

## ARTICLE OPEN



# Flexible entanglement-distribution network with an AlGaAs chip for secure communications

Félicien Appas<sup>1</sup>, Florent Baboux<sup>1</sup>, Maria I. Amanti<sup>1</sup>, Aristide Lemaître<sup>2</sup>, Fabien Boitier<sup>3</sup>, Eleni Diamanti<sup>4</sup> and Sara Ducci<sup>1</sup>✉

Quantum communication networks enable applications ranging from highly secure communication to clock synchronization and distributed quantum computing. Miniaturized, flexible, and cost-efficient resources will be key elements for ensuring the scalability of such networks as they progress towards large-scale deployed infrastructures. Here, we bring these elements together by combining an on-chip, telecom-wavelength, broadband entangled photon source with industry-grade flexible-grid wavelength division multiplexing techniques, to demonstrate reconfigurable entanglement distribution between up to 8 users in a resource-optimized quantum network topology. As a benchmark application we use quantum key distribution, and show low error and high secret key generation rates across several frequency channels, over both symmetric and asymmetric metropolitan-distance optical fibered links and including finite-size effects. By adapting the bandwidth allocation to specific network constraints, we also illustrate the flexible networking capability of our configuration. Together with the potential of our semiconductor source for distributing secret keys over a 60 nm bandwidth with commercial multiplexing technology, these results offer a promising route to the deployment of scalable quantum network architectures.

npj Quantum Information (2021)7:118; <https://doi.org/10.1038/s41534-021-00454-7>

## INTRODUCTION

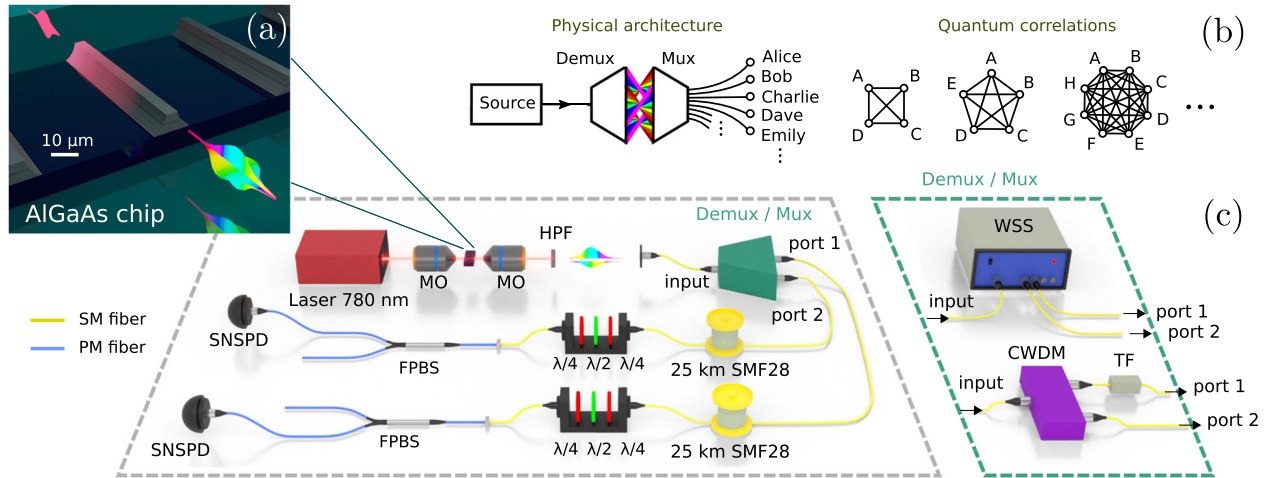
Quantum technologies have the potential to enhance in an unprecedented way the security of communications across network infrastructures. Services and applications that large-scale quantum communication networks can provide span secure communication with security guarantees impossible to achieve only with classical systems<sup>1</sup>, delegated and blind quantum computing<sup>2</sup>, or distributed quantum computing and sensing<sup>3</sup>, eventually leading to the full capabilities of a quantum internet<sup>4</sup>. The choice of network topology and the optimization of the corresponding required resources are crucial when designing the architecture of such infrastructures. This is particularly true for the entangled photonic resources that need to be deployed to enable some of the most advanced applications, but also to alleviate the need for trusted nodes in cryptographic scenarios<sup>5,6</sup>.

In this context, a topology that has naturally attracted much attention exploits the presence of polarization and time-energy photonic entanglement in state-of-the-art sources to distribute polarization-entangled photons from a single source to multiple receivers (users) that hold energy-matched channel pairs<sup>7–14</sup>. This concept was in particular ingeniously pushed in<sup>11</sup>, which proposed and demonstrated a scheme allowing each user of the network to share quantum correlations with every other user, hence forming a fully connected entanglement network. Several challenges come, however, with such an architecture. First, the number of required frequency channels increases quadratically with the number of users, making the bandwidth of the source a critical feature for ensuring scalability to large multi-user networks. Although the scaling was improved in<sup>13</sup>, the relatively narrow band over which polarization-entangled photon pairs were emitted does not permit to increase the number of users. Furthermore, scalability can also be hindered by the use of cascaded passive elements such as dense wavelength division multiplexers (DWDM) and beamsplitters, which also come with

high losses<sup>11,13</sup>. Employing instead advanced multiplexing techniques based on wavelength selective switch (WSS) technology offers a number of attractive features for flexible entanglement distribution, as was recently shown in<sup>14</sup>, albeit again with a relatively narrowband entangled photon source.

In this work, we demonstrate a scalable approach to the fully connected architecture of<sup>11</sup>. To this end, we use a broadband source, emitting photon pairs at telecom wavelength that is based on an AlGaAs semiconductor chip. AlGaAs exhibits direct bandgap, strong electro-optical effect, and small birefringence enabling the generation of polarization-entangled states without any additional optical components<sup>15–18</sup>. We show that thanks to the features of our source, we can maintain an entanglement fidelity above 85% over a 60 nm wide spectral region and across long-distance fiber links. To benchmark the performance of our system, we then run the flagship quantum communication application, namely QKD, and in particular, the BBM92 protocol<sup>19</sup>, both in the asymptotic and finite-size regime, over symmetric and asymmetric fibre-optic links, separating the users by up to 50 km in the symmetric case. We distribute entanglement using Flexgrid multiplexing based on WSS technology, which is the current industry standard in classical communications, and offers straightforward reconfigurability in terms of central frequency and channel bandwidth adjustment while displaying wavelength-insensitive insertion loss and polarization independence. This allows us to show that each of the two-user links in a fully connected entangled network of 4, 5, or 8 users, can support high-quality entanglement distribution and efficient QKD at metropolitan scale distances. We further showcase the flexibility of our scheme in an unbalanced network scenario, featuring several local users and one distant user. We demonstrate that the bandwidth reallocation enabled by the WSS can be used to equilibrate the resulting rates, hence materializing an elastic network

<sup>1</sup>Laboratoire Matériaux et Phénomènes Quantiques, Université de Paris, Paris, France. <sup>2</sup>Université Paris-Saclay, CNRS, Palaiseau, France. <sup>3</sup>Nokia Bell Labs, Nozay, France. <sup>4</sup>Sorbonne Université, CNRS, Paris, France. ✉email: [sara.ducci@u-paris.fr](mailto:sara.ducci@u-paris.fr)



**Fig. 1 Source, network architecture and experimental setup.** **a** Artist view of an AlGaAs chip under operation. An incoming pump photon is depicted on the top left corner, at the input of the waveguide. The generated entangled two-photon state is represented in the bottom right corner. **b** Schematic view of the entanglement network architecture. The physical structure of the network consists of an entangled photon source, a demux/mux stage and a distribution stage. The resulting quantum correlation topology takes the form of a fully connected graph of variable size (here  $N = 4, 5, 8$ ), where each user node shares an entangled state with all other nodes in the network. **c** Experimental setup. MO: Microscope Objective. HPF: High Pass Filter. WSS: Wavelength Selective Switch. CWDM: Coarse Wavelength Division Multiplexing unit. TF: Tunable Filter. FPBS: Fibered Polarizing Beam Splitter. SNSPD: Superconducting Nanowire Single Photon Detector. SM: Single Mode fiber. PM: Polarization Maintaining fiber.

configuration and highlighting its potential for the deployment of flexible, scalable quantum network architectures.

