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

nature photonics

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

Photonic integrated circuits hold great promise in enabling the practical wide-scale deployment of quantum communications; however, despite impressive experiments of component functionality, a fully operational quantum communication system using photonic chips is yet to be demonstrated. Here we demonstrate an entirely standalone secure communication system based on photonic integrated circuits—assembled into compact modules—for quantum random number generation and quantum key distribution at gigahertz clock rates. The bit values, basis selection and decoy pulse intensities used for quantum key distribution are chosen at random, and are based on the output of a chip-based quantum random number generator operating at 4 Gb s^{-1}. Error correction and privacy amplification are performed in real time to produce information-theoretic secure keys for a 100 Gb s^{-1} line speed data encryption system. We demonstrate long-term continuous operation of the quantum secured communication system using feedback controls to stabilize the qubit phase and propagation delay over metropolitan fibre lengths. These results mark an important milestone for the realistic deployment of quantum communications based on quantum photonic chips.

Quantum key distribution (QKD) offers the ultimate resource allowing two distant parties to agree on secret symmetric cryptographic keys regardless of the capabilities of potential eavesdroppers[1]. It replaces the computational security of public key cryptography with physics-based protocols that can be proven information-theoretic secure[2]. In most protocols, photonic qubits are prepared by a transmitter (Alice) in one of two states {0,1} chosen at random along two non-orthogonal bases $\{X,Y\}$ and measured at the receiver (Bob) with random basis selection. An eavesdropper (Eve) cannot measure the exchanged qubits without introducing a measurable error rate δ, which can be used to estimate Bob's information entropy $H(\delta)$. This entropy directly relates to the information gained by the eavesdropper, who is only left with a probability of guessing the key among $2^{N(1-H(\delta))}$ possible candidates, where N is the key length[3,4]. The vulnerability of widely used public key algorithms to attacks by quantum computers[5] strongly stimulated interest in this technology. Although QKD systems based on discrete optics[6] have been demonstrated in many scenarios, reducing their size, weight and power is essential to stimulate a ubiquitous deployment of quantum communications.

Integrated quantum photonics seems to be a natural approach to achieve this goal[7]. In pioneering studies, quantum photonic chips have been fabricated to demonstrate discrete-variable and distributed phase reference protocols with time-bin[8–11], polarization[12–14] or path encoding[15], measurement-device-independent protocols[16–18] and continuous-variable protocols[19]. High potential for metropolitan QKD links has been evidenced in the laboratory[8,11,16–19], using deployed fibres[13] or in free-space links[14]; however, realizing a fully deployable chip-based QKD system proved challenging as it requires overcoming various shortcomings arising from the photonic design, the choice of integrated platform and the integration with high-speed electronics.

For example, although silicon-based chips[9,10,12–17,19] are attractive for complementary metal–oxide–semiconductor integration, they still require discrete optics external laser sources and intensity modulators. Indium phosphide (InP) chips[8,11,18] allow monolithic integration of laser diodes and high-speed phase modulators but the latter require large footprints or high modulation voltages, which hinders the development of scalable electronics. Hybrid integration offers attractive solutions to combine optically active materials and silicon, but it still needs to reach higher levels of maturity[20].

Another substantial limitation is that quantum random number generators (QRNGs) have been missing from these early stage demonstrations. This is an important conceptual drawback as formally the security of a QKD key is bound to the true unpredictability of the information encoded in the qubits and measurement bases. Chip-based QRNGs were successfully demonstrated in recent years[21–25] but have never been used to supply QKD hardware with random numbers in real-time. Aside from bit rates often simply being too low to consider such application, the complexity of generating and processing quantum random numbers in real-time also hindered an efficient interface with quantum communication chips.

Multichip quantum communication system

In this work we introduce a fully deployable QKD system in which quantum photonic chips of different functionalities are interfaced in real-time using compact high-speed electronics (see Fig. 1). Random bits for preparing and measuring the qubits are produced in QRNG chips[21] and are in real time converted into high-speed modulation patterns for the chip-based QKD transmitter (QTx) and receiver (QRx) using field-programmable gate array (FPGA) cores. Photons are detected using fast-gated InGaAs avalanche photodiodes (APDs)[26]. Two local servers execute real-time error correction and privacy amplification. Sifting, photon statistics evaluation, time synchronization and phase stabilization are performed via a 10 Gb s^{-1} optical link between the FPGA cores, enabling autonomous operation over extended periods of time at a stable quantum bit error rate (QBER) and secret key rate (SKR). The system performance in real conditions is further illustrated by interfacing it with a 100 Gb s^{-1} line speed data encryption system (not shown).

