O-band Polarization-Entanglement Quantum Key Distribution with Co-Propagating Classical Channel

Justin Yu Xiang Peh,[1] Syed Abdullah Aljunid,[2] Hou Shun Poh,[1]
Darren Ming Zhi Koh,[1] Cyrus Proctor,[2] Lijiong Shen,[3] and Christian Kurtsiefer[1,4,*]

[1] *Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543*
[2] *S-Fifteen Instruments Pte. Ltd., 71 Ayer Rajah Crescent, Singapore 139951*
[3] *School of Physics, Hangzhou Normal University, Hangzhou, Zhejiang 311121, China*
[4] *Department of Physics, National University of Singapore, 2 Science Drive 3, Singapore 117542*

(Dated: April 13, 2026)

Abstract pending.

I. INTRODUCTION

Quantum key distribution (QKD) provides information-theoretic secure key exchange [1] between two remote parties, bounded only by the laws of quantum physics. Early QKD proposals like BB84 [2] have since been extended to other protocols like BBM92 [3] which use entanglement as a resource. This protocol is well-suited for metropolitan-scale networks due to its balance between security and usability, particularly in mitigating source side-channel attacks [4] whilst providing practical key rates.

Fiber-based BBM92 QKD systems generally use the C-band optical spectrum (e.g., 1550 nm wavelength) for the quantum signal [5–8], leveraging the low-loss optical window in standard telecommunication fibers to increase key rates. This however comes at the expense of higher quantum bit-error rates (QBER) due to noise from strong chromatic dispersion effects [5, 6], as well as Raman and Brillouin scattering [9, 10] when running classical copropagating traffic within the same fiber [11, 12].

In contrast, the O-band optical spectrum (e.g., 1310 nm wavelength) is designed to fall within the zero-dispersion window of the same fibers, likely already deployed as part of existing telecommunication infrastructure [13, 14]. This facilitates interoperability with existing classical traffic deployed on the ITU-T G.698.4 dense-wavelength division multiplexing (DWDM) channel grids spanning the C-band spectrum [15], without the need for dedicated dark fibers. The corresponding scattering noise is predominantly from spontaneous Raman scattering, with a lower scattering probability into the more energetic anti-Stokes O-band [16].

In this paper, we demonstrate O-band BBM92 QKD co-propagating with C-band classical traffic over 29.5 km of deployed standard telecommunication fibers, using commercial off-the-shelf avalanche photodetectors (APDs). Using a highly wavelength-asymmetric polarization-entangled photon pair source [17], we generate intrinsically narrow bandwidth pairs (≈ 120 GHz) that can be efficiently filtered with a bandpass filter for rejection of scattering noise. To our knowledge, this is the first explicit demonstration of O-band BBM92 QKD with classical coexistence over deployed fiber.

II. EXPERIMENTAL SETUP

The QKD system is deployed across physically separate locations, as illustrated in Fig. 1(a). The local node (denoted "Alice") and the entanglement source are co-located at the Centre for Quantum Technologies, while the remote node (denoted "Bob") is situated at the Netlink Sembawang Central Office. The nodes are connected via a deployed fiber link comprising multiple stretches of G.652D- and G.657A-compatible telecommunication fibers, spanning a total distance of 29.5 km (see Appendix B).

A simplified schematic of the setup is shown in Fig. 1(b). The source generates polarization-entangled photon pairs of wavelengths 586 nm and 1310 nm via spontaneous parametric down-conversion (SPDC) with the Bell state

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}\left(|HH\rangle + |VV\rangle\right) \tag{1}$$

shared between Alice and Bob. The source exhibits a visibility of $> 95\%$ in both the rectilinear (H/V) and diagonal (D/A) bases (see Appendix A) corresponding to an entanglement fidelity of at least 97%, and a raw heralding efficiency of approximately 8.2%.

Utilizing a wavelength-asymmetric pair source provides two distinct advantages: (1) The intrinsic bandwidth of the entangled photons is narrower compared to a wavelength-degenerate setup due to the smaller wavelength acceptance during the down-conversion process [cite], allowing for more efficient downstream noise filtering; (2) Highly efficient detectors for the visible wavelength regime can be used without the need for infrared up-conversion, simplifying the setup while increasing the overall heralding efficiency.

The signal photons of wavelength 586 nm undergo projective measurements locally at Alice in the H/V and D/A bases using four Si APDs (Excelitas SPCM) in a passive basis choice configuration, denoted as the polarization analyzer in Fig. 1(b). Photodetection event

* phyck@nus.edu.sg

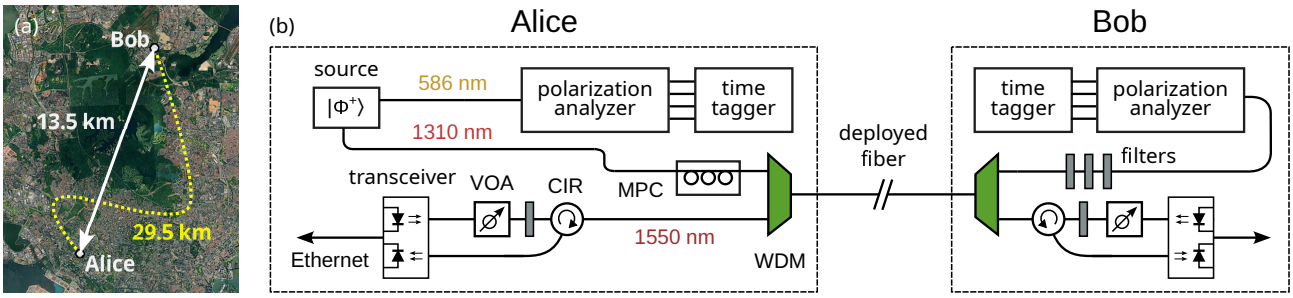

FIG. 1. **(a)** Bird-eye view of both QKD nodes, with the approximate path of the 29.5 km deployed fiber marked in dotted yellow. **(b)** Simplified schematic of the experimental setup with co-propagating classical channel. The source generates polarization-entangled photon pairs of wavelengths 586 nm and 1310 nm in the $|\Phi^+\rangle$ Bell state, whose correlated detections are used for timing synchronization and key distillation. Classical communication between Alice and Bob is performed over a bidirectional optical link at 1550 nm with wavelength-division multiplexing (WDM). Optical filters upstream of the polarization analyzer reject noise from the classical channel and scattered light at 1310 nm. MPC: motorized polarization controller; CIR: circulator; VOA: variable optical attenuator. See Appendix A for a more detailed description.

timestamping is performed with a time tagger of 4 ps nominal resolution (S-Fifteen Instruments TDC2), with a total detection rate $s_a = 2.5 \times 10^6$ counts/s and overall dark count rate of 1.0×10^3 counts/s.

