

ARTICLE

Open Access

Frequency-bin-encoded entanglement-based quantum key distribution in a reconfigurable frequency-multiplexed network

Anahita Khodadad Kashi^{1,2} and Michael Kues^{1,2}✉

Abstract

Large-scale quantum networks require dynamic and resource-efficient solutions to reduce system complexity with maintained security and performance to support growing number of users over large distances. Current encoding schemes including time-bin, polarization, and orbital angular momentum, suffer from the lack of reconfigurability and thus scalability issues. Here, we demonstrate the first-time implementation of frequency-bin-encoded entanglement-based quantum key distribution and a reconfigurable distribution of entanglement using frequency-bin encoding. Specifically, we demonstrate a novel scalable frequency-bin basis analyzer module that allows for a passive random basis selection as a crucial step in quantum protocols, and importantly equips each user with a single detector rather than four detectors. This minimizes massively the resource overhead, reduces the dark count contribution, vulnerability to detector side-channel attacks, and the detector imbalance, hence providing an enhanced security. Our approach offers an adaptive frequency-multiplexing capability to increase the number of channels without hardware overhead, enabling increased secret key rate and reconfigurable multi-user operations. In perspective, our approach enables dynamic resource-minimized quantum key distribution among multiple users across diverse network topologies, and facilitates scalability to large-scale quantum networks.

Introduction

The advent of the quantum internet will introduce a new era of communications, outperforming the classical internet¹. Central to this new technology is the distributed entanglement-based quantum information processing, which, for example, enables via quantum key distribution (QKD) protocols the establishment of cryptographic keys between distant users^{2–7}. Entanglement-based quantum key distribution (EBQKD) protocols offer – compared to prepare-and-measure schemes such as BB84 – an enhanced security against coherent attacks and a greater tolerance to channel loss^{8–11}.

Scalability is crucial for large-scale QKD networks, ensuring efficient accommodation of a growing number of users over large distances while upholding security and performance standards^{12,13}. However, issues arising from

distance limitations, degraded security in face of advanced attacks, resource overhead, and growing hardware complexity/cost emerging from static implementations, hinder a scalable realization of EBQKD^{14,15}. In particular, to meet the growing network demands and to accommodate multi-user operations, optimization and stabilization techniques are required to be adapted for polarization^{16–19}, time-bin^{20–23}, and orbital angular momentum^{24–29} encoding schemes.

The photonic frequency degree-of-freedom has the potential to address the scalability challenge of QKD systems. The inherent multimodal nature of frequency allows for an increased data throughput through parallel transmission of signals at different frequencies. High-dimensional key encryption per photon serves to an intrinsically increased robustness to noise, hence a preserved security^{30–34}. Importantly, in contrast to polarization and time-bin encoding, frequency-encoded signals are less susceptible to decoherence induced by environmental factors such as temperature variations

Correspondence: Michael Kues (Michael.kues@iop.uni-hannover.de)

¹Institute of Photonics, Leibniz University Hannover, 30167 Hannover, Germany

²Cluster of Excellence PhoenixD (Photonics, Optics, Engineering – Innovation Across Disciplines), Leibniz University Hannover, 30167 Hannover, Germany

© The Author(s) 2025



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



and mechanical vibrations. This characteristic supports the development of scalable QKD networks over extended geographical areas without significant loss of quality and coherence. Additionally, the photonic frequency degree-of-freedom could play an interfacing role in hybrid platforms, thanks to the frequency's convertible nature between different energy-based physical systems^{35–37}.

The frequency degree-of-freedom paired with time-bin encoding has been exploited in some QKD protocols, such as prepare-and-measure schemes, measurement-device-independent QKD, twin-field QKD (TFQKD), and has been suggested for the development of quantum network architectures^{38–47}. In these implementations, the frequency degree was deployed as part of a hybrid encoding scheme requiring non-scalable bulky interferometric setups with passive or active phase stabilization requirements.

Here, we demonstrate the first-time frequency-bin-encoded implementation of the entanglement-based BBM92 QKD protocol. Additionally, we demonstrate flexible entanglement distribution over long fiber links. By utilizing the frequency-bin encoding approach, we were enabled to develop a novel frequency-bin-basis analyzer module whose employment considerably reduces system complexity and hardware overhead, hence addressing the scalability challenge in large-scale quantum networks. The functionality of this module is based on the deployment of off-the-shelf telecommunication components such as a programmable filter (PF), a frequency mixer (FM) based on electro-optic phase modulation (EOPM), a frequency-to-time mapping (FTM) unit, and a superconducting nanowire single-photon detector (SNSPD) of high timing resolution. With a fine-tuned frequency mixing, our scheme allows for performing passive frequency-bin projection measurements in two mutually unbiased bases (MUB), realizing a random basis choice as a fundamental security condition in QKD protocols^{9,10}. Direct frequency-to-time mapping provides each user with simultaneous access to the projection measurement results corresponding to four basis states, using only a single SNSPD. Via an adaptive frequency de/multiplexing functionality we demonstrate the multiplexing of multiple frequency channels for QKD between two users without adding to the hardware overhead. This facilitates enhanced key rates in a single point-to-point QKD with a maintained security level, and enables the scalable expansion of the network to accommodate additional users. Remarkably, we demonstrate that projection states corresponding to multiple quantum channels become as well detectable using the same single detector by each user, hence a maintained system complexity with a growing number of users.

Results

Concept and experimental setup of frequency-bin EBQKD

The experimental setup for the frequency-bin-encoded implementation of the BBM92 EBQKD protocol is illustrated in Fig. 1a. A periodically poled lithium niobate (PPLN) waveguide was pumped by a pulsed laser with a repetition rate of 50 MHz and a bandwidth spectrally filtered (via a 4f-configuration optical setup; see Methods and materials) to 200 GHz full-width at half-maximum. The pump photons underwent type-0 spontaneous parametric down conversion (SPDC) process within the PPLN waveguide and split into highly correlated photon pairs distributed symmetrically around the SPDC degeneracy frequency $f_d^{\text{SPDC}} = 193.46$ THz. The photon-pair source was followed by a central programmable wavelength switch (PWS) separating the propagation path of the higher- (signal) and lower- (idler) energy photons to two users, named Alice and Bob, respectively (see Methods and materials).

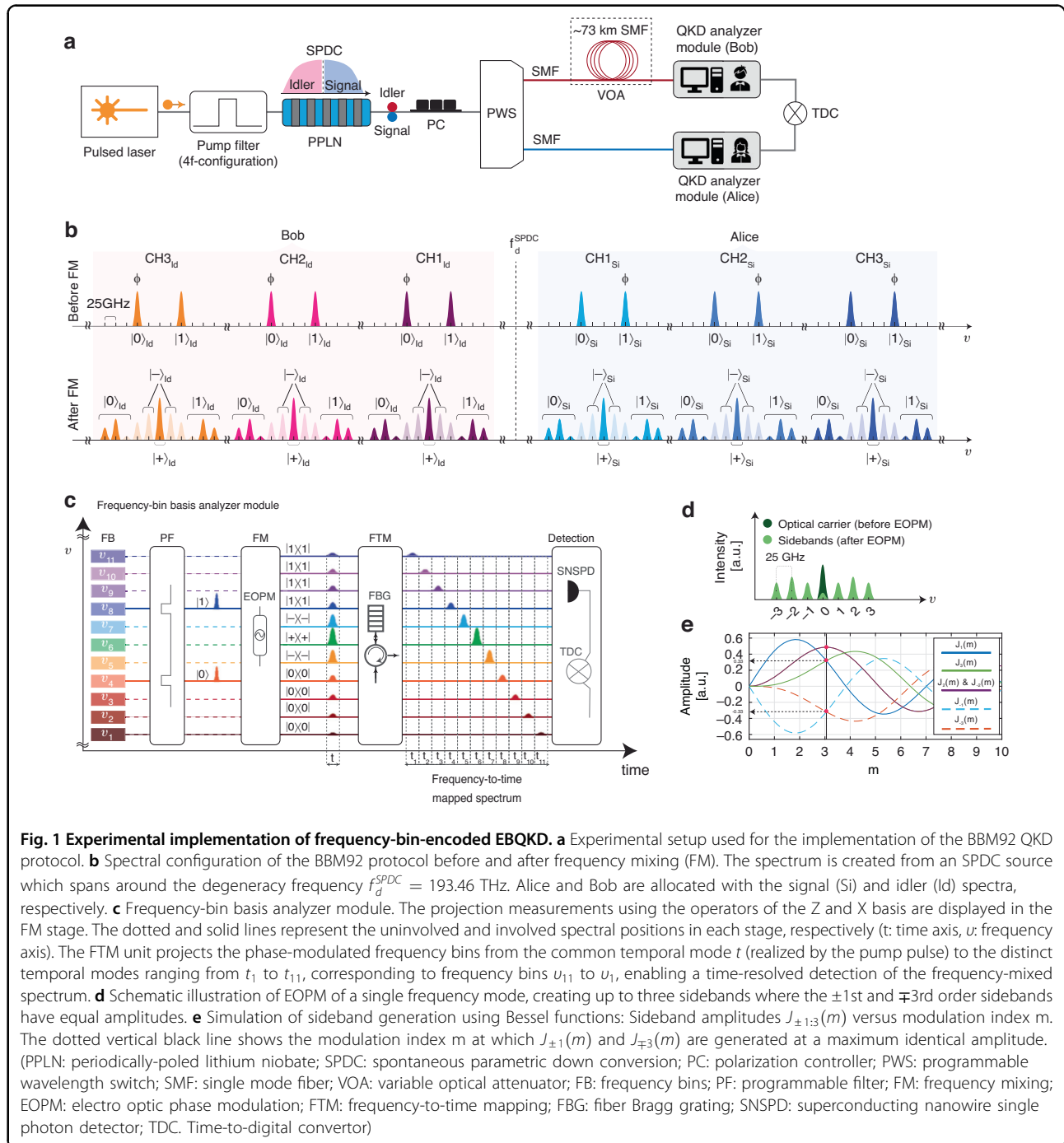
The PWS served to define the spectral channels on the signal and idler spectrum (CH_{si} and CH_{id} ; see Fig. 1b; before FM). Each channel was composed of two frequency bins, labeled $|0\rangle$ and $|1\rangle$. The frequency bins are 20 GHz wide and separated by 100 GHz. The symmetric signal and idler pairs were energy-time correlated with their exact spectral positions determined through correlation measurements. The state amplitude of $|0\rangle$ and $|1\rangle$ were prepared equal to provide a maximally frequency-bin entangled state. To demonstrate scalability, we multiplexed three channels, namely CH1, CH2, and CH3, into the single-mode fiber (SMF) of each user. The channels were separated by 300 GHz on the signal and idler spectrum, respectively. Given the specific definition of the frequency bins in each channel shown in Fig. 1b, the frequency-bin entangled states can be defined as follows:

$$\begin{aligned} |\Psi\rangle^{\text{CH1}} &= 1/\sqrt{2} \left(|0; t\rangle_{\text{si}}^{\text{CH1}} |1; t\rangle_{\text{id}}^{\text{CH1}} + |1; t\rangle_{\text{si}}^{\text{CH1}} |0; t\rangle_{\text{id}}^{\text{CH1}} \right), \\ |\Psi\rangle^{\text{CH2}} &= 1/\sqrt{2} \left(|0; t\rangle_{\text{si}}^{\text{CH2}} |1; t\rangle_{\text{id}}^{\text{CH2}} + |1; t\rangle_{\text{si}}^{\text{CH2}} |0; t\rangle_{\text{id}}^{\text{CH2}} \right), \\ |\Psi\rangle^{\text{CH3}} &= 1/\sqrt{2} \left(|0; t\rangle_{\text{si}}^{\text{CH3}} |1; t\rangle_{\text{id}}^{\text{CH3}} + |1; t\rangle_{\text{si}}^{\text{CH3}} |0; t\rangle_{\text{id}}^{\text{CH3}} \right) \end{aligned} \quad (1)$$

where t denotes the common temporal mode (defined by the excitation pulse) for the signal and idler frequency bins for all quantum channels. A variable optical attenuator (VOA) was employed to exert incremental optical attenuation corresponding to the loss experienced at different lengths of a SMF placed in Bob's arm (see Methods and materials), hence creating an asymmetric optical fiber link between the users.