Toshiba Europe Ltd, Cambridge, UK. ✉e-mail: taofiq.paraiso@crl.toshiba.co.uk

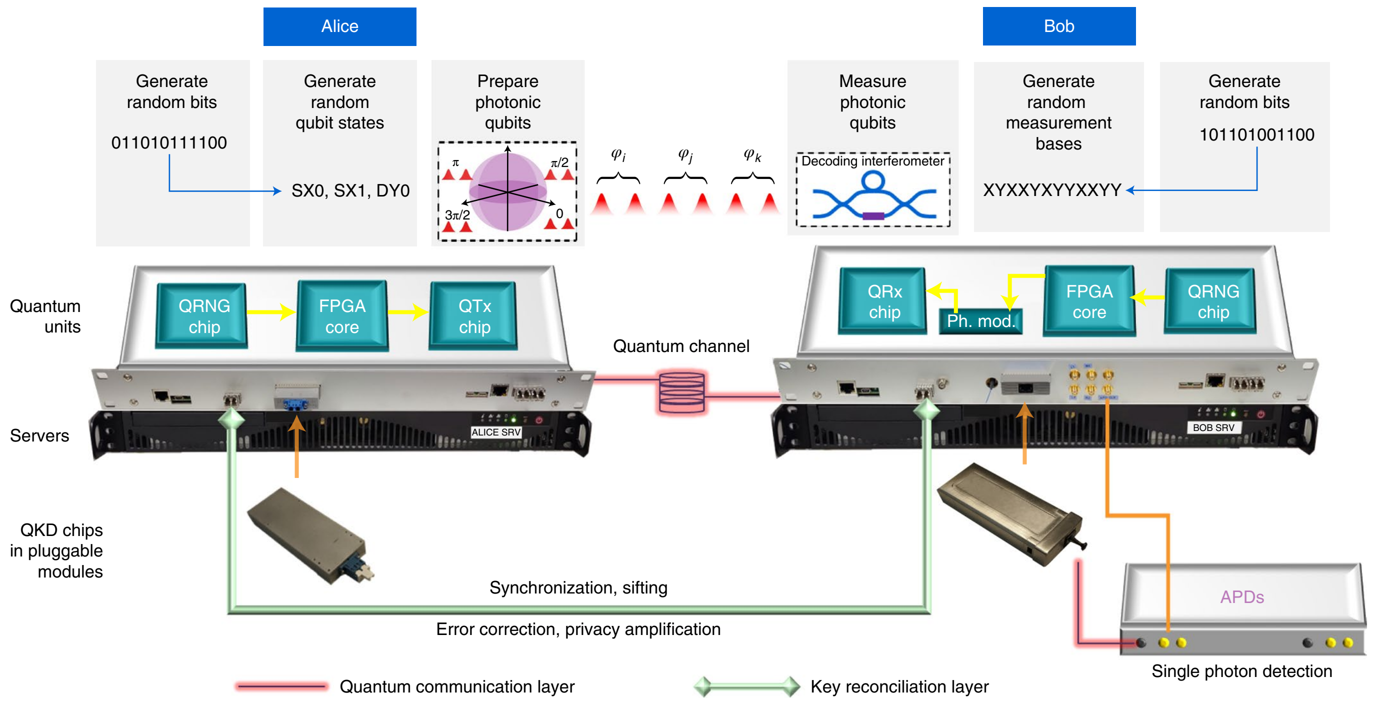

Fig. 1 | Integrated QKD system comprising a QKD transmitter unit (Alice) interfaced with a QKD receiver unit (Bob) and local servers. All layers of the key exchange process are taken into account. Quantum communication takes place over a dedicated fibre. Each unit contains a QRNG chip that continuously produces random numbers, used in the control FPGAs to generate the prepare and measure QKD patterns in real-time. Pairs of coherent pulses are encoded at the transmitter in four equatorial states of the time-bin Bloch sphere—corresponding to the eigenstates of the *X* and *Y* bases—and three intensities, signal (S), decoy (D) and vacuum (V). The pulses are decoded at the receiver in an AMZI preceded by an external phase modulator. The photons are detected in a dual channel fast-gated APD box. The sifting and FPGA synchronization is performed over a 10 Gb s^{-1} optical interface between the quantum units. The sifted keys are continuously transferred to the servers, where the error correction and privacy amplification codes generate the final secret keys in real time.

By addressing all communication layers, we not only prove the practicality of photonic integrated QKD systems but we also establish for the first time their viability for wide-scale deployment.

Pluggable QKD optics. We assembled the QKD units into compact 1U rackmount boxes to promote integration into conventional communication infrastructures. The optical communication hardware is packaged into compact pluggable modules. The QRx and QTx chips are packaged into C-form-factor-pluggable-2 (CFP2) modules (a widespread form-factor in coherent optical communications) to ensure forward compatibility of the system with successive QKD chip generations, making it easily upgradable. Off-the-shelf 10 Gb s^{-1} small-form-factor-pluggable modules are used for the public communication channels.

Protocol. We implement the T12 protocol[27], which is an optimized version of the decoy-state BB84 protocol, at a 1 GHz clock rate. We select four equatorial states of the time-bin Bloch sphere, corresponding to four linear superposition states of the early $|e\rangle$ and late $|l\rangle$ pulses, and into which the information relative to two bases $\{X,Y\}$ and two bits $\{0,1\}$ is encoded in the differential phase φ of the pulse pair $\frac{1}{\sqrt{2}}\left(|e\rangle + e^{i\varphi}\,|l\rangle\right)$ as $\{\varphi\left(0_X\right), \varphi(1_X)\} = \{0, \pi\}$ and $\{\varphi\left(0_Y\right), \varphi(1_Y)\} = \left\{\frac{\pi}{2}, \frac{3\pi}{2}\right\}$. Each QKD unit features an interferometric QRNG chip that exploits spontaneous emission phase noise in gain-switched laser diodes as the quantum source of entropy[21]. True random numbers are extracted continuously to feed the FPGA cores that generate the prepare (*P*) and measure (*M*) pattern streams. At the QTx, the photonic chip generates a 2 GHz pulse train of phase-encoded photons according to the *P* pattern. The emitted photonic qubits travel in the fibre-optic link to reach the QRx, where the pulse train is measured according to the *M* pattern. In the practical implementations of the BB84 protocol one basis (the majority basis, *X*) is used to distil the key and evaluate the quantum bit error rate *e*. The other basis (the minority basis, *Y*) is used to evaluate the phase error rate δ, and estimate the information gained by Eve. Optimally biasing the basis selection probabilities $p\left(X\right) > p(Y)$ ensures a maximum number of events where the *P* and *M* bases match while guaranteeing a sufficient number of events in the minority basis to provide a reliable estimation of δ[28]. In the absence of imperfections, after error correction and privacy amplification, the asymptotic secret key generation rate is given by $R = 1 - H\left(e\right) - H(\delta)$, where $H\left(x\right) = -x\log_2\left(x\right) - \left(1-x\right)\log_2\left(1-x\right)$ is the Shannon binary entropy.