The corresponding 1310 nm idler photons are transmitted over the deployed fiber to the remote polarization analyzer at Bob. Detection is similarly performed using a set of four passively-quenched InGaAs APDs (S-Fifteen Instruments IRSPD1), which have detection efficiency of 10% and a measured afterpulsing probability of 4%. The total detection and dark count rates are around $s_b = 1.3 \times 10^4$ counts/s and 8.1×10^3 counts/s, respectively.

Dispersive contributions from the fiber are minimal, since chromatic dispersion is at most 4 ps due to the narrow idler bandwidth at the zero-dispersion wavelength [18], so timing jitter is dominated by the detector opto-electronics (300 ps for InGaAs APD, 350 ps for Si APD). The expected polarization mode dispersion of 0.2 ps is also significantly less than the idler coherence time of 8 ps. Convolution of both detector jitters yields an overall timing uncertainty of around 0.5 ns, so a coincidence window $\delta t = 0.75$ ns is chosen to capture about 90% of photon pair events [19].

The BBM92 protocol itself is executed using the `qcrypto` [20] QKD suite for coincidence matching, error correction, and privacy amplification. This is wrapped by `QKDServer` [21] that performs auxiliary QKD operations such as coincidence peak finding, and adds process watchdog capabilities. Detection events are downsampled to 125 ps resolution and processed in 2^{29} ns (0.537 s) timing packets to minimize communication overhead. A block size of 10^4 bits is used for error estimation and correction utilizing a modified CASCADE/BICONF algorithm [22, 23]. The resulting secret keys are fed into `guardian` [24], a key management layer that implements a key delivery interface compliant with the ETSI GS QKD 014 specification [25] and authenticated over mutual TLS 1.3.

Over a continuous 9-day QKD run, the system achieved an average secret key rate of 60 bits/s, as shown in Fig. 2(a). The average quantum bit error rate (QBER) during this period was 6.7(1.0)% from Fig. 2(b), with the lowest QBER reached of 4.3% indicative of the intrinsic system entanglement fidelity. The total and accidental coincidence rates averaged 470(70) and 46(11) counts/s, respectively, as shown in Fig. 2(c), corresponding to a coincidence-accidental ratio (CAR) of 10(1). Uncorrelated coincidences due to Bob's detectors operating near the dark count regime account for roughly 60% of the accidentals.

Due to suboptimal locking of the coincidence window to the photon pair coincidences as a result of configuration error, the total coincidence rate was also observed to frequently drop, but quickly recovers after repeating the coincidence signal search (see Appendix C). This behaviour manifests as sharp jumps in total coincidences as shown in Fig. 2(c), which have been smoothed out using a 10 s sliding window for visual clarity. The average uninterrupted key generation interval is 6 mins with a maximum duration of 147 mins observed. The suboptimal locking unfortunately also results in higher accidental count rates than what would be expected from a stable lock, i.e., $s_a s_b \delta t = 25$ counts/s. This is further discussed in Section IV and Appendix C.

To ensure key generation security, mitigations are implemented against discrete-variable QKD detector side-channel vulnerabilities [26]. These include countermeasures addressing breakdown flash leakage and wavelength-dependent transmission using interference filters [27, 28], detector blinding by self-testing [29], and timing mismatch by delay compensation [30]. Source side-channel vulnerabilities are intrinsically mitigated by the use of entanglement as a resource [4].

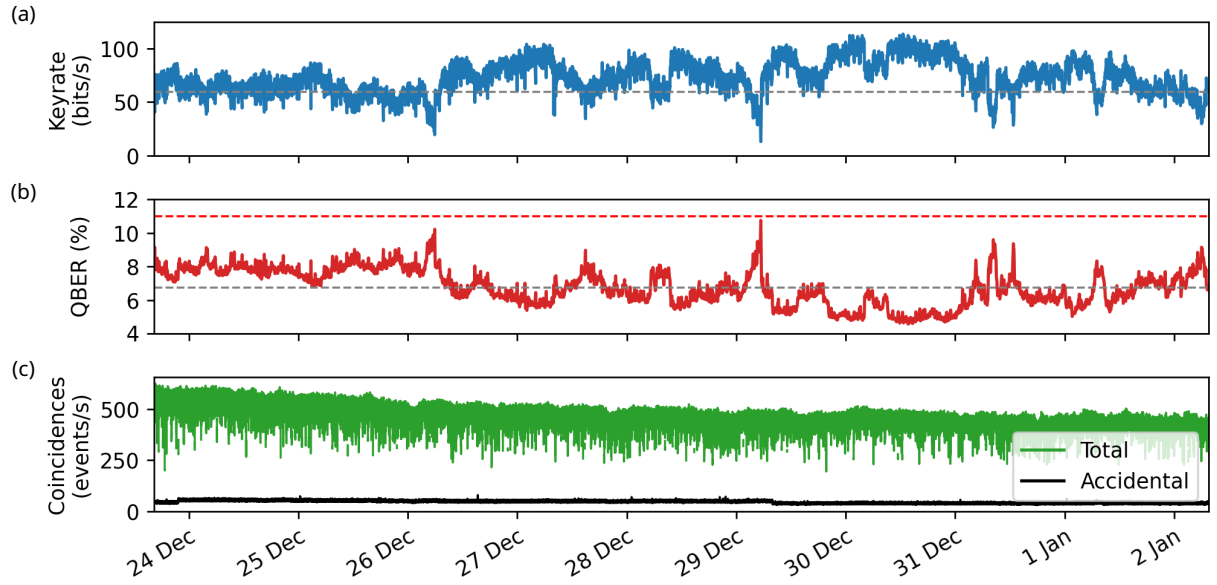

FIG. 2. **(a)** Measured secret keyrate during BBM92 QKD running over a consecutive period of 9 days. The average keyrate is 60 bits/s marked in dashed grey line. **(b)** Corresponding QBER during the same period. The average QBER is 6.7% marked in dashed grey, as well as the 11% QBER limit in dashed red. **(c)** Total and accidental coincidence rates, smoothed with a 10 s sliding window. The average total and accidental coincidence rates are 470 and 46 events/s, respectively. Fluctuations and breaks in the coincidence rates arise from suboptimal locking of the coincidence window.