To implement the BBM92 QKD protocol, we developed a novel frequency-bin basis analyzer module (see Fig. 1c), with one of which each user was equipped. This module





was composed of a programmable filter (PF), a frequency mixing (FM) unit, a frequency-to-time mapping (FTM) component, a single SNSPD followed by a time-to-digital converter (TDC).

In general, the BBM92 protocol requires the users to individually perform projection measurements on the received photons by randomly selecting among the two MUB^{9,48}, here $Z = \{|0\rangle, |1\rangle\}$ and $X = \{|+\rangle, |-\rangle\}$ (where $|+\rangle = 1/\sqrt{2}(|0\rangle + |1\rangle)$ and $|-\rangle = 1/\sqrt{2}(|0\rangle - |1\rangle)$). In

our approach, the random choice between the Z and X basis and the corresponding projection measurements using the operators $\{|0\rangle\langle 0|, |1\rangle\langle 1|, |+\rangle\langle +|, |-\rangle\langle -|\}$ were realized in the frequency mixing stage.

For simplicity, we explain the operation of the basis analyzer for one given channel. In this module, the PF is configured for each user to let pass the photons of the specified frequency bins with an equal intensity. For clarity, we identify the spectral computational space of a

given channel on the signal/idler spectrum with $v_1, \dots, v_{11}$ with the input frequency bins $|0\rangle$ and $|1\rangle$ residing in v_4 and v_8 , respectively, (see Fig. 1c).

Electro-optic phase modulation leads to the generation of sidebands around the original optical carrier at integer multiples of the modulation frequency, here $\Omega = 25\text{GHz}$. In our scenario, the modulation voltage amplitude was fine-tuned (see Methods and materials) to enable the generation of maximum three positive and negative order sidebands (see Fig. 1d). This configuration led to the superposition of $|0\rangle$ and $|1\rangle$ on the spectral positions v_5, v_6 and v_7 .

To experimentally realize the projection measurement onto the $|+\rangle$ and $|-\rangle$ states, in these spectral positions, a specific amplitude and phase relationship between the sidebands were required (see Fig. 1b; after FM). The projection onto $|+\rangle$ was realized in the spectral position v_6 , where the positive and negative second-order sidebands superimpose with an intrinsic equal amplitude and a relative phase difference of 0 (even-order sidebands have an intrinsic phase factor of 0). Projections on $|-\rangle$ were realized in v_5 and v_7 , where the first- and third-order sidebands superimpose with a relative phase difference of π (negative odd-order sidebands have an intrinsic phase factor of π). In this realization, it was required to have the first and third-order sidebands $J_{1,3}(m)$ generated at equal amplitudes. By simulating the sideband generation in electro-optic phase modulation using the Bessel functions (see Fig. 1e), we extracted an optimal modulation RF voltage amplitude (see Methods and materials), where this condition is met, i.e., for a specific modulation index m the following equality $|J_{\pm 1}(m)| = |J_{\mp 3}(m)|$ is valid. Remarkably, at this modulation index almost maximal amplitude for the second-order sidebands were as well obtained, such that efficient projections onto $|+\rangle$ and $|-\rangle$ were simultaneously feasible. It was verified that the sum of the superposition of first- and third-order sideband amplitudes in v_5 and v_7 were with good approximation equal to the superposition of sideband amplitudes in v_6 , realizing equal probability for projections on $|+\rangle$ or $|-\rangle$.

Furthermore, an extent of sideband generation limited to three, renders the spectral region v_1 to v_4 and v_8 to v_{11} devoid of any superpositions. These spectral regions thus represent the projection measurements in the Z basis, realized via the following operators $|0\rangle\langle 0|$ and $|1\rangle\langle 1|$, respectively (see Fig. 1b; after FM). Due to the symmetry in the sideband generation, the probability amplitudes for projection onto $|0\rangle$ and $|1\rangle$ states were equal.

Importantly, the sum of the probability amplitudes of the states in Z basis yield nearly identical value to that of the X basis, ensuring that projection measurements in the two MUB occur randomly. In our approach, phase modulation thus projects a single-photon randomly to either the spectral region corresponding to the X basis or

to that of the Z basis, hence realizing a stable, passive and random implementation of the projection measurements. The explained concept can be extended to additional frequency channels, hence enabling scalability.

To measure the frequency-mixed single-photon spectrum directly with a single SNSPD (labeled D1 and D2 for Bob and Alice, respectively), the frequency-bins $v_1, \dots, v_{11}$ were resolved in time by implementing a FTM technique⁴⁹ using a fiber Bragg grating (FBG) as a dispersive component.

In this experiment, the timing reference between the users is realized using the trigger signal from the common pulsed laser source, captured via the TDC module. By exploiting the pulsed laser signal as a time reference in post processing, the time-resolved spectral components of the single photons became accessible using only a single detector. Given the fine timing jitter of the SNSPD (~ 25 ps), the dispersion in the FBG was precisely selected so as to enable time-resolved detection of adjacent 25-GHz frequency bins. Specifically, the FBG possessed by Alice and Bob featured negative and positive second-order dispersion of $\pm 0.0568 \text{ ps/nm}^2/\text{km}$, respectively. It is important to note that due to the use of the same pulsed laser as the source of the reference signal for both users and in light of similar timing jitters of both detectors, the accuracy for determining the temporal detection windows associated with the projection basis states for Alice and Bob were identical.

By this detection technique, each user is granted simultaneous access to the projection measurement results in all four basis states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ using only a single detector, hence a considerably reduced resource overhead compared to conventional schemes requiring four detectors^{4,48}.

In our approach, the basis analyzer is capable of multiplexing several frequency channels without suffering from hardware overhead. A determining factor for the number of frequency channels that could be resolved is the repetition rate of the pulsed laser. In our case, the 300 GHz spectral distance between the adjacent frequency channels, and the $T = 20 \text{ ns}$ pulse period combined with the dispersion of the FBG, enabled us to demultiplex three frequency channels CH1, CH2, CH3 for each user (see Fig. 2).

Frequency-bin-encoded BBM92 QKD protocol

With our novel frequency-bin basis analyzer, we implemented a frequency-bin-encoded BBM92 EBQKD protocol (see Methods and materials). The raw key bits in the Z and X basis were obtained from the coincidence events between D1 and D2 and by identifying the spectral regions associated with the following projections $|00\rangle, |11\rangle, |01\rangle, |10\rangle, |++\rangle, |--\rangle, |+-\rangle, |-+\rangle$. The raw coincidence counts in the Z and X basis, $CC_{Z(X)}^{\text{raw}}$, consist



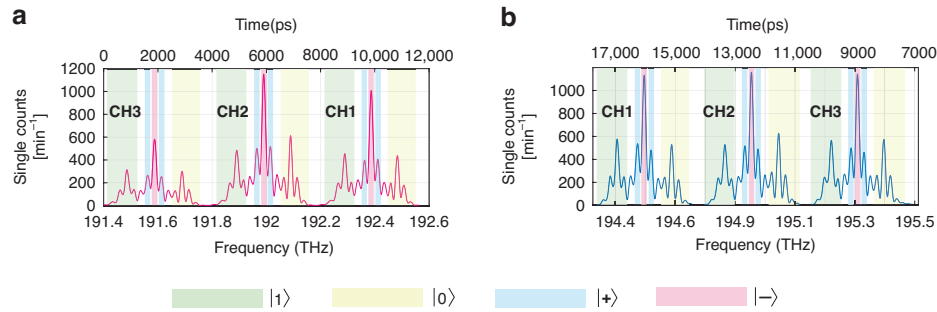


Fig. 2 Frequency-to-time mapped spectral profiles of the frequency channels CH1, CH2, and CH3. Frequency-to-time mapped spectral profiles detected by the detectors (a) D1 (owned by Bob) and (b) D2 (owned by Alice). The colored green, yellow, blue and red spectral regions correspond to the projections onto the states $|1\rangle$, $|0\rangle$, $|-\rangle$, and $|+\rangle$, respectively

Table 1 Performance metrics of the frequency-bin-encoded BBM92 QKD protocol at different optical attenuations corresponding to different lengths of the optical fiber link, prior to error reconciliation and privacy amplification

	Optical attenuation (dB) [corresponding fiber length]					
	0 dB [0 km]	1.64 dB [7 km]	3.71 dB [17 km]	5.73 dB [26 km]	7.98 dB [37 km]	15.6 dB [73 km]
CH1						
RCC	25431	18952	12248	7334	4033	652
ACC	1034	759	513	323	158	29
RKR	16.30 ± 0.07	12.14 ± 0.08	7.85 ± 0.07	4.70 ± 0.05	2.58 ± 0.04	0.41 ± 0.01
QBER	$(4.12 \pm 0.18)\%$	$(4.05 \pm 0.15)\%$	$(4.19 \pm 0.19)\%$	$(4.40 \pm 0.25)\%$	$(3.92 \pm 0.32)\%$	$(4.45 \pm 0.85)\%$
CH2						
RCC	34603	24571	14464	9513	5504	922
ACC	1797	1198	647	473	273	60
RKR	22.18 ± 0.17	15.75 ± 0.09	9.27 ± 0.07	6.09 ± 0.05	3.52 ± 0.04	0.59 ± 0.01
QBER	$(5.20 \pm 0.17)\%$	$(4.88 \pm 0.14)\%$	$(4.47 \pm 0.18)\%$	$(4.97 \pm 0.23)\%$	$(4.96 \pm 0.32)\%$	$(6.51 \pm 0.86)\%$
CH3						
RCC	19485	11941	7322	4490	2937	453
ACC	836	525	315	226	142	28
RKR	12.4904 ± 0.06	7.65 ± 0.07	4.69 ± 0.05	2.88 ± 0.04	1.88 ± 0.03	0.29 ± 0.01
QBER	$(4.25 \pm 0.21)\%$	$(4.40 \pm 0.19)\%$	$(4.30 \pm 0.25)\%$	$(5.03 \pm 0.34)\%$	$(4.83 \pm 0.41)\%$	$(6.18 \pm 1.17)\%$