Decoy states. The performance of QKD with weak coherent optical pulses would be severely limited without the use of decoy intensity states[29]. By engineering a photon number splitting attack on the multiphoton terms of the Poissonian distribution, Eve could gain information about the key while remaining undetected[30]. The use of decoy states is the most effective counter-measure to this important vulnerability. Instead of emitting pulses that all obey to the same distribution of photon number, Alice prepares pulses from a finite set of Poissonian distributions with distinct mean photon numbers $\left\{\mu_i \ldots \mu_j\right\}$. The distribution from which a given pulse qubit is emitted is selected randomly, so Eve is incapable of manipulating the statistics of one distribution without introducing errors in the others[29,30]. Three intensities are employed, labelled signal, decoy and vacuum. The signal is used for the actual communication while the other intensities are used to estimate the detection rate and the phase-error rate corresponding to pulses containing only one

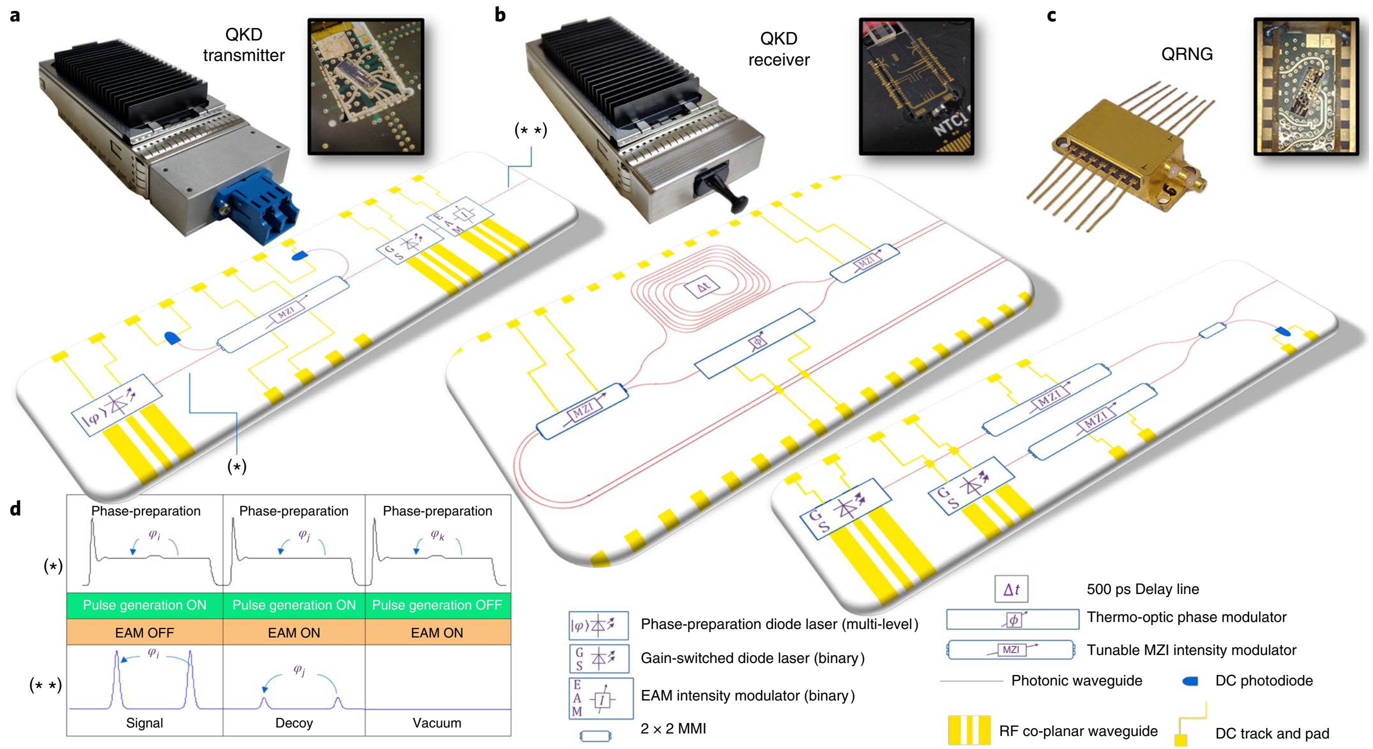

Fig. 2 | QKD chips, modules and circuits. a, The decoy-state QTx chip is a phase-seeded QKD transmitter including two diode lasers and an EAM intensity modulator. The phase preparation diode laser is directly modulated with a multilevel radiofrrequency (RF) signal to generate an 800 ps phase encoded pulse. Optical injection locking into the second diode laser (pulse generation laser) is used to shape the initial pulse into two short (<70 ps) coherent pulses forming the final qubit. The decoy and vacuum states are then generated by interleaving binary signals to the EAM and pulse generation laser. Direct current (DC) photodiodes are used to monitor the optical power on chip. **b**, The QRx chip consists of a fully tunable AMZI with a 500 ps delay line and a thermo-optic phase modulator in the short arm for phase alignment. Both QTx and QRx chips are packaged into pluggable CFP2-type modules (41.7 × 107 × 12.4 mm^3), shown here in their host cages, featuring heatsinks for temperature stabilization. **c**, A QRNG chip and 14-pin butterfly package (12.7 × 30 × 8 mm^3). Two gain-switched lasers diodes interfere in a multimode interferometer (MMI) to measure the quantum randomness from the spontaneous emission phase noise. At the output of the MMI, pulses of random intensities are fibre-coupled to a high-speed photodiode on the QRNG electronic board for detection and post-processing. **d**, An illustration of the operating principles of the QTx chip.

photon, and thereby provide correction terms to the secret key rate[27]. Appropriate choices of the mean photon number per pulse and their respective selection probabilities further improve the protocol efficiency.

Following ref. [27], we encode the bit, basis and intensity variables, which we denote Q, B and I, respectively, where $Q \in \{0, 1\}$, $B \in \{X, Y\}$ and $I \in \{\text{vacuum, signal, decoy}\}$, with probabilities $p(Q=1) = 1/2$, $p(B=Y) = 1/16$ and $p(I=\text{vacuum}) = 1/16$, $p(I=\text{decoy}) = 15/256$.

Integrated quantum photonic modules

All of the chips were designed to be interconnected and exchange photonic qubits at high clock rates. The QTx and QRNG chips are fabricated on InP heterostructures for full monolithic integration of high-bandwidth photon sources, electro-absorption modulators and detectors on a same circuit. Propagation losses (typically a few decibels per centimetre in InP) are not a concern for these functionalities. For the QRx chip, however, low propagation losses (<<1 dB cm^{-1}) are desirable to avoid losing photons before measurement, therefore silicon-based substrates are a better choice than InP.

