a function of time without the fiber spool inserted in the Bob path.

Table 1 | QBER measured in the X and Z basis for different length of fiber spools inserted in the Bob arm

Fiber length (km)	ε_Z	ε_X
0	0.049(2)	0.13(1)
2.6	0.054(2)	0.14(1)
8	0.057(2)	0.138(8)
10.6	0.057(2)	0.14(1)
26	0.065(3)	0.143(8)

We evaluate the QBER and the SKR for fiber spools of different lengths, which are 0 km (no spool), 2.6 km, 8 km, 10.6 km and 26 km. The QBER in both the X and Z basis is listed in Table 1. We see that $\varepsilon_X > \varepsilon_Z$ for all the investigated fiber lengths. This is expected because the measurements in the X-basis are phase-sensitive, and systematic errors are also introduced by the imperfect indistinguishability of the sources. In contrast, the QBER in the Z basis is primarily affected by the CAR, which remain stable as the photons travel through different fiber lengths without undergoing dephasing. The impact of dark counts from the detectors (< 120 Hz) on the

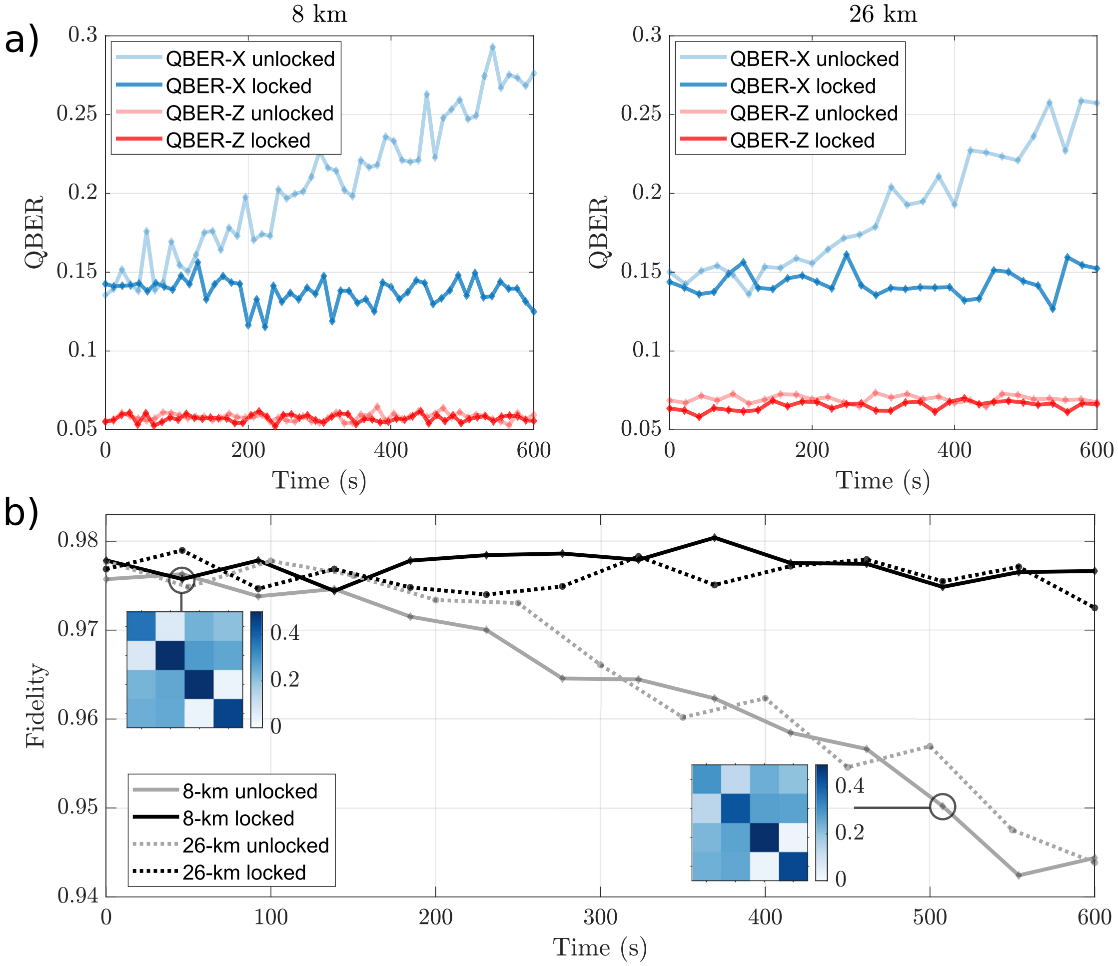

Fig. 4 | Stability of the QBER and evolution of the correlation matrix over time. **a** QBER variations on the X and Z basis as a function of time with (locked) and without (unlocked) active phase compensation. In left-panel, the signal photon propagates along 8 km of fiber spool, while in the right panel along 26 km. **b** Fidelity between the experimental and the theoretical correlation matrix of the outcomes between the X and Z basis as a function of time. The black(gray) lines indicate the fidelity with the active phase compensation turned on(off). The two insets show the correlation matrix at two different times.

QBER is minimal because the associated coincidence rate is ~ 10^{-3} Hz. Figure 3a shows the SKR achieved for the different lengths of the inserted fiber spool. Successful SKR extraction is demonstrated up to a fiber spool length of 26 km, for which SKR≥ 4.5 bps. The (fixed) high losses of the Alice and Bob receiving stages (~ 30 dB, see Fig. 3a) account for most of the loss budget, limiting the maximum propagation distance to ~30 km. We did not noticed any impairment induced by the transmission in the fiber (for example fiber dispersion and/or spontaneous Raman scattering). The experimentally measured secure key rate aligns well with the expected results (dashed curve in Fig. 3a), which are simulated by taking into account the source generation rate, the losses, and the detector efficiencies. Up to 2.6 km, the SKR is also stable over time, as shown in Fig. 3b in the case where no fiber spool inserted into Bob's path.

Active phase-drift compensation

