

Continuous entanglement distribution from an AlGaAs-on-insulator microcomb for quantum communications

TREVOR J. STEINER,^{1,*}  MAXIMILIAN SHEN,¹ JOSHUA E. CASTRO,² JOHN E. BOWERS,^{1,2}  AND GALAN MOODY^{2,3} 

¹Materials Department, University of California, Santa Barbara, California 93106, USA

²Electrical and Computer Engineering Department, University of California, Santa Barbara, California 93106, USA

³moody@ucsb.edu

*trevorsteiner@ucsb.edu

Received 23 October 2023; revised 21 November 2023; accepted 23 November 2023; published 15 December 2023

Using an aluminum gallium arsenide microring resonator, we demonstrate a bright quantum optical microcomb with >300 nm (>40 THz) bandwidth and more than 20 sets of time-energy entangled modes, enabling spectral demultiplexing with simple, off-the-shelf commercial telecom components. We report high-rate continuous entanglement distribution for two sets of entangled-photon pair frequency modes exhibiting up to 20 GHz/mW² pair generation rate. As an illustrative example of entanglement distribution, we perform a continuous-wave time-bin quantum key distribution protocol with 8 kbps sifted key rates while maintaining less than 10% error rate and sufficient two-photon visibility to ensure security of the channel. When the >20 frequency modes are multiplexed, we estimate >100 kbps entanglement-based key rates or the creation of a multi-user quantum communications network. The entire system requires less than 110 μ W of on-chip optical power, demonstrating an efficient source of entangled frequency modes for quantum communications. As a proof of principle, a quantum key is distributed across 12 km of deployed fiber on the University of California Santa Barbara (UCSB) campus and used to encrypt a 21 kB image with $<9\%$ error.

© 2023 Optica Publishing Group under the terms of the [Optica Open Access Publishing Agreement](#)

<https://doi.org/10.1364/OPTICAQ.510032>

1. INTRODUCTION

The distribution and joint measurement of time-energy entangled-photon pairs is important for applications of quantum technologies such as distributed computing, repeater-based quantum networks, and quantum communication [1–4]. The generation of entangled-photon pairs near the 1.5 μ m telecommunications band is especially desirable for low-loss transmission, allowing for quantum communication networks using established optical fiber systems [5]. Photonic integrated circuits (PICs) provide additional benefits for low size, weight, and power (SWaP) quantum light transmitters and receivers [6]. Numerous chip-scale platforms have been demonstrated for entanglement generation and distribution, many of which operate near the 1.5 μ m telecommunications band [7]. Of these platforms, one of the most promising is aluminum gallium arsenide-on-insulator (AlGaAsOI), which has recently demonstrated ultra-bright, high-quality entangled-photon pairs from a spontaneous four-wave mixing process in a microring resonator [8]. Improvements to the fabrication process have enabled low propagation loss <0.2 dB/cm and high quality factor microcomb resonators with $Q>3.5 \times 10^6$ [9]. Other standard photonic components including beam splitters, filters, interferometers,

and detectors have also been demonstrated with performance comparable to their silicon counterparts [10,11]. Finally, the AlGaAsOI platform is naturally compatible with InGaAs quantum dot laser sources and boasts large second- and third-order nonlinearities, making it an excellent platform for quantum photonic integrated circuits (QPICs) with advanced functionality for the generation, manipulation, and detection of quantum photonic signals.

One particularly impactful use of entangled-photon pairs generated in the telecom C-band is for quantum key distribution (QKD). QKD is a method to create a secret and random bit string shared between two remote users for secure information distribution [12]. Since the first proposal of QKD in 1984 by Bennett and Brassard [13], numerous protocols and techniques have been implemented to demonstrate secure key distribution [14–16] including system demonstrations with up to 830 km of deployed optical fiber [17] and satellite-based QKD exceeding 1200 km [18,19]. Sources for the secure key are typically entangled-photon pairs, single photons, squeezed light, or weak coherent states [6,12,20]. As source and detector technologies have advanced in recent years, there has been a push for low-SWaP approaches relying on chip-scale implementations that

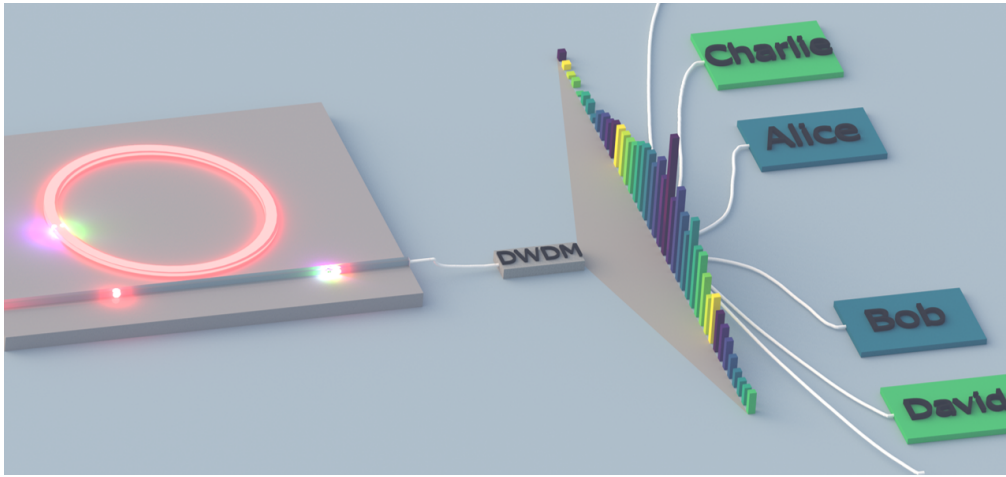


Fig. 1. AlGaAsOI quantum optical microcomb enabling multi-user entanglement distribution. A microring resonator generates pairs of entangled photons across many spectral modes that can be distributed to various users over long distances using low-loss telecommunication optical fibers. The frequency comb spectrum shown is from the device characterized in this work and shows the ability to create a user network with more than 20 nodes with ultrabright entanglement generation requiring $<100\ \mu\text{W}$ on-chip power. In this illustration, Alice and Bob each receive a photon from one set of modes, and Charlie and David each receive a photon from a different set.

take advantage of existing semiconductor and photonic manufacturing techniques (see Ref. [6] for a summary of recent advancements in chip-based QKD technologies). Here we focus on entanglement-based QKD, which is inherently secure due to the quantum no-cloning theorem and the collapse of the quantum state upon measurement [12,21]. For entanglement-based protocols, two photons are generated simultaneously through a nonlinear optical process such as spontaneous parametric down-conversion (SPDC) or spontaneous four wave mixing (SFWM), and each photon is sent to either Alice or Bob for measurement to establish a key [22].