Decoy-state QTx chip. Figure 2a shows the QTx module and a schematic of the circuit implemented on the chip. We generate all of the states needed for a decoy-state protocol with a minimal number of integrated components using only phase-seeding and electro-absorption modulation (EAM). The phase-seeding circuit was proven to efficiently generate photonic qubits using only two cascaded diode lasers, a phase preparation laser and a pulse generation laser[11,31]. The phase preparation laser is driven with multilevel direct modulation to produce long phase-encoded pulses with a deterministic phase shift between the pulse regions surrounding the modulation. Optical injection locking of the phase-encoded pulses into the gain-switched pulse generation laser is then used to generate pairs of short (<70 ps) coherent pulses forming the time-bin qubits. Furthermore, gain-switching the phase preparation laser allows intrinsic quantum randomization of the global phase of the qubits through spontaneous emission noise. Note that achieving global phase randomization without this feature would require an additional dedicated phase modulator and QRNG. The use of the EAM to modulate the pulse intensity for the decoy protocol further improves previous implementations, which used either off-chip discrete optics intensity modulators or on-chip electro-optic Mach–Zehnder modulators (MZMs). The main benefit of using an EAM instead of MZMs is to drastically reduce the footprint of the on-chip intensity modulation component. InP MZMs are generally 4–5 mm long compared to 300 μm long for the EAMs. As a result, the whole photonic integrated circuit can fit on a 1 mm × 6 mm footprint.

Figure 2d illustrates the operating principles of the QTx chip. Long phase-randomized pulses are generated in the phase preparation laser at 1 GHz and with an 80% duty cycle. The long pulses are injected into the pulse generation laser, gain-switched at 2 GHz to generate short pulses, such that each long pulse of the phase

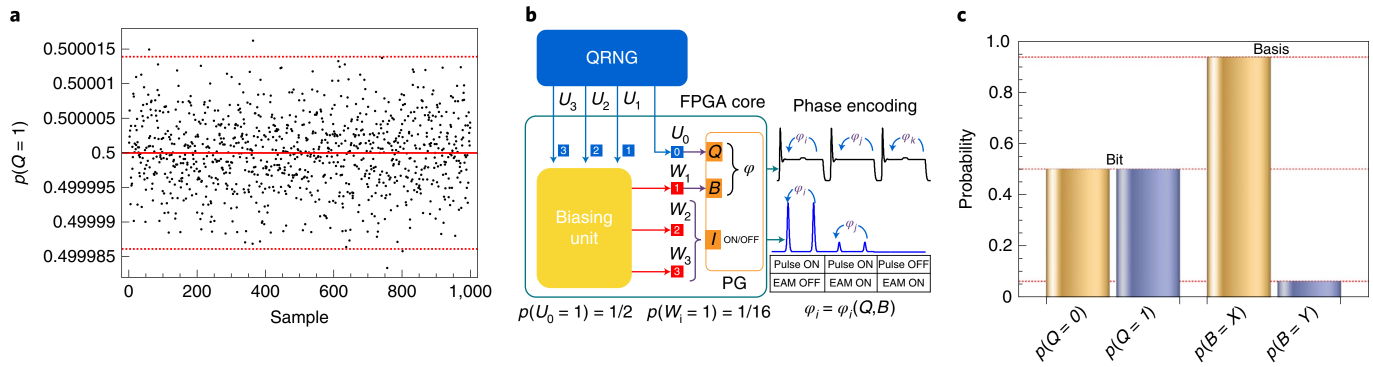

Fig. 3 | Real-time pattern generation from quantum random numbers. a, At the output of the randomness extractor the quantum random numbers are uniformly distributed. The probability of obtaining the value 1 is shown for 1,000 consecutive samples, with each sample comprising 8.6×10^{9} bit of quantum random data. The dashed red lines correspond to the 99% confidence intervals. **b**, The block diagram illustrates the so-called biasing unit of Alice, which is used for the selection of *B* and *I*. The Alice QRNG generates four bits $\{U_0, U_1, U_2, U_3\}$ at every clock cycle. Bit U_0 is unbiased and can be directly used for the qubit encoding *Q*. The remaining bits are input to the biasing unit and processed to output the bits $\{W_1, W_2, W_3\}$ with probabilities set by the protocol. These bits are then processed by the FPGA pattern generator (PG) to generate the driving signals for the encoding of the actual optical pulses. **c**, Experimental probabilities for *Q* and *B* measured on a typical set of 1.2×10^{6} detected events: the bins are within the corresponding 99% confidence intervals (dashed red lines).

preparation laser transfers its coherence to two short pulses of the pulse generation laser by optical injection locking. This generates a 2 GHz pulse train consisting of pairs of phase coherent pulses, with a random phase relation between consecutive pairs, as required for long-distance BB84 protocols[32]. Each pair is therefore an independent coherent superposition of an early and late pulse, $\frac{1}{\sqrt{2}}\left(|e\rangle + e^{i\varphi}\,|l\rangle\right)$. To encode the qubit state (bit, basis), the differential phase φ between the early and late pulses of each pair is encoded by synchronizing ultrashort four-level direct modulations of the optically injected pulse between the two pulses of the pair. The modulation width and amplitude need to be precisely adjusted to generate the four phase states needed to encode the bit and the basis as described above. Supplementary Note 1 describes how the driving conditions may affect the phase randomization and the generation of phase encoded pairs in the light of the diode laser rate equations. The phase encoded pulse pairs are then attenuated to signal intensity. Conventionally, decoy and vacuum states are generated through multilevel modulation of the intensity modulator. Here, as the vacuum state can simply be generated by not triggering the pulse generation laser, we generate the decoy and vacuum states by selectively driving the pulse generation laser and the EAM with interleaved binary modulations (see Fig. 2d, bottom row). The pulses hence generated showed minimal interpulse intensity correlations thus avoiding the patterning effect security loopholes often observed with intensity-modulator-based set-ups[33,34] (see Supplementary Note 2). Overall, only three radiofrequency signals (one multilevel and two binary) are needed to operate the decoy-state QTx chip. This substantially simplifies the driving electronics and improves scalability at the system level.

QRx chip. Our QRx circuit consists of a fully tunable asymmetric Mach–Zehnder interferometer (AMZI) fabricated on a silicon-based chip. The module and the circuit are shown in Fig. 2b. The 2 GHz free-spectral range of the AMZI matches the repetition rate of the attenuated pulse train. The *X*-basis alignment between Alice and Bob is performed using a thermo-optic phase modulator in the short arm of the AMZI. As the QRx chip is fully passive, the measurement basis is selected externally by controlling the phase of the incoming reference pulse using a compact lithium niobate phase modulator mounted on the receiver electronic board. For packaging convenience, the QRx chip input and output waveguides are routed from and to the same facet and interfaced with an identical fibre array inside of the pluggable module (see Fig. 2b). The output of the QRx chip is coupled to 1 GHz gated APDs for the bit detection. We achieve optimal operation of the QRx through precise control over excess losses and thermal phase fluctuations (see Methods).

