Article:
Pittaluga, Mirko, Minder, Mariella, Lucamarini, Marco orcid.org/0000-0002-7351-4622 et al. (5 more authors) (2021) 600-km repeater-like quantum communications with dual-band stabilization. Nature photonics. pp. 530-535. ISSN 1749-4885

https://doi.org/10.1038/s41566-021-00811-0

600 km repeater-like quantum communications with dual-band stabilisation

Mirko Pittaluga[1,2†*], Mariella Minder[1,3†], Marco Lucamarini[1,4⋆], Mirko Sanzaro[1], Robert I. Woodward[1], Ming-Jun Li[5], Zhiliang Yuan[1] & Andrew J. Shields[1]

[1] *Toshiba Europe Limited, 208 Cambridge Science Park, Cambridge CB4 0GZ, UK*

[2] *School of Electronic and Electrical Engineering, University of Leeds, Leeds LS2 9JT, UK*

[3] *Department of Engineering, Cambridge University, 9JJ Thomson Avenue, Cambridge CB3 0FA, UK*

[4] *Department of Physics and York Centre for Quantum Technologies, University of York, York YO10 5DD, UK*

[5] *Corning Incorporated, Corning, New York, 14831, USA*

[†] *These authors contributed equally to this work*

[*] *mirko.pittaluga@crl.toshiba.co.uk*

[⋆] *marco.lucamarini@york.ac.uk*

Twin-field (TF) quantum key distribution (QKD) fundamentally alters the rate-distance relationship of QKD, offering the scaling of a single-node quantum repeater. Although recent experiments have demonstrated the new opportunities for secure long-distance communications allowed by TF-QKD, formidable challenges remain to unlock its true potential. Previous demonstrations have required intense stabilisation signals at the same wavelength as the quantum signals, thereby unavoidably generating Rayleigh scattering noise that limits the distance and bit rate. Here, we introduce a novel dual-band stabilisation scheme that overcomes past limitations and can be adapted to other phase-sensitive single-photon applications. Using two different optical wavelengths multiplexed together for channel stabilisation and protocol encoding, we develop a setup that provides repeater-like key rates over record communication distances of 555 km and 605 km in the finite-size and asymptotic regimes respectively, and increases the secure key rate at long distance by two orders of magnitude to values of practical significance.

INTRODUCTION

Quantum key distribution (QKD) [1, 2] allows two distant users to establish a common secret string of bits by sending photons through a communication line, often an optical fibre. The photons, however, are scattered by the propagation medium and have only a small probability of reaching the end of the line, which restrains the QKD key rate and transmission range. A rigorous theorem [3] (see also [4]) limits to 1.44η the number of secure bits delivered by QKD over a line with small transmission probability η, a limit known as 'repeaterless secret key capacity' (SKC_0) or PLOB bound [3]. Quantum repeaters offer a theoretical solution to extend the range of QKD [5–8]. However, a full-fledged quantum repeater remains outside the reach of present technology, due to the difficulty in building and reliably operating a low-loss quantum memory. A partial implementation of a memory-assisted repeater has been recently achieved [9] in the form of measurement-device-independent QKD [10] (see also [11]).

An alternative method to extend the transmission range of QKD without using a quantum memory has been recently discovered and named 'twin-field' (TF) QKD [12] due to the peculiar interference between two fields that have related, though not necessarily identical, optical phase. The secret key rate (SKR) of TF-QKD scales proportionally to $\sqrt{\eta}$, similar to a quantum repeater with a single node, thus entailing a major increase in the SKR-vs-distance figure of QKD. This has led to the realisation of several experiments that display formidable long-range (or high-loss) characteristics [13–18].

The security of the original TF-QKD protocol was first proved in [12] for a limited class of attacks and then extended to general attacks in [19] and [20]. Soon after, its experimental implementation was also considerably simplified thanks to protocol variants that waived the need for phase randomisation and reconciliation for signal states [21–26]. The 'phase-matching' protocols [21–23] feature signal states with a constant global phase while the 'sending' or 'not-sending' protocol (SNS) [24–26] encode qubits upon optical pulses with random and unknown phases. With the help of 'two-way classical communication' (TWCC) [27, 28], the SNS protocol is able to remove the quantum bit error rate (QBER) floor intrinsic to the encoding method thereby extending the communication distance [29]. By running the TWCC protocol over ultralow-loss (ULL) optical fibres, a distance of 509 km has been achieved [18], which represents the current record distance for secure quantum communications over optical fibres.

RESULTS

Dual-band phase stabilisation

In order to perform TF-QKD, it is necessary to com-

pensate the phase drift of the encoded pulses interfering in the intermediate node (Charlie) after travelling through hundreds of kilometres in fibre. The typical phase drift for a 100 km fibre was measured to exceed 1000 rad/s [12]. Active compensation of rapid drift requires bright reference light to be transmitted in the same fibre along with the quantum signals for phase calibration. The longer the fibre, the brighter the reference pulses have to be, as phase calibration requires a minimum power level to be received at the detectors. So far, all the TF-QKD experiments used the same wavelength for both quantum and reference signals, with the help of time-divisional modulation to achieve the necessary intensity contrast. However, this approach ceases to work for ultralong fibres. The ever-increasing intensity of the reference pulses causes a strong Rayleigh scattering that travels back and forth along the fibre and dramatically reduces the quantum signal to noise ratio. As proven in [18], the noise due to double Rayleigh backscattering becomes comparable with the dark counts noise of Charlie's detectors around 500 km of ultralow-loss fibre. Moreover, the performance of a system using a single wavelength for both dim and bright signals will be inevitably limited by the finite dynamic range of the detectors. These two aspects fundamentally limit 'single-band' TF-QKD.

In this work, we adopt a novel 'dual-band' phase control using two wavelengths multiplexed on a single fibre, which as well as solving the phase stabilisation problem in TF-QKD, could have broad applicability in a range of optical applications that require space-separated phase control. The technique allows strong intensity contrast between reference and quantum signals while the wavelength separation prevents the Rayleigh scattering from contaminating the quantum signals. An active phase compensation of the intense reference light leads to an immediate reduction of the phase drift by more than a factor 1000, allowing the residual drift to be compensated at a much slower pace using light signals that have comparable intensity and identical wavelength as the quantum signals. It is worth noticing that the two wavelengths are generated by independent lasers and are not phase-locked, i.e., the stabilisation mechanism works also without an exact phase relation between the two bands. This counter-intuitive detail is fundamental to guarantee the practicality of the setup, which makes ultra-stable cavities or complex light modulation schemes unnecessary.

The resulting setup is versatile, capable of implementing all kinds of TF-QKD protocols proposed so far, including the phase-matching ones [21–23], which cannot be efficiently run without an active phase stabilisation method. With this setup, clocked at 1 GHz, we run various protocols and achieve record SKRs and distances for secure quantum communications over optical fibres. The SKR overcomes the absolute SKC_0 at several distances, thus proving the quantum repeater-like behaviour of our system. In addition to estimating the SKR, we also extract, for the first time, actual raw bits from a TF-QKD protocol. This is a necessary requisite for a system that aims to distribute secure cryptographic keys to remote users in a real-world scenario.

