nature portfolio

https://doi.org/10.1038/s41566-021-00873-0

Supplementary information

A photonic integrated quantum secure communication system

In the format provided by the
authors and unedited

SUPPLEMENTARY INFORMATION

A Photonic Integrated Quantum Secure Communication System

Taofiq K. Paraïso*, Thomas Roger, Davide G. Marangon, Innocenzo De Marco, Mirko Sanzaro, Robert I. Woodward, James F. Dynes, Zhiliang Yuan and Andrew J. Shields
Toshiba Europe Ltd., 208 Cambridge Science Park, Milton Road, Cambridge CB4 0GZ, UK.
**taofiq.paraiso@crl.toshiba.co.uk*

1. Supplementary Note 1: Elements of diode laser theory

1.1. Laser rate equations

Our QKD transmitter chip is based on phase-seeding, which exploits laser properties at their most to encode complex phase states in stream of optical pulses with minimum components. The main physical processes at the core of this technology are the interplay between spontaneous and stimulated emission, as well as direct laser modulation induced by high-speed current modulation. In this note we show how, when driven appropriately, diode lasers can produce pulses meeting the stringent requirements of quantum communications. We refer the reader to Refs. [11] and [27] of the main text for experimental demonstrations of phase-seeding applied to multi-protocol QKD.

A diode laser is described by a set of differential equations governing the time evolution of the carrier density $N(t)$, the photon density $S(t)$ and the phase $\phi(t)$:

$$(1) \qquad \frac{dN(t)}{dt} = \frac{I(t)}{eV_a} - \frac{N(t)}{\tau_n} - \nu_g a_0 \frac{N(t)-N_0}{1+\epsilon S(t)} S(t) + F_N(t)$$

$$(2) \qquad \frac{dS(t)}{dt} = \Gamma \nu_g a_0 \frac{N(t)-N_0}{1+\epsilon S(t)} S(t) - \frac{S(t)}{\tau_p} + \frac{\beta \Gamma N(t)}{\tau_n} + \kappa S_{\mathrm{OIL}}(t) + F_S(t)$$

$$(3) \qquad \frac{d\phi(t)}{dt} = \frac{\alpha}{2} \left(\Gamma \nu_g a_0 (N(t) - N_0) - \frac{1}{\tau_p} \right) + \kappa \phi_{\mathrm{OIL}}(t) + F_\phi(t)$$

where $I(t)$ is the injection current, e the electron charge, V_a the volume of the active layer, τ_n the carrier lifetime, τ_p the photon lifetime, v_g the group velocity, a_0 the gain factor, N_0 the carrier density at transparency, ϵ the gain compression factor, Γ the optical confinement factor, α the linewidth enhancement factor and β the spontaneous emission fraction in the lasing mode.

F_N, F_S and F_ϕ are the Langevin noise terms accounting for different noise sources (spontaneous emission, carrier recombination)

$$F_S(t) = \sqrt{\frac{2\Gamma\beta N(t)S(t)}{\tau_n \Delta t}} \cdot x_S \tag{4}$$

$$F_\phi(t) = \sqrt{\frac{\Gamma\beta N(t)}{2\tau_n S(t)\Delta t}} \cdot x_\phi \tag{5}$$

$$F_N(t) = \sqrt{\frac{2N(t)}{V_a \tau_n \Delta t}} \cdot x_N - \sqrt{\frac{2\Gamma\,\beta\, N(t)S(t)}{\tau_n \Delta t}} \cdot x_S \tag{6}$$

where $x_{S,\phi,N}$ are independent Gaussian distributed random variables of mean 0.

The physics of optical injection locking is described by κ, the coupling rate, and the injection terms

$$S_{OIL}(t) = 2\sqrt{S_{inj}(t)S(t)}\, cos(\phi(t) - \phi_{inj}(t) - \Delta\omega_{inj} t) \tag{7}$$

$$\phi_{OIL}(t) = -\sqrt{\frac{S_{inj}(t)}{S(t)}} sin(\phi(t) - \phi_{inj}(t) - \Delta\omega_{inj} t) \tag{8}$$

with S_{inj} the injected photon density, ϕ_{inj} the injected photon phase and $\Delta\omega_{inj}$ the frequency detuning.