In this work, we generate entangled-photon pairs generated from SFWM in an AlGaAsOI microring resonator [8] in conjunction with a low-loss photonic testbed consisting of double-pass dense wavelength division multiplexers (DWDMs from Fiberdyne Labs) to demonstrate a three-detector, continuously pumped, time-bin QKD protocol [23]. The AlGaAsOI resonator generates a broad spectrum spanning $>300\ \text{nm}$ ($>40\ \text{THz}$) of entangled-photon pairs with larger free-spectral range for simple DWDM, which can be used to either spectrally multiplex for higher secure key distribution rates or used to send different pairs to numerous users, creating a multi-user connected quantum information network as demonstrated in Fig. 1. We demonstrate entanglement-based QKD using two sets of time-bin entangled modes from the comb. We record sifted key rates and sifted key efficiencies up to 8 kbps and 74 kbps/mW of pump power (up to $120\ \mu\text{W}$ for the studied device), respectively, for a single pair. The efficiency, which surpasses the record efficiency from bulk poled lithium niobate (PPLN) [24], is enabled by the tight optical confinement in the highly nonlinear and low-loss microring resonator, demonstrating the advantage of PICs for quantum communication applications that require low-SWaP.

1.1. Protocol

We follow a recently developed three-detector asymmetric sifting QKD protocol [23] that does not require a pulsed laser for clock synchronization. The protocol also enhances the secure key rate by a factor of two by requiring one fewer detector than

similar implementations [25], which enabled 7 kbps sifted key rates using a bulk SPDC source [23]. Here, we expand on this demonstration through the use of a SFWM chip-scale source that reduces the input optical power while maintaining high key rates.

The protocol is shown in Fig. 2. A tunable CW laser source is sent through ASE filters to remove any pump power at the adjacent signal and idler frequencies used for the protocol. The pump light is coupled into/out of an AlGaAsOI ring resonator with 1 THz free-spectral range using lensed optical fibers, whereby entangled-photon pairs are generated in spectral modes adjacent to the pump through SFWM. In Fig. 2, the inset shows the energy conservation of the SFWM process, where λ_p , λ_i , and λ_s correspond to the pump, idler, and signal photons [26]. Once the photon pair is generated, the signal and idler photon are demultiplexed using double-pass 100 GHz DWDMs to provide sufficient extinction of the pump light and to separate the signal and idler photons into respective fiber channels. The signal photons are sent to Bob while the idler photons are sent to Alice. Both Alice and Bob utilize a beam splitter to send their stream of photons to either the X or the Z basis; the Z basis is used to generate the key and measures the photon arrival time in one of two time bins separated by a user-defined, fixed delay τ . The X basis monitors the signal-idler two-photon interference visibility to determine the security of the key, where a visibility $>50\%$ surpasses the classical limit and $>70.7\%$ violates the Clauser-Horne (CH) visibility [27,28].

A key innovation for CW time-bin QKD introduced by Pelet *et al.* is that Alice and Bob have unique Z basis measurement systems [23]. The table in Fig. 2 shows an example of eight sets of photon pairs arriving to Alice and Bob's Z bases. Bob's Z basis measurement consists of a 3 dB beam splitter to randomly send the signal photons along one of two optical paths corresponding to a 0-bit (short optical path with time t_n in the table in Fig. 2) or a 1-bit (long optical path with time $t_n + \tau$). Bob uses two SNSPDs to measure the photon's arrival time within 100 ps time-bins and $>85\%$ detector efficiency. Contrary to Bob, Alice utilizes a single SNSPD to detect the arrival time of the idler photons. With her arrival times, she creates a second, electronically delayed