## RESULTS

### AlGaAs photonic chip and experimental setup

The schematic of our experimental setup is presented in Fig. 1c and consists of three stages: entanglement generation with an AlGaAs chip, frequency demultiplexing/multiplexing (demux/mux) of the generated signal, and a distribution stage. Note that two different frequency demultiplexing/multiplexing approaches can be implemented, depending on the spectral region of interest: in the telecom C-Band (1530–1565 nm) we use a WSS and in the L-Band (1565–1625 nm) a coarse wavelength division multiplexing unit (CWDM) with 13 nm wide channels followed by a tunable filter. The WSS enables the implementation of flexible reconfigurable fully-connected multi-user entanglement networks as shown in Fig. 1b<sup>20</sup>.

The AlGaAs chip, depicted in Fig. 1a, consists of a Bragg reflection ridge waveguide emitting photon pairs through type-II spontaneous parametric downconversion (SPDC) in the C+L-Band<sup>10</sup>. The sample is pumped with a tunable CW diode laser leading to a pair production rate of the order of  $10^7$  pairs/s at the chip output, corresponding to a brightness of  $3.6 \times 10^5$  pairs/s/mW (see Methods section for details).

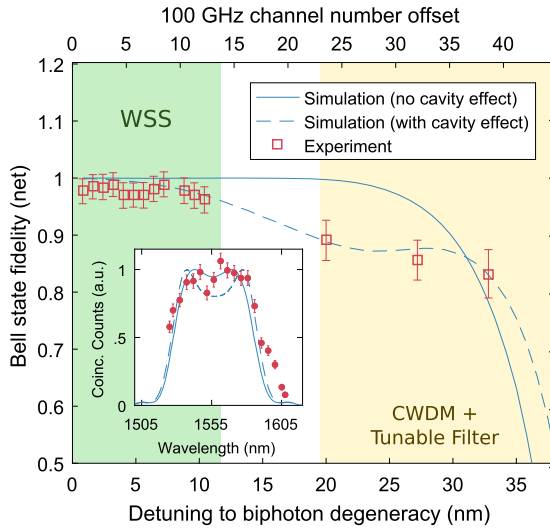
Thanks to the dispersion and nonlinear properties of the AlGaAs platform, the quantum state produced by the chip presents several features making it appealing for the implementation of quantum networks. Our chip generates time-energy and polarization-entangled photons in a  $|\Psi^+\rangle$  polarization Bell state<sup>10,15</sup>. The pairs being generated in a broad spectral band, we can multiplex the generated photons in a large number of wavelength channels using standard telecom components and share polarization entanglement between users receiving energy-matched channels<sup>10</sup>. Besides, the group velocity mismatch between orthogonally polarized photons in the AlGaAs chip is so small that no off-chip walk-off compensation is required to obtain polarization entanglement<sup>15,16</sup>. This is a key feature enabling the direct use of the emitted pairs at the output of the

chip, opening the way to its easy integration into simple and robust architectures.

The biphoton bandwidth has been measured by injecting the generated photon pairs into a fibered 50/50 beam splitter (BS) with a fibered C+L-Bands tunable filter inserted in one of its output ports and detecting the coincidences between the two output ports via superconducting nanowire single-photon detectors (SNSPD) and a time-to-digital converter (TDC). The result is shown in the inset of Fig. 2: the full-width at half-maximum of the output signal is 60 nm, corresponding to approximately 72 ITU 100 GHz channels, 36 on each side of the quantum state degeneracy frequency.

### Broadband entanglement characterization

In order to assess the effective biphoton bandwidth for entanglement distribution we have selected symmetric output channels with respect to the biphoton degeneracy frequency and we have estimated the fidelity of the transmitted photon pairs to the  $|\Psi^+\rangle$  Bell state as a function of the channel number. In the spectral region around degeneracy (C-Band) the measurement has been performed by defining channels using the WSS, while in the spectral region far from degeneracy (L-Band) we have used the CWDM followed by a fibered tunable filter. As shown in Fig. 1c, after demultiplexing, the photons are sent through a polarization analysis stage consisting of a set of  $\lambda/4, \lambda/2, \lambda/4$  waveplates, then through a fibered polarizing beam splitter (FPBS), and finally detected. The waveplates and FPBS are used to project the polarization of the measured photons onto the states of two mutually unbiased bases (MUB), namely  $\mathbb{Z} = \{|H\rangle, |V\rangle\}$  and  $\mathbb{X} = \{|D\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle), |A\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle)\}$ . A lower bound to the fidelity  $F$  to the  $|\Psi^+\rangle$  Bell state is estimated by coincidence measurements in those two bases by recording the number of coincidence counts between the two detectors in 8 different configurations:  $C_{HH}, C_{HV}, C_{VH}, C_{VV}, C_{DD}, C_{DA}, C_{AD}, C_{AA}$  (see Methods for details). From these quantities, we can access the diagonal elements of the density matrix in both MUBs. For  $(\alpha, \beta) \in \mathcal{B} \times \mathcal{B}$ , with  $\mathcal{B} \in \{\mathbb{Z}, \mathbb{X}\}$ , the matrix element  $\rho_{\alpha\beta}$  corresponding to the first (second) photon in  $\alpha$  ( $\beta$ ) polarization state is calculated as  $\rho_{\alpha\beta} = C_{\alpha\beta} / (\sum_{\mathcal{B} \times \mathcal{B}} C_{\alpha'\beta'})$ . Note that the normalization factor has to be calculated independently for the two bases. The lower bound



**Fig. 2 Broadband entanglement characterization.** Main graph: Lower bound to the fidelity to a  $|\Psi^+\rangle$  Bell state as a function of the detuning to biphoton degeneracy wavelength (1556.55 nm) in nm (lower x-axis) and in units of 100 GHz channels (upper x-axis). Error bars take into account the Poissonian statistics of both signal counts and subtracted background counts. The different color areas correspond to the two different wavelength demultiplexing schemes (see main text for details). Inset: Coincidence counts as a function of filter wavelength.

to  $F$  is then obtained through the relation<sup>21,22</sup>

$$F \geq \frac{1}{2} (\rho_{HV} + \rho_{VH} - \rho_{HH} - \rho_{VV} + \rho_{DD} + \rho_{AA} - \rho_{DA} - \rho_{AD}). \quad (1)$$

The experimental results, along with the fidelity of the numerically simulated quantum state emitted by the AlGaAs chip, are shown in Fig. 2. The observed lower bound of the fidelity is above 95% over a 26 nm spectral range corresponding to the first 13 pairs of 100 GHz ITU channels around degeneracy, and stays above 85% for up to 38 channels pairs around degeneracy, spanning a total 60 nm wavelength range. Since the channels of the CWDM are not centered around the biphoton degeneracy wavelength, measurements in the L-Band are limited to the conjugate channels that fall within the transmission window of the CWDM ports. For this reason, only 3 data points have been acquired in the orange region of Fig. 2.

A theoretical model describing the SPDC process within the device taking into account its dispersion and nonlinear properties has been developed. Close to degeneracy, the experimental data are in good agreement with theoretical predictions (solid line). However, moving away from degeneracy, cavity effects arising from facets reflectivity have to be taken into account. The inclusion of these effects in the calculation of the Joint Spectral Amplitude of the generated state is done using a two-mode Airy distribution<sup>23</sup>. This leads to the calculated fidelity represented with a dashed line, reproducing the experimental data with a very good quantitative agreement. The fidelity drop for large values of the detuning is due to the effect of the residual birefringence of the H/V mode. Details on the calculation of the fidelity can be found in the Methods.

The ability to maintain high-quality polarization entanglement over a broad spectral region establishes the high potential of AlGaAs-based devices as ready-to-use miniature sources of broadband polarization-entangled biphoton states.

### QKD performance before the long-distance distribution stage

Next, we exploit the broadband polarization-entangled biphoton state generated with the AlGaAs chip to implement the BBM92

QKD protocol<sup>19</sup>. In this scenario, two users share a maximally entangled Bell state, in our case:  $|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|H\rangle_s|V\rangle_i + |V\rangle_s|H\rangle_i)$  with signal ( $s$ ) and idler ( $i$ ) denoting the high and low energy photon respectively. We deterministically separate the photons of each pair into two fiber paths according to their frequency ( $s$  or  $i$ ) using the WSS. As explained previously, each photon is then sent to a measurement station, consisting of a polarization analysis stage and an SNSPD as shown in Fig. 1c. In the full BBM92 protocol, the basic choice is random, with each user having 4 detectors, one for each measurement outcome ( $H, V, D, A$ ). The random basis choice can be implemented by using, for instance, passive 50/50 BS<sup>24</sup> or polarization-to-time-bin conversion<sup>12</sup>. However, in our proof-of-principle measurement, we choose for simplicity to manually configure the waveplates in each path ( $s$  and  $i$ ) and record the coincidence counts in the same 8 configurations as presented previously, in order to assess the performance of our QKD scheme.