III. CLASSICAL CO-PROPAGATION

An authenticated classical channel is required in QKD for error correction, privacy amplification, and key delivery. We establish this over the same deployed fiber by wavelength-division multiplexing (WDM) with the quantum channel.

Using the 1310 nm wavelength (O-band) for the quantum channel frees up the lower loss 1550 nm wavelength (C-band) for the classical channel. Since scattering in fiber scales with input laser power, a lower launch power required to sustain the classical connection reduces the overall noise coupled into the quantum channel.

In this configuration, optical noise coupled into Bob's detectors arise from three distinct mechanisms, specifically: (1) the 1550 nm carrier itself from both Alice's and Bob's transceivers; (2) spontaneous emission directly at 1310 nm from the transceivers (see Appendix D); (3) spontaneous Raman scattering in fiber from 1550 nm to 1310 nm as a result of optical phonon interactions. Four-wave mixing does not contribute significantly due to high chromatic dispersion within C-band as per G.652 specification [13, 14].

We quantify the magnitude of forward Raman scattering using the setup shown in Fig. 3(a). Light from a laser of 1550 nm wavelength and 2.5 GHz bandwidth is sent into either a 30 km SMF-28e fiber spool or an attenuation-equivalent channel, after sufficient filtering to remove spontaneous emission at 1310 nm. The output light is then filtered using the same chain of 1310 nm filters as with the main setup in Fig. 1(b), so any residual

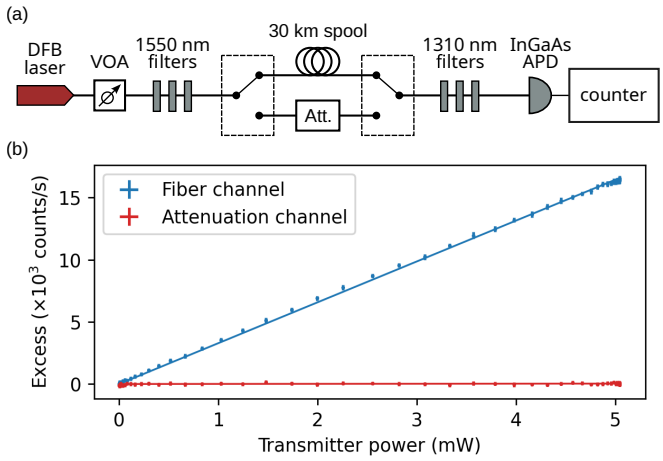

FIG. 3. **(a)** Schematic of setup to estimate anti-Stokes scattering in fiber from 1550 nm to 1310 nm. The fiber channel is swapped with an attenuation channel of equivalent transmission to measure leakage not attributed to fiber. DFB: distributed fiber Bragg; VOA: variable optical attenuator; Att.: attenuator. **(b)** Measurement of InGaAs APD count rates after dark count subtraction, for launch powers of up to 5 mW into the fiber. Lines represent linear fits, with slopes of $3.29(1) \times 10^3$ and 6.6(2.5) counts/s/mW for the fiber channel and attenuation-equivalent channel, respectively.

counts must be attributed to scattering in fiber.

A linear relationship in count rates with launch power can be seen in Fig. 3(b), which indicates the presence of spontaneous forward Raman scattering at a rate of

3.29(1) × 10^3 counts/s/mW. Leakage of 1550 nm light through the filters is insignificant. This also contrasts with four-wave mixing that scales quadratically as a two-photon input process [cite].

A sketch of the classical co-propagation architecture is shown in Fig. 1(b). The classical link is established using a pair of 1 GbE media converters (Transition Networks M/GE-PSW-SFP-01), each equipped with 1.25 G SFP 1550 nm transceivers (Starview International SV-SFP-ZXD6) that implement the 1000BASE-ZX physical layer interface rated for 60 km fiber length. Both the transmit and receive channels of the transceiver are combined with a circulator (CIR; Thorlabs 6015-3-APC) to create a full-duplex connection.

The 1000BASE-ZX interface of the transceivers uses the 8b/10b line code which is DC-balanced [31], resulting in a near-constant optical power during operation suitable for direct attenuation. Fine-tuning of the transmitter power with optical attenuators (VOA; Thorlabs V1550F) yields launch powers of 0.19(4) mW from Alice and 1.13(2) mW from Bob into the deployed fiber.

The remaining scattering noise is then filtered using a series of cascaded 1310 nm optical filters, as previously depicted in Fig. 1(b) and Fig. 3. Leakage of 1550 nm light into Bob's receiver is mostly rejected with the use of a free-space bandpass filter (Thorlabs FBH1310-12; > -50 dB attenuation within 1345–1800 nm) in combination with a pair of aspheric collimating lenses (Thorlabs C220TMD-C). Finally, a 100 GHz fiber bandpass filter (AFW Technologies BPF-1-1310-L-1-0) is used to filter out the remaining scattered light near 1310 nm. The overall transmission efficiency of this filter chain for the quantum channel is measured to be around -3.4 dB, with the fiber bandpass filter contributing -2.2 dB.

The asymmetry between Alice's and Bob's launch power is intentional: we observe less noise contributions from backward Raman scattering as opposed to forward Raman, so minimal attenuation on Bob's transmitter is required. On the other hand, Alice's transmitter is carefully attenuated to near the threshold launch power needed to sustain the optical connection. For a launch power of 0.19 mW, the corresponding noise contribution from forward spontaneous Raman scattering is estimated at 650 counts/s.

IV. ACTIVE POLARIZATION AND FREQUENCY COMPENSATION

Polarization control is necessary to align the polarization measurement basis on both nodes to obtain correlated outcomes. Due to polarization drifts in the fiber as a result of temperature variations and mechanical strain, polarization compensation needs to be actively performed to maintain basis alignment over time.

Polarization compensation is performed using an inline motorized "bat-ear" fiber polarization controller (MPC; Thorlabs MPC320) with fiber loops in a quarter-half-quarter waveplate (QWP1-HWP-QWP2) configuration, shown in Fig. 1(b). This configuration allows the controller to implement any arbitrary polarization rotation, one of which inverts the rotation induced by the optical fiber link for basis alignment.