Setup

The experimental setup (Fig. 1) is composed of three modules. The modules of Alice and Bob, who are the communicating users, transmit their quantum signals to Charlie's module via the quantum channel, made of spools of Corning SMF-28 ULL fibre. The spools are spliced into different sets, thus enabling experiments over 5 different communication distances, ranging from 153.2 to 605.2 km. The average loss coefficient of the fibre channel, including splices and connectors, is 0.171 dB/km. For detailed information on the fibre properties, refer to Table II in the Supplementary Material.

The setup uses two wavelengths: λ_1 (1550.12 nm) and λ_2 (1548.51 nm), disseminated by Charlie's L1 and L2 lasers over long servo fibre links. Each servo link spans 305.7 km of standard single mode fibre, giving a total separation between the two communicating users exceeding 611 km. To ensure sufficient power arriving at each user, two erbium-doped fibre amplifiers (EDFAs) are placed in each servo link to compensate for channel losses: one EDFA is placed mid-span and the other is just before the entrance to Alice/Bob. Despite the long distance and periodic amplification, we verified the absence of detrimental nonlinear optical effects (i.e., stimulated Brillouin scattering, four-wave mixing etc.).

The users' local lasers ($L1_A$ and $L1_B$) have a free running linewidth of 50 kHz. They are locked to the disseminated λ_1 signal through an optical phase-looked loop (OPLL), and generate light for encoding dim quantum signals. The encoders in the users' stations operate at 1 GHz, and they carve the λ_1 input light into a train of 250 ps pulses. The even-numbered pulses are modulated in intensity and phase, according to the requirements of the different TF-QKD protocols to be implemented. We refer to these as 'quantum signals'. The odd-numbered pulses do not receive any further modulation and are used to track the phase drift of the quantum signals. Hence, we refer to them as 'dim reference'. All pulses are attenuated to the single-photon level before entering the quantum channel. A step-by-step description of the encoder modulation is given in the Methods. The disseminated λ_2 signal is routed via dense wavelength division multiplexing (DWDM) within users' modules for transmitting to Charlie together with the quantum signal.

Alice and Bob provide independent pre-compensation of the polarisation rotation of the signals at the two wavelengths so that all photons arrive with identical polarisation at Charlie's receiving 50/50 beam splitter (for more details on this aspect refer to Sec. III of the Supplementary Material). The interference output at the beam splitter are is separated by DWDM filters before detection by three superconducting nanowire single photon detectors (SNSPD's): D_0 and D_1 for λ_1 photons and D_2 for λ_2 photons. Charlie's module further contains a phase modulator (PM) in one input arm and a fibre

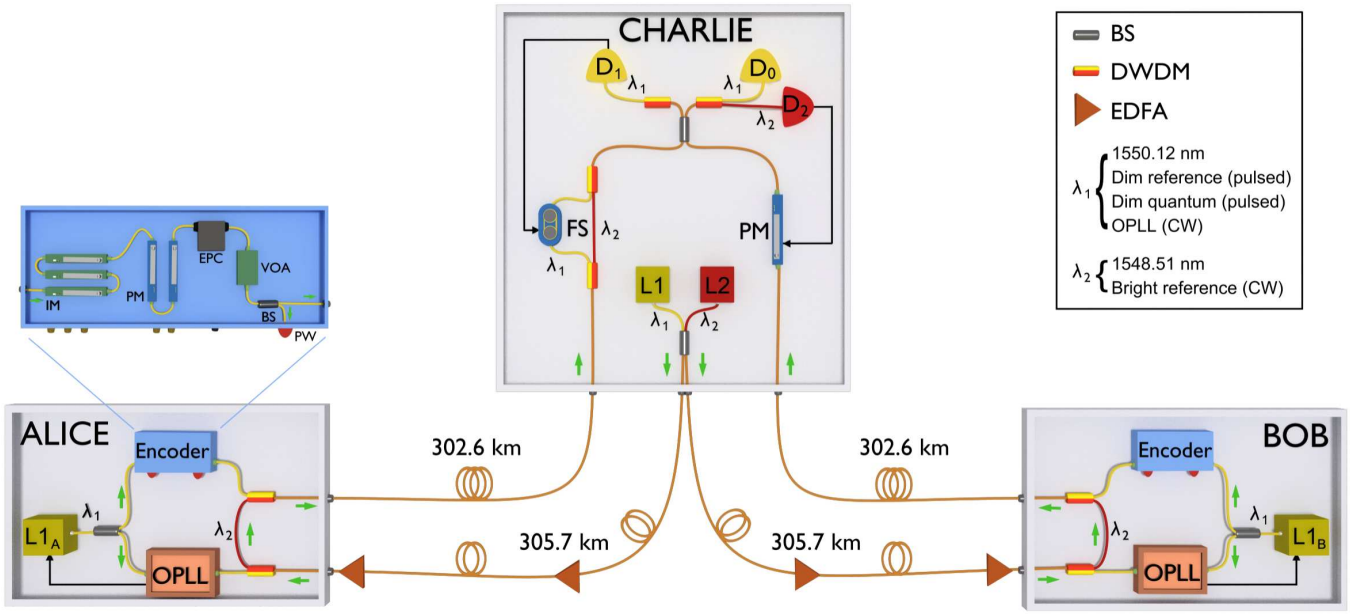

FIG. 1. **Experimental setup.** Charlie's L1 (λ_1) and L2 (λ_2) lasers provide continuous-wave signals for wavelength dissemination and phase tracking, respectively. Combined via a beam splitter (BS), they are transmitted to the symmetric users (Alice and Bob) over long servo links (305.7 km in each arm) equipped with periodic erbium doped fibre amplifiers (EDFAs). Each user owns an optical phase-locked loop (OPLL) to clone the λ_1 wavelength to their local lasers ($L1_A$ and $L1_B$). The cloned output is encoded before being wavelength multiplexed with the disseminated λ_2 light into the quantum channel. Alice and Bob's signals meet at Charlie's second BS and interfere. Detectors D_0 and D_1 record the interference output for λ_1, while D_2 records the one for λ_2. The dual band phase stabilisation realised by a phase modulator (PM) and a fibre stretcher (FS) removes fast and slow phase drifts respectively. **Encoder boxes.** A set of intensity and phase modulators inside each user's Encoder allow them to run different TF-QKD protocols. IM: intensity modulator, EPC: electrical polarisation controller, VOA: Variable optical attenuator, PW: Power meter, DWDM: dense wavelength division multiplexer/demultiplexer.