To evaluate the intrinsic QKD performance of our scheme, we measure the figures of merit of the BBM92 protocol right after the demultiplexing stage: a) the asymptotic secret key rate  $R_{\text{key}}$ , which corresponds to the number of secret bits per second established by the two users following basis reconciliation (sifting), error correction and privacy amplification, and b) the quantum bit error rate  $e$  (QBER), which is the fraction of erroneous bits in the raw key. We repeat the measurement for 13 different choices of signal and idler 100 GHz channel pairs. Note that this spectral range is limited by the upper cutoff wavelength (1565 nm) of the WSS corresponding to the boundary of the C-Band, and not by the spectral bandwidth of the generated biphoton state.

We first express  $R_{\text{key}}$  and  $e$  in terms of the recorded coincidence counts<sup>12</sup>. The raw coincidence counts in each basis ( $\mathbb{X}$  and  $\mathbb{Z}$ ) read:

$$C_{\mathbb{X}}^{(\text{raw})} = C_{HH} + C_{HV} + C_{VH} + C_{VV} \quad (2)$$

$$C_{\mathbb{Z}}^{(\text{raw})} = C_{DD} + C_{DA} + C_{AD} + C_{AA} \quad (3)$$

The QBER can be readily obtained by taking the ratio of accidental counts against the total number of recorded raw coincidence counts:

$$e = \frac{C_{HH} + C_{VV} + C_{DA} + C_{AD}}{C_{\mathbb{X}}^{(\text{raw})} + C_{\mathbb{Z}}^{(\text{raw})}}. \quad (4)$$

Next, we compute the raw key rate as the arithmetic mean between the raw count rate in the  $\mathbb{X}$  and in the  $\mathbb{Z}$  basis:

$$R_{\text{raw}} = \frac{1}{2} \frac{C_{\mathbb{X}}^{(\text{raw})} + C_{\mathbb{Z}}^{(\text{raw})}}{\tau}, \quad (5)$$

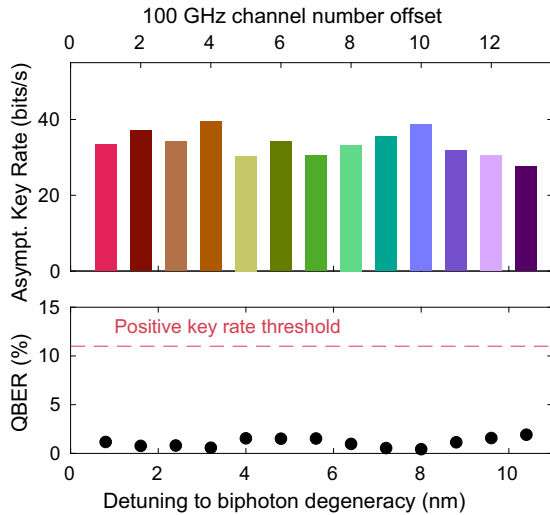
with  $\tau$  the integration time. Finally, the asymptotic key rate is obtained as<sup>25,26</sup>:

$$R_{\text{key}} \geq R_{\text{raw}} \frac{1}{2} (1 - f(e)H_2(e) - H_2(e)), \quad (6)$$

where  $H_2(e) = -e \log_2(e) - (1-e) \log_2(1-e)$  is the binary entropy function. This corresponds to the maximum number of key bits per unit time that can be securely extracted by the two parties in the limit of infinite key length. The factor 1/2 accounts for the basis reconciliation process (sifting) of the BBM92 protocol.  $f(e)H_2(e)$  is the portion of the key that has to be used for error correction, with  $f(e) \geq 1$  a function that quantifies the efficiency of the error correction code. In this work, we use interpolation of tabulated values for  $f(e)$ <sup>25</sup> assuming the standard bidirectional code presented in Ref. 27. Finally, the last term in  $H_2(e)$  is the lower bound of the fraction of the raw key that is lost after privacy amplification<sup>28</sup>.

The calculated  $R_{\text{key}}$  and QBER are plotted in Fig. 3. We see that both quantities are stable over the 13 ITU 100 GHz channels

spanning a 10.4 nm wavelength range. The QBER stays below 2%, well under the positive key rate threshold of 11% for which  $1 - f(e)H_2(e) - H_2(e) = 0$ , assuming an error-correcting code operating at the Shannon limit ( $f(e) = 1$ ). This stability can be attributed to the flatness of the source spectrum and fidelity in this spectral region (Fig. 2) and to the wavelength-independent insertion losses of the WSS. The entanglement quality of the emitted quantum state, combined with the high conversion efficiency of AlGaAs, yields high asymptotic key rates of 28 to 39 bits/s, over a very broad spectral range. The ability to support high key rates with low error over many frequency channels makes our AlGaAs entangled photon source an ideal technology for a chip-based quantum network, as will be illustrated later.



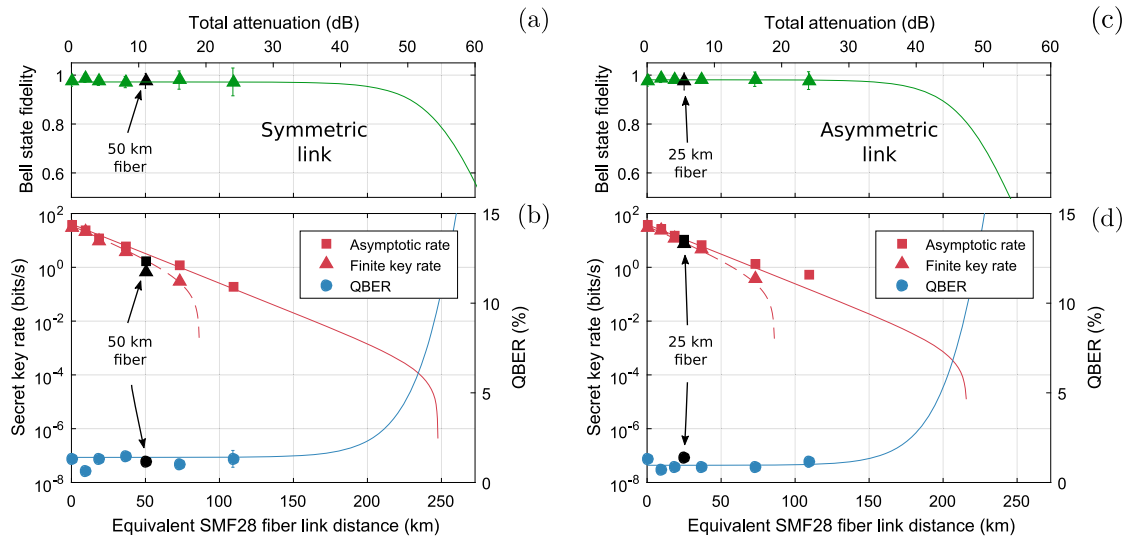
**Fig. 3** **BBM92 performance at 0 km.** Asymptotic BBM92 key rate (upper panel) and QBER (lower panel) as a function of the detuning to biphoton degeneracy in nm (lower x-axis) and in units of 100 GHz channels (upper x-axis). The 11% error threshold for a positive key rate is given for an error-correcting code operating at the Shannon limit.

## Entanglement distribution and secret key distribution over long-distance fiber links

After quantifying the intrinsic entanglement generation and QKD performance of the source over a broad spectral range, we assess the long-distance performance of our architecture. To certify the capability of our setup to maintain high-quality entanglement over long fiber links, we measure the lower bound to the fidelity given in Eq. (1) after adding 25 km SMF28 fiber spools between the demux/mux stage and the user's measurement station. This measurement is performed in two configurations: symmetric (both users separated from the source by 25 km of fiber) and asymmetric (one user at 0 km and the other at 25 km) in order to compare the performances and provide the optimized solution for entanglement distribution. All measurement runs are performed by selecting entangled photons from 100 GHz ITU channels 23 (1558.98 nm) and 29 (1554.13 nm) chosen as representative of all the available channels. We note that in our experimental setup we have manually adjusted the position of the polarization analysis stage for each value of the link's length to compensate for polarization rotation in the fibers. However, this operation could be completely automatized by using active polarization controllers and pilot signals. The results are shown as black symbols in Fig. 4a and c for the symmetric and asymmetric configurations respectively.