We assessed the stability of the QBER on the X and Z basis over time for all the different lengths of fiber spool. Up to 2.5 km, the QBER on both basis does not vary significantly during a monitoring time of 600 s, with an root mean square variation < 6%. At longer propagation lengths, we systematically observed an increase of the ε_X with time, with no variations of the ε_Z. This trend is shown in Fig. 4a for a fiber length of 8 km and 26 km. Consequently, the fidelity $\mathcal{F}$ between the experimental and the ideal correlation matrix decreases over time, as shown in Fig. 4b. From an initial value of $\mathcal{F} \sim 0.98$, the fidelity drops to a final value of $\mathcal{F} \sim 0.94$ after ~600 s. By comparing the initial and the final correlation matrices (insets in Fig. 4b), we notice that only the elements in the XX subspace are changed. In particular, the off-diagonal components increased, indicating that the state at the Alice and Bob's modulators is no longer $|\Psi^+\rangle$ but gets rotated in time by some angle θ, i.e $|\Psi^+\rangle \to \left(1/\sqrt{2}\right)\left(|00\rangle + e^{i\theta}|11\rangle\right)$. Importantly, this rotation does not affect the correlations on the ZX and ZZ subspaces. We attributed the rotation to a time-varying variation of the optical path between the $|0\rangle_s$ and $|1\rangle_s$ frequency-bin states during the propagation along the fiber spool. Indeed, if the signal and idler photon are sent to two different fibers of length L_s and L_i, with $L_s \gg L_i$, then $\theta = 2\pi\Delta\nu\delta[n(L_s - L_i)]/c \sim 2\pi\Delta\nu\backslash\delta[nL_s]/c$, where $\delta[nL_s]$ is the variation of the optical path nL_s, n is the effective index of the optical fiber and c is the speed of light. Thus, an optical path variation of the order of few cm is sufficient to transform the state from $|\Psi^+\rangle$ to $|\Psi^-\rangle$, modifying the measurement outcomes on the XX subspace from being perfectly correlated to be completely anti-correlated. To the first order, $\delta[nL_s] = \delta[n]L_s + n\delta[L_s]$, i.e., both refractive index variations and changes in the physical length of the fiber affect the optical path length. The slow drift of θ (hence of ε_X and of $\mathcal{F}$) seen in Fig. 4 suggests that such variations could be induced by temperature fluctuations of the environment. To verify this hypothesis, we conducted an experiment in which the temperature of a 26 km fiber spool is changed, and the optical path length $\Delta L_{\mathrm{eff}} = \delta[nL_s]$ is continuously monitored from the time of flight of a ps laser pulse propagating in the spool, which is measured by a fast APD with 40 ps of timing jitter. By correlating ΔL_{eff} with the temperature variation, which is measured by a thermistor placed in direct contact with the spool, a linear relationship is found, with a slope of $1.01(1)\,\frac{\mathrm{cm}}{\mathrm{km}\,^{\circ}\mathrm{C}}$. In addition, we continuously monitored