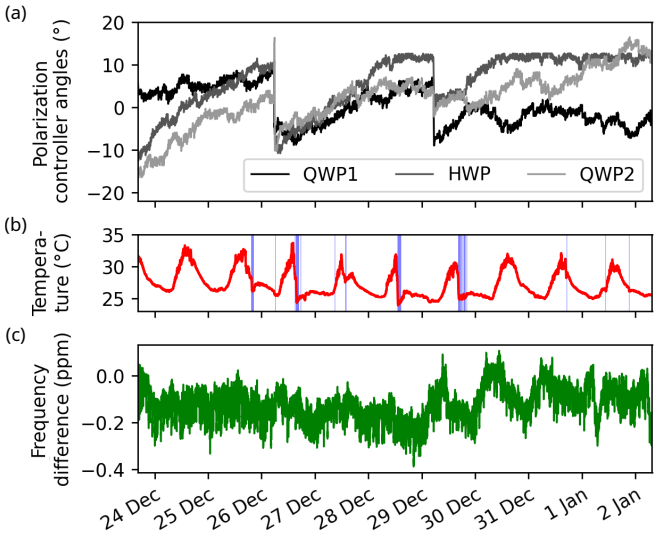

FIG. 4. **(a)** Rotation angles of a motorized fiber polarization controller containing a series of three fiber loops in a quarter-half-quarter waveplate (QWP1-HWP-QWP2) configuration. Angular variations centered for visual clarity. **(b)** Air temperatures (in red) and rainfall periods in 5-minute blocks (in blue) measured at the S50 Clementi automated weather station near the fiber deployment path. **(c)** Reconstructed frequency difference between Alice and Bob relative to the nominal clock reference frequency, obtained by tracking the drift in timing of the coincidence signal. ppm: parts-per-million ($\times 10^{-6}$).

Initial full polarization compensation is done via a Nelder-Mead optimization procedure [32] with early termination—which has been shown to be robust against noise [33]—and using estimated QBER as the minimization function [34]. During key generation, polarization measurement outcomes are no longer publicly announced. Active compensation is then performed by stochastic perturbations across different fiber loop rotation angles in the controller and monitoring the measured QBER after error correction instead (occurring once every 21 s on average). The perturbations are small to avoid large QBER changes that adversely affect key generation rates.

The drift in polarization controller angles is shown in Fig. 4(a), indicative of the polarization stability in the deployed fiber assuming ideal polarization compensation. We observe polarization stability on the order of several hours, consistent with previous QKD demonstrations on deployed fiber in Singapore [35]. No significant correlations are also found with air temperatures and rainfall patterns collected from a nearby weather station [36, 37] (seen in Fig. 4(b)) as the fibers are located underground and experience minimal external disturbance.

Overall drifts in QBER as seen in Fig. 2(b) are attributed to undercompensation of the active polarization compensation algorithm, i.e., conservative perturbation step sizes. This eventually interrupted key generation when the 10% QBER threshold was exceeded on 26 Dec to repeat the full polarization compensation algorithm, shown in Fig. 4(a) as sharp transitions across all three polarization controller loops.

The HWP fiber loop was also observed to hit rotation limits in the polarization controller from 28 Dec, leading to the second key generation interruption and full compensation. This issue however can be easily mitigated by introducing an additional polarization rotation such that the initial controller angles are far from the rotation limits.

Timing synchronization between the QKD nodes is also necessary to identify photon pair coincidences for key distillation. We rely on the timing correlations within the photon pairs themselves for timing synchronization to ∼ns accuracy [38], after an initial coarse timing synchronization to ∼ms accuracy using Network Time Protocol (NTP)[1]. This opens up the use of local clock references with poorer frequency stability on the order of 100 ns/s^2, without dependence on atomic clocks or Global Navigation Satellite System (GNSS) receivers.

The crystal oscillator circuit onboard the time tagger is directly used as the weak frequency reference. We perform active software-based frequency compensation (nominal resolution of 0.23 ppb) to correct for frequency drifts arising from temperature and voltage fluctuations [39, 40], effectively syntonizing both Alice's and Bob's time taggers to ∼ppb accuracy [40]. A 35 ms time constant on the exponential averaging filter is used in damping noise during coincidence signal tracking.

The instantaneous frequency difference between the time taggers is estimated by tracking drifts in the coincidence timing signal over a 5.36 s averaging window, shown in Fig. 4(c). The frequency differences show no strong correlation with temperature and rainfall patterns in Fig. 4(b) are observed as well, with the exception of cyclic 24 h drift patterns from 29 Dec onwards that may suggest human-related activity.

As previously mentioned in Section II, the coincidence window lock to the coincidence signal is frequently lost due to a misconfigured damping constant used in peak tracking, which causes occasional failure under fast drifts in frequency differences. This is further discussed in Appendix C. The frequency drifts were measured to be normally distributed with a standard deviation of 1.8 ppb/s, and we do still observe instantaneous frequency drifts of up to 7.6 ppb/s that were successfully compensated for (i.e., without loss of lock).

[1] While the QKD nodes currently rely on external NTP servers for the coarse synchronization, this dependency can be removed by having one node masquerade as a stratum-1 NTP server.

[2] Or equivalently, 100 parts-per-billion (ppb).

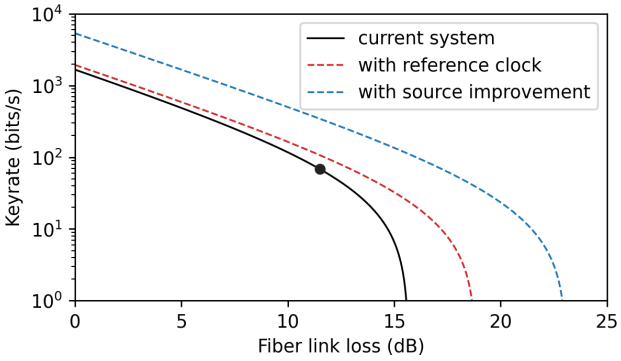

FIG. 5. Extrapolated keyrate against different fiber link losses, for the current system (solid black), with reference clock (dashed red), and additionally with improvements to the source efficiency (dashed blue).

V. DISCUSSION

We demonstrated O-band BBM92 QKD with a co-propagating classical channel in C-band over a single 29.5 km deployed telecommunication fiber. The system was run for 9 days with an average QBER of 6.7% and secret key rate of 60 bits/s. Active polarization compensation was implemented to keep QBER low. Frequency standards were not used in the setup, instead using a crystal oscillator circuit as a weak frequency reference and perfoming active frequency compensation.