To estimate the maximum distance of a repeaterless link we also perform this measurement by replacing the fiber spools by variable channel attenuation programmed on the WSS. The attenuation can then be converted into an equivalent length of SMF28 fibers assuming a standard value of  $0.22 \text{ dB km}^{-1}$  for the SMF28 optical losses. Results for a symmetric and asymmetric link are shown in Fig. 4a and c respectively as color symbols. The theoretical value of the lower bound to  $F$  as a function of channel attenuation (solid lines in Fig. 4a and c) is computed using the model of Ref. <sup>26</sup>.

We observe that the fidelity stays above 95% up to 204 km in the symmetric case and 178 km in the asymmetric case. At longer distances, the decrease of the signal-to-noise ratio induces a drop of the estimated fidelity. We conclude that our entanglement distribution scheme is robust to link asymmetry enabling applications in real-world networks of arbitrary topology.



**Fig. 4** **Long-distance entanglement distribution and quantum key distribution.** Lower bound to the fidelity to a  $|\Psi^+\rangle$  Bell state, asymptotic and finite-size key rates and QBER for a (a, b) symmetric and an (c, d) asymmetric two-user link supported by 100 GHz ITU channels 23 (1558.98 nm) and 29 (1554.13 nm) as a function of SMF28 fiber distance (lower x-axis) and attenuation (upper x-axis). Symbols represent experimental data and continuous lines theoretical predictions for a BBM92 scheme. Finite key rates are estimated assuming 10 min block size.



We stress that the performance of our device being practically insensitive to wavelength in the C-band, as shown in Fig. 2, the measured performance for the two particular channels (23 and 29) can be extrapolated to the 12 other available 100 GHz channel pairs within the operating range of the WSS. This means that each channel pair can support a high-quality long-distance entanglement distribution channel, making our scheme compatible with entanglement-based quantum information protocols over metropolitan networks.

As a benchmark application, we run once again the BBM92 protocol onto our system and evaluate its performance. To do so, we estimate  $R_{\text{key}}$  and  $e$  in the presence of fiber spools (black symbols in Fig. 4b and d) and variable attenuation in both symmetric and asymmetric configurations (color symbols in Fig. 4b and d). We compare the experimental values of the asymptotic key rate to theoretical predictions (continuous lines) for a BBM92 scheme with passive basis selection following the model of Refs. <sup>26,29</sup>.

Furthermore, in order to highlight the relevance of these results for real-world implementations, we perform a finite key security analysis of our scheme. As mentioned previously, the secret key rate in Eq. (6) is only valid in the limit of infinite key length. However, in practice, raw key bits are exchanged in blocks of finite size. To guarantee a certain security threshold for a given block size, we resort to the framework developed in Refs. <sup>5,30</sup>. We set correctness and security bounds to  $\epsilon_{\text{corr}} = 10^{-10}$  and  $\epsilon_{\text{sec}} = 10^{-10}$  respectively for a 10 min block size. The resulting key rates are shown in Fig. 4b and d as triangles for experimental values and dashed lines for theoretical predictions.

Based on this data, we can compare experimentally the long-distance performance of the BBM92 protocol in symmetric and asymmetric configurations. We observe that, in both scenarios, the key rate including finite-size effects stays positive for distances of up to 75 km. We also observe, as expected, that the asymptotic key rate for a symmetric link stays positive for a longer distance (250 km) than that for an asymmetric link (215 km). Indeed, in the latter configuration, a strong attenuation in the link between the source and the distant user induces a strong increase of the QBER as the signal approaches the noise background. On the contrary, in the symmetric case, the losses are distributed between the two users and this critical situation is reached at higher levels of attenuation. In the finite key security regime in which we are operating, the finite key rates become negative before the difference between symmetric and asymmetric links comes into play. This result has practical implications in the context of deployed QKD schemes; indeed this proves that a scenario involving an entangled pair source connected to one local user and one distant user will not be detrimental to the BBM92 protocol efficiency, hence enabling the use of our scheme in realistic configurations.

### Multi-user entanglement networks with flexible bandwidth allocation

Building on the previously presented results, we now demonstrate the operation of a scalable multi-user network architecture by taking advantage of the broad entanglement bandwidth of our source and of the flexible frequency management enabled by the WSS.

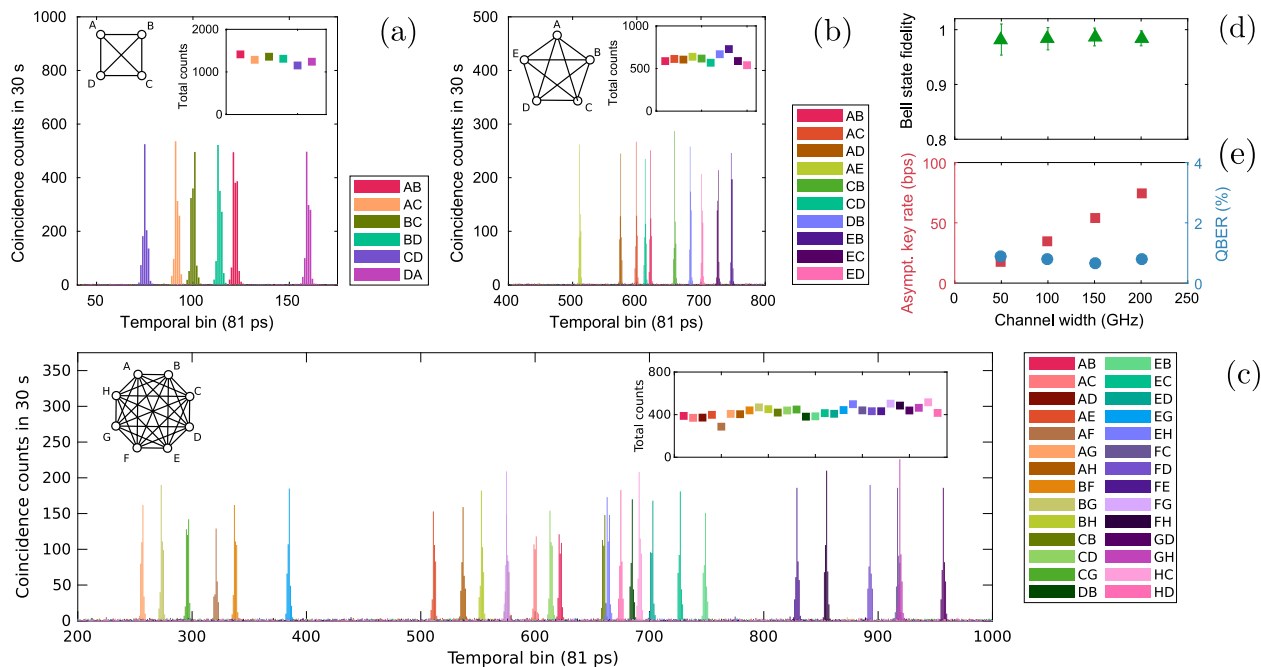
We consider a simple physical network consisting of one central server node which hosts the entangled photon source, and  $N$  user nodes. Each user has a polarization analyzing device and single-photon detectors to carry out the BBM92 protocol. We focus on a particular class of such networks, where each of the  $N$  users shares an entangled state with the remaining  $N - 1$  users<sup>11</sup>. We refer to these as fully connected networks, by analogy with graph theory: indeed, they can be represented by a complete graph where each vertex corresponds to one user node and the edges symbolize a

shared entangled state between two users. Graph representations for fully connected entanglement networks of size  $N = 4, 5, 8$  are shown in Fig. 1b. The number of edges in a complete graph of size  $N$  is  $N(N - 1)/2$ . Hence to get a complete entanglement network, one needs to establish  $N(N - 1)/2$  two-user links supported by  $N(N - 1)/2$  distinct conjugate channel pairs. To do so, we demultiplex the generated photons into  $N(N - 1)$  frequency channels. Then we recombine those channels into single optical fibers, one for each user. This is done via the WSS which implements both operations. Each user then receives photons from  $N - 1$  channels, one for each connected node. Photons from the  $N - 1$  conjugate channels are similarly distributed to the other users. As a result, each node effectively shares a Bell pair with every other node in the network. The number of required frequency channels scales quadratically with  $N$ . In this context, we see that the broadband entanglement of the biphoton state emitted by the AlGaAs chip is a crucial asset. In addition, the use of a WSS at the demultiplexing/multiplexing stage enables a reconfigurable multi-user network where the central frequency and the bandwidth of each channel can be adjusted. In our setup, we can increase the number of users in the network by simply reducing the bandwidth allocated to each channel. Using all the available wavelength overlap between the biphoton state and the WSS operating range, our reconfigurable complete graph network can accommodate from 4 users, with 200 GHz channels, to 8 users, where each link is supported by a 50 GHz conjugate channel pair. We note that a further reduction of the channel spectral width down to 12.5 GHz is also possible without degrading the signal-to-noise ratio since the temporal width of the coincidence histogram in this case ( $\approx 100$  ps) still stays smaller than the timing jitter of the detection stage (200 ps).