Table 2 | Reported values of SKR and QBER (average between ε_X and ε_X) for the BBM89 protocol with different integrated photon-pair sources and types of encoding

Encoding	Source	Secure Key Rate (bps)	QBER (%)	Distance (km)	Ref.
Polarization	AlGaAs waveguide	30	< 2	25	25
Time-bin	Fiber-coupled PPLN waveguide	125	2.4	31.2	16
Time-energy	SiN ring resonator	205	3.08	0	22
Time-bin	High Index doped Silica spiral waveguide	200	–	25	29
Polarization	AlGaAs waveguide	0.21	6.9	50	47
Time-energy	Silicon spiral waveguide	4-6	7–8	12.3	48
Time-energy	AlGaAs ring resonator	2000	9	0	26
Frequency-bin	Silicon ring resonator	2.5	8-9	0	41
Frequency-bin	Two silicon ring resonators	4.5 (180 projected*)	10.4	26	This work

(*) Estimated using Eq. (2) by using channel loss of 7 dB for both the signal and the idler photon and the values of ε_X and ε_Z at 26 km in Table 1.

the temperature of the laboratory for 10 h, from which we evaluated an average variation of ~ 0.03(1)°C every 600 s. From this we extrapolated an average variation of the optical path of ~ 0.03 cm ($\theta \sim 0.1$ rad) per km of fiber every 600 s. These results indicate that the random temperature fluctuations of the environment are sufficient to cause a change of θ of the order of few radians for fiber spools of tens km of length, which justify the degradation of the ε_X over time shown in Fig. 4a.

The phase drift must be compensated to guarantee stable data transmission with a low QBER. To this goal, we developed a technique that tracks θ and actively compensates any variation by rotating the X-basis of the Bob's photon by the same amount. This is accomplished with few extra components, shown in Fig. 1a. A weak (~ -45 dBm) control beam at 1544.5 nm is multiplexed with the pump laser and passed into the PM. The control beam is then demultiplexed and injected into the fiber spool, where it co-propagates along with the signal photon. A DEMUX extracts the control beam after the fiber spool and a PM (denoted as control PM) is used to coherently mix the three frequency bins of the control comb. A FBG with a passband of 12.5 GHz is used to filter the baseband signal, which is detected by a photodiode. This scheme effectively realizes a multi-mode Mach-Zehnder interferometer in the frequency domain which is sensitive to θ (see supplemental document for more details). We repeatedly swept the phase of the RF signal of the control PM, and from the recorded inference fringe we tracked the phase drift θ between the $|0\rangle_s$ and $|1\rangle_s$ frequency-bins. This phase is then added to the RF modulator of the signal, thus compensating the rotation of the state in the Bloch sphere by applying an analogous rotation to the Bob's reference frame. The phase correction is provided every ~2 s, which is sufficiently fast to compensate the slow phase drift caused by the temperature variation of the environment. As shown in Fig. 4a, when the active phase compensation mechanism is turned on, the slow drift of the ε_X over time is eliminated and its value remains constant around 15% for every investigated fiber length. At the same time, the fidelity $\mathcal{F}$ of the whole correlation matrix lies always above 0.975 (see Fig. 4b), and is limited only by the CAR and the indistinguishability of the sources. It is worth noting that the QBER is stable for a much longer period than the 10-minute recording shown in Fig. 3 and in Fig. 4 (we tested stability up to one hour of continuous monitoring, see Appendix B of the supplemental document for a related discussion). The SKR reported in Fig. 3 and the QBER values listed in Table 1 are all calculated with the active phase compensation system turned on.