stretcher (FS) sandwiched between a pair of DWDMs in the other arm. Full stabilisation of the quantum signal is achieved in two steps (a block diagram representation of the feedback systems is reported in Fig. 2 of the Supplementary Material), each step using a specific wavelength of the dual-band stabilisation. First, Charlie measures the bright reference and uses a field programmable gate array (FPGA) with an integrated counter to apply a proportional-integral-differential (PID) control to the bias of his PM. The brightness of the signal detected by D_2 allows this control loop to operate at 200 kHz, sufficient to stabilise the phase drift caused by the long fibre channels. Since λ_1 and λ_2 are spectrally close and travel along the same fibre between the users and the central node, the λ_2 light can be used to stabilise the phase of the pulses at λ_1. Assuming unidirectional phase drift, the λ_2-stabilisation will reduce the phase drift in λ_2 by approximately $\lambda_1/|\lambda_2 - \lambda_1| \approx 1000$. In the real scenario, the non-unidirectionality of the phase drift makes the actual reduction even greater, as we will show later. The slowed drift can then be comfortably corrected through a second PID controller adjusting the bias of the FS at a rate of 10-20 Hz, without requiring an intense input signal. The input signal for this feedback is provided by the interference outcome of the dim reference pulses at λ_1 recorded by D_1. More information about the feedback systems and on the sources of the residual slow drift is provided in the Methods.

Experimental Results

Figure 2 shows the interference outcome for λ_1, over a 605 km long quantum channel, at different stages of the stabilisation process. The purple dots in Fig. 2a represent the interference when no phase stabilisation is applied. At this distance, the free drift is so rapid (in the order of 10^4 rad/s) that it is impossible to discern any interference fringe over a 1 s time scale. Only on a millisecond time scale (Fig. 2b) we can distinguish the interference fringes. The phase drift rate distribution associated with this measurement is shown in the purple histogram in Fig. 2c. Its standard deviation allows us to quantify the phase drift in $11.89 \cdot 10^3$ rad/s.

After activating the stabilisation from λ_2, the phase drift rate for λ_1 reduces drastically (see orange points in Fig. 2a). It is now possible to follow the evolution of constructive or destructive interference over a time scale of tens of seconds. The effectiveness of this stabilisation is quantifiable by the reduction in the phase drift rate for the recorded data (orange histogram in Fig. 2d). When feedback from the bright reference at λ_2 is enabled, the standard deviation of the drift rate decreases to 1.74 rad/s, a value ∼6800 times smaller than without

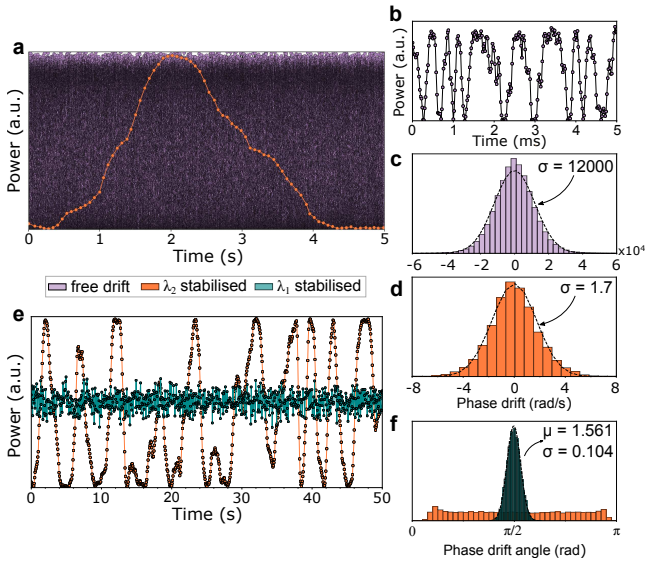

FIG. 2. **Dual-band stabilisation.** Data in this figure shows the interference of λ_1 light at different stabilisation stages. Data was acquired over 605 km quantum and 611 km servo fibres, in a configuration identical to that in Fig. 1 except Encoder boxes were bypassed. Detector D_1 (Fig. 1) was used to record the data. The colour code is: purple for free drift, orange for λ_2-stabilised data and teal for λ_1-stabilised data. **a**, Comparison between free drifting and λ_2-stabilised data. Integration times were 20 μs and 60 ms for free drifting and λ_2-stabilised data, respectively, due to the different time scales. An interference visibility measurement over the free drifting (λ_2-stabilised) data yields 98.22% (96.24%). **b**, Same data set as in (a) but over a ms time scale. **c**, Histogram of the free drifting phase drift. The standard deviation is 11890 rad/s. **d**, Histogram of the λ_2-stabilised phase drift. The standard deviation is 1.74 rad/s , i.e. about 6800 times smaller than in sub-figure (c). **e**, Comparison between λ_2-stabilised data (orange) and data stabilised using both wavelengths, λ_1 and λ_2 (teal). **f**, Phase offset distributions for the data shown in (e). λ_2-stabilised data has an almost uniform distribution over $[0, \pi]$ whereas λ_1-stabilised data has a distribution peaked around $\pi/2$.

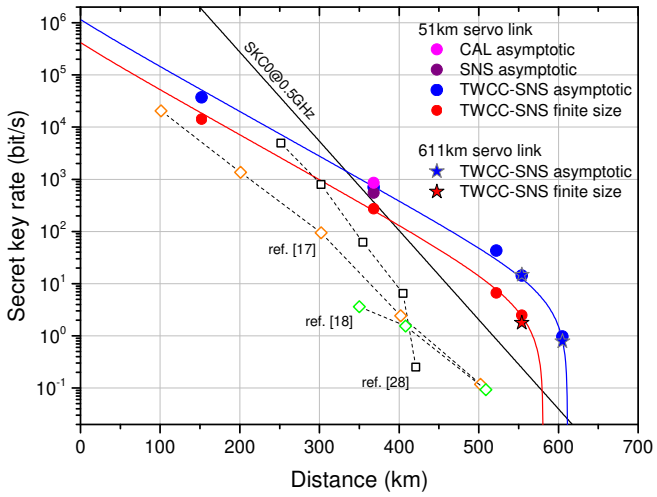

FIG. 3. **Key rate simulations and results.** Secret key rates are plotted against the quantum channel length. This is constituted by ultra-low loss (ULL) fibres of 0.171 dB/km loss. The SKC_0 bound for unitary detection efficiency (black line) is plotted along the simulations for the TWCC SNS TF-QKD protocol in the asymptotic and finite size regimes (blue and red curves respectively). Filled markers show the experimental results we obtained for the different protocols whereas unfilled markers are the state-of-the-art results in term of SKR over distance for fibre-based TF-QKD [17, 18] (diamonds) and QKD [30] (squares).

the bright reference stabilisation. This reduction is considerably better than the estimated factor 1000 due to the cancellation of rapid opposite drifts. The residual slow phase drift of λ_1 can be readily compensated by using the dim reference pulses at this wavelength, which leads to a stable interference output (teal dots in Fig. 2e). Figure 2f shows the phase distribution between the interfering λ_1 signals locked to have $\pi/2$ difference. The locking error is only 0.10 rad (standard deviation of the teal coloured distribution in the figure), which contributes to the QBER by approximately 2%.