Insertion losses in a QRx unit result in a penalty in the overall channel range, with main contributions from the QRx module, the phase modulator and the non-ideal APD efficiency. Propagation and fibre alignment losses in the QRx module are subject to statistical fluctuations, and hence the pluggable feature allows us to easily swap and test different QRx modules in a plug-and-play fashion. Although we observed insertion losses up to 9.5 dB insertion losses, comparable with other realizations of AMZI-QRx chips[8,10], the results presented here were obtained with a QRx module featuring 4.5 dB total insertion losses. Details and comparisons on the loss budget and penalty are provided in Supplementary Note 3.

QRNG chip. The interferometric QRNG circuit comprises two independent gain-switched laser diodes brought to interfere in a multimode interferometer yielding a pulse train of random intensities (Fig. 2c). The QRNG chips are packaged into a 14-pin butterfly package and mounted on a standalone printed circuit board that includes a high-speed photodiode and FPGA-based driving and processing electronics[35], operating at 1 GHz. From the raw random numbers generated by an analogue-to-digital converter (ADC) at 8 Gb s^{-1} and following the typical arcsine distribution[21], a real-time randomness extractor produces uniformly distributed random numbers at 4 Gb s^{-1}. At every clock cycle the QRNG processing electronics feeds the QTx and QRx FPGAs with a four-bit word $\{U_0, U_1, U_2, U_3\}$ from a uniform distribution of 0s and 1s such that $P(U_i) = 0.5$ (see Fig. 3a). The FPGAs interpret these continuous streams of words to generate the *P* and *M* patterns in real time. In case of symmetric basis and intensity selections, the FPGA pattern generator can readily encode the *P* pattern by assigning 1 bit to *Q*, 1 bit to *B* and 2 bits to *I*. In the T12 protocol biased selection probabilities are used to improve the SKR. In the case of the QTx, the QRNG word $\{U_0, U_1, U_2, U_3\}$ is therefore interpreted as follows.

The bit U_0 is left unbiased and associated with *Q* (Fig. 3b) to keep the probability of measuring 0 or 1 perfectly even (see Fig. 3c). The other three unbiased bits enter a biasing unit that outputs a three-bit word $\{W_1, W_2, W_3\}$, where each bit W_i follows a binomial distribution with $p(W_i = 1) = 1/16$. Hence, to encode bases and intensities with the desired probabilities,

Table 1 | Performance figures of the QKD chip system in back-to-back configuration and over 10, 25 and 50 km of standard single mode fibre. s.d., standard deviation

Channel loss	Direct link	10 km	25 km	50 km
Measurement duration	2.5 days	5.5 days	0.5 day	0.5 day
SKR	726 kbps	470 kbps	235 kbps	28 kbps
SKR s.d.	35 kbps	110 kbps	52 kbps	12 kbps
QBER	3.72%	4.50%	4.66%	6.15%
QBER s.d.	0.03%	0.26%	0.41%	0.33%
Sift rate	5.02 Mbps	3.1 Mbps	1.62 Mbps	0.46 Mbps
Flux (photons per nanosecond)	0.3	0.3	0.3	0.3
Feedback	Phase (basis)	Phase (basis) and pulse timing	Phase (basis) and pulse timing	Phase (basis) and pulse timing
QKD key block size	98.5 Mb	98.5 Mb	98.5 Mb	98.5 Mb
AES key size	N/A	256 + 96 bit (init.)	256 + 96 bit (init.)	256 + 96 bit (init.)
Average AES keys per second	N/A	1,335	667	79

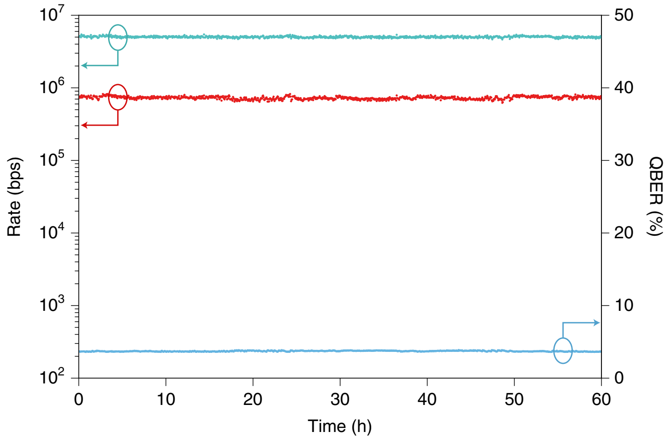

Fig. 4 | Performance and long-term stability. The sifted key rate (teal), SKR (red) and QBER (blue) of the system are shown for a period of 60 h of continuous back-to-back operation. We plot one point per every ten blocks, where one block corresponds to 94 × 1 Mbit of data. The sift rate is 5.02 Mbit s^{-1}, giving one point every 3.13 min. We measure an average SKR of 726 kbps ± 35 kbps and an average QBER of 3.72%.

we associate B and I, respectively to the following outcomes: $W_1 = 1 \rightarrow B = Y$, $\{W_2, W_3\} = \{0, 1\} \vee \{1, 1\} \rightarrow I =$ vacuum, $\{W_2, W_3\} = \{1, 0\} \rightarrow I =$ decoy, $\{W_2, W_3\} = \{0, 0\} \rightarrow I =$ signal (Fig. 3c). The pattern generator unit uses U_0 and W_1 to generate the qubit states, W_2 and W_3 to generate the intensity states. The P pattern is translated into radiofrequency signals that drive the quantum transmitter chip, where the qubit state becomes a phase encoded in the phase preparation laser pulses and the intensity state becomes binary ON/OFF signals to trigger the pulse preparation laser and the EAM as explained above.