The results correspond to a measurement integration time of $\tau = 1560$ s. RCC raw coincidence counts, ACC accidental coincidence counts, RKR raw key rate (per second), QBER qubit error ratio

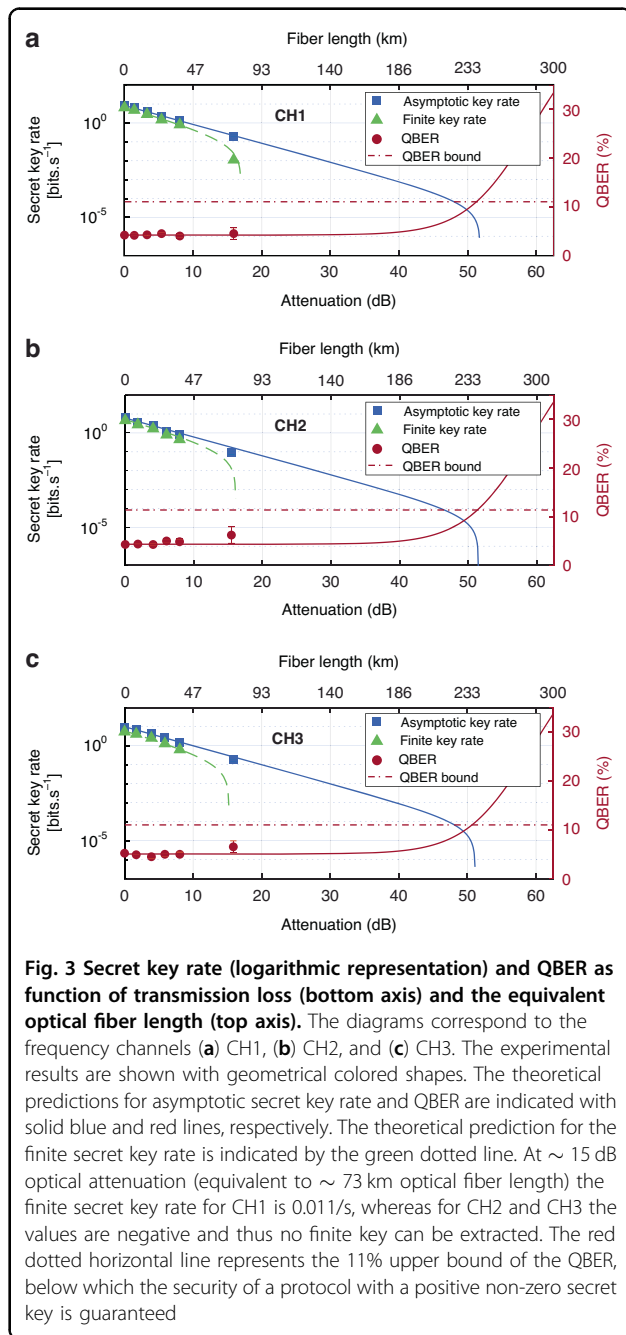
of the true and accidental counts, i.e., $CC_{Z(X)}^{\text{True}}$ and $CC_{Z(X)}^{\text{Acc}}$, such that $CC_{Z(X)}^{\text{raw}} = CC_{Z(X)}^{\text{Acc}} + CC_{Z(X)}^{\text{True}}$. The true and accidental counts are defined as $CC_Z^{\text{Acc}} = CC_{00} + CC_{11}$, $CC_X^{\text{Acc}} = CC_{+-} + CC_{-+}$, $CC_Z^{\text{True}} = CC_{01} + CC_{10}$ and $CC_X^{\text{True}} = CC_{++} + CC_{--}$.

The coincidence events were collected over an integration time of $\tau = 1560$ s. The coincidence counts averaged over time in each basis are referred to as the raw key rates, i.e., $R_Z = CC_Z^{\text{raw}}/\tau$ and $R_X = CC_X^{\text{raw}}/\tau$. The ratio between the accidental and the raw coincidence counts in the Z and X basis is termed quantum bit error ratio (QBER) and is

denoted by $E_Z = CC_Z^{\text{Acc}}/CC_Z^{\text{raw}}$ and $E_X = CC_X^{\text{Acc}}/CC_X^{\text{raw}}$, respectively. In Table 1, the experimentally obtained performance metrics for the BBM92 protocol are presented for channels CH1, CH2, and CH3 at different optical attenuations corresponding to different fiber lengths. At 15.6 dB of attenuation, corresponding to ~ 73 km fiber length, the QBER remained for all frequency channels well below the 11% upper bound for a secure QKD protocol¹⁸, guaranteeing the security of the protocol.

We calculated the secret key rate and length for the asymptotic and non-asymptotic (finite) regimes. The





asymptotic regime assumes an infinite number of signals to be exchanged between Alice and Bob. Following the Shor-Preiskill security proof for an ideal QKD protocol¹⁸, from the raw key bits we quantified the asymptotic secret key rate S^A (see Methods and materials), shown in Fig. 3. Our theoretical calculations predicted a positive non-zero asymptotic secret key rate for up to 233 km. For a ~ 73 km fiber link, we obtained a maximum asymptotic secret key length l^A of 310-bits, 283-bits and 149-bits for channels CH1, CH2, and CH3, respectively (see Methods and materials).

Table 2 Maximum detection probability mismatch δ in the Z and X basis for frequency channels CH1, CH2, and CH3

	CH1	CH2	CH3
Z basis	1.72%	6.3%	0.7%
X basis	2.24%	3.41%	3.66%

In the non-asymptotic regime, a finite number of signals is considered to be exchanged. In practice, the statistical fluctuations introduced by the finite key size effect, combined with failure probabilities in performing error correcting codes, impede the establishment of perfectly secure and correct key bits. Here, we assumed that our protocol is correct and secret up to failure probabilities of $\epsilon_{\text{cor}} = 10^{-10}$ and $\epsilon_{\text{sec}} = 10^{-10}$, respectively. (It is important to note that the source-independent nature of EBQKD protocols renders the inefficiencies in the source irrelevant for the secret key analysis). Additionally, we accounted for the asymmetry in the implementation of the protocol arising from unavoidable experimental imperfections. Specifically, an asymmetry in the detection probability in our experimental implementation arises from the different modulation efficiencies in sideband generation, the different quantum channels and in turn the different amounts of loss, the specific selection of detection windows for post-selecting the coincidence events in the Z and X basis states, as well as the slight difference in the intrinsic efficiencies of the detectors. In Table 2, the maximum detection probability mismatch δ between the states in the Z basis and the states in the X basis is presented for frequency channels CH1, CH2, and CH3. We accounted for such deviations (from an ideal protocol) by adjusting the amount of privacy amplification (see Methods and materials), using the approach proposed by ref. 50. Additionally, we accounted for the detection probability mismatch between the Z and X basis by performing the secret key analysis for each basis independently. The total finite secret key rate S^F in our protocol was thus obtained collectively from the sum of the finite secret key rates in the Z and X basis (see Fig. 3). Our finite secret key analysis provided a positive non-zero secret key rate of up to approximately a fiber length of 73 km. At ~ 15.6 dB optical attenuation (equivalent to ~ 73 km optical fiber length) the finite secret key rate for CH1 has a positive value, whereas for CH2 and CH3 the finite secret key analysis resulted in negative values and thus no secret key could be extracted. This can be explained by the larger overall detection mismatch for channels CH2 and CH3 compared to CH1 (see Table 2), requiring larger amount of raw key bits to be sacrificed for privacy amplification.



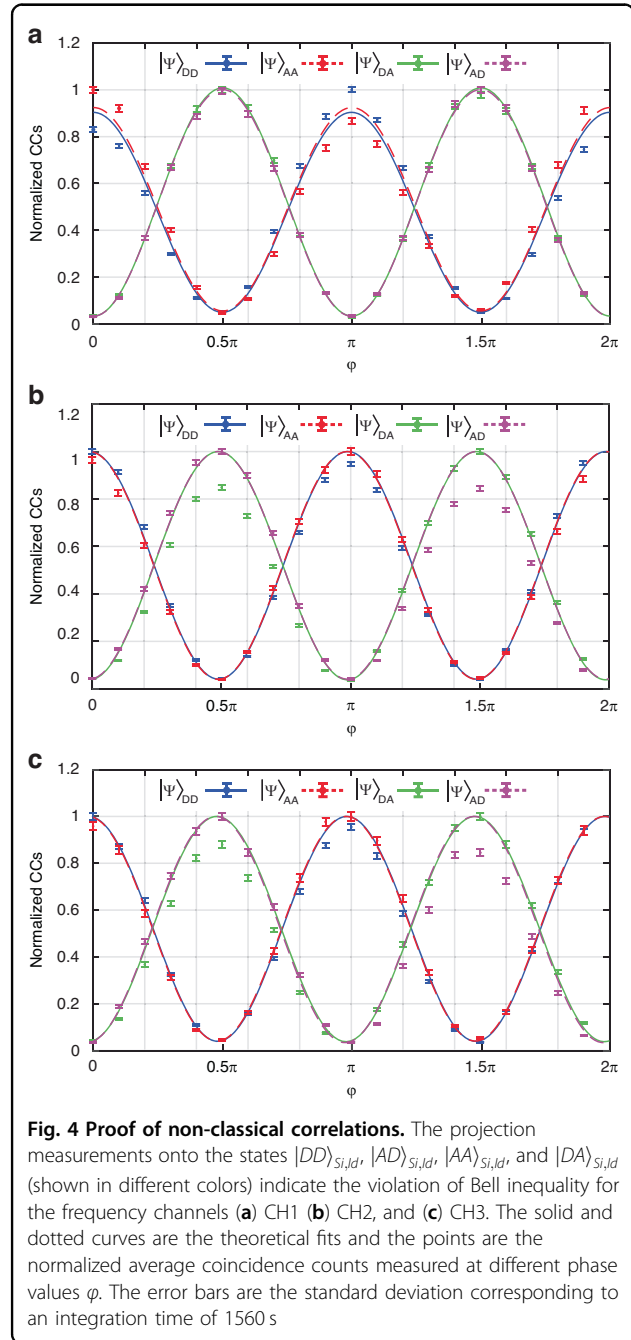
Frequency-based entanglement distribution