Using the described dual-band stabilisation, we performed four experiments with different TF-QKD protocols, varying the operational regimes and optimising the parameters in each case. Firstly, the CAL [22] and SNS [24] protocols in the asymptotic regime, then the SNS with the TWCC method [29], both in the asymptotic and in the finite-size regimes [25, 26]. In the practically relevant case of finite-size TWCC-SNS, we also extracted real bits of the raw key. We performed these experiments in two stages. First, we developed a simplified asymmetric setup to assess the feasibility of long-distance TF-QKD with dual-band phase stabilisation, featuring a single OPLL and a 51 km servo fibre. We then moved on to a symmetrical configuration where the frequency reference is disseminated by Charlie (Fig. 1) via 611 km servo fibre for the final experiments over the two longest quantum channel fibre distances. Details about the asymmetric experimental setup, the protocol parameters, together with additional information on the patterns used for encoding, are given in Sec. I and V of the Supplementary Material.

In Fig. 3 we report our results in terms of SKR versus distance, together with the simulation curves and the state-of-the-art SKRs for long-distance TF-QKD [17, 18] and QKD [30] over optical fibres. In the same graph we also plot the absolute SKC_0, which assumes ideal equipment for Alice and Bob and hence is the most difficult bound to overcome. Surpassing this limit proves the repeater-like behaviour of our setup. The complete experimental results can be found in Sec. VI of the Supplementary Material. The CAL and SNS protocols have been implemented on a 368.7 km-long optical fibre (62.8 dB loss) and analysed in the asymptotic scenario. For CAL, we obtain an SKR of 852.7 bit/s, 2.39 times larger than SKC_0. For SNS, the SKR is 549.2 bit/s, 1.54

times larger than SKC_0.

Using the TWCC SNS version of TF-QKD, we take measurements at 153.3, 368.7, 522.0, 555.2 and 605.2 km, i.e., from 26.5 dB to 104.8 dB loss, and we extract positive SKRs both in the asymptotic and in the finite-size regimes. In Fig. 3, blue (red) symbols refer to the experimental results obtained in the asymptotic (finite-size) case scenario. Stars (dots) represent results obtained through the symmetric (asymmetric) setup with a 611 km (51 km) servo fibre. Despite periodic optical amplifications, the longer servo link introduces only a marginal reduction of the secret key rate. At a 555 km quantum channel and a 611 km servo link, with less than 2 h of continuous measurement, we are able to extract a finite-size SKR of 1.777 bit/s, a value 7.68 times higher than the absolute SKC_0. Extending the quantum channel to 605.2 km, with a loss budget of 104.8 dB, we achieve an asymptotic SKR of 0.778 bit/s, which is 24 times higher than the SKC_0. This represents the first fibre-based secure quantum communication beyond the barriers of 600 km and 100 dB.

To further appreciate the progress entailed by our new technique, we compare our results with the experimental points setting the current record distances for fibre-based QKD (421 km [30]) and TF-QKD (502 km [17], 509 km [18]). Distance-wise, there is an increase of tens of (more than a hundred) kilometres over TF-QKD (QKD) prior art. The main element enabling the distance improvement over previous TF-QKD implementations is the dual-band stabilisation technique, which leads to negligible contamination of the encoded signal by the bright reference. In previous experiments, the bright stabilisation signal was emitted at the same wavelength as the encoded signal, thus causing an intense double Rayleigh backscattering that ultimately limited the maximum communication distance. In our case, on the other hand, even at the longest distance the noise introduced by the stabilisation signal was below the detectors' dark counts.

The dual-band stabilisation technique leads also to an even more pronounced enhancement of the SKR, with an improvement of 2 orders of magnitude at 500 km, the furthest distance achieved by prior art. This is possible because we could keep the clock rate of the encoded signals at the high value of 500 MHz at all distances. In previous experiments, where the stabilisation signal was time-multiplexed, the protocol clock rate had to be reduced considerably to accommodate for reference signals, and to leave some recovery time at the detectors (after these received the bright intensity reference pulses).

All the TF-QKD experiments performed so far, as well as the vast majority of long-distance QKD experiments, have only provided an in-principle estimation of the SKR without a real extraction of the bits that form a cryptographic key after suitable post-processing. In our experiment, we extract real strings of bits from the SNS protocol and process them with the TWCC method. The generation of raw bits is a challenging task, especially with a clock rate as high as 1 GHz, as it requires individual tagging and real-time manipulation of the signals recorded at the detectors. Figure 4 gives a graphical representation of the TWCC method applied to a raw bit string extracted during the experiment performed at 522 km. The bits of the strings are displayed as white or black pixels depending on their value 0 or 1, respectively. The leftmost and central panels in the first row show Alice's and Bob's raw strings, distilled from the SNS protocol, whereas the rightmost panel reports the bitwise addition of the two strings. The density of the dots in the first two panels reveal a slight bias (53.8%) in the bit value which is intrinsic to the SNS protocol [24]. A simulation shows that with our parameters a bias of 52.7% has to be expected. On the other hand, the black dots in the rightmost panel highlight the conflicting bits in the users' raw keys, which amount to a 16% of the total. The second row of Fig. 4 shows the effect of TWCC on the users strings. TWCC induces a considerable reduction of the errors, from 16% to 3.5%, and of the bias in the strings at the expenses of the strings length, which decreases by ∼70%. However, the overall effect of TWCC is beneficial, as it increases the signal-to-noise ratio of the raw keys and so also the range of TF-QKD.

DISCUSSION

We have shown that dual-band phase stabilisation can dramatically reduce the phase fluctuations on optical fibre by almost four orders of magnitude. This has allowed us to overcome the fundamental noise limitation of long distance TF-QKD and increase its secret key rate from

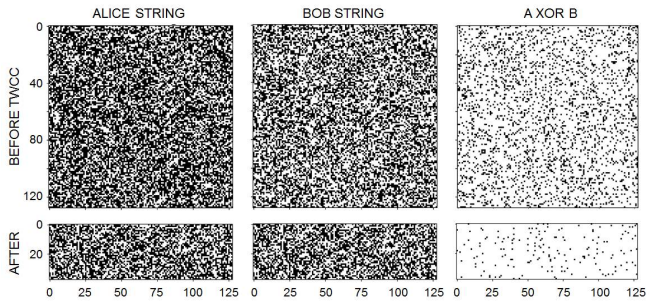

FIG. 4. **Binary maps of the extracted bit strings.** Samples of the bits extracted from the experiment performed at 522 km before (top panels) and after (bottom panels) TWCC is applied. *Top:* The first two squares on the left (128×128 pixels) are a sample of the users' raw strings before TWCC is applied, with white (black) pixels associated with the bit value 0 (1). The third square on the right is obtained by modulo-2 addition (XOR) of the first two. The black dots in this square represent the errors in the strings. *Bottom:* Refined keys after TWCC has been applied. The strings shrink by 70% into rectangles with 128×38 pixels. Reduction in key size is accompanied by a substantial reduction in the key errors, as is apparent from the rightmost rectangle.

the current millibit per second range to the bit per second range for the longest fibre length. We notice here that 1 bit/s key generation rate is sufficient to enable fast key refresh of symmetric cryptographic protocols, such as AES, several times per day. Our setup tolerates a maximum loss beyond 100 dB allowing quantum communication over 600 km of fibre for the first time. We believe these techniques will have more general application in quantum communications, for example enabling DLCZ-type quantum repeaters [6], longer-baseline telescopes [31], quantum fingerprint [32–34] over longer distances or a phase-based architecture for the quantum internet [35].