The use of O-band wavelengths for the QKD quantum channel provides distinct advantages when deploying across metropolitan networks with telecommunication infrastructure. The predominant noise source is from spontaneous Raman scattering, and the low scattering amplitude from C-band into the anti-Stokes O-band allows the scattering noise to be filtered out easily with a simple cascaded optical filter chain. This is highly compatible with the use of commercial off-the-shelf long-reach optical transceivers operating in the C-band, which today support distances of up to around 160 km.

The current asymmetric wavelength configuration optimizes for overall system detection efficiency, allowing the use of more efficient Si APDs locally on Alice, or even superconducting nanowire detectors if field-deployability is not a concern. The intrinsically narrow bandwidth idler (120 GHz) allows for strong filtering to remove Raman scattering noise, whose center wavelength can be easily temperature-tuned in the SPDC process to match the filtering passband.

The current system performance over different fiber link losses can be extrapolated using the Devetak-Winter keyrate [41]

$$r = qc(1 - (1 + f)H_2(\epsilon)) \tag{2}$$

given a true coincidence rate c and QBER ϵ, assuming equal bit and phase errors. H_2 is the Shannon entropy,

basis choice efficiency $q = 1/2$ for BBM92, and an estimated error correction efficiency $f = 1.1$. The extrapolation is plotted in Fig. 5.

Our present keyrate of 60 bits/s is consistent with our previous estimate [17] after accounting for:

- Lower pump power (8.1 mW) and heralding efficiency (8%) used in the photon pair source,
- Additional coupling losses in both the 586 nm signal (-2.2 dB) and 1310 nm idler (-2 dB) optical paths,
- Lower InGaAs APD efficiency ($\approx 10\%$) in reducing the dark count levels,
- Losses from scattering noise filtering (-3.4 dB),
- Coincidence tracking inefficiencies due to suboptimal configuration.

The use of an external reference clock would resolve any suboptimal coincidence tracking, which can be conservatively modeled as a decrease in accidental coincidences (dashed red in Fig. 5). Additionally, improving our source of polarization-entangled photon pairs to increase the heralding efficiency to 20% and operate at the original 15 mW pump set-point would also yield roughly 4× increase in coincidence rates, for which we expect an improvement in keyrate to 345 bits/s (dashed blue in Fig. 5).

Replacing our source with atomic sources that have even narrower ∼GHz bandwidth [42]—together with narrower etalon filters on the quantum channel—could reduce the QBER even further, allowing the QKD system to scale more effectively across metropolitan-scale links.

I'm not particularly confident in the way I'm selling this work... suggestions to modify this concluding section are greatly appreciated!

ACKNOWLEDGMENTS

This research was supported by the Quantum Engineering Programme through Grant NRF2021-QEP2-04-P01, the Ministry of Education, and the National Research Foundation, Prime Minister's Office, Singapore.

We would like to acknowledge: National Quantum Safe Network, National Quantum Office for provisioning of the deployed fiber, and loaning the S-Fifteen Instruments QKD receiver node; NetLink for assistance with fiber patching to SUTD and Sembawang Central Office; S-Fifteen Instruments for the equipment support; FCCLab, FCP SUTD for hosting the initial QKD trial over 50 km deployed fiber.

[1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, Reviews of Modern Physics **81**, 1301 (2009).
[2] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, Theoretical Computer Science **560**, 7 (1984), arxiv:2003.06557.
[3] C. H. Bennett, G. Brassard, and N. D. Mermin, Quantum cryptography without Bell's theorem, Physical Review Letters **68**, 557 (1992).
[4] E. Waks, A. Zeevi, and Y. Yamamoto, Security of quantum key distribution with entangled photons against individual attacks, Physical Review A **65**, 052310 (2002).
[5] A. Treiber, A. Poppe, M. Hentschel, D. Ferrini, T. Lorünser, E. Querasser, T. Matyus, H. Hübel, and A. Zeilinger, Fully automated entanglement-based quantum cryptography system for telecom fiber networks, New Journal of Physics **11**, 045013 (2009), arxiv:0901.2725.
[6] S. Wengerowsky, S. K. Joshi, F. Steinlechner, J. R. Zichi, S. M. Dobrovolskiy, R. van der Molen, J. W. N. Los, V. Zwiller, M. A. M. Versteegh, A. Mura, D. Calonico, M. Inguscio, H. Hübel, L. Bo, T. Scheidl, A. Zeilinger, A. Xuereb, and R. Ursin, Entanglement distribution over a 96-km-long submarine optical fiber, Proceedings of the National Academy of Sciences **116**, 6684 (2019).
[7] S. P. Neumann, A. Buchner, L. Bulla, M. Bohmann, and R. Ursin, Continuous entanglement distribution over a transnational 248 km fiber link, Nature Communications **13**, 6134 (2022).
[8] M. J. Clark, O. Alia, S. Bahrani, G. T. Jasion, H. Sakr, P. Petropoulos, F. Poletti, G. T. Kanellos, J. Rarity, R. Nejabati, *et al.*, Coexistence of entanglement-based quantum channels with dwdm classical channels over hollow core fibre in a four node quantum communication network, npj Quantum Information **11**, 181 (2025).
[9] R. G. Smith, Optical Power Handling Capacity of Low Loss Optical Fibers as Determined by Stimulated Raman and Brillouin Scattering, Applied Optics **11**, 2489 (1972).
[10] J. AuYeung and A. Yariv, Spontaneous and stimulated Raman scattering in long low loss fibers, IEEE Journal of Quantum Electronics **14**, 347 (1978).
[11] Y.-R. Fan, Y. Luo, Z.-C. Zhang, Y.-B. Li, S. Liu, D. Wang, D.-C. Zhang, G.-W. Deng, Y. Wang, H.-Z. Song, *et al.*, Energy-time entanglement coexisting with fiber-optical communication in the telecom c band, Physical Review A **108**, L020601 (2023).
[12] A. Sanz, A. Atutxa, D. Franco, J. Astorga, and E. Jacob, Adapting communication networks to the quantum safe era: lessons learned in the coexistence of polarization-entangled qkd and classical channels, in *2025 International Conference on Quantum Communications, Networking, and Computing (QCNC)* (IEEE, 2025) pp. 110–116.
[13] International Telecommunication Union, Telecommunication Standardization Sector (ITU-T), *ITU-T G.652. Characteristics of a single-mode optical fibre and cable*, Tech. Rep. (Geneva: International Telecommunication Union, 2024).
[14] International Telecommunication Union, Telecommunication Standardization Sector (ITU-T), *ITU-T G.657. Characteristics of a bending-loss insensitive single-mode*