In our experiment, the SPDC source produces biphoton frequency-bin entangled states. To assess the entanglement quality supported by each channel, we performed Bell-test measurements at zero optical attenuation. In this measurement, Bob and Alice use their programmable filters to impart an identical phase term φ on their frequency bins $|0\rangle$ and $|1\rangle$, respectively. By sweeping a phase term from $\varphi = 0$ to 2π , we performed projection measurements onto the following vector states $|\psi\rangle_{DD} = \frac{1}{2} (e^{i\varphi}|0\rangle_{Id} + |1\rangle_{Id}) \otimes (|0\rangle_{Si} + e^{i\varphi}|1\rangle_{Si})$, $|\psi\rangle_{AA} = \frac{1}{2} (e^{i\varphi}|0\rangle_{Id} - |1\rangle_{Id}) \otimes (|0\rangle_{Si} - e^{i\varphi}|1\rangle_{Si})$, $|\psi\rangle_{DA} = \frac{1}{2} (e^{i\varphi}|0\rangle_{Id} + |1\rangle_{Id}) \otimes (|0\rangle_{Si} - e^{i\varphi}|1\rangle_{Si})$, and $|\psi\rangle_{AD} = \frac{1}{2} (e^{i\varphi}|0\rangle_{Id} - |1\rangle_{Id}) \otimes (|0\rangle_{Si} + e^{i\varphi}|1\rangle_{Si})$. Here, D and A correspond to measurements on the spectral positions ν_6 as well as ν_5 and ν_7 , respectively. The quantum interference corresponding to these projections are shown in Fig. 4. We calculated the quantum interference visibilities through the following formulation $V = (CC_{\max} - CC_{\min}) / (CC_{\max} + CC_{\min})$ where $CC_{\max}$ and $CC_{\min}$ are the maximum and minimum coincidence counts without subtracting the background accidental counts (see Table 3). The obtained visibilities for frequency channels CH1, CH2, and CH3 indicate the violation of Bell inequality ($V > 70.71\%$ ³¹) by more than ~ 13 standard deviation which certifies the high quality entanglement supported at different spectral regions. The exploited phase difference in odd-order negative sidebands for the basis analyzer is here reflected in a shift of the interference pattern by $\frac{\pi}{2}$ between the projection states $|\psi\rangle_{DD}$ and $|\psi\rangle_{AA}$ and the projection states $|\psi\rangle_{AD}$ and $|\psi\rangle_{DA}$.

To assess the capability of our system in preserving entanglement across remote fiber links, we conducted Bell test measurements at varying amounts of optical attenuation. The average visibilities for each frequency channel can be found in Table 4 and Fig. 5. We observed that for all frequency channels at ~ 15 dB optical attenuation (equivalent to ~ 73 km fiber link), the average visibility remains above the lower threshold 70.71%, hence the Bell inequality was violated. To obtain the maximum length of the optical fiber link at which high entanglement quality is preserved, we modeled the variation of average visibility as function of channel loss. Our theoretical model adopted from refs.^{4,51,52} predicts the violation of Bell inequality across all channels up to approximately ~ 55 dB channel loss (equivalent to ~ 257 km fiber link). This underscores the capability of our scheme to enable frequency-insensitive entanglement distribution.

Network capabilities of frequency-bin-encoded EBQKD

The presented experimental approach can be extended to include multi-user EBQKD network architecture. In such network, the central PWS allows for the specification of an arbitrary number of frequency channels and their



dynamic allocation to an arbitrary number of users, hence allowing for different network topologies. According to the graph theory, for a fully-connected network of N users, at least $N(N-1)/2$ links are required to be established evenly among the users^{53–56}. This can be applied to our approach by considering a network with a single entanglement source shared among N users and a PWS that functions as a central service provider multiplexing $N-1$ frequency channels into the SMF of each user. In such a network, with growing number of users, the network



Table 3 Visibilities of the quantum interferences corresponding to the projections vectors $|DD\rangle_{Si,Id}$, $|AD\rangle_{Si,Id}$, $|AA\rangle_{Si,Id}$ and $|DA\rangle_{Si,Id}$

Biphoton projection vector states versus the visibility of quantum interference				
Channels	$ DD\rangle_{Si,Id}$	$ DA\rangle_{Si,Id}$	$ AA\rangle_{Si,Id}$	$ AD\rangle_{Si,Id}$
CH1	$(89.59 \pm 2.23) \%$	$(93.50 \pm 2.11) \%$	$(88.66 \pm 3.19) \%$	$(93.56 \pm 2.25) \%$
CH2	$(92.16 \pm 1.78) \%$	$(92.68 \pm 1.99) \%$	$(92.25 \pm 2.45) \%$	$(92.17 \pm 2.12) \%$
CH3	$(92.43 \pm 2.43) \%$	$(92.70 \pm 2.71) \%$	$(92.22 \pm 3.41) \%$	$(93.45 \pm 2.80) \%$

The visibilities are calculated without background subtraction. The errors correspond to an integration time of 1560 s

Table 4 Average visibility of the quantum interference corresponding to projection vector states $|DA\rangle_{Si,Id}$ and $|AD\rangle_{Si,Id}$ at different lengths of the optical fiber link for frequency channels CH1, CH2, and CH3

Average visibility of quantum interference versus different optical attenuations (dB) [corresponding fiber length]						
Channels	0dB [0 km]	1.64 dB [7 km]	3.71 dB [17 km]	5.73 dB [26 km]	7.98 dB [37 km]	15.6 dB [73 km]
CH1	$(93.53 \pm 1.54) \%$	$(93.39 \pm 1.84) \%$	$(94.22 \pm 2.19) \%$	$(92.89 \pm 3.04) \%$	$(92.43 \pm 4.13) \%$	$(91.44 \pm 10.96) \%$
CH2	$(92.43 \pm 1.45) \%$	$(92.62 \pm 1.72) \%$	$(94.20 \pm 2.00) \%$	$(92.22 \pm 2.84) \%$	$(91.43 \pm 3.79) \%$	$(91.02 \pm 09.55) \%$
CH3	$(93.07 \pm 1.95) \%$	$(93.98 \pm 2.35) \%$	$(93.46 \pm 3.07) \%$	$(94.35 \pm 3.66) \%$	$(92.63 \pm 5.25) \%$	$(92.43 \pm 12.74) \%$

The standard deviation for each channel corresponds to an integration time of 1560 s

scales linearly since the additional quantum channels are defined within the same source of entanglement.

In Fig. 6, a schematic illustration of a fully-connected 4-user EBQKD network is presented. In Fig. 6a, the physical layer of this network is shown, where each user is connected to the service provider via a SMF and owns a personal frequency-bin basis analyzer module. In the quantum correlation layer, at least 6 frequency channels are required to form a fully-connected quantum network. As illustrated in Fig. 6b, each user is linked to the other three users through at least three frequency channels. The specification of the frequency channels and their distribution among the four users to form a fully-connected network is shown in Fig. 6c. As is demonstrated, the channels embrace correlated signal-idler pairs of frequency-bins defined within the broadband spectrum of a single SPDC-based entanglement source. Noteworthy, in this implementation, given the 50 GHz single mode bandwidth and the 25 GHz modulation tone, a frequency spacing of 100 GHz was required to be defined between the frequency bins in each channel. As a result, in a four-user fully-connected EBQKD network, some frequency-bins are left unassigned such as I04, I08 and I09. However, the frequency bins I04 and I08 could also be deployed together as an additional QKD channel and multiplexed to a fifth added user. With this specific spectral configuration for channel allocation, the frequency bin I09 would ultimately be left unassigned as the adjacent frequency bin to I09 needs to be necessarily selected either I13 or I05. Modified RF modulation tones could realize an

optimized sideband modulation setting to save on the available frequency bins for allocation of further QKD channels to additional users in the network.

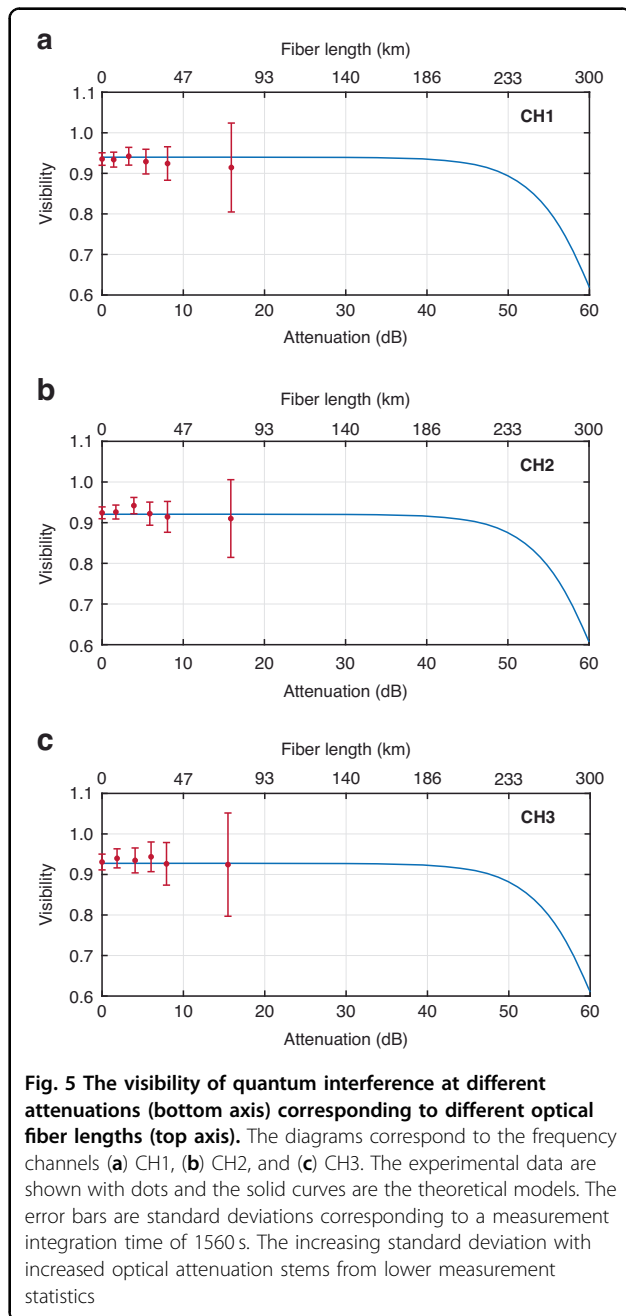
Note that our approach allows for the connection of two users through more than one quantum channel (see Charlie and Fiona in Fig. 6), which increases the key rate while preserving the security as the secret key bits from each channel can be simply added. This is in contrast to increasing the photon flux by applying higher excitation powers aiming at improving the finite secret key rate. In the latter case, the coincidence to accidental ratio will decrease, the entanglement quality degrades, and the QBER will increase accordingly. To create the finite key, more raw key bits will in turn be required. The allocation of more than one quantum channel for finite key extraction can be an alternative solution to increasing the pump power. Note that for the case where two users are connected by more than one quantum channel, the channel in which projection measurement is performed does not necessarily need to be announced in the sifting stage (however, at the cost of increased QBER).