Note added - During the completion of our work, one of the anonymous referees noted that the finite-size equations we borrowed from Refs. [25, 26] only hold if the variables are i.i.d., a result not known at the time of writing. A full analysis of this point has only recently appeared in a preprint [36] and suggests that the removal of the i.i.d. assumption only entails a slight increase in the failure probability of the protocol.

ACKNOWLEDGMENTS

We thank Xiang-Bin Wang and Hai Xu for their useful feedback on the TWCC protocol. The authors acknowledge funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement No 857156 "OPENQKD" and under the Marie Skłodowska-Curie grant agreement No 675662. M.M. acknowledges financial support from the Engineering and Physical Sciences Research Council (EPSRC) and Toshiba Europe Ltd.

Author contributions. M.P. and M.M. developed the experimental set-up, performed the measurements and analysed the data. M.S. and R.I.W. supported the experimental work. M.-J.L. provided the ultralow-loss fibres. Z.L.Y., M.L. and A.J.S. guided the work. M.L., M.P. and M.M. provided the simulations and wrote the manuscript, with contributions from all the authors.

Competing interests. The authors declare no competing interests.

Data availability. The data that support the plots within this paper and other findings of this study are available from the corresponding authors on reasonable request.

Code availability. The codes used to process the data for this paper are available from the corresponding authors on reasonable request.

Correspondence and requests for materials. should be addressed to M.P. and M.L.

[1] Bennett, C. H. & Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theor. Comput. Sci.* **560**, 7–11 (2014).

[2] Ekert, A. K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67**, 661–663 (1991).

[3] Pirandola, S., Laurenza, R., Ottaviani, C. & Banchi, L. Fundamental limits of repeaterless quantum communications. *Nat. Commun.* **8**, 15043 (2017).

[4] Takeoka, M., Guha, S. & Wilde, M. M. Fundamental rate-loss tradeoff for optical quantum key distribution. *Nat. Commun.* **5**, 5235 (2014).

[5] Briegel, H.-J., Dür, W., Cirac, J. I. & Zoller, P. Quantum repeaters: The role of imperfect local operations in quantum communication. *Phys. Rev. Lett.* **81**, 5932–5935 (1998).

[6] Duan, L.-M., Lukin, M. D., Cirac, J. I. & Zoller, P. Long-distance quantum communication with atomic ensembles and linear optics. *Nature* **414**, 413–418 (2001).

[7] Sangouard, N., Simon, C., de Riedmatten, H. & Gisin, N. Quantum repeaters based on atomic ensembles and linear optics. *Rev. Mod. Phys.* **83**, 33–80 (2011).

[8] Guha, S. *et al.* Rate-loss analysis of an efficient quantum repeater architecture. *Phys. Rev. A* **92**, 022357 (2015).

[9] Bhaskar, M. K. *et al.* Experimental demonstration of memory-enhanced quantum communication. *Nature* **580**, 60–64 (2020).

[10] Lo, H.-K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108**, 130503 (2012).

[11] Braunstein, S. L. & Pirandola, S. Side-channel-free quantum key distribution. *Phys. Rev. Lett.* **108**, 130502 (2012).

[12] Lucamarini, M., Yuan, Z. L., Dynes, J. F. & Shields, A. J. Overcoming the rate-distance limit of quantum key distribution without quantum repeaters. *Nature* **557**, 400–403 (2018).

[13] Minder, M. *et al.* Experimental quantum key distribution beyond the repeaterless secret key capacity. *Nat. Photonics* **13**, 334–338 (2019).

[14] Wang, S. *et al.* Beating the fundamental rate-distance limit in a proof-of-principle quantum key distribution system. *Phys. Rev. X* **9**, 021046 (2019).

[15] Liu, Y. *et al.* Experimental twin-field quantum key distribution through sending or not sending. *Phys. Rev. Lett.* **123**, 100505 (2019).

[16] Zhong, X., Hu, J., Curty, M., Qian, L. & Lo, H.-K. Proof-of-principle experimental demonstration of twin-field type quantum key distribution. *Phys. Rev. Lett.* **123**, 100506 (2019).

[17] Fang, X.-T. *et al.* Implementation of quantum key distribution surpassing the linear rate-transmittance bound. *Nature Photonics* **14**, 422–425 (2020).

[18] Chen, J.-P. *et al.* Sending-or-not-sending with independent lasers: Secure twin-field quantum key distribution over 509 km. *Phys. Rev. Lett.* **124**, 070501 (2020).

[19] Tamaki, K., Lo, H.-K., Wang, W. & Lucamarini, M. Information theoretic security of quantum key distribution overcoming the repeaterless secret key capacity bound.