We found an almost perfect (Pearson correlation coefficient of 0.995) correlation between the phase variation θ and the temperature change of the fiber spool, with a slope of 19(1) deg · km^{-1}GHz^{-1} °C^{-1} (see supplemental document). By assuming a thermo-optic coefficient of $1.1 \cdot 10^{-5}$ C^{-1} and a thermal expansion coefficient of $5 \cdot 10^{-7}$ C^{-1}m^{-1} for the silica fiber[39], the predicted slope is ~ 14 deg · km^{-1}GHz^{-1} °C^{-1}, very close to the experimental value. The higher slope found in the experiment could be due to the underestimation of the temperature variation of the fiber, which is sensed by the thermistor in the outermost part of the spool.

Discussion

The aforementioned results are a proof-of-concept demonstration of entangelement-based QKD with frequeny-bin encoding. However, despite the high-brightness of the source, the SKR at the detector is not competitive with state-of-the art works using integrated sources of time-bin or polarization entangled photons[16,25,26,29]. The main limiting factor are the high-losses from pair generation to detection. They result from the poor coupling efficiency with the chip and from the high insertion losses of the optical components, such as the pump filters, the PMs and the connector loss. Indeed, the average loss from generation (excluding the losses due to the fiber spool) to detection is ~10 dB for Alice and ~ 24 dB for Bob (see Table 2 in supplemental document). The higher loss of the Bob's path are due to the lossy tunable bandpass filters and the MUX/DEMUX of the control laser beam. In addition, the projectors on the X-basis use post-selection[34], which introduces an excess loss of ~ 2.2 dB (included in the total insertion loss reported before).

These are not intrinsic limiting factors of our protocol, for losses can be greatly reduced. For example, by choosing a resonator FSR that is a multiple of the standard ITU grid ($100 - 200$ GHz), would allow us to use MUX/DEMUX with low loss (< 0.5 dB) and high-exctintion ratio, which could replace our lossy tunable filters. Coupling loss could be brought below 1 dB by using optimized inverse tapers[40]. Reducing the losses induced by post-selection represent a major challenge. Indeed, Hadamard gates without post-selection have been demonstrated using a combination of waveshaper and electro-optic modulators, but this solution has an insertion loss of ~10 dB when implemented with standard fiber-optic components[41]. Nevertheless, on chip-waveshapers with GHz resolution have been recently reported[42], and there is hope that hybrid-platforms embedding PM could decrease the loss of aggregate components[43]. In light of these considerations, it is realistic to expect that losses between 5 and 7 dB could be reached with minor optimizations, which by virtue of Eq. (2) would increase the coincidence rate at the detectors by a factor ~ 40, thus reaching 8 kbps without fiber spool, and 180 bps with a fiber length of 26 km. These values align well with similar works using integrated sources of time-energy, time-bin and polarization entangled photon pairs, which we briefly review in Table 2.

In parallel, the number of pairs delivered per second could be increased by frequency multiplexing. One could use the $|0\rangle_{s(i)}$ and $|1\rangle_{s(i)}$ frequency-bins of multiple FSR to encode multiple qubits and process them in the same spatial mode[41,44]. For example, in[35] the authors report the simultaneous manipulation of 17 frequency-bin qubits with an offset frequency of 21 GHz and separated by a guard-band of ~ 40 GHz.

The high-dimensional encoding of frequency-bin qudits could also be harnessed to increase the information content per photon and the resilience against errors which are introduced by the transmission loss and imperfections of the receiver[45]. In[33] some of the authors demonstrated the generation of reconfigurable frequency-bin entangled qudits up to a dimension of four by scaling the number of rings in this work from two to four, with the possibility to directly manage the pump power on chip and to choose the frequency-bin separation. The use of multiple rings of high-finesse in place of a single resonator of large-volume allows one to increase the source efficiency, thereby decreasing the input pump power required to achieve a target pair generation rate, without compromising the quantum information density[29]. Indeed, our system has a large quantum information density that can be exploited, which is defined as $d^N/(\Delta t\Delta \nu)$ [5]. In this expression, d^N denotes the Hilbert space dimensionality (with d and N being the number of levels and photons, respectively), and $\Delta t\Delta \nu$ is the time-bandwidth product of the entire N-photon state (with Δt and $\Delta \nu$ being the coherence time of the individual photons and $\Delta \nu$ the total bandwidth). Specifically, in our system we have $d = 2$, $N = 2$, $\Delta t = 80$ ps and $\Delta \nu = 2 \times 15$ GHz, yielding a quantum information density of 1.66, much higher than in conventional microresonators with 200 GHz of FSR and a photon lifetime on the nanosecond scale (~ 0.001). This implies that there is significant room for improving the secure key rates by using high-dimensional states or by using frequency multiplexing. Furthermore, the use of multiple rings allows the group of resonances encoding the qudit state, which are typically separated by few tens of GHz, to be naturally isolated from the subsequent FSR, providing a guard-band that prevents mixing with the other comb lines. This is an important advantage over the use of a single resonator of low-finesse, where guard-band modes must be filtered before applying electro-optic modulation.