1.2. Gain switching and phase randomisation

In order to generate pulses with random phases the gain switching parameters should be appropriately adjusted. Eqs. (4-6) show that the noise is dictated by the spontaneous emission term β. In a series of plots we provide the reader with an understanding of the laser dynamics yielding pulses with random phases.

1.2.1. Gain-switching and spontaneous emission noise

Fig. S1 shows the result of a gain switching simulation. The laser was driven with a DC bias of 35 mA and a 1 GHz modulation current of 70 mA amplitude and 90 % duty cycle. Fig. S1a shows the resulting laser pulses and the relative phase between successive pulses. Fig. S1b shows the drive current and the carrier density. After the initial overshoot, the carrier density (hence the optical power resulting from carrier relaxation) reaches a plateau due to the long duty cycle.

The spontaneous emission term was set to $\beta = 1e^{-5}$, and the related noise can be observed as minor ripples on the plateaus. The relative phase between successive pulses spans 2π, indicating a complete phase randomisation. In the case of a negligible β, the plateaus would appear noiseless and the relative phase would be the same for all pairs of consecutive pulses. Other parameters are $N_0 = 0.8 \cdot 10^{24}\mathrm{m}^{-3}$, $v_g a_0 = 1.27 \cdot 10^{-12}$ m/s, $\tau_n = 10^3 \cdot \tau_p = 0.74 \cdot 10^{-9}$ s, $\alpha = 2.7$, $\Gamma = 0.27$, $\epsilon = 1.18 \cdot 10^{-23}\mathrm{m}^3$.

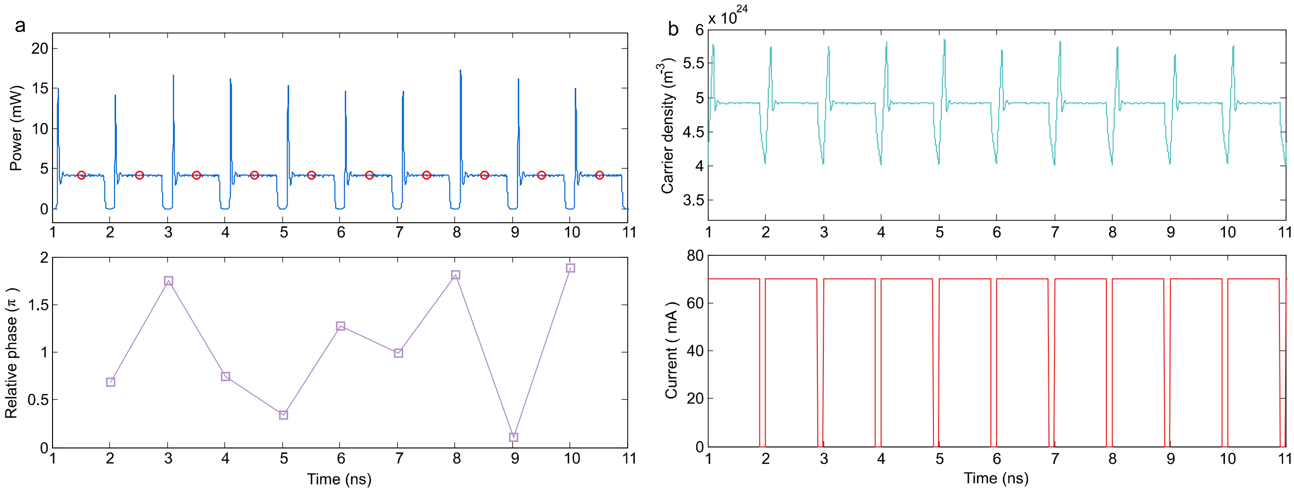

Figure S1: (a) 1 GHz repetition rate, 90% duty cycle, 35 mA bias current and 70 mA peak-to-peak, $\beta = 1e^{-5}$. The red circles indicate the reference points to calculate the relative phase between successive pulses. (b) Depletion of the carriers during the off time of the current modulation suppresses stimulated emission. New pulses are triggered by spontaneous emission the relative phase spans 2 π showing full randomisation A 10'000 pulse simulation returns a mean relative phase of π and a standard deviation $\sigma_{ph} = 0.56\,\pi$.

1.2.2. Gain-switching with remnant stimulated emission

Phase randomisation arises when the carrier density reaches a level sufficiently low for spontaneous emission to play the dominant role in the generation of a new lasing pulse. If this condition is not met and sufficient carriers remain in the cavity at the onset of a new pulse, then the phase will be dictated by stimulated emission. Despite the presence of noise, there will be no phase randomisation. This can be observed in Figs. S2 and S3.