We sequentially characterize the  $N(N - 1)/2$  two-user links for different network sizes:  $N = 4, 5$ , and  $N = 8$ . Due to the lack of additional single-photon detectors, we did not run real-time QKD sessions for  $N$  users in parallel. Instead, we measure the time-correlation histograms for all  $N(N - 1)/2$  two-user links in the three different configurations. The obtained coincidence histograms are shown in Fig. 5a–c. The total number of counts contained in each coincidence peak is reported in the insets. We observe that the number of recorded coincidence counts is stable across all links with a relative standard deviation of 7, 9, and 11% for  $N = 4, 5, 8$  respectively. As already discussed previously, this stability is a consequence of the broadband character of the source and of the wavelength-insensitive insertion losses of the WSS. In contrast, in networks based on passive thin-film WDM filters, the channel transmission can be subject to strong variations, leading to unbalanced networks where some links carry more signal than others.

We consolidate this result by recalling that, as shown in Figs. 2 and 3, the distributed quantum state fidelity and BBM92 asymptotic key rate and QBER have a very weak dependence on the frequency channel. Therefore, in view of QKD applications, we expect the key rate to be evenly distributed among all two-user links in each configuration.

We further check that the entanglement quality is not reduced when changing the channel bandwidth. To do so, we estimate the lower bound to  $F$  for ITU channels 23 and 29 as a function of channel bandwidth. The measurement result, displayed in Fig. 5d, shows that the fidelity is essentially insensitive to the channel bandwidth. Accordingly, we observe that the QBER has also a very weak dependence on the bandwidth and the asymptotic key rate features a linear scaling, as shown in Fig. 5e. We conclude that these values for  $R_{\text{key}}$  and QBER, alongside with those of Fig. 3, provide an estimate for the achievable QKD performances in the various  $N$ -user graphs presented in Fig. 5a–c. In a real-time QKD session, the users detect several frequency channels on a single detector. If the propagation times of all frequency channels at the distribution stage are not equalized, the users have to open a



**Fig. 5** Reconfigurable multi-user entanglement network. **a–c** Time-correlation histograms for all two-user links in a fully connected network of size **(a)**  $N = 4$  with 200 GHz channels, **(b)**  $N = 5$  with 100 GHz channels, and **(c)**  $N = 8$  with 50 GHz channels. Artificial time delays were added in the different frequency channels to facilitate the visualization of all histograms in the same figure. **d** Lower bound to the fidelity to a  $|\Psi^+\rangle$  Bell state and **(e)** Measured asymptotic key rate and QBER for ITU channels 23 (1558.98 nm) and 29 (1554.13 nm), as a function of channel width.

different coincidence window for each incident wavelength channel thus increasing the QBER due to additional noise counts. This problem can be solved by adjusting the propagation time of each channel such that all the coincidence peaks corresponding to the links with the other  $N - 1$  users are superimposed in a single coincidence window, as suggested in the Supplementary Materials of Ref. <sup>13</sup>.

Our scheme presents several advantages in terms of scalability over passive WDM quantum networking schemes. Indeed, the flexibility offered by the WSS makes it possible to fully reconfigure the network without modifying the hardware. On the contrary, using passive WDM demux/mux the addition of more users to the network requires either changing the complex combination of cascaded WDM filters or non-deterministically splitting some channels by combining WDM filters and multiport fiber splitters<sup>13,31</sup>, which, either way, comes at the cost of extra optical losses. In contrast, the fixed insertion losses of the WSS makes it possible to extend the network without degrading the signal, a major asset in a fully deployed network scenario.

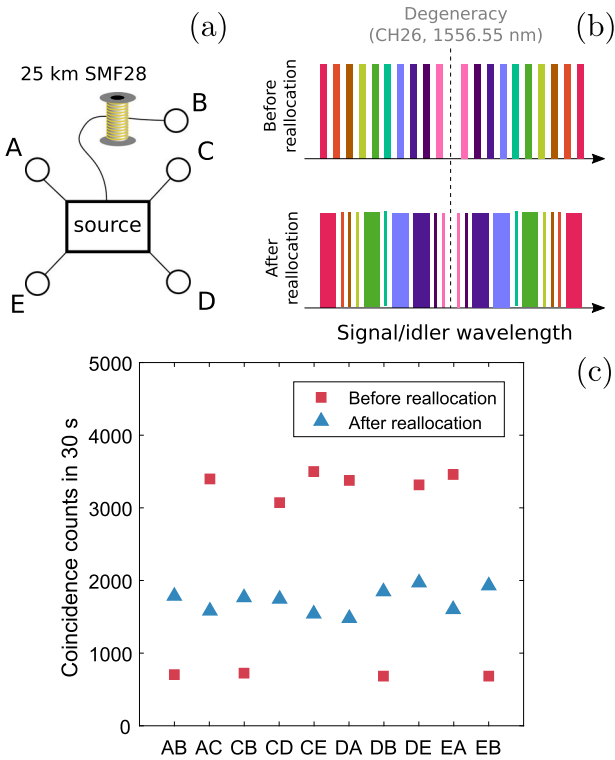
Finally, we exploit the flexibility of our scheme to demonstrate a quantum network where the signal of each link is optimized following a structural constraint. This experiment represents the first step towards a fully autonomous smart network, where communication rates are automatically optimized based on bidirectional information exchange between the users and the network provider. We consider a fully connected entanglement network where one of the user nodes is located far apart from the entangled photon source, while all the other nodes are located close to the source as schematically depicted in Fig. 6a. We implement this situation for  $N = 5$  by separating node B's detector from the source by a 25 km-long SMF28 fiber spool. If all two-user links have the same fixed bandwidth, the coincidence rate of the four links connecting the distant user to the rest of the network, i.e., AB CB DB EB, will be lower than the others. To avoid this problem, we reallocate the state bandwidth by changing the channel widths, assigning more bandwidth to long links, and less

bandwidth to short links, as schematically depicted in Fig. 6b. We use a simple algorithm and distribute the available bandwidth with a 12.5 GHz resolution corresponding to current ITU standards for channel bandwidth granularity.

In order to demonstrate that we can efficiently level the measured signal across the whole network, we measure one by one the 10 two-user coincidence counts rates for each link. The results are shown in Fig. 6c. Red squares represent the raw coincidence counts of the 10 two-user links for fixed 100 GHz channels and blue triangles are the raw coincidence counts recorded after bandwidth reallocation. We observe that, starting from a very unbalanced initial configuration, we can bring all users to a similar level of a signal. The same technique could be applied to other ends, such as boosting the signal across specific links according to user needs. This proof-of-principle experiment shows that our scheme is fully compatible with state-of-the-art telecom network management, opening the way for flexible metropolitan-scale entanglement distribution.