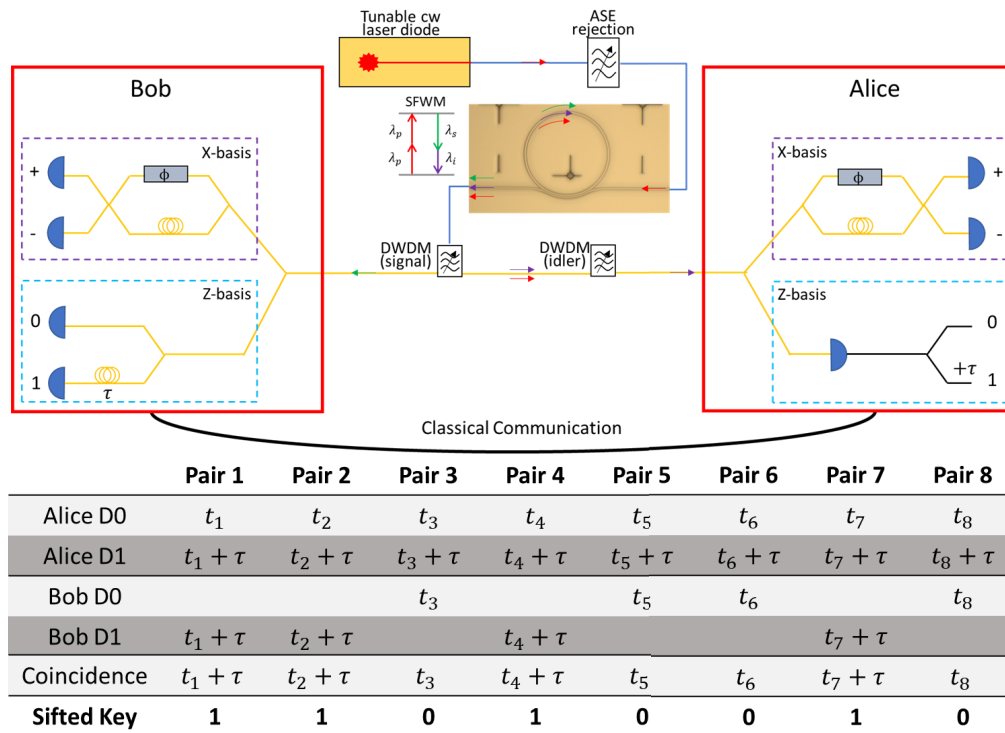


Fig. 2. Experimental design for a three-detector time-bin QKD protocol. A tunable continuous wave (CW) laser source pumps the resonator source after passing through amplified spontaneous emission (ASE) filters. The pump light along with the entangled-photon pairs generated via SFWM couple from the chip to lensed optical fibers and enter dense wavelength division demultiplexer (DWDM) filters. The signal photon travels to Bob's measurement setup, and the idler photon travels to Alice. Alice and Bob establish visibility measurements in the X basis via locked Franson interferometry. Alice has a tunable phase shifter and sweeps the relative phase between the short and long path to show two-photon interference of the $\frac{1}{\sqrt{2}}(|SS\rangle + \exp(i\phi)|LL\rangle)$ state. In the Z basis, Alice uses a single superconducting nanowire single photon detector (SNSPD) and collects the single photon arrival times as well as an electronically delayed channel (black lines). Bob splits his signal photons into two paths using a fiber-based 3 dB splitter. Each path has an SNSPD, and Bob records detection events in either the "0" time bin (short path) or "1" time bin (long path). The table shows how a sifted key is established.

channel with a delay equal to Bob's long fiber path delay, τ . Alice thus records a detection event at t_n and $t_n + \tau$ for each detected idler photon from the source. Using a classical channel, Bob only communicates to Alice the arrival time of photons at his detector without sharing any path information. By comparing the arrival times and looking for coincidences within a 1 ns window (which is set based on the biphoton cavity lifetime of the source), Alice is able to determine whether Bob detected the photon in his 0- or 1-bit path. Alice sends the coincidence event information back to Bob over the classical channel, only communicating the arrival time. Bob determines whether this event corresponds to the 0- or 1-bit by finding the detector that received the corresponding click. Through this post-selection, Alice and Bob establish their sifted key based on the photon coincidence with Bob's 0-bit or 1-bit detector. The table in Fig. 2 illustrates the protocol with eight exemplary measurement outcomes and the corresponding sifted key. Common time-bin protocols utilize a pulsed laser for synchronization and a 3 dB splitter on both Alice and Bob's Z basis measurement, which limits the secure key rate to 25% of the generated coincidence count rate [25]. Here, the raw coincidence count rate usage is improved to 50% by removing the choice of two paths on Alice's side.

The X basis monitors the entanglement visibility via Franson interferometry [29]. Each photon enters an unbalanced Mach-Zehnder interferometer separating the photon coincidences into three distinct time bins: an early bin when the idler

takes the short path and the signal takes the long path; a late time bin when the idler takes the long path and the signal takes the short path; and a central bin when both photons take the same path (see Fig. S2). This central bin corresponds to the photon state: $\frac{1}{\sqrt{2}}(|SS\rangle + \exp(i\phi)|LL\rangle)$, where the phase ϕ is set by a tunable phase shifter in the short arm. Alice's and Bob's interferometers are locked to maintain a consistent relative phase during the measurement, and Alice's voltage controlled phase shifter can be swept to change the phase between the two states. Bob uses the phase shifter in his interferometer to locally stabilize the X basis to any environmental fluctuations. Since Alice sweeps her phase shifter across the full π range, relative phase drift between Alice and Bob's interferometers do not impact the visibility measurement (provided each interferometer is stable for the duration of a π phase sweep). Importantly, because the time bins are defined at Alice and Bob, only the interferometers at Alice and Bob need to be phase stable, whereas phase fluctuations in the fibers from the source to Alice and Bob do not impact the phase of the time-bin entangled pairs defined once the photons arrive at the nodes.

2. SOURCE CHARACTERIZATION

The source used to generate entangled-photon pairs is an AlGaAs-SOI microring resonator (a microscope image of a comparable source is shown in Fig. 2). The microring resonator studied in