In Fig. S2, the current modulation duty cycle was increased to 95 %. The inter-pulse interval is shorter than the carrier depletion time and stimulated emission is not suppressed. In Fig. S3, the minimum of the current modulation is set to 15 mA, just above the lasing threshold of 14 mA. Despite the 90 % duty cycle as used in Fig. S1, carriers are still being injected into the cavity during the 'low' part of the current modulation, and participate to stimulated emission. In both examples one observes that the relative phase between successive pulses is not randomised.

1.2.3. Phase encoding

In Fig. S4, we introduce a phase-encoding current modulation between two regions of the gain-switched pulse. Precisely tuning the amplitude and duration of the phase encoding modulation makes it possible to encode any phase state. In Fig. S4a we show that 4 phase shifts compatible with BB84 can be encoded between two regions of the gain switched pulse. In Fig. S4b we now simulate transfer of the encoded phase via optical injection locking into a second diode laser, gain-switched at 2 GHz and with a 40 % duty cycle to produce short optical pulses (< 100 ps). Remarkably, the phase shifts encoded between the regions of the seeding laser are transferred to the pulse train of the injected laser. One can also verify that the phase randomness between successive phase encoded pulses is also transferred to the pulse train.

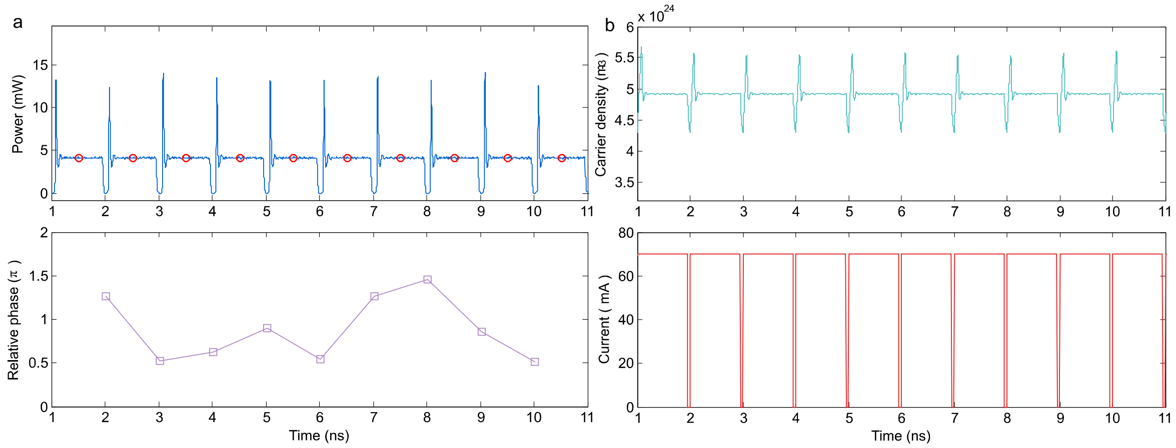

Figure S2: (a) 1 GHz repetition rate, 95% duty cycle, 35 mA bias current and 70 mA peak-to-peak. (b) Because of the short off duration, the carrier density does not have time to deplete to a level where stimulated emission is suppressed compared to spontaneous emission. The phase randomisation is incomplete. Simulation of 10'000 pulses. Mean relative phase $0.8\,\pi$, $\sigma_{ph} = 0.28\,\pi$.