Results

Sifting and secret key generation. The key reconciliation is done between Alice and Bob FPGAs communicating over an optical link. In Bob, the QRx-FPGA proceeds to the readout of the detectors and sends the time tagged successful detection events to Alice where the QTx-FPGA proceed to the sifting of the events with matched P and M bases. The count imbalance relative to the mismatched basis events is used to calculate a real-time feedback parameter for phase stabilization (see Methods). A number of counters are implemented to record significant extents to analyse the photon statistics for the three different intensities. The FPGAs then transfer the sifted keys and the statistics data to Alice's and Bob's servers. An error-correction code corrects for the bit flip errors between the sifted keys[36]; e and δ are evaluated from the error counts in the X and Y bases and from the photon statistics, following the finite-size statistical analysis and parameter estimation procedure of the T12 protocol[27]. A privacy amplification algorithm is finally applied to produce the final information-theoretic secure keys[36].

Performance and long-term stability. We first assessed the system's stability in back-to-back operation. Figure 4 shows the result of a 2.5-day-long experiment where we recorded the sifted rate, secure key rate and QBER. The signal, decoy and vacuum fluxes were set to 0.3, 0.06 and 0 photons per nanosecond, respectively. These values were optimized to provide the highest secure key rate for the given QBER and channel loss. The APDs operated with 10% efficiency and a dark count rate of 7 kc s^{-1}. The sifted keys were generated continuously at a rate of 5.02 Mbps. Each data point corresponds to one block of data containing 94 × 1 Mbit of sifted data. From each block, the error correction and privacy amplification algorithms produce a certified quantum key, at a QBER of 3.72% and secure key rate of 726 kbps ± 35 kbps over the measurement duration. This remarkably low SKR standard deviation indicates that all the layers of the photonic integrated QKD system, including QRNG, qubit preparation and measurement, and final post-processing are implemented and stabilized optimally.

We then acquired measurements over 10 km of standard SMF-28e fibre, where our feedback system also corrected the thermal induced fibre length fluctuations. The fibre added 1.8 dB excess loss, resulting in a sift rate of 3.1 Mbps. Once optimized, we achieved an average QBER of 4.5% and an average secure key rate of 470 ± 110 kbps over 5.5 days of continuous measurement. This can readily serve one-time-pad encryption of one-to-one video calls with video codecs operating up to 384 kbps. Although a 10 km distance is well suited for metropolitan networks with trusted-node architecture, as demonstrated in the Cambridge Quantum Network[37], we also confirmed the capability of our feedback system to handle longer metropolitan links during extended periods of time and without user intervention. In Table 1 we report SKRs of 235 kbps and 28 kbps over 25 and 50 km, respectively (also see Supplementary Note 4).

Interface with classical cryptography system. We illustrate real-world applicability of the system by connecting our system to industrial-grade 100 Gb s^{-1} encryptors (Fig. 5a). Our key management

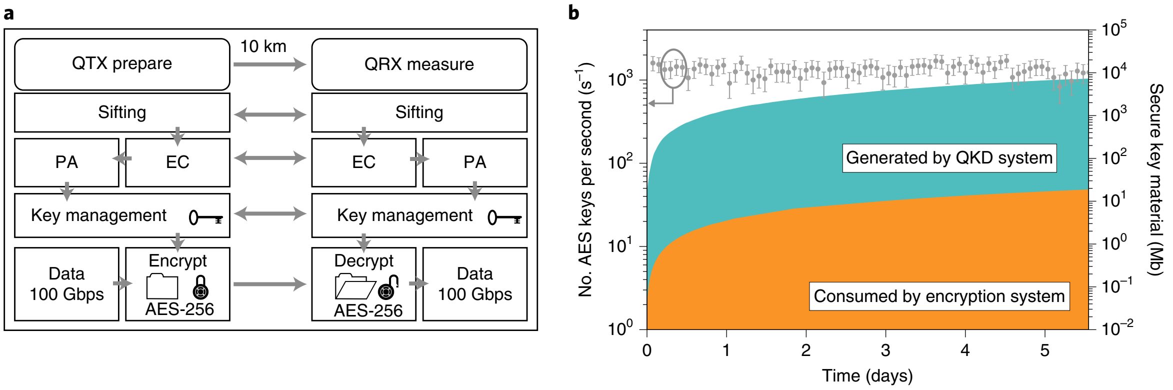

Fig. 5 | Applicability of the photonic integrated QKD system. a, The interface between the photonic integrated quantum communication system and the 100 Gb s^{-1} line speed data encryption system via a dedicated key management system. EC, error correction; PA, privacy amplication; AES, advanced encryption standard. **b**, The encryption key generation rate (left axis) and the total amount of secure keys generated and consumed in 5.5 days of continuous operation over a 10 km fibre link. The key material was generated at an equivalent average rate of 1,335 AES-256 keys per second. Data is plotted every 200 min. The error bars report the overall SKR s.d.

software layer provides a route to serve quantum keys ready for use by a third-party classical cryptography system[38] using the standardized ETSI GS QKD 014 interface[39]. We further added duplex fibres of the same length as the quantum channel to the public channel, demonstrating a quantum secure communication system ready to load with high-bandwidth data. The encryption system used here consumed 352 bit of key material per minute (256 bit of an advanced encryption standard or AES key and 96 bit initialization vector for the algorithm). Owing to the high bit rate of our photonic integrated QKD system we are able to sustain the uninterrupted operation of the encryptors flawlessly. Figure 5b shows that our quantum cryptography system is capable of serving an average of 1,335 keys per second, which could therefore serve multiple encryption applications simultaneously. The figures are 10, 25 and 50 km and reported in Table 1. Over the 5.5 days of operation at 10 km, the encryption system consumed 8,061 AES keys to encrypt/decrypt the equivalent of 48 Pb of data.

Miniaturizing the optical hardware onto small footprint chips offers means to drastically reduce the production cost and replicate QKD systems in large volumes. Targeted innovations shall further improve performance and miniaturization of such systems. For example, progress toward the integration of single photon detectors integrated onto waveguide chips[40–42] recently led to the demonstration of a detector integrated QKD receiver[43]. We also expect the capabilities of quantum photonic integrated circuits to improve considerably in the near future, with the continuous efforts to develop ultra-low loss waveguide chips[44,45] non-reciprocal elements[46], low-modulation-voltage electro-optic in-phase/quadrature modulators[47] and hybrid integration schemes[20]. Last but not least, approaches to combine photonic and electronic integrated circuits[48] will soon enable the development of chip-sized systems. We anticipate our demonstration to serve as a stepping stone for the development of integrated quantum photonics and to stimulate further developments towards compact quantum communication components widely deployable within our existing network infrastructure.