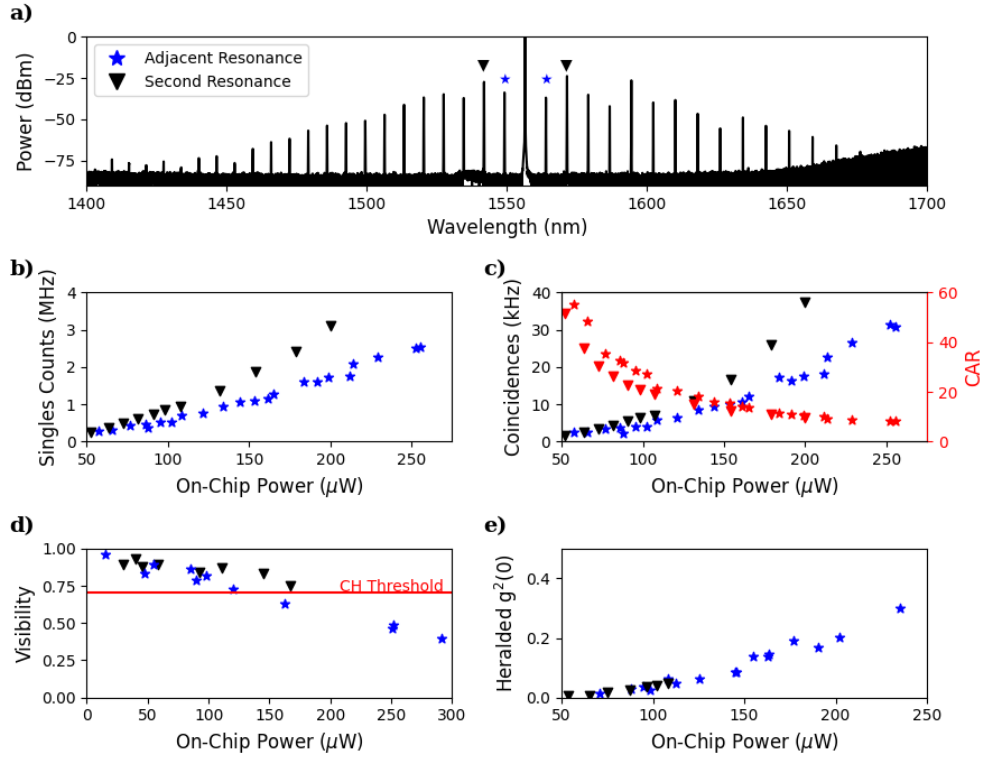


Fig. 3. Characterization of the entangled-photon pair source used for the QKD protocol. (a) The frequency comb spectrum from the ring resonator source when pumped with sufficient pump power to generate a frequency comb visible using an optical spectrum analyzer. The blue stars indicate the adjacent resonance and the black triangles indicate the second nearest resonance. (b) Collected raw single photon counts as a function of the on-chip pump power. (c) Measured coincidence count rate as a function of on-chip power along with the coincidence-to-accidental ratio (CAR). (d) Raw (without background subtraction) two-photon interference visibility as a function of the on-chip power. The visibility is largely limited by the pump leakage at higher powers. Figure S3 in Supplement 1 shows the visibility after background subtraction. (e) Heralded single photon purity measurement as a function of power.

the following experiment had a radius of $13.91 \mu\text{m}$. The width of the bus waveguide was $0.48 \mu\text{m}$, and the ring waveguide was $0.69 \mu\text{m}$ wide. The gap between the waveguide and the ring was $0.48 \mu\text{m}$, and the AlGaAs layer was $0.4 \mu\text{m}$ thick. For full device fabrication details as well as additional device characterization, refer to our previous work [8]. The resonator is pumped at the resonance near 1557 nm to generate a quantum frequency comb that spans over 300 nm . When pumped with sufficient power (above the optical parametric oscillator threshold), the frequency comb is visible with an optical spectrum analyzer showing the possible generation of >20 pairs of entangled-photon pair frequencies, as shown in Fig. 3(a). Above 1650 nm , the optical spectrum analyzer has a limited responsivity and thus exhibits an increasing background that eventually surpasses the generated comb lines. In Fig. 3(a), the adjacent and second nearest resonances are denoted by the blue star and black triangle, respectively. Throughout this work, data collected from both resonances will be presented. Data from the adjacent resonance will be plotted using blue stars, and data from the second nearest resonance will be black triangles. As described in the previous section, the QKD protocol relies on a single pair of photon modes, thus such a large bandwidth can be used for either wavelength multiplexing (enhancing the key rate by a factor of ~ 20) or for multi-user distribution of quantum information.

First, we bypass the beam splitters that distribute photons to the X and Z basis shown in Fig. 2 and send the signal and idler photons directly to the SNSPDs to characterize the raw single

photon count rate and coincidence count rates. The low-loss DWDM filters ($<3 \text{ dB}$ insertion loss with $>100 \text{ dB}$ extinction) and optimized chip-to-fiber coupling ($\sim 3.5 \text{ dB}$ per facet) enable efficient collection of signal and idler photons with high coincidence count rates for low pump powers. The pump resonance (near 1557 nm) has a loaded quality factor $Q = 1.24 \times 10^6$ corresponding to a full width at half maximum (FWHM) of 220 MHz while the adjacent resonances (blue stars) have quality factors of 0.67 and 0.39×10^6 corresponding to a FWHM of 340 MHz and 575 MHz , and the second nearest resonances have quality factors of 1.05×10^6 and 1.00×10^6 (black triangles) corresponding to a FWHM of 239 MHz and 279 MHz . The lower quality factors for the nearest resonance modes reduces the entangled-photon pair generation rate, however, even with the nearest modes, over 2.5 MHz detected single photon counts and 30 kHz coincidence counts are recorded [Figs. 3(b) and 3(c)] with less than $300 \mu\text{W}$ of on-chip pump power. The CAR of the source remains above eight at all powers, indicating a high quality, low loss photonic testbed capable of generating a secure key with low errors and high rates. For the second nearest resonance, we measure up to 40 kHz raw coincidences and a measured singles count rate above 4 MHz , which is limited by latching of the SNSPDs.

The security of the protocol relies on monitoring the entanglement visibility of the source during operation. Figure 3(d) shows the visibility of the source as a function of on-chip power without background subtraction. Here, the visibility is monitored using a folded Franson interferometer where both the signal and idler

photon enter the same interferometer before being demultiplexed from each other. In a field-deployed version of the quantum key distribution system, Alice and Bob would each have their own interferometer with a calibrated relative phase. As an example, the visibility of the second resonance mode using 170 μW of on-chip power is shown in Fig. S2. At higher powers, the extinction of our filters is not sufficient to block all of the pump light from reaching the detectors, which degrades the two-photon visibility. As a result, above 120 μW of on-chip power, the visibility is below the CH threshold [27]. We thus keep the on-chip pump power below 140 μW during the QKD protocol. The second resonance has greater pump extinction since the modes are 2 THz from the pump mode, allowing for a higher pump power to be used while maintaining sufficient visibility; however, to keep the data compatible with multiplexed QKD systems, the pump power is limited to 120 μW to be well above the CH threshold for both the adjacent and second resonance modes. In Supplement 1, the visibility with background subtraction is reported (Fig. S3), indicating that with additional pump filtering, up to 275 μW of pump power can be used while still remaining above the CH threshold. At large enough powers, the multi-photon pair emission probability begins to contribute considerably, opening up the potential risk of photon-number splitting attacks on the QKD system [30].