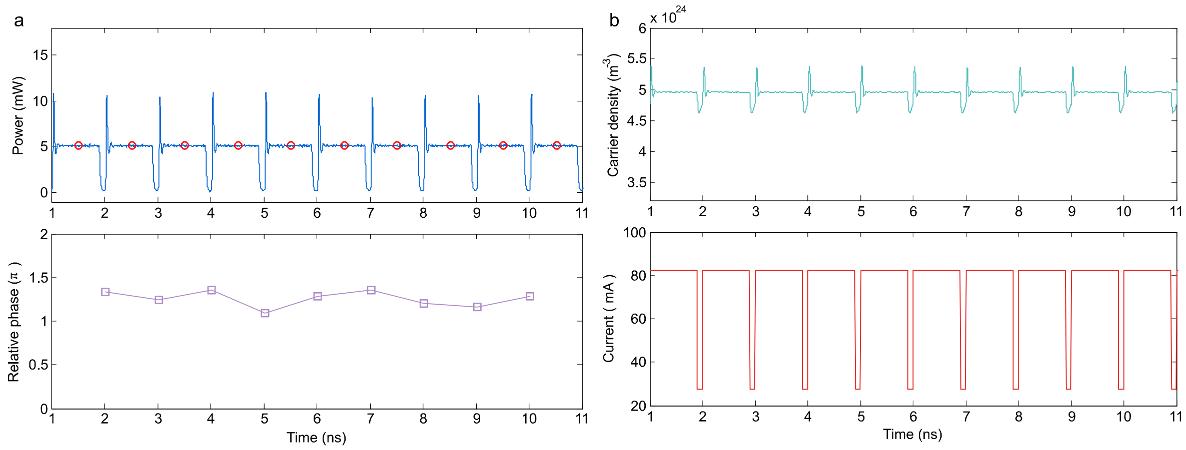

Figure S3: (a) 1 GHz repetition rate, 90% duty cycle, current modulation from 15 mA (lasing threshold), to 70 mA. (b) The high bias current prevents a full depletion of the carrier density and therefore the relative phase is not randomised. Simulation of 10'000 pulses. Mean relative phase $1.24\,\pi$ and $\sigma_{ph} = 0.09\,\pi$.

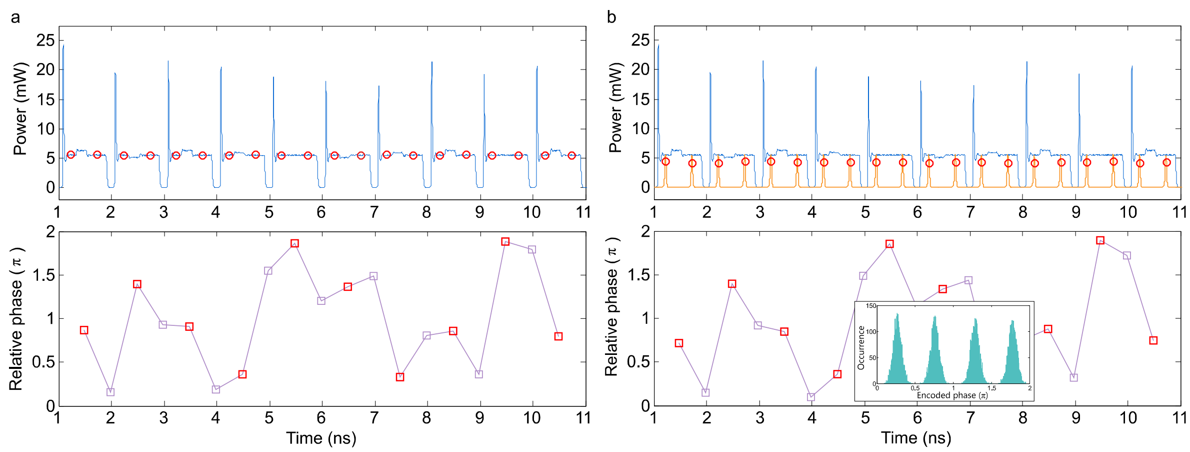

Figure S4: Phase encoded gain-switched pulses. (a) Ultra-short modulations are used to induce a phase shift within two regions of the plateau. 4 phases are meant to be encoded for the BB84 protocol (red squares). Between pulses, the phase is random (purple squares). (b) The phase-encoded pulses are then injected in a secondary laser, in turn gain switched ($I_{pp} = 50$ mA, 40 % duty cycle) to produce short pulses in the flat regions of the phase encoded pulse. The relative phase between the short pulses follows exactly the phase shifts encoded in the seed pulses. Inset: histogram of the relative phases encoded within BB84 pulse pairs (red squares) confirming 4 distinct phase states. Simulation of 10'000 pulses. Phase-encoding modulation I_{π}= 5 mA, duration 200 ps.