## DISCUSSION

We have demonstrated a scalable approach to a fully connected entanglement distribution network using an AlGaAs chip emitting broadband polarization-entangled photon pairs in the telecom band. The lower bound on entanglement fidelity of the quantum state generated by our chip stays above 95% over a 26 nm wide spectral range around biphoton degeneracy and above 85% over a 60 nm range. We deterministically separate the photons of each pair into energy-matched frequency channels and distribute them to the network users using a wavelength selective switch. We benchmark the performance of our quantum network by running the entanglement-based BBM92 QKD protocol. We perform key distribution between two users with a QBER below 2% across fibered optical links of up to 50 km including finite-key effects and we extrapolate a positive key rate for distances of up to 75 km in both symmetric and asymmetric configurations. We have



**Fig. 6 Flexible bandwidth allocation in an unbalanced network.** **a** Sketch of the experiment. In a fully connected network with  $N = 5$  users, user B is separated from the source by a 25 km long SMF28 fiber spool. **b** Schematic of the bandwidth distribution between all two-user links before and after applying the bandwidth reallocation algorithm. After reallocation, the four links (red, dark green, light blue, and dark blue) that connect user B to the rest of the network are allowed a broader bandwidth. **c** Coincidence counts for each two-user link before (squares) and after (triangles) bandwidth reallocation.

extended our study to the multi-user case, taking advantage of the flexibility offered by our setup. By reconfiguring the frequency grid, we show that our network can accommodate up to 8 users over 50 GHz ITU channels. We further demonstrate the insensitivity of the QBER with respect to channel width, indicating that every two-user link in the network can support high-performance QKD at metropolitan-scale distances. Finally, we demonstrate that the bandwidth reallocation enabled by the WSS can be used to equilibrate an unbalanced network scenario, which is compatible with an elastic network configuration. Future work includes the implementation of our architecture in a metropolitan quantum communication network to test its performance and robustness in a real-world situation.

Further progress is possible in different ways. On one hand, extreme miniaturization of the AlGaAs source can be achieved thanks to its compliance with electrical injection as already shown in<sup>18</sup>, giving a clear advantage to our approach in terms of portability, energy consumption and integration with future quantum technologies. On the other hand, the cavity effects presently limiting the fidelity to a polarization Bell state far from degeneracy can be avoided by applying an anti-reflection coating to the waveguide facets. Optimization of the design can also be implemented to reduce the modal birefringence in order to further broaden the entangled photon pair bandwidth<sup>32</sup> and to place the degeneracy wavelength at the center of the telecom C-band to fully exploit the WSS bandwidth. Using WSS technology covering both the C and L bands would further allow to exploit the full bandwidth of our source. Besides, the biphoton bandwidth and brightness could be optimized by choosing the optimal

sample length taking into account SPDC efficiency and propagation losses.

In addition to the improvement of the photon-pair source, future investigations of different entanglement-distribution topologies can benefit from the flexibility of our setup. In particular, using the full potential of our 60 nm entanglement bandwidth, non-fully connected networks which can host up to 28 users over 50 GHz ITU channels could readily be implemented. In this topology, the network is broken up into independent fully-connected 4-user subnets which are all interconnected via extra links. Owing to the broad bandwidth of our source, this scheme can be demonstrated without the need to resort to passive BS multiplexing, as suggested in Refs.<sup>13,31</sup> thus avoiding the reduction of the signal caused by extra optical losses.

Finally, in another approach we could take advantage of the cavity effects present in our sample to generate and coherently control biphoton frequency combs<sup>23</sup>, opening the way to the utilization of frequency for quantum information processing<sup>33,34</sup> and to the combined exploitation of both polarization and frequency entanglement for future quantum networks.

## METHODS

### Sample and experimental setup

The sample consists of a 6-period  $\text{Al}_{0.80}\text{Ga}_{0.20}\text{As}/\text{Al}_{0.25}\text{Ga}_{0.75}\text{As}$  Bragg reflector (lower mirror), a 366 nm  $\text{Al}_{0.45}\text{Ga}_{0.55}\text{As}$  core and a 2-period  $\text{Al}_{0.25}\text{Ga}_{0.75}\text{As}/\text{Al}_{0.80}\text{Ga}_{0.20}$  Bragg reflector (upper mirror). Waveguides are fabricated using wet chemical etching to define 5  $\mu\text{m}$  wide and around 800 nm deep ridges; the waveguide length is 4 mm. The sample is pumped with a tunable CW diode laser (TOPTICA TM Photonics DL pro 780) which is coupled into the waveguide through a microscope objective (NA = 0.95, 63 $\times$ ); light emerging from the opposite end is collected with a second identical microscope objective and sent to a fibre coupler, after filtering out the pump wavelength with a high pass filter. A thermocouple and a Peltier cooler, connected to a PID controller, monitor and keep the waveguide temperature constant at 19.3  $^{\circ}\text{C}$ , fixing the wavelength degeneracy of the photon pairs to 1556.55 nm, which corresponds to the center of the ITU 100 GHz channel number 26. The demux/mux stage is realized either with a Wavelength Selective Switch (model Finisar 4000s) or with a Coarse Wavelength Division Multiplexing unit (model FS 78163) followed by a tunable C+L band filter (model Alnair Labs CVF-220-CL) depending on the spectral region of interest. After the analysis and distribution stage photons are detected with superconducting nanowire single-photon detectors (SNSPD, Quantum Opus) and temporal correlation measurements are performed with a time-to-digital converter (TDC, quTools). The heralding efficiency of the source in this experimental configuration is 9.4%.

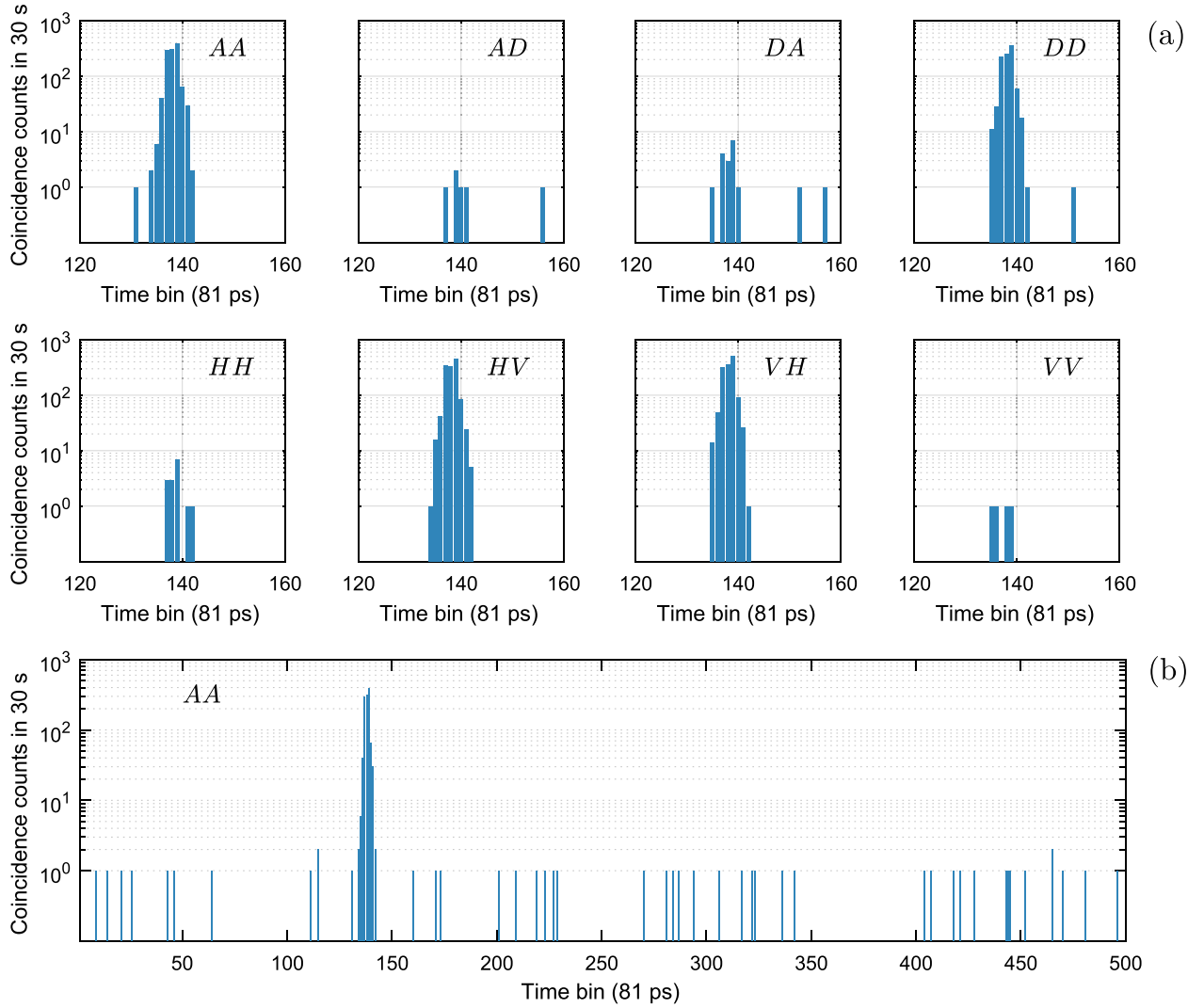
## Theory

We provide the expression of the quantum state of the source and derive the theoretical fidelity  $F$  as a function of channel frequency.