A separate issue that we did not address in this work is the RF synchronization of the PM at the two remote nodes where the Alice and Bob receivers are located. In our proof-of-concept demonstration, we used a fiber spool to emulate the link distance between the two parties, which are physically located in the same place. This allowed us to drive the two PM using standard RF cables that carry the signal from a common oscillator. In a real implementation Alice and Bob are physically separated, which implies that two remote oscillators must be synchronized to sub-ps precision to achieve stable coherent operation. An important step towards this goal was taken in[46], where the authors demonstrated the distribution of a 19 GHz clock over 5.5 km using a radio-over-fiber (RFoF) system, with a drift of less than 0.5 ps on 30 min of operation. In this demonstration, the RF tone driving the PM at the sender node is intensity-encoded and multiplexed together with the quantum signal towards the end node, where it is demultiplexed and used to drive the end-node PM after electro-optic conversion and amplification. This strategy has been proved to be robust against thermal fluctuations, and could be used to simultaneously distribute the clock and to eliminate the phase drift between the frequency bins.

A final comment concerns the performance of frequency-bin encoding compared to the more-standard approaches for entanglement based QKD using time-energy, time-bin and polarization encoding. In general, the performance of a given QKD protocol depends on the characteristics of the communication channel, and there is no encoding type that performs equally well in every scenario. For example, polarization encoding is more suited for free-space communication due to the limited impact of atmospheric turbulence on the polarization state, which would be otherwise heavily impacted by propagation into standard optical fibers. Time-bin encoding is robust to both bit-flip errors and phase errors along fiber links, but requires precise time-synchronization between the users, low group velocity dispersion, low timing jitter of the detectors, and the stabilization of unbalanced interferometers. Frequency-bin encoding has the advantage that it is inherently high-dimensional, and multiple operations can be performed in parallel on different frequencies and in the same spatial mode. Furthermore, it is robust to bit-flip errors, while phase errors can be easily tracked and corrected, especially when considering the transmission of high-dimensional states. In particular, when a single photon lies in a superposition of N equally-spaced frequency-bins, the relative phase noise between pairs of adjacent bins is perfectly correlated, which implies that it is sufficient to track a single phase to adapt the measurement basis. As far as we know, this is an exclusive property of frequency-bin encoding. On the other hand, the compensation of the phase noise in time-bin qudits relies on the stabilization of nested interferometers, in which the phase noise of each stage is uncorrelated from the others.

Data availability

Data is available from the corresponding author upon reasonable request.

Received: 19 November 2024; Accepted: 13 February 2025;