The connection between the users can be dynamically reconfigured enabling to adjust to demand on the key exchange load. Moreover, this fully-connected network architecture can also be reduced to subset topologies to enable QKD between any given two or three users.

Discussion

We demonstrated a proof-of-concept experimental realization of a frequency-bin encoded BBM92 EBQKD





protocol and developed a novel, scalable and resource-efficient frequency-bin basis analyzer module.

Random projection measurements in the Z and X basis were realized simultaneously based on electro-optic phase modulation of the signal and idler photons in each frequency channel. Importantly, as opposed to previous implementations of the BBM92 protocol⁵⁷, the constant phase modulation settings throughout the protocol renders the users needless of any active switching between the different settings to enable the transition between the Z and X basis projection measurements. This is a

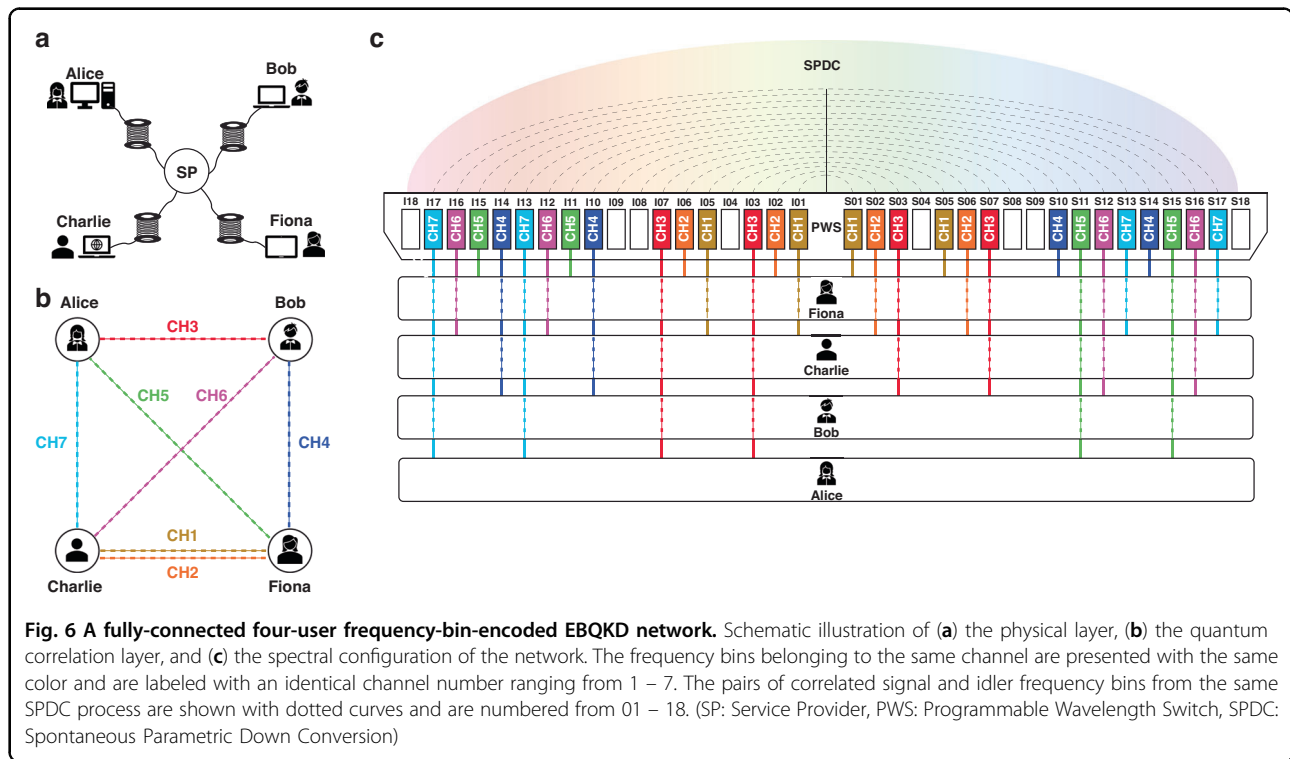
significant advantage of our approach for that it realizes directly the condition of random choice of basis (required by the BBM92 protocol to ensure security) as well as a speed-up in communications.

Based on the FTM technique, we showcased a frequency demultiplexing capability in time, providing each user with access to the projection states using only a single SNSPD. In contrast to schemes where each user is necessarily equipped with four detectors to detect the four Z and X basis projection states for one quantum channel, the employment of a single detector by each user reduces considerably the resource overhead, minimizes the dark count contribution and the overall vulnerability of the protocol to the detector side-channel attacks. Moreover, the use of a single detector mitigates the imbalance (the asymmetry arising from different amounts of loss encountered in users' optical paths as well as the detectors' intrinsic detection efficiency mismatch), required to meet the fair sampling condition to maintain the security level of the protocol. In enabling such characteristics, our approach contributes significantly to reducing the complexity while maintaining the security of the protocol.

The frequency-insensitivity of our approach in preserving high-quality entanglement over long fiber links enables entanglement distribution in quantum networks of metropolitan scale. Noteworthy, with a common transmission mode technique for the RF signal and the optical field, phase stability for the basis state projections required in practical scenarios (see Methods and materials) can be readily achieved. The compatibility of the photonic frequency domain with standard fiber-optic telecommunication infrastructure renders it directly deployable.

The architecture of the presented analyzer module allows for the inclusion of additional frequency channels to the QKD network without any hardware overhead. Remarkably, we showcased the capability of our approach in detecting the projection states corresponding to $N > 1$ quantum channels using the same single detector rather than $N \times 4$ detectors. Additionally, for N quantum channels, a single electro-optic phase modulator can be employed rather than N phase modulators, hence providing a simultaneous frequency-mixing and random projection measurements of all channels, in turn addressing the scalability hurdles in large-scale quantum networks.

The FTM technique adopted in our approach provides simultaneous demultiplexing-in-time of the measurement outcomes of all channels to enable their detection with one single detector. However, a tradeoff between the pulsed laser repetition rate and the number of multiplexed frequency channels needs to be considered. The lower the repetition rate of the pulsed laser, the larger the capacity for multiplexing additional frequency



channels. The frequency-channel multiplexing can be directly used to increase the key exchange rate in a point-to-point QKD. This is an alternative solution to increasing the pump power, which is unavoidably accompanied by a degraded signal-to-noise ratio, hence detrimental to entanglement fidelity. At the same time, using the same quantum light source and adding further basis analyzers, the frequency-channel multiplexing can be exploited to expand the network for multi-user operations within different network topologies. It is important to note that the efficiency of photon pair generation in SPDC process can differ over its spectral emission range which affects the key exchange rate of different channels. However, the affected key rate of such channels could be compensated by shaping the source's emission characteristics.

The frequency domain combined with PWS provides an adaptive implementation platform capable of supporting dynamic networking functionalities, in contrast to static wavelength-division-multiplexing components. Specifically, our frequency multiplexing approach can support a dynamic architecture for wavelength allocation to multiple users (hence a further optimized resource-overhead). The basis analyzer directly accepts different frequency channels without a change of system hardware and only by adaptation in measurement operation via a software control. Our approach thus allows for a scalable multi-user QKD network with an adaptive topology, wherein the key rate could be

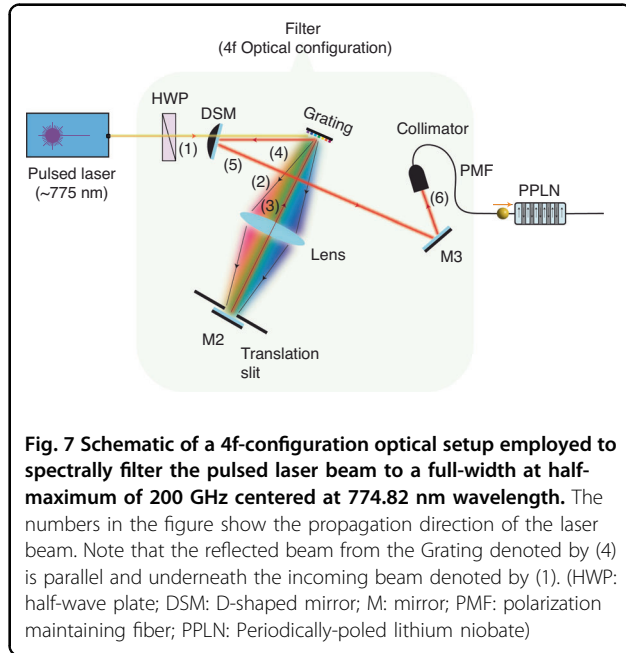
optimized dynamically on-demand with maintained security.

Our proof-of-concept demonstration for frequency-bin EBQKD lays the foundation for further advancements. For example, on-chip integration can be adopted in future steps to reduce loss by an amount of 4–5 dB per module and brightness-enhanced sources could be considered to further improve the key rates. Overall, our solution demonstrates dynamic resource-efficient QKD for multi-user operation with different topologies, thus supporting scalability to future quantum networks.

Materials And Methods

Entangled photon pair source, distribution and detection

The entangled photon-pair source was composed of a 40 mm-long 5%-MgO-doped PPLN waveguide (*Covesion Ltd.*) excited by 180 μ W input power from a mode-locked laser (*C-Fiber 780 Femtosecond Erbium laser by Menlo systems*) with 50 MHz repetition rate and 10 ps pulse duration. The laser beam was spectrally filtered to a full-width at half maximum of 200 GHz via a 4f-configuration optical setup (see Fig. 7) which consisted in a half-wave plate (to adjust the incoming polarization of the laser beam, hence enabling maximum conversion efficiency inside the PPLN), a ruled optical grating, a coated bi-convex lens with a focal length of $F=100$, and an adjustable mechanical slit to center the output wavelength to the PPLN's phase matching wavelength of 774.82 nm (386.92 THz). A pulsed-driven type-0 SPDC process



within the PPLN waveguide created a broad-band biphoton spectrum over the C-band spectral region. A temperature controller (*Covesion OC3*) was used to maintain the PPLN's temperature at its phase matching value, 43.4 °C, to enable photon-pair generation with maximum efficiency at the PPLN's SPDC degeneracy wavelength, 1549.6 nm (193.46 THz).