2. Supplementary Note 2: Intensity modulation and fluctuations

Conventional approaches to generate decoy states and vacuum states rely on high-speed multi-level intensity modulation using one or more Mach-Zehnder modulators (MZMs). Our QTx chip features a high-speed EAM rather than MZMs, which are generally bulkier: an EAM can fit within 500 microns or less while MZMs are typically at least 4 mm long. Our EAMs have a > 25 dB extinction ratio and it is possible to generate the 3 intensity levels using multi-level RF driving signals. However, in order to keep the driving electronic circuit simple, we generate the decoy and vacuum states by interleaving binary modulation signals driving the pulse generation laser and EAM. In this note, we show that our method also helps avoiding large intensity fluctuations, which can open detrimental side channels as variations in the decoy pulse intensities may lead to underestimations of the phase-error rate. In realizations based on Mach Zehnder Modulators (MZM), the difficulty of stabilising an MZM to the slope of the modulation leads to inter-pulse intensity correlations, or patterning effect: transiting the MZM from one set-point to another introduces intensity deviations that can be larger than the standard deviation (Refs. [33, 34] of the main manuscript).

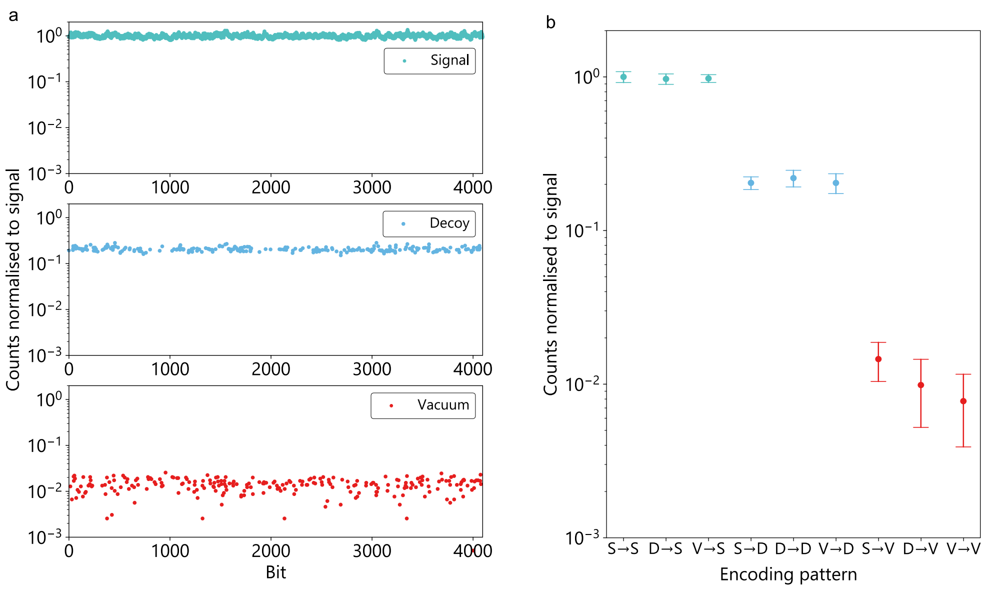

Figure S5: (a) Signal, decoy and vacuum pulse intensities post-selected from a random stream of 4096 pulses. Intensity fluctuations are below 8 % and 12.5% for signal and decoy, respectively. Fluctuations are not relevant for the vacuum counts, which are dominated by the dark counts. (b) Mean intensities and deviations for different encoding patterns. The pattern-induced deviations of the mean value are lower than the standard deviation, evidencing minor inter-pulse correlations. Note that vacuum pulses are 20 dB lower in intensity than the signal pulses, and therefore dominated by the noise; their intensity analysis is not relevant.

In Ref. [34], pattern-induced intensity deviations up to 3 times larger than the standard deviation were reported for the decoy pulses using an MZM-based transmitter. Our approach does not rely on MZMs and therefore prevents strong patterning effect. Fig. S5 a presents plots of the *signal (S)*, *decoy (D)* and *vacuum (V)* pulses extracted from a stream of 4096 random BB84 pulses measured with single photon detectors.

In Fig. S5 b we plot the mean and standard deviations for pulses post-selected according to their predecessor. The pattern-induced intensity deviations are smaller than the standard deviation for both the signal and decoy pulses. The extracted values are reported in Supplementary Table 1.
An alternative approach, based on Sagnac interferometers was proposed and demonstrated to yield even lower patterning [33], however implementing it on chip would have been more complex.