optical fibre and cable, Tech. Rep. (Geneva: International Telecommunication Union, 2024).
[15] International Telecommunication Union, Telecommunication Standardization Sector (ITU-T), *ITU-T G.698.4. Multichannel bi-direction DWDM applications with port agnostic single-channel optical interfaces*, Tech. Rep. (Geneva: International Telecommunication Union, 2025).
[16] S. P. Singh, R. Gangwar, and N. Singh, NONLINEAR SCATTERING EFFECTS IN OPTICAL FIBERS, Progress In Electromagnetics Research **74**, 379 (2007).
[17] L. Shen, C. H. Chow, J. Y. X. Peh, X. J. Yeo, P. K. Tan, and C. Kurtsiefer, Distributing Polarization Entangled Photon Pairs with High Rate over Long Distance through Standard Telecommunication Fiber, Physical Review Applied **18**, 044075 (2022), arxiv:2204.10571 [quant-ph].
[18] *Corning® SMF-28® Ultra Optical Fiber*, Tech. Rep. PI1424 (Corning Inc., 2014).
[19] S. P. Neumann, T. Scheidl, M. Selimovic, M. Pivoluska, B. Liu, M. Bohmann, and R. Ursin, Model for optimizing quantum key distribution with continuous-wave pumped entangled-photon sources, Physical Review A **104**, 022406 (2021).
[20] C. Kurtsiefer, M. Seidler, and S. A. Aljunied, qcrypto, `https://github.com/s-fifteen-instruments/qcrypto` (2023).
[21] M. Seidler, S. A. Aljunied, and J. Y. X. Peh, Qkdserver, `https://github.com/s-fifteen-instruments/QKDServer` (2025).
[22] G. Brassard and L. Salvail, Secret-Key Reconciliation by Public Discussion, in *Advances in Cryptology — EUROCRYPT '93*, Vol. 765, edited by T. Helleseth (Springer Berlin Heidelberg, Berlin, Heidelberg, 1994) pp. 410–423.
[23] T. Sugimoto and K. Yamazaki, A Study on Secret Key Reconciliation Protocol, IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences **E83-A**, 1987 (2000).
[24] C. Proctor, S. A. Aljunied, and J. Y. X. Peh, guardian, `https://github.com/s-fifteen-instruments/guardian` (2023).
[25] European Telecommunications Standards Institute (ETSI), Industry Specification Groups (ISG), ETSI GS QKD 014. Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API, Group Specification v1.1.1 (2019).
[26] Bundesamt für Sicherheit in der Informationstechnik (BSI), Implementation Attacks against QKD Systems (2023).
[27] Y. Shi, J. Z. J. Lim, H. S. Poh, P. K. Tan, P. A. Tan, A. Ling, and C. Kurtsiefer, Breakdown flash at telecom wavelengths in InGaAs avalanche photodiodes, Optics Express **25**, 30388 (2017).
[28] H.-W. Li, S. Wang, J.-Z. Huang, W. Chen, Z.-Q. Yin, F.-Y. Li, Z. Zhou, D. Liu, Y. Zhang, G.-C. Guo, W.-S. Bao, and Z.-F. Han, Attacking a practical quantum-key-distribution system with wavelength-dependent beam-splitter and multiwavelength sources, Physical Review A **84**, 062308 (2011).
[29] L. Shen and C. Kurtsiefer, Countering detector manipulation attacks in quantum communication through detector self-testing, APL Photonics **10**, 016106 (2025).
[30] A. Lamas-Linares and C. Kurtsiefer, Breaking a quantum key distribution system through a timing side channel, Optics Express **15**, 9388 (2007), arxiv:0704.3297.
[31] 802.3 WG - Ethernet Working Group, *IEEE 802.3-2022. IEEE Standard for Ethernet*, Tech. Rep. (IEEE Standards Association, 2022).
[32] J. A. Nelder and R. Mead, A simplex method for function minimization, The Computer Journal **7**, 308 (1965), https://academic.oup.com/comjnl/article-pdf/7/4/308/1013182/7-4-308.pdf.
[33] E. F. Rocha, E. M. Neves, E. F. Wanner, R. H. C. Takahashi, and A. R. da Cruz, Nelder-Mead Based Algorithms for Noisy Functions, in *Optimization, Learning Algorithms and Applications*, edited by A. I. Pereira, F. P. Fernandes, J. P. Coelho, J. P. Teixeira, J. Lima, M. F. Pacheco, R. P. Lopes, and S. T. Álvarez (Springer Nature Switzerland, Cham, 2024) pp. 272–286.
[34] M. F. Ramos, N. A. Silva, N. J. Muga, and A. N. Pinto, Reversal operator to compensate polarization random drifts in quantum communications, Optics Express **28**, 5035 (2020).
[35] Y. Shi, S. Moe Thar, H. S. Poh, J. A. Grieve, C. Kurtsiefer, and A. Ling, Stable polarization entanglement based quantum key distribution over a deployed metropolitan fiber, Applied Physics Letters **117**, 124002 (2020).
[36] National Environment Agency, Air Temperature across Singapore, `https://data.gov.sg/datasets/d_66b77726bbae1b33f218db60ff5861f0/view` (2025).
[37] National Environment Agency, Rainfall across Singapore, `https://data.gov.sg/datasets/d_6580738cdd7db79374ed3152159fbd69/view` (2025).
[38] C. Ho, A. Lamas-Linares, and C. Kurtsiefer, Clock synchronization by remote detection of correlated photon pairs, New Journal of Physics **11**, 045011 (2009).
[39] C. Spiess, S. Töpfer, S. Sharma, A. Kržič, M. Cabrejo-Ponce, U. Chandrashekara, N. L. Döll, D. Rieländer, and F. Steinlechner, Clock Synchronization with Correlated Photons, Physical Review Applied **19**, 054082 (2023).
[40] J. Y. X. Peh, D. M. Z. Koh, Z. Xu, X. J. Yeo, P. K. Tan, and C. Kurtsiefer, Clock Synchronization with Weakly Correlated Photons (2026), arXiv:2602.18147 [quant-ph].
[41] I. Devetak and A. Winter, Distillation of secret key and entanglement from quantum states, Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences **461**, 207 (2005), arXiv:quant-ph/0306078.
[42] A. N. Craddock, A. Lazenby, G. B. Portmann, R. Sekelsky, M. Flament, and M. Namazi, Automated Distribution of Polarization-Entangled Photons Using Deployed New York City Fibers, PRX Quantum **5**, 030330 (2024).