arXiv:1805.05511 (2018).
[20] Ma, X., Zeng, P. & Zhou, H. Phase-matching quantum key distribution. *Phys. Rev. X* **8**, 031043 (2018).
[21] Lin, J. & Lütkenhaus, N. Simple security analysis of phase-matching measurement-device-independent quantum key distribution. *Phys. Rev. A* **98**, 042332 (2018).
[22] Curty, M., Azuma, K. & Lo, H.-K. Simple security proof of twin-field type quantum key distribution protocol. *npj Quantum Information* **5**, 64 (2019).
[23] Cui, C. *et al.* Twin-field quantum key distribution without phase postselection. *Phys. Rev. Applied* **11**, 034053 (2019).
[24] Wang, X.-B., Yu, Z.-W. & Hu, X.-L. Twin-field quantum key distribution with large misalignment error. *Phys. Rev. A* **98**, 062323 (2018).
[25] Jiang, C., Yu, Z.-W., Hu, X.-L. & Wang, X.-B. Unconditional security of sending or not sending twin-field quantum key distribution with finite pulses. *Phys. Rev. Applied* **12**, 024061 (2019).
[26] Yu, Z.-W., Hu, X.-L., Jiang, C., Xu, H. & Wang, X.-B. Sending-or-not-sending twin-field quantum key distribution in practice. *Sci. Rep.* **9**, 3080 (2019).
[27] Gottesman, D. & Lo Hoi-Kwong. Proof of security of quantum key distribution with two-way classical communications. *IEEE Trans. Inf. Theory* **49**, 457–475 (2003).
[28] Chau, H. F. Practical scheme to share a secret key through a quantum channel with a 27.6% bit error rate. *Physical Review A* **66**, 802 (2002).
[29] Xu, H., Yu, Z.-W., Jiang, C., Hu, X.-L. & Wang, X.-B. Sending-or-not-sending twin-field quantum key distribution: Breaking the direct transmission key rate. *Phys. Rev. A* **101**, 042330 (2020).
[30] Boaron, A. *et al.* Secure quantum key distribution over 421 km of optical fiber. *Phys. Rev. Lett.* **121**, 190502 (2018).
[31] Gottesman, D., Jennewein, T. & Croke, S. Longer-baseline telescopes using quantum repeaters. *Phys. Rev. Lett.* **109**, 070503 (2012).
[32] Arrazola, J. M. & Lütkenhaus, N. Quantum fingerprinting with coherent states and a constant mean number of photons. *Phys. Rev. A* **89**, 062305 (2014).
[33] Xu, F. *et al.* Experimental quantum fingerprinting with weak coherent pulses. *Nat. Commun.* **6**, 8735 (2015).
[34] Zhong, X., Xu, F., Lo, H.-K. & Qian, L. Efficient experimental quantum fingerprinting with wavelength division multiplexing. *arXiv:2005.06049v1* (2020).
[35] Kimble, H. J. The quantum internet. *Nature* **453**, 1023–1030 (2008).
[36] Jiang, C., Hu, X.-L., wen Yu, Z. & bin Wang, X. Composable security for practical quantum key distribution with two way classical communication. *arXiv:2102.00739v1* (2021).
[37] Lo, H.-K., Ma, X. & Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **94**, 230504 (2005).
[38] Wang, X.-B. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.* **94**, 230503 (2005).

METHODS

Encoder boxes. For a detailed representation of the components inside the encoder boxes see inset diagram in Fig. 1. The incoming CW light arrives already aligned in polarisation with the optical axes of the subsequent modulators. The first components in the encoders are three intensity modulators (IMs), used to carve 250 ps long pulses at a 1 GHz rate, with three possible intensity levels (u, v, w). The intensity ratios between the different intensity levels can be adjusted by the AC amplitude driving the IMs.

Two phase modulators (PMs) are then used to encode the phase of the optical pulses. In this system, we cascade two PMs instead of using just one to reduce their RF signal amplitudes. Limiting each PM to a modulation range of $[-\frac{\pi}{2}, \frac{\pi}{2})$, we achieve a phase modulation that covers the whole $[0, 2\pi)$ range and that is linear with its driving signals amplitude. Each PM is driven by a 8-bit DACs, and with two cascaded we are able to encode 512 different phase values over the 2π phase range.

All the modulators are driven by two synchronised 12 GSa/s waveform generators, one for each user, programmed to encode a 25040-pulse long pseudo-random pattern. For more information on the encoded pattern refer to Sec. VI of the Supplementary Material.

The PMs are followed by an electrically driven polarisation controller (EPC), a variable optical attenuator (VOA), and a 99:1 beam splitter (BS). The EPC is used to control the polarisation of the λ_1 photons after transmission through the channel. Each user has a continuous polarisation optimisation routine that aligns the quantum signals along the preferred optical axis at Charlie.

The VOA sets the flux of the quantum signal before injection into the quantum channel, through a flux calibration control loop that continuously adjusts the VOA so as to have a stable optical output, monitored at the strong output of the BS.

Feedback systems. The dual-band phase-stabilisation strategy employed in this experiment enabled us to stabilise the quantum channel without affecting the encoding in the wavelength reserved for the quantum signal (λ_1) or the clock rate of the protocol, which was kept at 500 MHz at all the tested distances. Its general design is presented in Fig. 1 and its detailed block diagram is given in Fig. 2 of the Supplementary Material.

There, Fig. 2a shows the stabilisation method based on the bright reference at λ_2. It features a closed loop cycle that locks the interference between Alice's and Bob's bright reference beams to a given intensity level. This, in turn, locks the phase offset between these signals to a fixed value. The bright reference interference is monitored by the SNSPD D_2. Single photons detected by D_2 are integrated over a period of 5 μs. The difference between the integrated number of counts and the set value, constitutes the error signal of a PID controller implemented with an FPGA clocked at 200 kHz. By tuning the DC offset of a phase modulator (PM) that acts on the light coming from Bob, the FPGA controls the interference between the bright references. It is important to notice here that the phase shift applied by the PM affects both the wavelengths λ_2 and λ_1. The feedback based on λ_2 fully stabilises the bright reference light while it only partially stabilises the quantum one.

The remaining (slow) phase drift on λ_1 is related to two factors: the fact that λ_1 and λ_2 travel separately in certain sections of the setup (necessary for the protocol encoding over λ_1 at the transmitting stations), and the fact that the fast feedback introduces a phase drift over λ_1 when the length difference between the two channels varies over time. The former component of the slow phase drift can be seen as the phase noise picked up by an asymmetric Mach-Zender interferometer having the dimensions of those sections of the setup where the two wavelengths travel separately. The latter component can be explained as a consequence of the finite range of the PM, and of the phase locking of the fast feedback over λ_2, rather than λ_1.

The PM in the fast feedback actively compensates the fast phase drift. However, its finite adjustment range is incapable of compensating at entirety the phase drift caused by fibre length variation. It must rely on multiple (M) resets in order to maintain the λ_2 phase difference to $\phi = 2\pi M + \phi_t$, where ϕ_t is the target phase. Due to the $\lambda_2 - \lambda_1$ wavelength difference, this compensation will introduce a residual phase drift ($\Delta\phi$) over λ_1 equal to:

$$\Delta\phi = 2\pi M \cdot \left(\frac{\lambda_2 - \lambda_1}{\lambda_1}\right). \tag{1}$$

The residual drift introduced by the λ_2-stabilisation over λ_1 is estimated to be $\frac{\phi}{\Delta\phi} = \frac{\lambda_1}{\lambda_2 - \lambda_1} \approx 1000$ times smaller than the original fibre phase drift, if assuming unidirectional fibre length drift. In reality, the fibre length drift direction is random. With cancellation of positive and negative 2π resets, we obtain experimentally a higher reduction factor of ~ 6800 (as shown in Fig. 2).

Supplementary Material Fig. 2b shows the stabilisation mechanism that corrects the residual phase drift on λ_1. The error signal for it is provided by the overall interference of quantum signals and dim reference. The quantum signals are interleaved with the dim reference pulses, which are unmodulated and have the same intensity as the brightest decoy pulse (u). The presence of dim reference pulses guarantees that the averaged output of the interference is directly related to the residual phase offset in λ_1. This is retrieved by integrating the single photons detected by SNSPD D_1 over 50 ms or 100 ms, depending on the distance. The difference between this value and a set value provides the error signal for a PID controller implemented with a micro-controller operating at the frequency of 20 Hz or 10 Hz, depending on the distance. The micro-controller corrects the phase offset by modulating a fibre stretcher acting on the quantum signal coming from Alice. Differently from the stabilisation in λ_2, the one in λ_1 acts solely on the quantum signals and can therefore correct its residual phase drift.