Online content

Any methods, additional references, Nature Research reporting summaries, source data, extended data, supplementary information, acknowledgements, peer review information; details of author contributions and competing interests; and statements of data and code availability are available at https://doi.org/10.1038/s41566-021-00873-0.

Received: 11 December 2020; Accepted: 11 August 2021;
Published online: 21 October 2021

References

1. Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **74**, 145 (2002).
2. Gottesman, D., Lo, H.-K., Lütkenhaus, N. & Preskill, J. Security of quantum key distribution with imperfect devices. *Quant. Inf. Comput.* **5**, 325–360 (2004).
3. Koashi, M. Efficient quantum key distribution with practical sources and detectors. Preprint at http://arxiv.org/abs/quant-ph/0609180 (2006).
4. Xu, F., Ma, X., Zhang, Q., Lo, H.-K. & Pan, J.-W. Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.* **92**, 25002 (2020).
5. Arute, F. et al. Quantum supremacy using a programmable superconducting processor. *Nature* **574**, 505–510 (2019).
6. Qiu, J. Quantum communications leap out of the lab. *Nature* **508**, 441–442 (2014).
7. Wang, J., Sciarrino, F., Laing, A. & Thompson, M. G. Integrated photonic quantum technologies. *Nat. Photon.* **14**, 273–284 (2020).
8. Sibson, P. et al. Chip-based quantum key distribution. *Nat. Commun.* **8**, 13984 (2017).
9. Sibson, P. et al. Integrated silicon photonics for high-speed quantum key distribution. *Optica* **4**, 172–177 (2017).
10. Geng, W. et al. Stable quantum key distribution using a silicon photonic transceiver. *Opt. Express* **27**, 29045–29054 (2019).
11. Paraïso, T. K. et al. A modulator-free quantum key distribution transmitter chip. *npj Quantum Inf.* **5**, 1–6 (2019).
12. Ma, C. et al. Silicon photonic transmitter for polarization-encoded quantum key distribution. *Optica* **3**, 1274–1278 (2016).
13. Bunandar, D. et al. Metropolitan quantum key distribution with silicon photonics. *Phys. Rev. X* **8**, 21009 (2018).
14. Avesani, M. et al. Full daylight quantum-key-distribution at 1550 nm enabled by integrated silicon photonics. *npj Quantum Inf.* **7**, 93. (2019).
15. Ding, Y. et al. High-dimensional quantum key distribution based on multicore fiber using silicon photonic integrated circuits. *npj Quantum Inf* **3**, 25 (2017).
16. Cao, L. et al. Chip-based measurement-device-independent quantum key distribution using integrated silicon photonic systems. *Phys. Rev. Applied* **14**, 11001 (2020).
17. Wei, K. et al. High-speed measurement-device-independent quantum key distribution with integrated silicon photonics. *Phys. Rev. X* **10**, 31030 (2020).
18. Semenenko, H. et al. Chip-based measurement-device-independent quantum key distribution. *Optica* **7**, 238–242 (2020).
19. Zhang, G. et al. An integrated silicon photonic chip platform for continuous-variable quantum key distribution. *Nat. Photon.* **13**, 839–842 (2019).
20. Elshaari, A. W., Pernice, W., Srinivasan, K., Benson, O. & Zwiller, V. Hybrid integrated quantum photonic circuits. *Nat. Photon.* **14**, 285–298 (2020).
21. Roger, T. et al. Real-time interferometric quantum random number generation on chip. *J. Opt. Soc. Am. B* **36**, B137 (2019).
22. Abellan, C. et al. Quantum entropy source on an InP photonic integrated circuit for random number generation. *Optica* **3**, 989–994 (2016).

23. Rudé, M. et al. Interferometric photodetection in silicon photonics for phase diffusion quantum entropy sources. *Opt. Express* **26**, 31957–31964 (2018).
24. Raffaelli, F. et al. A homodyne detector integrated onto a photonic chip for measuring quantum states and generating random numbers. *Quantum Sci. Technol.* **3**, 25003 (2018).
25. Raffaelli, F. et al. Generation of random numbers by measuring phase fluctuations from a laser diode with a silicon-on-insulator chip. *Opt. Express* **26**, 19730–19741 (2018).
26. Comandar, L. C. et al. Room temperature single-photon detectors for high bit rate quantum key distribution. *Appl. Phys. Lett.* **104**, 21101 (2014).
27. Lucamarini, M. et al. Efficient decoy-state quantum key distribution with quantified security. *Opt. Express* **21**, 24550–24565 (2013).
28. Lo, H.-K., Chau, H. F. & Ardehali, M. Efficient quantum key distribution scheme and a proof of its unconditional security. *J. Cryptol.* **18**, 133–165 (2005).
29. Lo, H.-K., Ma, X. & Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **94**, 230504 (2005).
30. Hwang, W.-Y. Quantum key distribution with high loss: toward global secure communication. *Phys. Rev. Lett.* **91**, 57901 (2003).
31. Yuan, Z. L. et al. Directly phase-modulated light source. *Phys. Rev. X* **6**, 031044 (2016).
32. Lo, H.-K. & Preskill, J. Security of quantum key distribution using weak coherent states with nonrandom phases. *Quant. Inf. Comput.* **8**, 431–458 (2007).
33. Roberts, G. L. et al. Patterning-effect mitigating intensity modulator for secure decoy-state quantum key distribution. *Opt. Lett.* **43**, 5110–5113 (2018).
34. Yoshino, K.-I. et al. Quantum key distribution with an efficient countermeasure against correlated intensity fluctuations in optical pulses. *npj Quantum Inf* **4**, 8 (2018).
35. Marangon, D. G. et al. Long-term test of a fast and compact quantum random number generator. *J. Lightwave Technol.* **36**, 3778–3784 (2018).
36. Yuan, Z. et al. 10-Mb/s quantum key distribution. *J. Lightwave Technol.* **36**, 3427–3433 (2018).
37. Dynes, J. F. et al. Cambridge quantum network. *npj Quantum Inf.* **5**, 101 (2019).
38. Tanizawa, Y., Takahashi, R., Sato, H. & Dixon, A. R. in *ICUFN 2017. July 4 (Tue.)-July 7 (Fri.), 2017, Milan, Italy: the Ninth International Conference on Ubiquitous and Future Networks* 880–886 (IEEE, 2017).
39. *Quantum Key Distribution (QKD); Protocol and Data Format of REST-based Key Delivery API* GS QKD 014 v.1.1.1 (European Telecommunications Standards Institute, 2019).
40. Ceccarelli, F. et al. Recent advances and future perspectives of single-photon avalanche diodes for quantum photonics applications. *Adv. Quantum Technol.* **4**, 2000102 (2021).
41. Reithmaier, G. et al. On-chip time resolved detection of quantum dot emission using integrated superconducting single photon detectors. *Sci Rep* **3**, 1–6 (2013).
42. Gyger, S. et al. Reconfigurable photonics with on-chip single-photon detectors. *Nat. Commun.* **12**, 1–8 (2021).
43. Beutel, F., Gehring, H., Wolff, M. A., Schuck, C. & Pernice, W. Detector-integrated on-chip QKD receiver for GHz clock rates. *npj Quantum Inf* **7**, 40 (2021).
44. Roeloffzen, C. G. H. et al. Low-loss Si_3N_4 TriPleX optical waveguides: technology and applications overview. *IEEE J. Select. Topics Quantum Electron.* **24**, 1–21 (2018).
45. Liu, J. et al. High-yield, wafer-scale fabrication of ultralow-loss, dispersion-engineered silicon nitride photonic circuits. *Nat. Commun.* **12**, 2236 (2021).
46. Yang, K. Y. et al. Inverse-designed non-reciprocal pulse router for chip-based LiDAR. *Nat. Photon.* **14**, 369–374 (2020).
47. Ogiso, Y. et al. Over 67 GHz bandwidth and 1.5 V V_π InP-based optical IQ modulator with n–i–p–n heterostructure. *J. Lightwave Technol.* **35**, 1450–1455 (2017).
48. Yao, W. et al. Towards the integration of InP photonics with silicon electronics: design and technology challenges. *J. Lightwave Technol.* **39**, 999–1009 (2021).