We start from the generic form of the two-photon state generated by collinear Type-II parametric downconversion:

$$|\psi\rangle = \int \int_{-\infty}^{+\infty} d\omega_1 d\omega_2 \mathcal{C}(\omega_1, \omega_2) |\omega_1, H\rangle |\omega_2, V\rangle \quad (7)$$

where  $|\omega, \alpha\rangle = \hat{a}_{\alpha}^{\dagger}(\omega)|\text{vac}\rangle$  denotes the state of the electromagnetic field with one photon in a mode of polarization  $\alpha = H, V$  and angular frequency  $\omega$ . The complex function  $\mathcal{C}(\omega_1, \omega_2)$  is called the joint spectral amplitude (JSA) and it is normalized to unity  $\iint d\omega_1 d\omega_2 |\mathcal{C}(\omega_1, \omega_2)|^2 = 1$ . By rewriting the quantum state in the rotated basis:  $\omega_+ = \omega_1 + \omega_2$  and  $\omega_- = \omega_1 - \omega_2$ , the JSA takes the form:  $\mathcal{C}(\omega_1, \omega_2) = f_+(\omega_+)f_-(\omega_-)$ . The first term of the product corresponds to energy conservation during the downconversion process and the second term is related to momentum conservation (phase matching). The latter can be numerically calculated using the dispersion properties of the guided modes involved in the downconversion process. Cavity effects arising from the nonzero reflectivity of the AlGaAs waveguide facets can be included in the numerically-calculated JSA using a two-mode Airy distribution<sup>23</sup>. Since the waveguide is pumped by a narrow-linewidth CW laser, one can approximate  $f_+$  to a Dirac delta function centered on the pump laser



**Fig. 7 Raw data for time-correlation histograms. a** Measured time-correlation histograms for the 8 projective measurements performed to obtain the lower bound on  $F$  for 100 GHz ITU channels 23 (1558.98 nm) and 29 (1554.13 nm). **b** Extended time-correlation histogram in the AA configuration showing the low level of recorded background counts.

angular frequency  $f_+(\omega_+) = \delta(\omega_+ - \omega_p)$  and the resulting generated quantum state is strongly frequency-anticorrelated. In this case, the state can be rewritten:

$$|\psi\rangle = \int_{-\infty}^{+\infty} d\Omega \Phi(\Omega) |\omega_d + \Omega, H\rangle |\omega_d - \Omega, V\rangle, \quad (8)$$

where we defined for convenience  $\omega_d = \omega_p/2$  the degeneracy angular frequency,  $\Omega = \omega_-/2$  the detuning with respect to the degeneracy and  $\Phi(\Omega) = f_-(\omega_-)$ .

We then rewrite the state as a continuous superposition of bipartite polarization-entangled states. To do so, we split the summation in Eq. (8) into two parts using the identity:  $\int_{-\infty}^{+\infty} = \int_0^{+\infty} + \int_0^{+\infty}$  then make the change of variable  $\Omega \rightarrow -\Omega$  into the second term and finally recombine the two integrals to obtain:

$$|\psi\rangle = \int_0^{+\infty} d\Omega [\Phi(\Omega) |\omega_d + \Omega, H\rangle |\omega_d - \Omega, V\rangle + \Phi(-\Omega) |\omega_d - \Omega, H\rangle |\omega_d + \Omega, V\rangle]. \quad (9)$$

To calculate the fidelity to a  $|\Psi^+\rangle$  Bell state as a function of channel frequency, we derive the reduced density matrix in polarization space after spectral filtering. At the demultiplexing stage, signal and idler photons lying in energy matched frequency channels are sent onto separate fiber paths  $A$  and  $B$ . Namely, all signal photons within the frequency window  $[\omega_d + (\Omega_0 - \Delta/2), \omega_d + (\Omega_0 + \Delta/2)]$  are sent in path  $A$  and all idler photons within the frequency window  $[\omega_d - (\Omega_0 + \Delta/2), \omega_d - (\Omega_0 - \Delta/2)]$  in path  $B$ ,

where  $\Delta$  is the channel width and  $\Omega_0$  the detuning of the channel central frequency with respect to degeneracy. The resulting post-selected quantum state takes the form:

$$|\psi'\rangle = \int_0^{+\infty} d\Omega f(\Omega) [\Phi(\Omega) |\omega_d + \Omega, H\rangle_A |\omega_d - \Omega, V\rangle_B + \Phi(-\Omega) |\omega_d - \Omega, H\rangle_B |\omega_d + \Omega, V\rangle_A] \quad (10)$$

with  $f(\Omega)$  the filter lineshape, which in our case is assumed to be rectangular:

$$f(\Omega) = \begin{cases} 1, & \text{for } \Omega \in [\Omega_0 - \Delta/2, \Omega_0 + \Delta/2] \\ 0, & \text{elsewhere.} \end{cases} \quad (11)$$

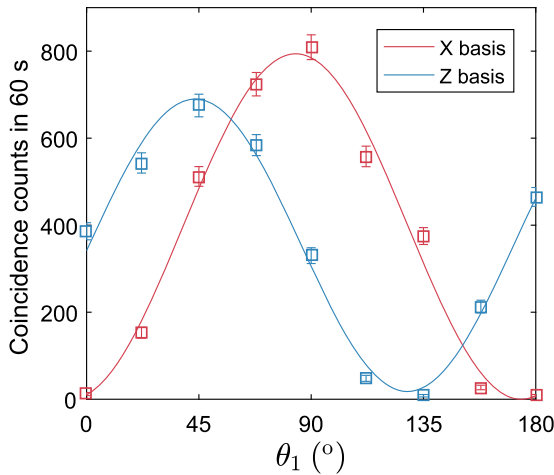
The corresponding density operator is  $\tilde{\rho} = |\psi'\rangle\langle\psi'|$ . By following the approach of Ref. <sup>35</sup>, we compute the reduced polarization density matrix  $\rho$  by tracing out the frequency part of the density operator:

$$\rho = \frac{1}{\mathcal{N}} \iint d\omega' d\omega'' \langle \omega' |_B \langle \omega'' | \tilde{\rho} | \omega'' \rangle_B | \omega' \rangle_A. \quad (12)$$

with  $\mathcal{N}$  a normalization constant. After some straightforward algebra, one obtains:

$$\rho = \alpha |HV\rangle_{ABAB} \langle HV| + \mathcal{D} |HV\rangle_{ABAB} \langle VH| + \mathcal{D}^* |VH\rangle_{ABAB} \langle HV| + \beta |VH\rangle_{ABAB} \langle VH|, \quad (13)$$





**Fig. 8** Measured correlation curves for 100 GHz ITU channels 23 and 29. Squares correspond to experimental raw counts and solid lines to a fit to a sine square.

where the 4 non-zero matrix elements are:

$$\alpha = \frac{1}{\mathcal{N}} \int_0^\infty d\Omega f(\Omega) |\Phi(\Omega)|^2 \quad (14)$$

$$\beta = \frac{1}{\mathcal{N}} \int_0^\infty d\Omega f(\Omega) |\Phi(-\Omega)|^2 \quad (15)$$

$$\mathcal{D} = \frac{1}{\mathcal{N}} \int_0^\infty d\Omega f(\Omega) \Phi(\Omega) \Phi^*(-\Omega) \quad (16)$$

and the normalization constant is set to  $\mathcal{N} = \int_0^\infty d\Omega f(\Omega) [|\Phi(\Omega)|^2 + |\Phi(-\Omega)|^2]$  such that  $\text{Tr} \rho = 1$ . Finally, the fidelity to a  $|\Psi^+\rangle$  Bell state can be evaluated from the definition:  $F = \left( \text{Tr} \sqrt{\sqrt{\rho} |\Psi^+\rangle \langle \Psi^+| \sqrt{\rho}} \right)^2$ .

### Coincidence histograms and Bell correlation curves

We display an example of data for the 8 projective measurements that are used to estimate the Bell state fidelity and the corresponding Bell correlation curves.

The time-correlation histograms that have been recorded for 100 GHz ITU channels 23 and 29 are displayed in Fig. 7. The number of coincidence counts in each configuration is given by the sum of the counts in the 6 central time-bins. The width of the time bins is 81 ps corresponding to the temporal resolution of our TDC.