Another important property of the source is the heralded single-photon purity, which can be used to quantify the probability of generating multiple photon pairs in a given time bin. This characterization is completed using a heralded $g^2(0)$ measurement where the signal photons are detected directly, and the idler photons are sent to a 3 dB splitter before being detected at one of two detectors. Since the photon pairs should be generated simultaneously, recording the three-fold coincidences between

the detectors should show a dip at zero time delay. The value of the heralded $g_H^{(2)}(0) = \frac{N_{ABC}N_A}{N_{AB}N_{AC}}$, where N_{ABC} is the number of threefold coincidences, N_A is the heralding count rate, and $N_{AB,AC}$ are the twofold coincidences between the heralding channel and one of the two idler channels. An exemplary scan of the heralded $g^2(0)$ for the source described here is shown in Supplement 1 (Fig. S1). Figure 3(e) shows the heralded $g^2(0)$ as a function of on-chip power. For both sets of signal and idler modes, the single photon purity remains above 90% when the on-chip power is below 150 μW .

3. TIME BIN QUANTUM KEY DISTRIBUTION

With a bright source of entangled-photon pairs operating in a regime with high visibility and high single-photon purity, the QKD protocol described in Section 1 can be implemented. We monitor the Z basis (shown in Fig. 2) to generate a sifted key at various pump powers to assess how the error rates and sifted key rates scale with power. Figure 4(a) shows the sifted key rates collected for the adjacent and second nearest resonance of the ring resonator source. As described in the source characterization section, the difference in resonance quality factors between these two pairs of modes creates a difference in the generated entangled-photon pair flux, and thus the key rate of the second resonance is approximately four times larger than that of the adjacent resonance. Additionally, the pump rejection filters used in this experiment have larger extinction ratios for larger detuning from the pump wavelength, so the error rates of the adjacent resonance are larger than the second nearest resonance due to pump leakage into the detectors. Figure 3(d) shows the visibility measurement (X basis) for the resonances at different pump powers. Since the CH threshold is surpassed

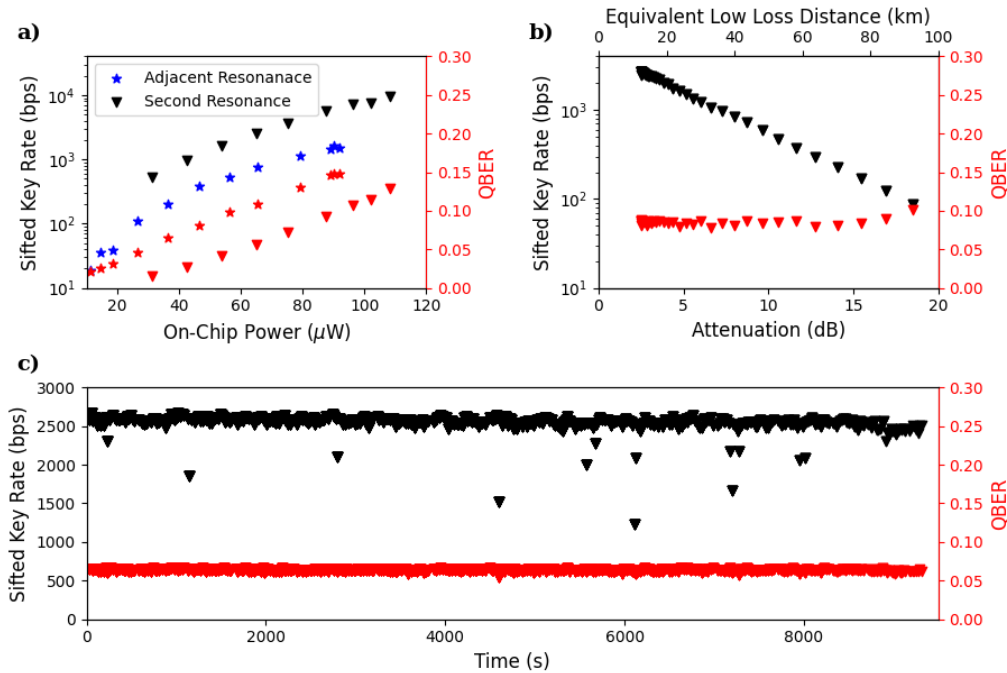


Fig. 4. (a) Sifted key rate and bit error rate as a function of on-chip pump power. The pump power is limited to $<120 \mu\text{W}$ to maintain a visibility above 70.7%. The triangles indicate the adjacent resonance characterization, and the stars indicate the second nearest resonance. (b) Sifted key rate and bit error rate of the second nearest resonance as a function of attenuation on Alice's path. The pump power is maintained at $\sim 90 \mu\text{W}$ while sweeping the voltage on a variable optical attenuator. The equivalent optical fiber distance is calculated and indicated on the top axis. (c) Key rate stability measurement. Pumping with $\sim 65 \mu\text{W}$ of on-chip power, the source consistently outputs 2.5 kbps sifted key rate for up to 10,000 s (limited by the measurement time of the experiment).