The frequency channels were defined via the central PWS (*Finisar 4000 s*; 4.8 dB insertion loss) symmetric with respect to the SPDC degeneracy frequency 193.46 THz (1549.6 nm). The spectral configuration of channels (embracing two frequency bins with 20 GHz bandwidth with 100 GHz frequency spacing) was defined taking into account the single frequency mode bandwidth of 50 GHz full-width at half-maximum, determined in a second-order autocorrelation measurement. The idler and signal frequency bins in each channel were defined at the following center frequencies: CH1_{id}: 192.36, 192.46, CH1_{si}: 194.46, 194.56, CH2_{id}: 191.96, 192.06, CH2_{si}: 194.86, 194.96, CH3_{id}: 191.56, 191.66, CH3_{si}: 195.26, 195.36 THz. It is important to note that in this experiment, the operation range of our programmable filter (191.250 to 196.275 THz; specified by the manufacturer; *Finisar, 4000S*) allowed for the definition of three frequency channels. A spectral filtering device providing a wider selection bandwidth would enable the definition of additional signal and idler frequency channels further apart from the SPDC degeneracy point.

In this experiment, the brightness of our SPDC source was characterized as 5.6×10^5 pairs/sec/mW. Under 180 uW input power, the photon pair detection rate for

Table 5 Optical attenuation and the corresponding optical fiber length

Optical attenuation (dB)	1.64	3.71	5.73	7.98	15.60
Equivalent optical fiber length (km)	7.65	17.31	26.66	37.14	73.06

Table 6 Gating loss corresponding to the detection windows

	CH1	CH2	CH3
D1 (Bob)	36.34%	31.63%	31.19%
D2 (Alice)	30.35%	30.49%	29.45%

channels CH1, CH2, and CH3 were ~ 695 , ~ 796 , and ~ 433 pairs/min, corresponding to ~ 3860 pairs/min/mW, ~ 4422 pairs/min/mW, and ~ 2405 pairs/min/mW, respectively. The coincidence to accidental ratio for channels CH1, CH2, and CH3, were obtained to ~ 46 , ~ 48 , and ~ 50 , respectively, signifying the high quality of the time-energy correlated photon pair source.

In this experiment, the FBGs owned by Bob and Alice support a wavelength range from 1528 nm to 1565 nm (equivalent to 191.47 THz to 196.23 THz) and feature approx. maximum insertion loss of 2.23 dB and 2.80 dB, respectively. The SNSPDs feature 100 Hz dark count rate and have approx. a timing jitter of 25 ps. The insertion loss of the components employed in the experimental setup were as follows, PWS: 4.80 dB, PF: 4.8 dB, EOPM_{Alice}: 2.98 dB, EOPM_{Bob}: 3.91 dB, FBG_{Alice}: 2.80 dB, FBG_{Bob}: 2.23 dB. In addition, the loss encountered at different lengths of an optical fiber link is exerted via incremental optical attenuation on Bob's arm (see Table 5).

In this experiment the detectors were operating in the free running mode. However, in post-processing, detection windows were defined at full-width half maximum, corresponding to four projection states, so as to exclude the contributions from adjacent sidebands. The specific definition of detection windows introduces a photon gating loss which we quantified for Alice and Bob's channels separately, shown in Table 6. The values in this table indicate that a wider detection window could be considered to obtain higher key rates.

Coherence stability of frequency-bin states

The coherence stability of the frequency-bin states was examined under propagation through an optical fiber link of 25 km length cascaded by a dispersion compensating module (DCM). In this experiment, the frequency-mixed single-photon spectrum was measured for two cases of 'without' and 'with' 25 km fiber link plus a DCM, shown in

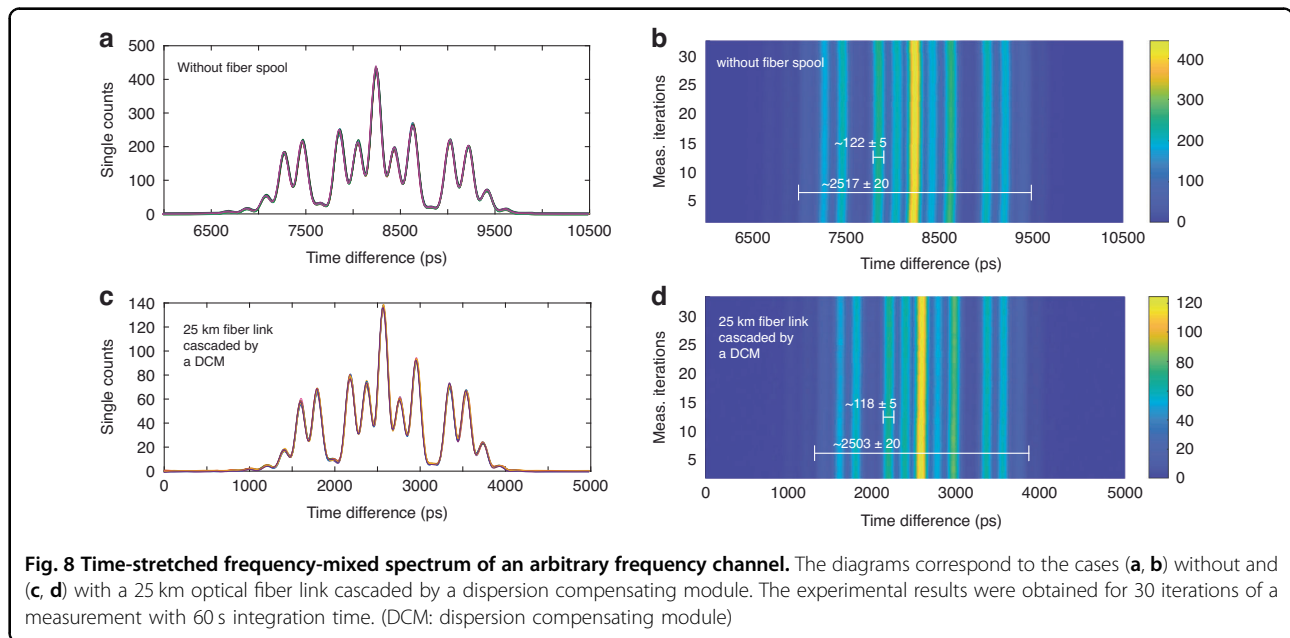
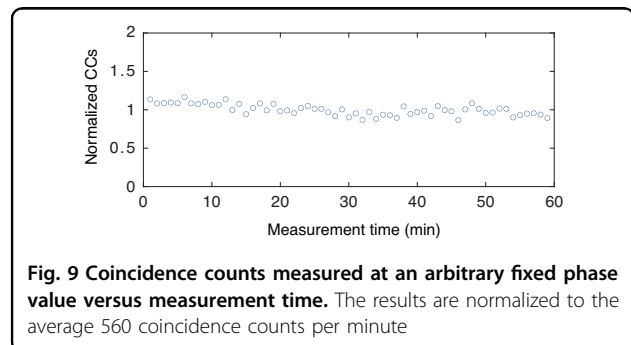


Fig. 8 a(b) & c(d), respectively. By comparing the results, it is observed that dispersion is compensated over the whole spectrum and that the profile shape of the frequency-mixed spectrum is not distorted. Specifically, the frequency-to-time mapped profiles with 122 ± 5 ps and 2517 ± 20 ps temporal widths (corresponding to ~ 25 GHz and ~ 325 GHz bandwidths, respectively) are maintained after propagation through the fiber link cascaded by a DCM. Moreover, given the 30-min measurement time, the impact of second-order dispersion-induced fluctuations on the spectral profile were measured to be negligible. The measurement results confirm the stability with respect to the reference signal obtained from the pulsed laser source.

In addition, the similarity of the spectral profile before and after transmission through 25 km fiber link signifies that the equivalence between the optical attenuation and the actual optical fiber link is a valid assumption. Noteworthy, for the propagation of single photons through long optical fiber links, non-linear noise, such as e.g. Raman scattering, is not observed.

To further assess the coherence stability of the frequency-bin states after propagation through the 25 km-long optical fiber link cascaded by a DCM, we performed a 1-h coincidence measurement from the phase-modulated signal/idler field at a fixed phase value. The normalized coincidence counts versus measurement time are shown in Fig. 9, revealing an almost flat response over time, which demonstrates phase stability for the basis state projection measurements within our thermally controlled laboratory environment. The slight deviation from a perfect phase



stable result can be ascribed to slight environmental fluctuations changing the relative photon arrival time with respect to the RF signal.

In practical scenarios, our approach can be adapted to address the larger environmental fluctuations in longer optical fiber lengths. In such cases, by employing a common transmission mode technique using RF signal over optical fiber, the phase instability can be mitigated. In this case, the common transmission mode of the RF tone and the photons' electric-field allows for their simultaneous accumulation of phase drifts, leading to a stable two-photon interference over time and thus stable projection measurements.

Electro-optic phase modulation

In electro-optic phase modulation, an arbitrary waveform generator (AWG; Keysight, M8196A) was employed to drive the modulators. The RF signals from channels 1 and 2 of the AWG were precisely adjusted at 415 mV and 240 mV voltage amplitudes to drive the electro-optic phase

modulators in possession by Bob and Alice, respectively. The EOMs possessed by Bob and Alice introduced an insertion loss of 3.91 dB and 2.98 dB, respectively.

Noteworthy, the EOMs were required to be phase-stable to maintain the phase relationship for the projections onto the X basis states. In this experiment, the EOMs were intrinsically phase-stable as they were referenced to the same oscillator within the AWG. In practical scenarios where the users reside in their independent laboratories, the transmission of the RF signal over optical fiber can be implemented to achieve phase stability.

QBER minimization

In this experiment, electro-optic phase modulation was tuned to provide power radiation into sidebands of maximum 3rd-order. However, a slight amount of power also radiates into the higher-order sidebands, leading to slight increase in the erroneous projections for the Z basis. Specifically, in post processing, the QBER corresponding to the Z basis was obtained on average between $\sim 5.2\%$ to $\sim 6.3\%$, whereas for the X basis, the QBER was obtained roughly within the range from $\sim 2.5\%$ to $\sim 3.5\%$. The larger QBER of the Z basis has raised the average QBER to roughly $\sim 4\%$ (see Table 1). To minimize the QBER, the detection window for the Z basis states could be defined from the second-order sideband. Alternatively, by tuning the RF signal waveform the sideband creation could be controlled such that the generation of higher order sidebands are better suppressed.

Polarization stability

In this experiment, the operation of EOPM is polarization-dependent. A polarization-mismatch between the propagating photons and the optical axis of the EOPM would lead to photon loss and in turn a decrease in the detection rate. However, this case does not lead to a rotation of the qubit's Bloch sphere coordinate system (as it would be the case for polarization encoding), since the qubits in our experiment are defined in the frequency space.

In our experiment, the single detection rates from the signal spectrum was characterized (see Table 7), suggesting that polarization was stable at different steps of the experiment (identified by incremental optical attenuation applied on Bob's arm).