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Methods

1. **QKD Receiver chip module stabilization**. A high interference contrast and high phase stability are crucial elements of QKD receiver circuits. In particular we need to ensure balanced detection probabilities for the 0 and 1 bits. To this end, the tunable MZI splitters ensure that the interferences at the output of the AMZI take place under perfectly symmetric conditions. The input splitter compensates for the excess propagation loss in the delay line while the output coupler is precisely tuned to realize a 50:50 splitting ratio beam splitter. It is important to maintain a very stable phase reference at the QRx. In particular, temperature fluctuations should be avoided. Using a thermistor flip-chip-mounted directly onto the QRx chip for a fast response, we are able to stabilize the temperature down to 0.001 °C (root mean square).
2. **Signal phase stabilization**. Once the QRx phase reference is set the stabilization of the system is done by acting on the phase of the transmitting signal bases. Sparsely distributed stabilization pulses are commonly used to stabilize the basis alignment. Mismatched events where the P and M bases do not match are commonly dismissed during the sifting process. Here we use the mismatched events to generate a directional feedback parameter. The mismatched probability is approximately 1/16 (eight times the typical 1/128 probability of stabilization pulse), which allows determining the feedback parameter with high accuracy and speed while avoiding dismissing more pulses than needed. Most importantly, a simple comparison of the APD counts cumulated during the integration time yields a directional feedback parameter that can readily be used in the phase stabilization loop. We note that a similar approach has been discussed in ref. [49].
3. **Pulse timing stabilization**. In addition to constant feedback of the transmitter sending basis, we also add feedback to the pulse timing with respect to the shared clock. This feedback again acts on the transmitter and shifts the pulses in time, such that they are centred within the gating window of the APDs at the receiver. This is required due to fluctuations in the optical path length between the two QKD units when using real fibres. Changes in the optical path length through the fibre are due to transients in temperature, affecting the fibre refractive index. In our use case this effect was particularly apparent due to use of a fibre spool whereby the entire length of fibre undergoes a uniform temperature transient. The feedback routine runs after each QKD key is generated (approximately once per minute) and adjusts the pulse timing to find the optimum timing within the APD gate. In Fig. 5b, periodic variations reflect strong length variations of the 10 km fibre. Note that the atmospheric conditions of the test room were left without active stabilization in this real-setting experiment.

Data availability

The datasets generated during and/or analysed during the current study are available from the corresponding author on reasonable request.

References

49. Wang, D., Song, X., Zhou, L. & Zhao, Y. Real-time phase tracking scheme with mismatched-basis data for phase-coding quantum key distribution. *IEEE Photon. J.* **12**, 1–7 (2020).

Acknowledgements

We thank M. Lucamarini and P. R. Smith for fruitful discussions. This work has been funded by the Innovate UK project AQUASEC, as part of the UK National Quantum Technologies Programme. I.D.M. acknowledges funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement no. 675662.

Author contributions

T.K.P., T.R., M.S., D.G.M., Z.Y. and A.J.S. conceived the experiment. T.K.P., T.R., M.S and D.G.M. developed the photonic integrated modules. T.R., I.D.M. and T.K.P. characterized the photonic modules. D.G.M. characterized and optimized the QRNG units. M.S. and D.G.M. developed the QKD and QRNG control electronics. T.R. assembled the systems, developed the stabilization routines and acquired the long-term data. R.I.W and J.F.D. assisted with the installation of the data encryption systems. All authors contributed to the data analysis. T.K.P. wrote the manuscript with contributions from all authors. T.K.P., Z.Y. and A.J.S. supervised the project.

Competing interests

The authors declare no competing interests.

Additional information

Supplementary information The online version contains supplementary material available at https://doi.org/10.1038/s41566-021-00873-0.

Correspondence and requests for materials should be addressed to Taofiq K. Paraïso.

Peer review information *Nature Photonics* thanks Feihu Xu and the other, anonymous, reviewer(s) for their contribution to the peer review of this work.

Reprints and permissions information is available at www.nature.com/reprints.