Table 1. Comparison of Entanglement-Based QKD Protocols^a

Platform	Type	Resource	Sifted Key Rate (kbps)	Error Rate	Pump Power (mW)	Reference
AlGaAsOI ring	SFWM	Time-bin	8	0.09	0.108	This work
Bulk PPLN	SPDC	Time-bin	7	0.047	<6	[23]
AlGaAs waveguide	SPDC	Polarization	0.039	0.02		[35]
Bulk PPKTP	SPDC	Polarization	0.109	0.064	2.4	[36]
Bulk PPLN	SPDC	Polarization	0.3	<0.06	1–10	[37]
Si waveguide	SFWM	Dispersive optics	0.04–0.06	0.07–0.08		[38]
Bulk PPLN	SPDC	Polarization	$>100 \times 10^3$	<0.07	422	[25]
Bulk PPLN	SPDC	Polarization	$>1.8 \times 10^4$ (simulated)		400	[24]

^aThe key rates are adjusted to reflect transmission without attenuation and are reported for a single set of photon pairs (i.e., without multiplexing).

for powers less than 126 μ W, we demonstrate the QKD protocol up to these powers. Without any error correction, sifted key rates with less than 10% error rates of up to 0.6 kbps and 8 kbps are recorded for the adjacent and second nearest resonance, respectively. A binary secure key can be established with up to $\sim 11\%$ error rates at which the Shannon rate $1 - 2H(x)$ reaches 0 (where $H(x) = -x \log_2(x) - (1-x) \log_2(1-x)$ is the binary entropy function) [31–34]. We report the sifted key rates up to this bound to ensure that a secure key can be established. With additional pump filtering for the adjacent resonance, it is expected that the rate can approach 2 kbps.

A comparison of this result with a subset of other entanglement-based QKD demonstrations is included in Table 1, and Ref. [12] has an extensive review of recent experimental works. For comparable error rates, our source does not outperform all of the demonstrations in this table; however, the efficiency of this source is improved, requiring only $\sim 100 \mu$ W of optical power to generate a comparable sifted key. For example, when normalizing to the pump power, the sifted key generation efficiency is >60 times higher in this work compared with bulk periodically PPLN used for the same protocol [23]. Through dense spectral multiplexing with >66 frequency channels, polarization encoding using bulk PPLN can boost the key rates to >1 Gbps [24] with 400 mW of pump power. Comparing efficiencies for low-SWaP applications such as space-based entanglement distribution, the AlGaAsOI PIC single-pair efficiency of 74 kbps/mW (up to $<120 \mu$ W for the studied device) is higher than polarization encoding with bulk PPLN (45 kbps/mW).

Next, the QKD protocol is extended to artificial distances using a variable optical attenuator placed before Alice's detection setup. Figure 4(b) shows the sifted key rate and bit error rate as a function of attenuation. The top axis shows the equivalent distance in kilometers for the attenuation assuming low-loss optical fiber with 0.2 dB/km attenuation. Since the protocol relies simply on the photon arrival times, photon loss will dominate all contributions to the degradation of the sifted key rate and increase in error rate. Using the second nearest resonance at an attenuation-free sifted key rate of 6 kbps and error rate of approximately 8.5%, the attenuator voltage is swept from 2.5 dB of attenuation (the insertion loss of the attenuator) to 18.5 dB of attenuation. The key rate remains above 100 bps for all attenuations, and the error rate remains consistent until approximately 15 dB of attenuation, where it gradually increases to $\sim 10\%$ at the largest attenuation. With this data, we show an effective key rate of 100 bps at an equivalent distance of 92.5 km with error rates below 10%.

To assess the long-term stability of the source, we show in Fig. 4(c) a sifted key and error rate measurement for up to 10,000 s. To align the pump laser with the resonance, the laser

wavelength is swept from 0.1 nm below the resonance up to the resonance wavelength, allowing for the resonance to thermally shift as power begins to couple into the ring. Since the extinction ratio of the pump resonance is >3 dB, an external power meter can be used to determine when the laser wavelength and resonance are aligned (showing a >3 dB dip in the monitored power). During the stability measurement, if the power meter reading increases by >3 dB, it is indicative of the laser and ring becoming misaligned. The wavelength sweep is repeated, taking <5 s, to realign the pump laser with the ring resonance. The data is sampled every 20 s during the stability measurement, and the data points with key rates lower than the others are caused by this realignment process. Other than this monitoring, the operation requires no additional adjustments to the source. The slight reduction in the key rate over time is caused by fiber drift in the experimental setup, which can be mitigated through fiber packaging. Throughout the 10,000 s, the error rate is stable at $\sim 6\%$.

4. DISCUSSION

To demonstrate the practical utility of the source, we send Alice's photon through a deployed, standard SMF-28 telecom fiber on the UCSB campus. The image in the background of Fig. 5 shows an illustration of the approximate deployed fiber path with a ~ 2 km fiber loop connecting our research lab with another building on campus which is used to demonstrate the robustness of the protocol to external environmental factors. Six fiber loops are made, allowing for >12 km transmission using real fiber lines. Figure 5(a) shows the key rate and errors for the second nearest resonance mode with an initial rate of 1 kbps and 3% error. The deployed fibers exhibit additional loss due to connectors instead of fiber splices being used to configure the number of fiber loops in the channel, which degrades the secure key rate. However, the error rate remains consistent and low for all fiber loop configurations indicating that the influence of environmental factors is negligible. Additionally, the visibility is monitored and is $>73.9\%$ at 12.3 km indicating that the state is not impacted through the long-distance distribution.

The stability of the system is also monitored for 6000 s to confirm that external factors such as vibrations from vehicles on the road above the fiber or temperature fluctuations do not influence the sifted key generation rate stability. As shown in the measurement in Fig. 5(b), fiber drift at the chip–fiber coupling interface is the largest factor in the key rate variation over time. To make sure this variation was from the chip–fiber interface and not a variation in the deployed fiber, a fiber realignment was completed showing that the initial rate can be recaptured and confirming that the deployed fiber does not impact the sifted key