References

1. Azuma, K. et al. Quantum repeaters: From quantum networks to the quantum internet. *Rev. Mod. Phys.* **95**, 045006 (2023).
2. Xu, F., Ma, X., Zhang, Q., Lo, H.-K. & Pan, J.-W. Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.* **92**, 025002 (2020).
3. Nadlinger, D. P. et al. Experimental quantum key distribution certified by bell's theorem. *Nature* **607**, 682–686 (2022).
4. Zapatero, V. et al. Advances in device-independent quantum key distribution. *npj quantum Inf.* **9**, 10 (2023).
5. Pirandola, S. et al. Advances in quantum cryptography. *Adv. Opt. Photonics* **12**, 1012–1236 (2020).
6. Scarani, V. et al. The security of practical quantum key distribution. *Rev. Mod. Phys.* **81**, 1301–1350 (2009).
7. Santagiustina, F. B. et al. Experimental post-selection loophole-free time-bin and energy-time nonlocality with integrated photonics. *Optica* **11**, 498–511 (2024).
8. Ecker, S. et al. Strategies for achieving high key rates in satellite-based qkd. *npj Quantum Inf.* **7**, 5 (2021).
9. Mueller, A. et al. High-rate multiplexed entanglement source based on time-bin qubits for advanced quantum networks. *Opt. Quantum* **2**, 64–71 (2024).
10. Yin, J. et al. Entanglement-based secure quantum cryptography over 1,120 kilometres. *Nature* **582**, 501–505 (2020).
11. Honjo, T. et al. Long-distance entanglement-based quantum key distribution over optical fiber. *Opt. Express* **16**, 19118–19126 (2008).
12. Joshi, S. K. et al. A trusted node–free eight-user metropolitan quantum communication network. *Sci. Adv.* **6**, eaba0959 (2020).
13. Liu, X. et al. 40-user fully connected entanglement-based quantum key distribution network without trusted node. *PhotoniX* **3**, 2 (2022).
14. Huang, Y. et al. A sixteen-user time-bin entangled quantum communication network with fully connected topology. *Laser Photon. Rev.* **19**, 2301026 (2024).
15. Yin, J. et al. Satellite-to-ground entanglement-based quantum key distribution. *Phys. Rev. Lett.* **119**, 200501 (2017).
16. Fitzke, E. et al. Scalable network for simultaneous pairwise quantum key distribution via entanglement-based time-bin coding. *PRX Quantum* **3**, 020341 (2022).
17. Shi, Y. et al. Stable polarization entanglement based quantum key distribution over a deployed metropolitan fiber. *Appl. Phys. Lett.* **117**, 24002-1-5 (2020).
18. Liu, Q. et al. Advances in chip-based quantum key distribution. *Entropy* **24**, 1334 (2022).
19. Sibson, P. et al. Chip-based quantum key distribution. *Nat. Commun.* **8**, 13984 (2017).
20. Bunandar, D. et al. Metropolitan quantum key distribution with silicon photonics. *Phys. Rev. X* **8**, 021009 (2018).
21. Steiner, T. J. et al. Ultrabright entangled-photon-pair generation from an al ga as-on-insulator microring resonator. *PRX Quantum* **2**, 010337 (2021).
22. Wen, W. et al. Realizing an entanglement-based multiuser quantum network with integrated photonics. *Phys. Rev. Appl.* **18**, 024059 (2022).
23. Francesconi, S. et al. On-chip generation of hybrid polarization-frequency entangled biphoton states. *Photonics Res.* **11**, 270–278 (2023).