Table 7 Single detection rates (kHz) on D2 (Alice) at different steps of the experiment (identified by incremental optical attenuation applied on Bob's arm)

Single detection rates (kHz) on D2 (Alice)						
CH1	12.22 kHz	12.74 kHz	12.27 kHz	12.32 kHz	12.81 kHz	13.16 kHz
CH2	12.52 kHz	13.50 kHz	13.31 kHz	13.33 kHz	13.31 kHz	13.50 kHz
CH3	12.15 kHz	11.69 kHz	11.77 kHz	11.63 kHz	11.46 kHz	11.60 kHz

BBM92 protocol

The BBM92 QKD protocol starts with Alice and Bob each receiving one qubit of the following frequency-bin-encoded entangled pair, represented in the Z and X basis as $|\Phi_Z\rangle = 1/\sqrt{2}(|01\rangle_{Si,Id} + |10\rangle_{Si,Id})$ and $|\Phi_X\rangle = 1/\sqrt{2}(|++\rangle_{Si,Id} - |--\rangle_{Si,Id})$, respectively, with Si and Id denoting Signal and Idler photons, respectively. The users perform independent projection measurements on their qubits based on a random selection among two mutually unbiased measurement basis Z and X. In the sifting stage, the users publicly announce their choices of measurement basis and discard their mismatched selections. In the parameter estimation step, the users reveal a random subset of their signals over the public channel to estimate the statistical error of their protocol. The remaining n_Z and n_X number of signals are denoted the raw key bits in the Z and X basis, respectively. To compensate for any potential security loss, error correction and privacy amplification steps are implemented and the final secret key string is extracted.

Theoretical modeling of the QKD performance metrics prior to privacy amplification and error correction

For an EBQKD with a pulsed laser source, the following relationships are valid for the raw key rate per pulse period $Q_{Z(X)}$ and the QBER in the Z and X basis denoted by $E_{Z(X)}$ ^{51,52}.

$$Q_{Z(X)} = 1 - \frac{(1 - D_{Z(X)}^A)}{(1 + \eta_A \frac{\mu_{Z(X)}}{2})^2} - \frac{(1 - D_{Z(X)}^B)}{(1 + \eta_B \frac{\mu_{Z(X)}}{2})^2} + \frac{(1 - D_{Z(X)}^A)(1 - D_{Z(X)}^B)}{(1 + \eta_A \frac{\mu_{Z(X)}}{2} + \eta_B \frac{\mu_{Z(X)}}{2} - \eta_A \eta_B \frac{\mu_{Z(X)}}{2})^2} \quad (2)$$

$$E_{Z(X)} = e_0 - \frac{2(e_0 - e_{Z(X)}^d)\eta_A\eta_B\frac{\mu_{Z(X)}}{2}(1 + \frac{\mu_{Z(X)}}{2})}{Q_{Z(X)}(1 + \eta_A\frac{\mu_{Z(X)}}{2})(1 + \eta_B\frac{\mu_{Z(X)}}{2})(1 + \eta_A\frac{\mu_{Z(X)}}{2} + \eta_B\frac{\mu_{Z(X)}}{2} - \eta_A\eta_B\frac{\mu_{Z(X)}}{2})} \quad (3)$$



Table 8 Calculation results for the average photon number per pulse period $\mu_{Z(X)}$ and the system detection error probability $e_{Z(X)}^d$ in the Z and X basis

	CH1	CH2	CH3
e_Z^d	0.05254	0.06099	0.04969
e_X^d	0.03008	0.03963	0.03627
μ_Z	3.54×10^{-5}	5.293×10^{-5}	2.91×10^{-5}
μ_X	3.761×10^{-5}	4.895×10^{-5}	2.611×10^{-5}

In Eq.(2), $D_Z^A \approx D_Z^B \approx 0.143 \times 10^{-6}$ (sec^{-1}) and $D_X^A \approx D_X^B \approx 0.033 \times 10^{-6}$ (sec^{-1}) are the dark count rates calculated for 1430 ps and 330 ps coincidence windows of the Z and X basis, respectively, with A and B denoting Alice and Bob. In this implementation, fixed amounts of -10.58 dB and -10.94 dB loss were measured on the optical path of Alice and Bob, respectively. These amounts were resulted from -2.98 dB and -3.91 dB insertion loss from the modulators, -4.8 dB insertion loss from the programmable filters, and 2.80 dB and 2.23 dB loss from the FBGs, for Alice and Bob, respectively. The fixed amounts of loss as well as the intrinsic detector efficiencies (~ 0.8) were considered in the calculation of the overall transmittance values $\eta_A = 0.07$ and $\eta_B = 0.0644$. Given the incremental optical attenuation on Bob's arm, the overall transmittance for Bob degrades at different optical attenuations, whereas for Alice the amount of loss persists at all lengths of the optical fiber link. In Eq.(2), $e_0 = 0.5$ is the error probability, $e_{Z(X)}^d$ is the intrinsic detection error probability arising from the experimental system, and $\mu_{Z(X)}$ is the average photon number per pulse period in the Z and X basis. In Table 8, our calculation results for $\mu_{Z(X)}$ and $e_{Z(X)}^d$ are presented for CH1, CH2, and CH3.

To assess the capability of our approach in entanglement distribution over long fiber links, we considered the following equation $\text{QBER} = (1 - \text{Visibility}_{\text{ave}})/2^4$, relating the QBER and the average visibilities associated with projections onto $|DA\rangle_{\text{Si,Id}}$ and $|AD\rangle_{\text{Si,Id}}$ states. With reference to Eq. (2 and 3), the average visibility is thus modeled as function of the channel loss through the following relationship.

$$\text{Visibility}_{\text{ave}} = 1 - 2e_0 + \frac{4(e_0 - e_{Z(X)}^d)\eta_A\eta_B\frac{\mu_{Z(X)}}{2}\left(1 + \frac{\mu_{Z(X)}}{2}\right)}{Q_{Z(X)}\left(1 + \eta_A\frac{\mu_{Z(X)}}{2}\right)\left(1 + \eta_B\frac{\mu_{Z(X)}}{2}\right)\left(1 + \eta_A\frac{\mu_{Z(X)}}{2} + \eta_B\frac{\mu_{Z(X)}}{2} - \eta_A\eta_B\frac{\mu_{Z(X)}}{2}\right)} \quad (4)$$

Secret key rate analysis

We calculate the secret key rate in the asymptotic and finite regime. For the asymptotic secret key analysis, we adopted the following equation $\ell_Z^A = n_Z(1 - H_2(E_X)) - \text{leak}_{\text{EC}}$ to calculate the asymptotic maximum length ℓ_Z^A of the final secret key in the Z basis^{58,59}. Here, $H_2(e) = -e\log_2(e) - (1-e)\log_2(1-e)$ denotes the binary entropy function, $\text{leak}_{\text{EC}} = n_Z f_e H_2(E_Z)$ accounts for the total number of raw key bits used for error correction, and $f_e \geq 1$ is the error correction inefficiency parameter. Here, we consider $f_e = 1$ as the Shannon limit for a given error correcting code. $H_2(E_X)$ represents the lower bound for the fraction of the raw key bits that are lost during privacy amplification. The same applies for the asymptotic maximum key length in the X basis, ℓ_X^A . The total secret key length in the asymptotic regime reads $\ell^A = \ell_Z^A + \ell_X^A$. In the Z basis, we compute the asymptotic secret key rate through the following formulations $S_Z^{A,(\text{sec}^{-1})} = R_Z(1 - H_2(E_X)) - \frac{1}{\tau}\text{leak}_{\text{EC}}$. The same applies to the asymptotic secret key rate in the X basis, S_X^A . The total secret key rate in the asymptotic limit is obtained from $S^{A,(\text{sec}^{-1})} = S_Z^{A,(\text{sec}^{-1})} + S_X^{A,(\text{sec}^{-1})}$.

In our finite secret key analysis and in the Z basis, we quantify the finite secret key length ℓ_Z^F from the following formulation $\ell_Z^F = n_Z(1 - H_2(\frac{E_X + \alpha}{1 - \Delta})) - \text{leak}_{\text{EC}} - n_Z\Delta - \log\frac{2}{\epsilon_{\text{cor}}\epsilon_{\text{sec}}^2}$ which we adopted from⁵⁰. Here, the term $\Delta = 1 - \frac{1}{(1+\delta)^2}$ accounts for the maximum fraction of the key bits in the Z basis removed in privacy amplification to counteract the sources of detection probability mismatch. The parameter α accounts for the statistical fluctuations associated with the finite key size and is obtained from the following $\alpha = \sqrt{(n_Z + 1)\log\left(\frac{1}{\epsilon_{\text{sec}}}\right)/2n_X(n_Z + n_X)}$ ⁵⁰. The same applies for the finite secret key length in the X basis, ℓ_X^F , and the total finite secret key length reads $\ell^F = \ell_Z^F + \ell_X^F$. We compute the finite secret key rate from the following formulations $S_{Z(X)}^{F,(\text{sec}^{-1})} = \ell_{Z(X)}^F/\tau$, and the total finite secret key rate of the protocol is calculated from $S^{F,(\text{sec}^{-1})} = S_Z^{F,(\text{sec}^{-1})} + S_X^{F,(\text{sec}^{-1})}$. In Table 9, our results of the asymptotic and finite secret key analysis for channels CH1, CH2, and CH3 are presented for different lengths of the optical fiber link.

Table 9 Performance metrics of the frequency-bin-encoded BBM92 QKD protocol at different optical attenuations, subsequent to error reconciliation and privacy amplification steps

	Optical attenuation (dB) [corresponding fiber length (km)]					
	0 dB [0 km]	1.64 dB [7 km]	3.71 dB [17 km]	5.73 dB [26 km]	7.98 dB [37 km]	15.6 dB [73 km]
CH1						
S^A (sec ⁻¹)	8.28 ± 0.13	6.23 ± 0.11	3.95 ± 0.09	2.24 ± 0.07	1.35 ± 0.05	0.19 ± 0.02
S^F (sec ⁻¹)	6.48	4.75	2.86	1.47	0.81	0.011
S^A (N ⁻¹)	0.50	0.51	0.50	0.47	0.52	0.47
S^F (N ⁻¹)	0.39	0.39	0.36	0.31	0.31	0.026
ℓ^A	12930	9724	6172	3506	2108	310
ℓ^F	10108	7424	4471	2308	1268	17
CH2						
S^A (sec ⁻¹)	9.16 ± 0.16	6.95 ± 0.13	4.40 ± 0.10	2.62 ± 0.08	1.51 ± 0.06	0.18 ± 0.02
S^F (sec ⁻¹)	5.30	4.04	2.50	1.26	0.61	—
S^A (N ⁻¹)	0.41	0.44	0.47	0.43	0.43	0.30
S^F (N ⁻¹)	0.24	0.25	0.26	0.20	0.17	—
ℓ^A	14302	10844	6867	4102	2367	283
ℓ^F	8271	6303	3901	1979	960	—
CH3						
S^A (sec ⁻¹)	6.16 ± 0.12	3.73 ± 0.09	2.34 ± 0.07	1.24 ± 0.05	0.83 ± 0.04	0.09 ± 0.02
S^F (sec ⁻¹)	4.56	2.73	1.67	0.78	0.44	—
S^A (N ⁻¹)	0.49	0.48	0.49	0.43	0.44	0.33
S^F (N ⁻¹)	0.40	0.38	0.36	0.27	0.24	—
ℓ^A	9609	5820	3659	1944	1298	149
ℓ^F	7928	4553	2691	1233	726	—

S^A and S^F denote the asymptotic and finite secret key rate, respectively. N refers to the transmitted sifted key. The maximum asymptotic and finite secret key lengths are denoted by ℓ^A and ℓ^F , respectively. The results correspond to an integration time of $\tau = 1560$ s

Acknowledgements

We acknowledge valuable discussions with Una Marvet and funding support from TÜV NORD / Alter Technology. We also acknowledge funding from German Federal Ministry of Education and Research (Bundesministerium für Bildung und Forschung; BMBF) within the project PQUMAL, the European Research Council (ERC) within the project QFreC under the grant agreement no. 947603, and the German Research Foundation (Deutsche Forschungsgemeinschaft; DFG) within the cluster of excellence PhoenixD (EXC 2122, Project ID 390833453).