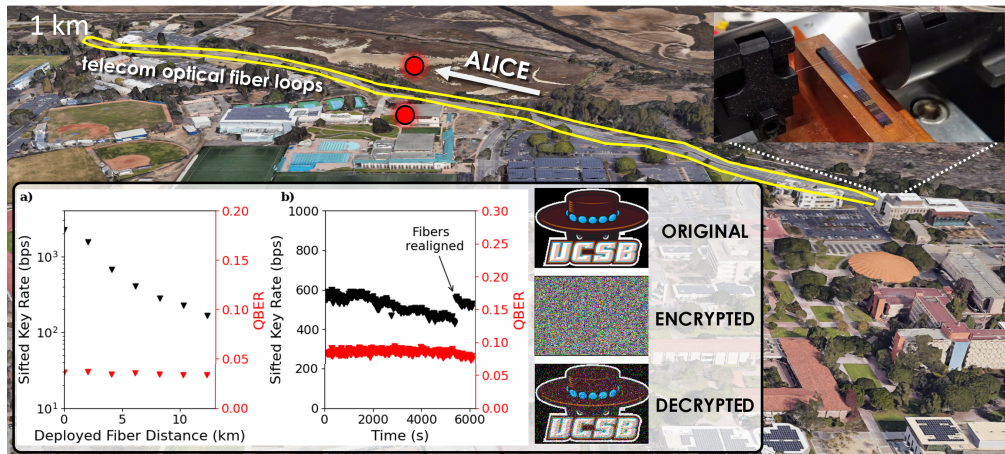


Fig. 5. Illustration of the deployed fiber experiment conducted on the University of California Santa Barbara (UCSB) campus. Six loops of ~ 2 km fibers are in place between our research lab in Henley Hall and the campus police station. The yellow lines indicate a rough estimate of the path of the deployed fibers which follow underneath the road connecting these parts of campus. The six independent loops allow for measurements to be completed at different deployed fiber lengths. (a) The sifted key rate and error rate of the QKD protocol after sending Alice's photons through the deployed fiber path. (b) The stability of the key rate and error rate at the longest deployed fiber distance of 12.3 km. The chip-to-fiber coupling drift is significant during this measurement, so a realignment is completed at the 5,300 s mark. Using the 12.3 km deployed fiber, the UCSB logo is transmitted and encrypted using the QKD protocol. The image is transmitted at 600 bps and a 9% error rate without any error correction.

rate. With this information, we hypothesize that the attenuation-based demonstration accurately models the impact of deployed fiber length on the error rate and key rate. We therefore predict the ability for >100 bps key rates with $<10\%$ error at 92.5 km without spectral multiplexing.

Finally, we use the deployed 12.3 km fiber to transmit a key to encrypt and decrypt an RGB image as shown in Fig. 5. Alice and Bob establish their key at 600 bps with an error rate $<9\%$ [at the same time as the stability measurement shown in Fig. 5(b)] to communicate the UCSB logo. The right-hand side of the inset of Fig. 5 shows the original image, encrypted image and decrypted image using the QKD protocol described in this work. Without error correction, the source shows the capability of transmitting a key across the 12.3 km real deployed fiber to securely encrypt/decrypt a 21 kB image.

5. CONCLUSION

Using a high-quality AlGaAs-on-insulator microring resonator, we generate a quantum optical microcomb spanning >300 nm with >20 time-energy entangled modes that can be easily demultiplexed and filtered using commercial, off-the-shelf telecom fiber components. We demonstrate the ability to demultiplex photon pairs for scalable entanglement distribution across standard telecom SMF-28 fiber. As an illustrative example, we demonstrate a continuous-wave time-bin quantum key distribution protocol that does not require pulsed optical excitation for clock synchronization. Requiring only ~ 100 μ W of optical power to generate up to 8 kbps sifted key rates with errors $<10\%$, we demonstrate the low SWaP capability and stability of the source and the protocol using a campus-deployed telecom fiber loop. The source operates with >20 frequency mode pairs allowing for key rates exceeding 100 kbps to be achieved through wavelength multiplexing or a connected >20 -user quantum photonic network to be established.

Looking forward, the low SWaP of the source while maintaining ultra-high entanglement distribution rates opens new opportunities for practical quantum networks and communications, such as space-based and long-distance metropolitan channels. While we show here spectral modes spaced by 1 THz across 300 nm of bandwidth, dense spectral multiplexing with high generation rates is possible by cascading arrays of microcombs. For example, our AlGaAsOI chip (shown on the inset to Fig. 5) has >100 individual microring resonators, which could each be independently tuned and spectrally aligned to match the 100 GHz telecom ITU grid and pumped with fiber arrays to further enhance the key rates or improve the network user capacity. This could enable >1000 independent users with a single photonic chip or end-to-end multiplexed entanglement key rates exceeding 10 MHz.

Funding. National Science Foundation (CAREER-2045246, DMR-1906325); National Aeronautics and Space Administration (Subcontract No. UCSB-01); Amethyst Research, Inc.; Cisco Systems (Research University Gift Program).

Acknowledgments. This work was supported by the NSF Quantum Foundry through Q-AMASE-i Program (award no. DMR-1906325), NSF (award no. CAREER-2045246), and the National Aeronautics and Space Administration under Subcontract No. UCSB-01 and Amethyst Research, Inc. We also gratefully acknowledge support from the Cisco Research University Gift Program.

Disclosures. The authors declare no conflicts of interest.

Data availability. The data that support the figures in this paper and other findings of this study are available from the corresponding author on reasonable request.

Supplemental document. See Supplement 1 for supporting content.

REFERENCES

1. P. J. Mosley, J. S. Lundeen, B. J. Smith, *et al.*, "Heralded generation of ultrafast single photons in pure quantum states," *Phys. Rev. Lett.* **100**(13), 133601 (2008).