Supplementary Table 1: Characterization of the pattern-induced intensity deviations

Pattern	Standard deviation σ	Pattern-induced deviation σ_P	σ_P/σ
S → S	0.081	0	0
D → S	0.078	0.03	0.38
V → S	0.058	0.023	0.39
S → D	0.095	0.07	0.73
D → D	0.123	0	0
V → D	0.148	0.072	0.49

3. Supplementary Note 3: Comparison with state-of-the-art discrete optics systems

3.1. Loss budget

We start with a comparison of the loss budget between the fibre based system used to demonstrate QKD operation over 10 Mb/s (Ref. [36] of the main manuscript) and the QKD chip system presented in the manuscript. Supplementary Tables 2 and 3 compare the loss budget at Bob (receiver + detector) between the discrete optics (D.O.) system and the chip based system using 2 QRx modules, QRx1 and QRx2, featuring different insertion losses. The main sources of excess loss in the receiver chip are the following:

- The AMZI delay line is lossier on chip than in a fibre. In average, we measured propagation losses of 4.5 ± 2 dB in the on-chip waveguides and delay lines. Some chips perform better than others, as expected due to inevitable waveguide fabrication imperfections. Accounting for all propagation losses and for the fibre array-to-chip coupling losses, we measured a total insertion loss (IL) of 9.5 dB for the packaged chip module QRx 1 and 4.5 dB for QRx 2 (used in the main text). Compared to QRx2, QRx1 suffered from higher on-chip propagation losses (5.5 dB vs 2.7 dB) and higher losses from the optical packaging (4 dB vs 1.8 dB). QRx2 benefitted from low propagation losses (0.3 dB/cm in average) and a refined optical packaging procedure.
- In D.O. systems, the early and late pulses are generated with orthogonal polarizations, which allows sending all the early pulse in the long arm and all the short pulse in the short arm of the receiver AMZI. This is not implemented on our chips, so half of each early and late pulse is split between both arms of the receiver AMZI, causing an effective 3 dB penalty.

Supplementary Table 2: Comparison between the discrete optics system [36] and the chip based system with the QRx1 module

	Discrete optics	QRx 1	Penalty
Polarization routing	0 dB	- 3.0 dB	- 3.0 dB
Bob's optics	- 2.0 dB (Fibre AMZI + Phase Modulator)	- 9.5 dB (QRx1 IL) - 2.5 dB (Phase Modulator)	-10.0 dB
APD detectors	- 5.2 dB (30 % efficiency)	- 10.0 dB (10 % efficiency)	-4.8 dB
Total	7.2 dB	25.0 dB	-17.8 dB

Supplementary Table 3: Comparison between the discrete optics system [36] and the chip based system with the QRx2 module

	Discrete optics	QRx 2	Penalty
Polarization routing	0 dB	- 3.0 dB	- 3.0 dB
Bob's optics	- 2.0 dB (Fibre AMZI + Phase Modulator)	- 4.5 dB (QRx2 IL) - 2.5 dB (Phase Mod.)	- 5.0 dB
APD detectors	- 5.2 dB (30 % efficiency)	- 10.0 dB (10% efficiency)	-4.8 dB
Total	7.2 dB	20.0 dB	-12.8 dB

3.2. Performance comparison

Ref. [36] reported a sift rate of 47.8 Mb/s and a QBER of 3.07 % over 2 dB channel loss. In our work, we measured a 0 dB sift rate of 1.675 Mb/s with QRx 1 and 5.02 Mb/s with QRx 2. The 0 dB QBERs were 3.98 % and 3.72 % for QRx1 and QRx2, respectively.

<u>Sift rate</u>

Compared to Ref. [36], the sift rate is 16.6 dB lower using the packaged module QRx1 and 11.8 dB lower with QRx2, which is consistent with the loss budget figures presented in Supplementary Tables 2 and 3.

<u>QBER</u>

The 16.6 dB penalty corresponds to a distance penalty of 83 km in standard single mode fibre. We expect the QBER to increase due to dark count contributions. Switching from QRx1 to QRx2 saved 5 dB in losses and reduced the QBER by 0.26 %. An extrapolation predicts a base QBER of 3.56 % if all sources of penalty were to be removed.

The excess losses at the receiver have a strong impact on both the measured sift rate and QBER compared to the system of Ref. [36]. This suggests that, at equivalent total channel loss, one can expect comparable performances from the chip-based and discrete optics QKD systems.