Author contributions

A.K.K. and M.K. developed the idea and performed the measurements. A.K.K. performed the evaluations and the calculations. A.K.K. wrote the manuscript in discussion with M.K. The project was supervised by M.K.

Funding

Open Access funding enabled and organized by Projekt DEAL.

Data availability

The data sets used and analyzed during the current study are available from the corresponding author on reasonable request.

Conflict of interest

The authors declare no competing interests.

Received: 11 June 2024 Revised: 13 November 2024 Accepted: 17 November 2024

Published online: 16 January 2025

References

- Wehner, S., Elkouss, D. & Hanson, R. Quantum internet: a vision for the road ahead. *Science* **362**, eaam9288 (2018).
- Wang, M. H. et al. Deterministic distribution of multipartite entanglement and steering in a quantum network by separable states. *Phys. Rev. Lett.* **125**, 260506 (2020).
- Guo, X. S. et al. Distributed quantum sensing in a continuous-variable entangled network. *Nat. Phys.* **16**, 281–284 (2020).
- Scheidl, T. et al. Feasibility of 300 km quantum key distribution with entangled states. *N. J. Phys.* **11**, 085002 (2009).
- Ribordy, G. et al. Long-distance entanglement-based quantum key distribution. *Phys. Rev. A* **63**, 012309 (2000).
- Madsen, L. S. et al. Continuous variable quantum key distribution with modulated entangled states. *Nat. Commun.* **3**, 1083 (2012).



7. Curty, M., Lewenstein, M. & Lütkenhaus, N. Entanglement as a precondition for secure quantum key distribution. *Phys. Rev. Lett.* **92**, 217903 (2004).
8. Ekert, A. K. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.* **67**, 661–663 (1991).
9. Bennett, C. H., Brassard, G. & Mermin, N. D. Quantum cryptography without bell's theorem. *Phys. Rev. Lett.* **68**, 557–559 (1992).
10. Scarani, V. et al. The security of practical quantum key distribution. *Rev. Mod. Phys.* **81**, 1301–1350 (2009).
11. Dušek, M., Lütkenhaus, N. & Hendrych, M. Quantum cryptography. *Prog. Opt.* **49**, 381 (2006).
12. Wei, S. H. et al. Towards real-world quantum networks: a review. *Laser Photon. Rev.* **16**, 2100219 (2022).
13. Lee, S. W., Ralph, T. C. & Jeong, H. Fundamental building block for all-optical scalable quantum networks. *Phys. Rev. A* **100**, 052303 (2019).
14. Cacciapuoti, A. S. et al. Quantum internet: networking challenges in distributed quantum computing. *IEEE Netw.* **34**, 137–143 (2020).
15. Zhang, Q. et al. Large scale quantum key distribution: challenges and solutions [Invited]. *Opt. Express* **26**, 24260–24273 (2018).
16. Peranić, M. et al. A study of polarization compensation for quantum networks. *EPJ Quant. Technol.* **10**, 30 (2023).
17. Wengerowsky, S. et al. Passively stable distribution of polarisation entanglement over 192 km of deployed optical fibre. *Npj Quant. Inform.* **6**, 5 (2020).
18. Shor, P. W. & Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **85**, 441–444 (2000).
19. Chatterjee, S. et al. Polarization bases compensation towards advantages in satellite-based QKD without active feedback. *Commun. Phys.* **6**, 116 (2023).
20. Fitzke, E. et al. Scalable network for simultaneous pairwise quantum key distribution via entanglement-based time-bin coding. *PRX Quant.* **3**, 020341 (2022).
21. Bouchard, F. et al. Quantum communication with ultrafast time-bin qubits. *PRX Quant.* **3**, 010332 (2022).
22. Kim, J. H. et al. Quantum communication with time-bin entanglement over a wavelength-multiplexed fiber network. *APL Photon.* **7**, 016106 (2022).
23. Chapman, J. C., Lim, C. C. W. & Kwiat, P. G. Hyperentangled time-bin and polarization quantum key distribution. *Phys. Rev. Appl.* **18**, 044027 (2022).
24. Wang, J. et al. Quantum orbital angular momentum in fibers: a review. *AVS Quant. Sci.* **4**, 031701 (2022).
25. Wang, Q. K. et al. High-dimensional quantum cryptography with hybrid orbital-angular-momentum states through 25 km of ring-core fiber: a proof-of-concept demonstration. *Phys. Rev. Appl.* **15**, 064034 (2021).
26. Cozzolino, D. et al. Orbital angular momentum states enabling fiber-based high-dimensional quantum communication. *Phys. Rev. Appl.* **11**, 064058 (2019).
27. Suciú et al. Quantum communication networks with optical vortices. *Phys. Rev. A* **108**, 052612 (2023).
28. Xavier, G. B. & Lima, G. Quantum information processing with space-division multiplexing optical fibres. *Commun. Phys.* **3**, 9 (2020).
29. Gröblacher, S. et al. Experimental quantum cryptography with qutrits. *N. J. Phys.* **8**, 75 (2006).
30. Osellame, R. A larger quantum alphabet. *Nature* **546**, 602–603 (2017).
31. Kues, M. et al. On-chip generation of high-dimensional entangled quantum states and their coherent control. *Nature* **546**, 622–626 (2017).
32. Mahmudlu, H. et al. Fully on-chip photonic turnkey quantum source for entangled qubit/qudit state generation. *Nat. Photon.* **17**, 518–524 (2023).
33. Lukens, J. M. & Lougovski, P. Frequency-encoded photonic qubits for scalable quantum information processing. *Optica* **4**, 8–16 (2017).
34. Reimer, C. et al. High-dimensional one-way quantum processing implemented on d -level cluster states. *Nat. Phys.* **15**, 148–153 (2019).
35. Arnold, G. et al. Converting microwave and telecom photons with a silicon photonic nanomechanical interface. *Nat. Commun.* **11**, 4460 (2020).
36. Weaver, M. J. et al. An integrated microwave-to-optics interface for scalable quantum computing. *Nat. Nanotechnol.* **19**, 166–172 (2024).
37. Elshaari, A. W. et al. Hybrid integrated quantum photonic circuits. *Nat. Photon.* **14**, 285–298 (2020).
38. Bloch, M. et al. Frequency-coded quantum key distribution. *Opt. Lett.* **32**, 301–303 (2007).
39. Islam, N. T. et al. Robust and stable delay interferometers with application to d -dimensional time-frequency quantum key distribution. *Phys. Rev. Appl.* **7**, 044010 (2017).
40. Sarihan, M. C. et al. Proof-of-principle frequency-bin quantum key distribution with biphoton frequency combs. *Proc. Conference on Lasers and Electro-Optics*. 1-2 (Optica Publishing Group, 2021).
41. Zhou, L. et al. Twin-field quantum key distribution without optical frequency dissemination. *Nat. Commun.* **14**, 928 (2023).
42. Ali-Khan, I., Broadbent, C. J. & Howell, J. C. Large-alphabet quantum key distribution using energy-time entangled bipartite states. *Phys. Rev. Lett.* **98**, 060503 (2007).
43. Nunn, J. et al. Large-alphabet time-frequency entangled quantum key distribution by means of time-to-frequency conversion. *Opt. Express* **21**, 15959–15973 (2013).
44. Liu, J. Y. et al. High-dimensional quantum key distribution using energy-time entanglement over 242 km partially deployed fiber. *Quant. Sci. Technol.* **9**, 015003 (2024).
45. Xue, R. et al. Measurement-device-independent quantum key distribution of frequency-nondegenerate photons. *Phys. Rev. Appl.* **17**, 024045 (2022).
46. Tittel, W. et al. Quantum cryptography using entangled photons in energy-time bell states. *Phys. Rev. Lett.* **84**, 4737–4740 (2000).
47. Hu, J. Y. et al. Experimental quantum secure direct communication with single photons. *Light Sci. Appl.* **5**, e16144 (2016).
48. Mishra, S. et al. BBM92 quantum key distribution over a free space dusty channel of 200 meters. *J. Opt.* **24**, 074002 (2022).
49. Khodadad Kashi, A. et al. Frequency-to-time mapping technique for direct spectral characterization of biphoton states from pulsed spontaneous parametric processes. *Front. Photon.* **3**, 834065 (2022).
50. Yin, J. et al. Entanglement-based secure quantum cryptography over 1,120 kilometres. *Nature* **582**, 501–505 (2020).
51. Zhong, Z. Q. et al. Realistic and general model for quantum key distribution with entangled-photon sources. *Phys. Rev. A* **106**, 052606 (2022).
52. Ma, X. F., Fung, C. H. F. & Lo, H. K. Quantum key distribution with entangled photon sources. *Phys. Rev. A* **76**, 012307 (2007).
53. Wengerowsky, S. et al. An entanglement-based wavelength-multiplexed quantum communication network. *Nature* **564**, 225–228 (2018).
54. Liu, X. et al. 40-user fully connected entanglement-based quantum key distribution network without trusted node. *Photonix* **3**, 2 (2022).
55. Alshowkan, M. et al. Reconfigurable quantum local area network over deployed fiber. *PRX Quant.* **2**, 040304 (2021).
56. Joshi, S. K. et al. A trusted node-free eight-user metropolitan quantum communication network. *Sci. Adv.* **6**, eaba0959 (2020).
57. Appas, F. et al. Flexible entanglement-distribution network with an AlGaAs chip for secure communications. *npj Quant. Inform.* **7**, 118 (2021).
58. Tomamichel, M. et al. Tight finite-key analysis for quantum cryptography. *Nat. Commun.* **3**, 634 (2012).
59. Bunandar, D. et al. Numerical finite-key analysis of quantum key distribution. *npj Quant. Inform.* **6**, 104 (2020).