Due to the different expansion/contraction rates of the channels connecting Charlie to the two users, during the protocol execution we had to compensate for the change in length of the quantum channels. We did that by opportunely delaying the pattern encoding of one user with respect to the other, aiming at obtaining always optimal time alignment of the users' pulses at Charlie's BS. The intervals between these alignment adjustments depended on the stability of the environmental conditions in the lab, and varied from once every 4 minutes, up to once every of 30 minutes. From the highest adjustments frequency, we estimated an upper limit of the length difference drift between the two sides of the communication channel (in our air-conditioning temperature stabilised lab) of $\sim$3 mm/min in the longest experimental setting.

Protocols. To demonstrate the multi-protocol aspect of our system, we implemented different variants of TF-QKD, in different regimes. We list them as CAL [22], SNS [24–26] and TWCC-SNS [29]. Their detailed description and security proofs can be found in the referenced papers. See also Methods in [13]. Here we describe our encoding method and the equations used to extract the secret key rate from each protocol.

In all protocols, we consider a symmetric situation, with identical photon fluxes for the users Alice and Bob. This is the real situation in the experiment, where fibre lengths and losses between the users and Charlie are nearly identical (see e.g. Table II in Supplementary Material). Therefore we only describe the relevant steps for the user Alice; Bob will execute similar operations in his own location. During the preparation stage, Alice generates weak coherent states of the form $|\sqrt{\mu}e^{i\theta}\rangle$. She randomly selects a basis X or Z with probabilities P_X or P_Z ($P_X+P_Z=1$). If she chooses X (test basis), she randomly selects a flux value $\mu=\{u,v,w\}$ with conditional probability $P_{\mu|X}=\{P_{u|X},P_{v|X},P_{w|X}\}$, $P_{u|X}+P_{v|X}+P_{w|X}=1$, and a random global phase value $\phi\in[0,2\pi)$. She then prepares and send the phase-randomised weak coherent state $|\sqrt{\mu}e^{i\phi}\rangle$. If she chooses Z (code basis), she randomly selects a bit value $\alpha=\{0,1\}$ and sets the photon flux to $\mu=\{s,n\}$ with conditional probability $P_{\mu|Z}=\{P_{s|Z},P_{n|Z}\}$, $P_{s|Z}+P_{n|Z}=1$. In CAL, bits are encoded as coherent states $|\sqrt{s}e^{i\alpha\pi}\rangle$. In SNS, bits are encoded on the photon flux, with s (n) representing a bit value 1 (0) for Alice and a bit value 0 (1) for Bob. With our encoder, the photon fluxes w and n are both very small, in the order of 10^{-4}. Therefore sending out a photon flux n, or w, is equivalent by all practical means to not sending out any flux at all. We denote the probability of 'not sending' conditional on choosing the Z basis as $P_{n|Z}$ and the probability of sending a photon flux s conditional on the Z basis as $P_{s|Z}$ or simply ϵ. The detailed values of the parameters used in the experiment depend on the protocol (CAL, SNS, TWCC) and on the regime (asymptotic or finite-size) adopted. They are listed in Tables III and IV in the Supplementary Material.

After the preparation stage, Alice and Bob send their pulses to central node, Charlie. Charlie should interfere the received pulses on a beam splitter and measure the result, announcing publicly which detector click. If Charlie is malicious and adopts a different detection and announcement strategy the security of TF-QKD remains unaffected. After a total of N_0 signals have been sent, the quantum transmission is over and Charlie publicly announces his measurements. When Charlie's announcement is complete, the users announce their bases. For the X basis, they also disclose their intensities μ and, limitedly to the SNS protocol, they announce the values of their global phases ϕ. Alice and Bob post-select the events for which they used matching bases and intensities. For SNS, they also select the events with global phase values not mismatched by more than Δ modulo π . The users extract the bits from the Z basis events and use the X basis events to perform the security analysis. In TWCC, the bits in the string distilled from the Z basis are randomly paired and bit-wise XOR-ed. More specifically, Bob randomly pairs the bits up and announces the positions and parities of each pair. Alice uses this information to repeat this step with her own string and announces the instances for which her parity calculation matches Bob's one. The users will discard both bits in the pair if the announced parities are different. If the parities are the same, the users keep the first bit of the pairs and form a new shorter string from which they will extract the final key. To this end, they run classical post-processing procedures such as error correction and privacy amplification. The amount of privacy amplification needed to securely distil a key depends on the security analysis and the resulting rate equation. In the following, we list the rate equation adopted for each situation analysed in the experiment.

CAL PROTOCOL. This protocol is analysed in the asymptotic scenario for which $P_Z\approx 1$. The corresponding SKR equation is the one given for 'protocol 3' in [22] and the procedure we use to calculate it is similar to the one described in [13]. See also [16]. The SKR is the sum of two separate contributions, calculated from each detector D_0 and D_1 independently: $R_{\rm CAL}=R_{\rm CAL}^{D_0}+R_{\rm CAL}^{D_1}$. We write the contribution from D_0 as

$$R_{\rm CAL}^{D_0}=Q^z[1-f_{EC}h(E^z)-h(\bar{e}_1^{\rm ph})]. \tag{2}$$

The SKR pertaining to D_1 has a similar expression. In Eq. (2), h is the binary entropy function, f_{EC} is the error correction factor and Q^z and E^z are the gain and the bit error rate, respectively, of the protocol, measured in the experiment from the D_0 clicks when the users announce the Z basis. The quantity $\bar{e}_1^{\rm ph}$ is the upper bound to the phase error rate, for which we have [22]

$$\bar{e}_1^{\rm ph}=\frac{1}{Q^z}\sum_{j=0,1}\left[\sum_{m,n=0}^{N_{\rm cut}}c_m^{(j)}c_n^{(j)}\sqrt{g_{mn}(\overline{Y}^x_{mn},Y_{\rm cut})}\right]^2. \tag{3}$$

In Eq. (3), the coefficient $c_k^{(0)}$ ($c_k^{(1)}$) is defined as $c_k^{(0)}=e^{-\mu/2}\mu^{k/2}/\sqrt{k!}$ when the integer k is even (odd) and 0 otherwise; $g_{mn}(\overline{Y}^x_{mn},Y_{\rm cut})$ is a function equal to $\overline{Y}^x_{mn}$ if $m+n<Y_{\rm cut}$ and equal to 1 otherwise; $Y_{\rm cut},N_{\rm cut}$ are two integers such that $Y_{\rm cut}<N_{\rm cut}$. In our experiment we set $Y_{\rm cut}=8$ and $N_{\rm cut}=12$. The quantities $\overline{Y}^x_{mn}$ are upper bounds for the yields obtained when Alice (Bob) sends m (n) photons. These are estimated using a constrained optimisation linear program [13] similar to the standard decoy state technique [37, 38], with the difference that the yields have to be maximised rather than minimised to provide the worst-case phase error rate. In our implementation, we measured all the intensity combinations uu, uv, uw, vv, vw and ww to improve the decoy-state estimation. In parallel to this numerical estimation, we also implemented the analytical estimation given in [16] to verify the correctness of our results.