Appendix A: Full setup description

We perform the BBM92 QKD protocol between Alice and Bob in an asymmetric configuration, where the polarization-entanglement photon pair source is housed locally at Alice. This is isomorphic to BB84 with source replacement, without the dependence on Alice for active polarization choice [cite].

Highly wavelength-asymmetric photon pairs are generated by Type-0 spontaneous parametric downconversion (SPDC) in a periodically-poled potassium titanyl phos-

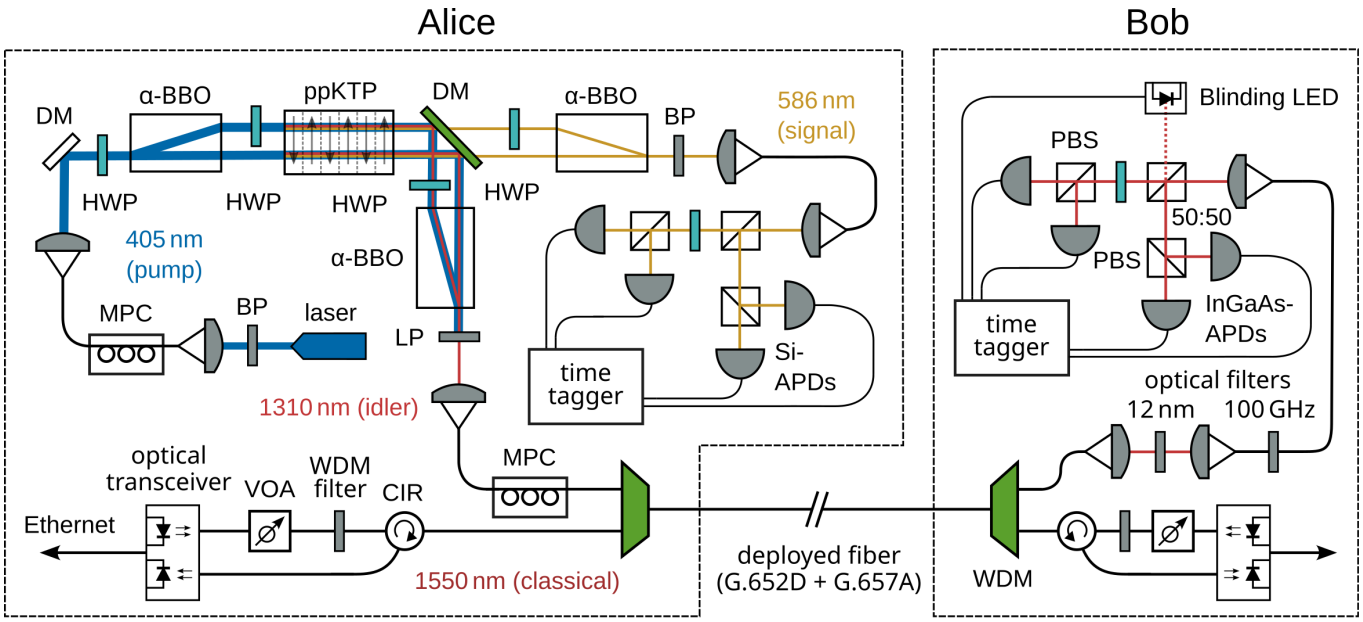

FIG. 6. Full schematic of the experimental setup. Schematic of the QKD setup with the non-degenerate entangled photon pair source scheme per construction in [17]. 405 nm pump light is split into two paths and undergoes Type-0 SPDC in a ppKTP crystal, generating photon pairs of non-degenerate wavelengths at 586 nm (signal) and 1310 nm (idler). A pair of α-BBO crystals separately recombine the signal and idler to create the polarization-entangled state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle)$. DM: Dichroic mirror; LP: Longpass filter; BP: Bandpass filter. Each photon is sent through a passive beamsplitter array consisting of 50:50 and polarizing beamsplitters (PBS) for measurement along the rectilinear (HV) and diagonal (DA) polarization bases. Detection events from the individual APDs are registered on the corresponding time taggers. A classical authenticated communication channel is used for photon pair coincidence tracking and frequency compensation.

phate (ppKTP) crystal, following the scheme

$$405\,\text{nm} \rightarrow 586\,\text{nm} + 1310\,\text{nm}.$$

This is illustrated in Fig. 6. The linear displacement interformetric configuration of the pair source generates the $|\Phi^+\rangle$ state, by spatially overlapping two downconversion beams from the same nonlinear crystal to yield the $(|HH\rangle + e^{i\theta}|VV\rangle)/\sqrt{2}$ state, with phase compensation achieved by tilts in the half-wave plate (HWP). The signal 586 nm and idler 1310 nm photons are wavelength-separated with a dichroic mirror, the former measured locally by Alice and the latter remotely by Bob. Figure 6 illustrates the aforementioned pair source setup.

We measured 150,000 photon pairs/s using a pair of APDs, using an input pump power of 8.1 mW. The high asymmetry in downconversion wavelengths results in an intrinsically narrow bandwidth of 0.7 nm (120 GHz) for the 1310 nm idler light, without the use of additional spectral filtering optics. Useful to either retake measurements for the 1310 nm output to show the 120 GHz bandwidth, or just quote [17].

Each photon of the pair is projected into either the rectilinear (HV) or diagonal (DA) polarization bases using a passive beamsplitter array, and detection events are timestamped on free-running time taggers. A motorised polarization controller (MPC) performs active polarization compensation for rotations in the fiber.

Alice and Bob each perform polarization measurements along the rectilinear (HV) and diagonal (DA) bases to obtain pair correlations used for secret key extraction. A free-space non-polarizing 50:50 beamsplitter functions as the random choice of measurement bases for the received light, and the polarizing beam splitters perform the measurement in the polarization measurement unit shown in Fig. 6. Detection of 586 nm and 1310 nm photons is made with Si APDs (Excelitas Technologies SPCM-AQRH) and InGaAs APDs (S-Fifteen Instruments IRSPD1), respectively.

An optical link (1000BASE-X) is established at 1 Gbps speeds. This bandwidth supports data transfer requirements in QKD. The estimated average network bandwidth used by the key generation process itself is XXX Mbit/s. This total comprises XXX Mbit/s for coincidence tracking, XXX Mbit/s for error correction, and a TCP/IP/Ethernet layer overhead of XXX Mbit/s.

The cause of the bimodality in accidental count rates is unknown, but is correlated to jumps in detection count rates at Bob. This is postulated to originate from increased dark counts due to ambient light at the Bob deployment site.