4. Supplementary Note 4 : System stability over real fibres

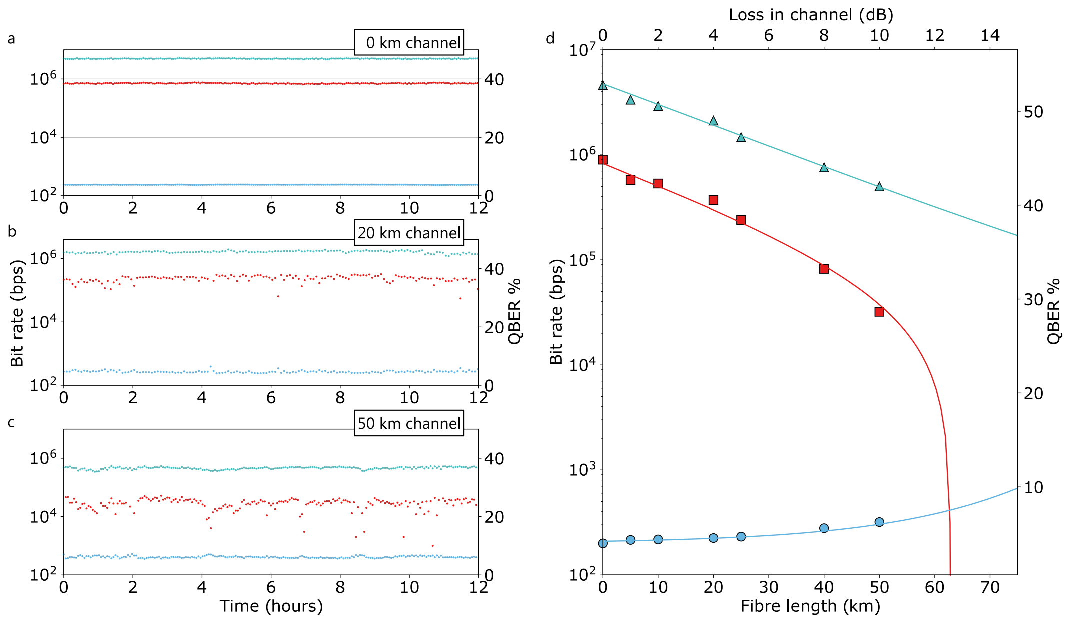

Figure S6: System stability over 12h of uninterrupted operation without user intervention, using fibre spools of different lengths. The traces show the sift rate (teal), the secret key rate (red) and the QBER (cyan, right axis). (a) 0 km, (b) 25 km and (c) 50 km. The average SKRs are 726 kbps, 235 kbps and 28 kbps, respectively. The PA key is generation time is (a) 18 s, (b) 58 s and (c) 204 s. We plot one every 10, 5, and 1 point, respectively, for convenience. (d) Rate-distance measurement with real fibres showing the sift rate (teal, triangles), the secret key rate (red squares) and the QBER (cyan circles, right axis).

The system operates continuously, without the need for user intervention, by implementation of feedback routines. One of the feedback routines aligns the phase encoding of the transmitter with respect to the receiver measurement basis. The second feedback routine works on the temporal alignment of the encoded pulses from the transmitter with respect to the gate window of the receiver's detectors. Fluctuations in the phase encoding occur due to small temperature fluctuations and are corrected at each integration step, in our case for every 1 Mbit of sifted data acquired. The temporal alignment drifts more slowly and is a result of the optical path length changing due to larger temperature transients. We correct the temporal alignment every time a privacy amplified QKD key is generated (94 x 1 Mbit). Stability measurements were acquired over 0 km, 25 km and 50 km long fibre channels in Fig. S6 a-c. Drifts away from the optimum performance seen in the figure are due to sudden temperature fluctuations that take time for the feedback system to recover. No user intervention was needed to re-align the system. In order to run the system over long fibre links (>50 km), where the integration time to acquire 1 Mbit of sift data becomes relatively long, an improved feedback mechanism would be required. For instance, high flux stabilisation pulses would enable sufficient data to be acquired over a short period of time to implement the feedback routine.

Fig. S6 d shows the rate distance performance of the system. All data points were acquired with QRx2 and using real single-mode fibre spools. The 11.6 penalty presented in Supplementary Note 3 accounts for 58 km reduction of the range. With 30 % APDs and a fully passive QRx chip the system would readily tolerate 7.3 dB higher channel loss, extending the current range by 36.5 km in standard single mode fibres.