SNS PROTOCOL. The SKR for this protocol in the asymptotic scenario ($P_Z\approx 1$) can be written as [24, 29]

$$R_{\rm SNS}=\underline{Q}_0+\underline{Q}_1[1-h(\bar{e}_1^{\rm ph})]-f_{EC}Q^zh(E^z). \tag{4}$$

In Eq. (4), Q^z and E^z are the gain and the bit error rate, respectively, of the protocol, measured in the experiment. The 0-photon gain and 1-photon gain in the Z basis are $\underline{Q}_0=2\epsilon(1-\epsilon)e^{-s}e^{-n}\underline{y}_0$ and $\underline{Q}_1=2\epsilon(1-\epsilon)(se^{-s}e^{-n}+ne^{-n}e^{-s})\underline{y}_1$, respectively. The parameters $\underline{y}_1$ ($\underline{y}_0$) and $\bar{e}_1^{\rm ph}$ are, respectively, the lower bound for the single-photon (zero-photon) yield and the upper bound for the single-photon phase error rate. These quantities are drawn from the X basis of the protocol using equations similar to the ones seen in decoy-states QKD [24, 37, 38].

TWCC PROTOCOL. With the addition of two-way classical communication (TWCC), the users can improve the quality of

their data before performing the standard error correction and privacy amplification operations. The SKR in the asymptotic scenario for this protocol is [29]

$$R_{\mathrm{TWCC}} = \frac{1}{N_0}\{\tilde{n}_1[1 - h(\tilde{e}_1^{\mathrm{ph}})] - \mathrm{leak}_{\mathrm{EC}}\}, \tag{5}$$

with $\tilde{n}_1 = n_1^2/(2n_t)$, $\tilde{e}_1^{\mathrm{ph}} = 2\overline{e}_1^{\mathrm{ph}}(1 - \overline{e}_1^{\mathrm{ph}})$, $\mathrm{leak}_{\mathrm{EC}} = f_{EC}[n_a h(E_a) + n_b h(E_a) + n_c h(E_c)]$. Here, $n_1 = N_0 \underline{Q}_1$ is the number of untagged bits, i.e. the number of bits generated by Charlie's detections when the users send out single-photon states in the Z basis. $n_t = N_0 Q^z$ is the number of successful detections, an observable of the protocol, with N_0 the total number of prepared states. The term '$\mathrm{leak}_{\mathrm{EC}}$' represents the number of bits to be exchanged during the error correction procedure. The quantities n_a and E_a are the number of bits and the error rate, respectively, in Bob's string associated with an odd parity when paired during the TWCC procedure. Similarly, the quantities n_b and E_b (n_c and E_c) are the number of bits and the error rate, respectively, in Bob's string associated with an even parity and when both bits are 0 (1), when paired during the TWCC procedure. The other quantities are as in Eq. (4).

Finite-size SNS and TWCC. The finite size analysis of TWCC [18] is derived directly from the one of SNS [25, 26]. The error correction term of the asymptotic rate equation (5) remains unchanged but the remaining terms are modified to take into account the leakage of information due to finite-size statistical effects. The number of secret bits in the finite-size regime after TWCC has been performed is given by

$$n_{\text{TWCC-FS}} = \hat{n}_1[1 - h(\hat{e}_1^{\mathrm{ph}})] - \mathrm{leak}_{\mathrm{EC}} - \Delta, \tag{6}$$

with $\Delta = \log_2(2/\epsilon_{\mathrm{EC}}) - 2\log_2(\sqrt{2}\epsilon_{\mathrm{PA}}\hat{\epsilon})$ the finite-size correction term and with ϵ_{EC}, ϵ_{PA} and $\hat{\epsilon}$ the failure probabilities for error correction, privacy amplification and the choice of the smoothing parameter, respectively. With the right choice of parameters, our implementation features a security parameter of 2.2×10^{-9}, which is the same as in [18]. The hatted quantities $\hat{n}_1$ and $\hat{e}_1^{\mathrm{ph}}$ correspond to the tilded quantities in Eq. (5), but calculated in the finite-size regime using a composable definition of security and the Chernoff bound. Their detailed expressions can be found in the reference paper [25].

Binary maps generation. From experiments of the SNS TF-QKD protocol described, real keys were extracted. To achieve this, single time-tagged events, acquired in 500 ps windows, were processed individually. Sifting Charlie's announcements, clicks in the Z basis from both detectors were isolated and concatenated. They were then used by Alice and Bob to separately generate their own initial key string. For every photon click recorded in Z basis, Alice (Bob) registers a bit 1 (0) if she (he) had sent a weak-coherent pulse within the time slot and a bit 0 (1) if she (he) had chosen not to send anything. As a result, they obtain matching bits in the cases where only one user has prepared and sent a pulse and opposite bits if both sent. The latter, accompanied by dark counts, contributes to the QBER in the key generation basis. A sample of these initial keys for Alice and Bob are shown in the first two squares of Fig. 4, in the form of binary maps comprised of 128x128 pixels, for the finite-size measurement taken at 522 km. Zeroes and ones are represented by white and black pixels respectively. The white-bias of Alice and black bias of Bob are expected and attributed to the send-send clicks that have the highest occurrence probability and in which Alice will always obtain a 1 while Bob will obtain a 0.

Initial keys were post-processed according to the two-way classical communication method to reduce their initial QBER of 16% and allow successful QKD at such long distances. During this process, Bob's bits are randomly paired up and their parity calculated. The pair positions and resulting parity must be publicly announced so that the procedure can be repeated by Alice who will also announce her results. The initial keys are then further sifted to include only the first bit of pairs whose parity matched in both users. For instance, given the SNS encoding in the key generation basis, pairs encoded as 'sn' by Alice (see Protocols in Methods) in a randomly selected pair will provide a matching parity if paired with bits encoded as 'ns' by Bob whereas will provide unmatched parity if paired with bits encoded as 'ss' by Bob. Although TWCC reduces the length of the secret key, it also significantly reduces the QBER so that the overall signal to noise ratio is increased. The effect of the process on the 522 km data is shown in the first two rectangles at the bottom of Fig. 4. The binary map is reduced in dimension by 70% to represent the equivalent reduction in the entire bit strings. The white, black bias is also visibly reduced. To better depict the QBER reduction the binary maps are bitwise XORed before and after TWCC in the rightmost boxes of Fig. 4. Matching and opposite bits are represented by white and black pixels respectively. In this case, the QBER is reduced by over a factor 4.5, from 16% to 3.5%, thus allowing us to extract a secret key at distances up to 605.2 km.