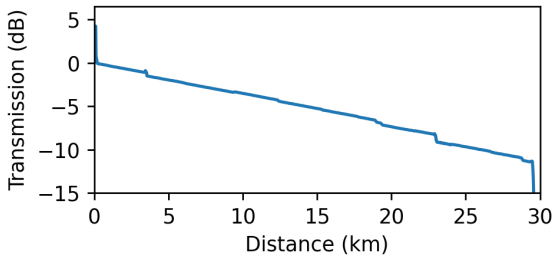

FIG. 7. Optical time-domain reflectometry measurement of the deployed fiber link between CQT and NetLink Sembawang Central Office, with a total distance of 29.5 km and cumulative loss of −11.5 dB for light at 1310 nm wavelength. Reflection spikes and dips are indicative of fiber patching points.

Appendix B: Deployed fiber characterization

The deployed fiber is a mix of G.652D- and G.657A-compatible optical fibers designed for transmission at 1550 nm and a zero-dispersion wavelength of 1310 nm. The stronger chromatic dispersion at 1550 nm is intended to minimize scattering from four-wave mixing processes that scale quadratically with launch power [13, 14]. This makes the C-band more appropriate for the classical channel with stronger input light as compared to O-band.

The total fiber attenuation at 1310 nm is measured to be −11.5 dB via optical time-domain reflectometry (Anritsu MT9083) as shown in Fig. 7, of which −10.0 dB is attributed to the fiber itself and the remaining −1.5 dB to splicing and mating losses. The observed attenuation slope of −0.34 dB/km in the fiber is higher than that of typical SMF-28e+ fiber spools rated at most −0.3 dB/km [18]. Perform and add measurements for 1550 nm classical channel in the plot as well.

Appendix C: Clock synchronization stability

Due to suboptimal coincidence tracking, the key generation experiences intermittent interruptions. This is visible in Fig. 8, with the distribution of interrupt durations shown in Fig. 9. This likely caused the coincidence peak signal to occasionally drift into the accidental window, resulting in an elevated accidental count rate.

Whenever costream drops (on average every 5 mins), some process is killed that results in the time tagger cooling down. Restarting the time tagger causes it to warm up again with a time constant of roughly 12 mins. After excluding the interruption periods, the actual average running key generation rate is 73(15) bits/s.

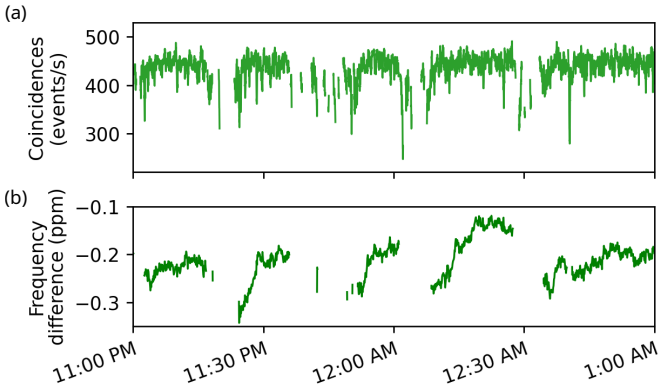

FIG. 8. **(a)** A 2-hour snapshot of total measured coincidences, centered at 29 Dec midnight, clearly showing coincidence tracking lost intermittently. **(b)** Corresponding plot of reconstructed frequencies. Positive frequency drift can be seen after each interrupted coincidences, due to temperature ramping up.

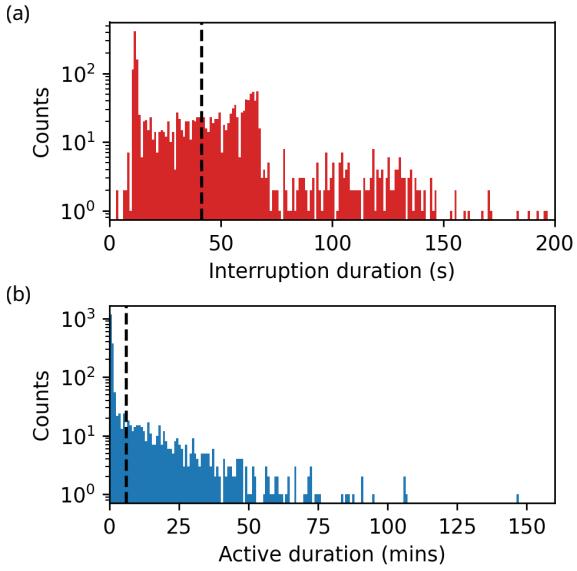

FIG. 9. **(a)** Histogram of durations for each instance of drop-off in coincidence tracking. The average interruption duration is 41 s marked in dashed grey, with a mode of 11 s. **(b)** Histogram of durations between coincidence drop-offs, i.e., key generation periods. The average uninterrupted key generation duration is 6 mins marked in dashed grey, with an observed maximum of 147 mins.

Appendix D: Transceiver optical spectrum

The spectrum of the C-band transceiver is shown in Fig. 10, measured by tapping one of the dual-simplex channels with a 50:50 fiber beamsplitter. The maximum power of the transceiver is -0.7 dBm. It has a -30 dB bandwidth of 0.4 nm and sidebands at -43.2 dB.

Significant light leakage is present in the laser, measuring at -83 dBm/nm at the 1310 nm wavelength. This is

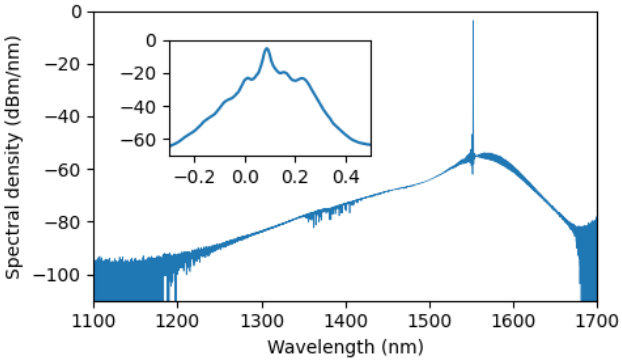

FIG. 10. Spectral density of the 1550 nm transceiver measured by using an optical spectrum analyzer (Yokogawa AQ6370E) at 0.1 nm resolution, with the inset showing the spectrum peak offset by 1550.2 nm.

easily suppressed by XXX orders of magnitude using an inline WDM, such that no excess O-band emission from the laser contributes to the noise counts.