2. E. Knill, R. Laflamme, and G. J. Milburn, "A scheme for efficient quantum computation with linear optics," *Nature* **409**(6816), 46–52 (2001).
3. Z. S. Yuan, X. H. Bao, C. Y. Lu, *et al.*, "Entangled photons and quantum communication," *Phys. Rep.* **497**(1), 1–40 (2010).
4. G. Moody, V. J. Sorger, D. J. Blumenthal, *et al.*, "2022 Roadmap on integrated quantum photonics," *JPhys Photonics* **4**, 012501 (2022).
5. N. Gisin and R. Thew, "Quantum communication," *Nat. Photonics* **1**(3), 165–171 (2007).
6. Q. Liu, Y. Huang, Y. Du, *et al.*, "Advances in chip-based quantum key distribution," *Entropy* **24**(10), 1334 (2022).
7. G. Moody, L. Chang, T. J. Steiner, *et al.*, "Chip-scale nonlinear photonics for quantum light generation," *AVS Quantum Science* **2**(4), 041702 (2020).
8. T. J. Steiner, J. E. Castro, L. Chang, *et al.*, "Ultra-bright entangled-photon pair generation from an AlGaAs-on-insulator microring resonator," *PRX Quantum* **2**(1), 010337 (2021).
9. W. Xie, L. Chang, H. Shu, *et al.*, "Ultrahigh-Q AlGaAs-on-insulator microresonators for integrated nonlinear photonics," *Opt. Express* **28**(22), 32894–32906 (2020).
10. J. E. Castro, T. J. Steiner, L. Thiel, *et al.*, "Expanding the quantum photonic toolbox in AlGaAsOI," *APL Photonics* **7**(9), 096103 (2022).
11. C. McDonald, G. Moody, S. W. Nam, *et al.*, "III-V photonic integrated circuit with waveguide-coupled light-emitting diodes and WSi superconducting single-photon detectors," *Appl. Phys. Lett.* **115**, 081105 (2019).
12. F. Xu, X. Ma, Q. Zhang, *et al.*, "Secure quantum key distribution with realistic devices," *Rev. Mod. Phys.* **92**(2), 025002 (2020).
13. C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," *Theor. Comput. Sci.* **560**, 7–11 (2014).
14. P. Sibson, C. Erven, M. Godfrey, *et al.*, "Chip-based quantum key distribution," *Nat. Commun.* **8**, 13984 (2017).
15. S. Pirandola, U. L. Andersen, L. Banchi, *et al.*, "Advances in quantum cryptography," *Adv. Opt. Photonics* **12**(4), 1012 (2020).
16. A. Kumar and S. Garhwal, "State-of-the-art survey of quantum cryptography," *Arch. Computat. Methods Eng.* **28**(5), 3831–3868 (2021).
17. S. Wang, Z. Q. Yin, D. Y. He, *et al.*, "Twin-field quantum key distribution over 830-km fibre," *Nat. Photonics* **16**(2), 154–161 (2022).
18. S. K. Liao, W. Q. Cai, W. Y. Liu, *et al.*, "Satellite-to-ground quantum key distribution," *Nature* **549**(7670), 43–47 (2017).
19. R. Bedington, J. M. Arrazola, and A. Ling, "Progress in satellite quantum key distribution," *npj Quantum Inf.* **3**(1), 30 (2017).
20. L. C. Kwek, L. Cao, W. Luo, *et al.*, "Chip-based quantum key distribution," *AAPPS Bull.* **31**(1), 15 (2021).
21. W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature* **299**(5886), 802–803 (1982).
22. E. Diamanti, H. K. Lo, B. Qi, *et al.*, "Practical challenges in quantum key distribution," *npj Quantum Inf.* **2**(1), 16025 (2016).
23. Y. Pelet, G. Sauder, M. Cohen, *et al.*, "Operational entanglement-based quantum key distribution over 50 km of field-deployed optical fibers," *Phys. Rev. Appl.* **20**, 044006 (2023).
24. S. P. Neumann, M. Selimovic, M. Bohmann, *et al.*, "Experimental entanglement generation for quantum key distribution beyond 1 Gbit/s," *Quantum* **6**, 822 (2022).
25. S. P. Neumann, A. Buchner, L. Bulla, *et al.*, "Continuous entanglement distribution over a transnational 248 km fiber link," *Nat. Commun.* **13**, 6134 (2022).
26. L. G. Helt, Z. Yang, M. Liscidini, *et al.*, "Spontaneous four-wave mixing in microring resonators," *Opt. Lett.* **35**(18), 3006 (2010).
27. J. F. Clauser and M. A. Horne, "Experimental consequences of objective local theories," *Phys. Rev. D* **10**(2), 526–535 (1974).
28. J. G. Rarity and P. R. Tapster, "Experimental violation of Bells inequality based on phase and momentum," *Phys. Rev. Lett.* **64**(21), 2495–2498 (1990).
29. J. D. Franson, "Bell inequality for position and time," *Phys. Rev. Lett.* **62**(19), 2205–2208 (1989).
30. S. Sun and A. Huang, "A review of security evaluation of practical quantum key distribution system," *Entropy* **24**(2), 260 (2022).
31. S. P. Neumann, T. Scheidl, M. Selimovic, *et al.*, "Model for optimizing quantum key distribution with continuous-wave pumped entangled-photon sources," *Phys. Rev. A* **104**(2), 022406 (2021).
32. X. Ma, C. H. F. Fung, and H. K. Lo, "Quantum key distribution with entangled photon sources," *Phys. Rev. A* **76**(1), 012307 (2007).
33. E. Waks, A. Zeevi, and Y. Yamamoto, "Security of quantum key distribution with entangled photons against individual attacks," *Phys. Rev. A* **65**(5), 052310 (2002).
34. P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," *Phys. Rev. Lett.* **85**(2), 441–444 (2000).
35. F. Appas, F. Baboux, M. I. Amanti, *et al.*, "Flexible entanglement-distribution network with an AlGaAs chip for secure communications," *npj Quantum Inf.* **7**(1), 118 (2021).
36. Y. Shi, S. Moe Thar, H. S. Poh, *et al.*, "Stable polarization entanglement based quantum key distribution over a deployed metropolitan fiber," *Appl. Phys. Lett.* **117**, 124002 (2020).
37. S. K. Joshi, D. Aktas, S. Wengerowsky, *et al.*, "A trusted node-free eight-user metropolitan quantum communication network," *Sci. Adv.* **6**, eaba0959 (2020).
38. X. Liu, J. Liu, R. Xue, *et al.*, "40-user fully connected entanglement-based quantum key distribution network without trusted node," *PhotonIX* **3**(1), 2 (2022).