We define the coincidence to an accidental ratio (CAR) as the mean number of counts in the 6 central bins over the mean number of counts in 6 bins outside the coincidence window. In the configurations where the number of counts is maximum (AA, DD, HV, VH) we achieve a CAR of the order of  $4 \times 10^3$ .

In addition, for each pair of 100 GHz channel, we measured the Bell correlation curves in both  $\mathbb{X}$  and  $\mathbb{Z}$  bases. To do so, we recorded coincidence counts when projecting the polarization of the signal photon onto an axis of angle  $\theta_1$  with respect to the horizontal axis of the laboratory frame, for values of  $\theta_1$  spanning  $[0^\circ, 180^\circ]$ , and the polarization of the idler photon on a fixed axis, either  $H(0^\circ)$  or  $D(45^\circ)$ . The visibility of the obtained two-photon interference fringes is an indicator of the quality of entanglement. As an illustration, we show the correlation curves obtained between ITU channels 23 and 29 in Fig. 8. Solid lines are least-square fits to the expression  $C = a \sin^2(\theta_1 - \theta_2) + b$  where  $\theta_1$  and  $\theta_2$  are the angles between the horizontal axis of the laboratory frame and the projection axes of signal and idler polarization respectively. We measured raw visibilities of 98.0% in the  $\mathbb{Z}$  basis and 97.7% in the  $\mathbb{X}$  basis.

### DATA AVAILABILITY

The data used in this work is available from the corresponding author upon request.

Received: 26 March 2021; Accepted: 23 June 2021;  
Published online: 23 July 2021

### REFERENCES

- Diamanti, E., Lo, H.-K., Qi, B. & Yuan, Z. Practical challenges in quantum key distribution. *npj Quantum Inf.* **2**, 16025 (2016).
- Gheorghiu, A., Kapourniotis, T. & Kashefi, E. Verification of quantum computation: an overview of existing approaches. *Theory Comput. Syst.* **63**, 715 (2019).
- Zhao, S.-R. et al. Field demonstration of distributed quantum sensing without post-selection. *Phys. Rev. X* **11**, 031009 (2021).
- Wehner, S., Elkouss, D. & Hanson, R. Quantum internet: a vision for the road ahead. *Science* **362**, eaam9288 (2018).
- Yin, J. et al. Entanglement-based secure quantum cryptography over 1,120 kilometres. *Nature* **582**, 501–505 (2020).
- Diamanti, E. A step closer to secure global communication. *Nature* **580**, 494–495 (2020).
- Lim, H. C., Yoshizawa, A., Tsuchida, H. & Kikuchi, K. Wavelength-multiplexed distribution of highly entangled photon-pairs over optical fiber. *Opt. Express* **16**, 22099–22104 (2008).
- Herbauts, I., Blauensteiner, B., Poppe, A., Jennewein, T. & Hübner, H. Demonstration of active routing of entanglement in a multi-user network. *Opt. Express* **21**, 29013 (2013).
- Aktas, D. et al. Entanglement distribution over 150 km in wavelength division multiplexed channels for quantum cryptography. *Laser Photonics Rev.* **10**, 451 (2016).
- Autebert, C. et al. Multi-user quantum key distribution with entangled photons from an AlGaAs chip. *Quantum Sci. Technol.* **1**, 01LT02 (2016).
- Wengerowsky, S., Joshi, S. K., Steinlechner, F., Hübner, H. & Ursin, R. An entanglement-based wavelength-multiplexed quantum communication network. *Nature* **564**, 225–228 (2018).
- Zhu, E. Y. et al. Toward a reconfigurable quantum network enabled by a broadband entangled source. *J. Opt. Soc. Am. B* **36**, B1 (2019).
- Joshi, S. K. et al. A trusted node-free eight-user metropolitan quantum communication network. *Sci. Adv.* **6**, eaab0959 (2020).
- Lingaraju, N. B. et al. Adaptive bandwidth management for entanglement distribution in quantum networks. *Optica* **8**, 329 (2021).
- Orieux, A. et al. Direct bell states generation on a III-V semiconductor chip at room temperature. *Phys. Rev. Lett.* **110**, 160502 (2013).
- Horn, R. et al. Monolithic source of photon pairs. *Phys. Rev. Lett.* **108**, 153605 (2012).
- Kang, D., Anirban, A. & Helmy, A. S. Monolithic semiconductor chips as a source for broadband wavelength-multiplexed polarization entangled photons. *Opt. Express* **24**, 15160 (2016).
- Boitier, F. et al. Electrically Injected Photon-Pair Source at Room Temperature. *Phys. Rev. Lett.* **112**, 183901 (2014).
- Bennett, C. H., Brassard, G. & Mermin, N. D. Quantum cryptography without bell's theorem. *Phys. Rev. Lett.* **68**, 557–559 (1992).
- Wavesaper 4000a datasheet. <https://ii-vi.com/product/wavesaper-4000a-multiport-optical-processor/>. Accessed 2021-05-26.
- Chang, X.-Y. et al. Experimental realization of an entanglement access network and secure multi-party computation. *Sci. Rep.* **6**, 29453 (2016).
- Blinov, B. B., Moehring, D. L., Duan, L.-M. & Monroe, C. Observation of entanglement between a single trapped atom and a single photon. *Nature* **428**, 153–157 (2004).
- Maltese, G. et al. Generation and symmetry control of quantum frequency combs. *npj Quantum Inf.* **6**, 13 (2020).
- Ursin, R. et al. Entanglement-based quantum communication over 144 km. *Nat. Phys.* **3**, 481–486 (2007).
- Lütkenhaus, N. Security against individual attacks for realistic quantum key distribution. *Phys. Rev. A* **61**, 052304 (2000).
- Ma, X., Fung, C.-H. F. & Lo, H.-K. Quantum key distribution with entangled photon sources. *Phys. Rev. A* **76**, 012307 (2007).
- Brassard, G. & Salvail, L. Secret-key reconciliation by public discussion. In Hellesteth, T. (ed.) *Advances in Cryptology — EUROCRYPT '93*, 410–423 (1994).
- Bennett, C. H., Brassard, G., Crépeau, C. & Maurer, U. M. Generalized privacy amplification. *IEEE Trans. Inf. Theory* **41**, 1915–1923 (1995).
- Scheidt, T. et al. Feasibility of 300 km quantum key distribution with entangled states. *N. J. Phys.* **11**, 085002 (2009).
- Tomamichel, M., Lim, C. C. W., Gisin, N. & Renner, R. Tight finite-key analysis for quantum cryptography. *Nat. Commun.* **3**, 634 (2012).
- Liu, X. et al. An entanglement-based quantum network based on symmetric dispersive optics quantum key distribution. *APL Photonics* **5**, 076104 (2020).
- Chen, H. et al. Optimizing the spectro-temporal properties of photon pairs from bragg-reflection waveguides. *J. opt.* **21**, 054001 (2019).
- Lukens, J. M. & Lougovski, P. Frequency-encoded photonic qubits for scalable quantum information processing. *Optica* **4**, 8 (2016).

34. Fabre, N. et al. Generation of a time-frequency grid state with integrated biphoton frequency combs. *Phys. Rev. A* **102**, 012607 (2020).
35. Schlager, A. et al. Temporally versatile polarization entanglement from bragg reflection waveguides. *Opt. Lett.* **42**, 2102 (2017).

## ACKNOWLEDGEMENTS

This work has been supported by ANR (Agence Nationale de la Recherche) through the QUANTIFY Project (Project No. ANR-19-ASTR-0018-01), the French RENATECH network, and by Paris Île-de-France Région in the framework of DIM SIRTEQ through the LION Project. The authors acknowledge Perola Milman for fruitful discussions and Yves Jaouen for the C+L band tunable filter loan.

## AUTHOR CONTRIBUTIONS

F.A. built the setup, processed the sample and carried out the experimental work. All the authors contributed to the conception of the experiment. A.L. performed the epitaxial growth of the AlGaAs sample. The paper was written by F.A., E.D. and S.D. All authors discussed the results and commented on the manuscript. E.D. and S.D. supervised the project.

## COMPETING INTERESTS

The authors declare no competing interests.

## ADDITIONAL INFORMATION

**Correspondence** and requests for materials should be addressed to S.D.

**Reprints and permission information** is available at <http://www.nature.com/reprints>

**Publisher's note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.



**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 license, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons license 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 license, visit <http://creativecommons.org/licenses/by/4.0/>.

© The Author(s) 2021