24. Zheng, Y. et al. Multichip multidimensional quantum networks with entanglement retrievability. *Science* **381**, 221–226 (2023).
25. Appas, F. et al. Flexible entanglement-distribution network with an algaas chip for secure communications. *npj Quantum Inf.* **7**, 118 (2021).
26. Steiner, T. J., Shen, M., Castro, J. E., Bowers, J. E. & Moody, G. Continuous entanglement distribution from an algaas-on-insulator microcomb for quantum communications. *Opt. Quantum* **1**, 55–62 (2023).
27. Llewellyn, D. et al. Chip-to-chip quantum teleportation and multi-photon entanglement in silicon. *Nat. Phys.* **16**, 148–153 (2020).
28. Wang, J. et al. Chip-to-chip quantum photonic interconnect by path-polarization interconversion. *Optica* **3**, 407–413 (2016).
29. Yu, H. et al. Quantum key distribution implemented with d-level time-bin entangled photons. *Nat. Commun.* **16**, 171 (2025).
30. Lukens, J. M. & Lougovski, P. Frequency-encoded photonic qubits for scalable quantum information processing. *Optica* **4**, 8–16 (2016).
31. Lu, H.-H., Liscidini, M., Gaeta, A. L., Weiner, A. M. & Lukens, J. M. Frequency-bin photonic quantum information. *Optica* **10**, 1655–1671 (2023).
32. Clementi, M. et al. Programmable frequency-bin quantum states in a nano-engineered silicon device. *Nat. Commun.* **14**, 176 (2023).
33. Borghi, M. et al. Reconfigurable silicon photonic chip for the generation of frequency-bin-entangled qudits. *Phys. Rev. Appl.* **19**, 064026 (2023).
34. Lu, H.-H., Simmerman, E. M., Lougovski, P., Weiner, A. M. & Lukens, J. M. Fully arbitrary control of frequency-bin qubits. *Phys. Rev. Lett.* **125**, 120503 (2020).
35. Henry, A. et al. Parallelization of frequency domain quantum gates: manipulation and distribution of frequency-entangled photon pairs generated by a 21 ghz silicon microresonator. *Adv. Photonics* **6**, 036003–036003 (2024).
36. Grassani, D. et al. Micrometer-scale integrated silicon source of time-energy entangled photons. *Optica* **2**, 88–94 (2015).
37. Bennett, C. H., Brassard, G. & Mermin, N. D. Quantum cryptography without bell’s theorem. *Phys. Rev. Lett.* **68**, 557 (1992).
38. Ma, X., Fung, C.-H. F. & Lo, H.-K. Quantum key distribution with entangled photon sources. *Phys. Rev. A-At., Mol., Optical Phys.* **76**, 012307 (2007).
39. Gao, H. et al. Investigation on the thermo-optic coefficient of silica fiber within a wide temperature range. *J. Lightwave Technol.* **36**, 5881–5886 (2018).
40. Du, J. et al. Demonstration of a low loss, highly stable and re-useable edge coupler for high heralding efficiency and low g (2)(0) soi correlated photon pair sources. *Opt. Express* **32**, 11406–11418 (2024).
41. Henry, A. et al. Parallelizable synthesis of arbitrary single-qubit gates with linear optics and time-frequency encoding. *Phys. Rev. A* **107**, 062610 (2023).
42. Cohen, L. M. et al. Silicon photonic microresonator-based high-resolution line-by-line pulse shaping. *Nat. Commun.* **15**, 7878 (2024).
43. Wang, X., Mere, V., Valdez, F. & Mookherjea, S. Integrated electro-optic control of biphoton generation using hybrid photonics. *Opt. Quantum* **1**, 19–25 (2023).
44. Lu, H.-H. et al. Electro-optic frequency beam splitters and tritters for high-fidelity photonic quantum information processing. *Phys. Rev. Lett.* **120**, 030502 (2018).
45. Cozzolino, D., Da Lio, B., Bacco, D. & Oxenløwe, L. K. High-dimensional quantum communication: benefits, progress, and future challenges. *Adv. Quantum Technol.* **2**, 1900038 (2019).
46. Chapman, S. D. et al. Quantum nonlocal modulation cancellation with distributed clocks. *Optica Quantum*. **3** 45–54, (2025).
47. Autebert, C. et al. Multi-user quantum key distribution with entangled photons from an algaas chip. *Quantum Sci. Technol.* **1**, 01LT02 (2016).
48. Liu, D. et al. Photonic-reconfigurable entanglement distribution network based on silicon quantum photonics. *Photonics Res.* **11**, 1314–1325 (2023).

Acknowledgements

The authors acknowledge Federico Andrea Sabattoli, Houssein El Dirani, Laurene Youssef, Camille Petit-Etienne, Erwine Pargon, and Corrado Sciancalepore for the design and fabrication of the sample. The device has been fabricated at CEA-LETI (Grenoble) on a 200 mm silicon-on-insulator wafer manufactured by SOITEC (Bernin), and is part of a previous collaboration. D.B. acknowledges the support of Italian MUR and the European Union - Next Generation EU through the PRIN project number F53D23000550006 - SIGNED. M.B., M.G and M.L. acknowledge the PNRR MUR project PE0000023-NQSTI. N.T acknowledges the HyperSpace project (project ID 101070168). D. Bacco acknowledges the support of the European Union (ERC, QOMUNE, 101077917, the Project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU. D.R. acknowledges the Project QUID (Quantum Italy Deployment) funded by the European Commission in the Digital Europe Programme under the grant agreement No 101091408.

Author contributions

M.B., Davide B., Daniele B., M.G. and M.L. conceived the original idea. N.T. and M.B. performed the experiment, analyzed the data and prepared the supplemental document. G.G. and D.R. analyzed the data on the QBER and the SKR. N.T., M.B., G.G. and D.R. wrote the manuscript. All the authors reviewed the manuscript. M.B., Davide B., Daniele B., M.G. and M.L. supervised the whole work.

Competing interests

The authors declare no competing interests.

Additional information

Supplementary information The online version contains supplementary material available at https://doi.org/10.1038/s41534-025-00991-5.

Correspondence and requests for materials should be addressed to Massimo Borghi.

Reprints and permissions information is available at http://www.nature.com/reprints