PHOTONICS Research

High-speed integrated QKD system

Rebecka Sax,[1,*] Alberto Boaron,[1] Gianluca Boso,[1,2] Simone Atzeni,[3,4] Andrea Crespi,[3,4] Fadri Grünenfelder,[1] Davide Rusca,[1] Aws Al-Saadi,[5] Danilo Bronzi,[5] Sebastian Kupijai,[5] Hanjo Rhee,[5] Roberto Osellame,[3,4] and Hugo Zbinden[1]

[1]Group of Applied Physics, University of Geneva, 1205 Genève, Switzerland
[2]ID Quantique SA, 1227 Genève, Switzerland
[3]Institute for Photonics and Nanotechnologies and NO-IFN, CNR-IFN, 20133 Milano, Italy
[4]Dipartimento di Fisica, Politecnico di Milano, 20133 Milano, Italy
[5]Sicoya GmbH, 12489 Berlin, Germany
*Corresponding author: rebecka.sax@unige.ch

Received 18 November 2022; accepted 6 April 2023; posted 7 April 2023 (Doc. ID 481475); published 25 May 2023

Quantum key distribution (QKD) is nowadays a well-established method for generating secret keys at a distance in an information-theoretically secure way, as the secrecy of QKD relies on the laws of quantum physics and not on computational complexity. In order to industrialize QKD, low-cost, mass-manufactured, and practical QKD setups are required. Hence, photonic and electronic integration of the sender's and receiver's respective components is currently in the spotlight. Here we present a high-speed (2.5 GHz) integrated QKD setup featuring a transmitter chip in silicon photonics allowing for high-speed modulation and accurate state preparation, as well as a polarization-independent low-loss receiver chip in aluminum borosilicate glass fabricated by the femtosecond laser micromachining technique. Our system achieves raw bit error rates, quantum bit error rates, and secret key rates equivalent to a much more complex state-of-the-art setup based on discrete components [A. Boaron *et al.*, Phys. Rev. Lett. 121, 190502 (2018)].

https://doi.org/10.1364/PRJ.481475

1. INTRODUCTION

The security of the exchange of an encrypted message is an extremely relevant issue in today's society, as disastrous consequences can arise when it is compromised. One rising threat is the quantum computer, which would be able to efficiently crack the current most-used encrypting techniques [1] and whose technology matures as the authors are writing this article [2,3]. Hence, the natural entry of quantum key distribution (QKD), which establishes an information-theoretically secure key exchange and provides long-term security.

Since the first proposal of a QKD protocol in 1984 [4] and its first experimental realization in 1992 [5], more protocols and a multitude of experiments have been established. This global enthusiasm has resulted in enormous increase in the communication distance (using fiber [6–8], as well as free space [9]) and in the secret key rate (SKR) [10,11].

In order to industrialize QKD and to merge it with existing networks, a vision of integrated transmitters and receivers separated at metropolitan distances seems rather judicious. The miniaturization of such systems is notably important, with advantages in terms of low cost, mass production, scalability, simple stabilization in temperature, and compatibility with CMOS-production.

The first realization of a fully integrated QKD system (both the transmitter and receiver integrated) consisted of a silicon transmitter and a SiO_xN_y receiver operating at 1.72 GHz clock rate, using the COW protocol at 20 km distance separation [12]. Subsequently, several integrated implementations have been reported for various QKD schemes [13–22]. Some included an integrated laser [13–15], and others presented hybrid versions that maintain one of the components as non-integrated (either the transmitter or the receiver device, or one of their sub-components) [14–17]. Integrated detectors on-chip have also been realized [23].

Here we present a 2.5 GHz integrated QKD system, the fastest integrated system to our knowledge [24], which features a precise state preparation and a polarization-independent receiver. At a distance of 151.5 km of standard single-mode fiber (SMF), we obtain an SKR of 1.3 kb/s using InGaAs/InP negative feedback avalanche photodiodes. We further demonstrate extremely low quantum bit error rates (QBERs) ($QBER_z$ of 0.9% and ϕ_z of 2.2%) using superconducting nanowire single-photon detectors (SNSPDs) at a distance of 202.0 km, thereupon raising the bar of the state-of-the-art integrated QKD and further laying the groundwork for its use.

2. QKD PROTOCOL

We apply a three-state BB84 protocol using the one-decoy state method [25,26] with time-bin encoding. The three states, and their respective decoys, prepared by Alice are shown in Fig. 1. They belong to one of the two bases, Z and X, and they are chosen at random. The two states in the Z basis are

$$|0\rangle = |\alpha\rangle_E|0\rangle_L, \tag{1}$$

$$|1\rangle = |0\rangle_E|\alpha\rangle_L. \tag{2}$$

The subscript E stands for early, L for late, and $|\alpha\rangle$ for a weak coherent state. The state in the X basis is

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle). \tag{3}$$

Qubits detected in the Z basis will undergo a time-of-arrival measurement and constitute the raw key. In order to preserve security, a second basis, the X basis, is used to check for any eavesdropping attempts. Qubits detected in the X basis will pass through an imbalanced Mach–Zehnder interferometer (imb-MZI). In an intuitive way, if an eavesdropper attempts to make a measurement on one of the states in the Z basis (in order to gain information about the key), the coherence of the state $|+\rangle$ will be altered, which will generate errors in the X basis [27].

3. EXPERIMENTAL SETUP

An overview of the full QKD setup is depicted in Fig. 2. Alice, the transmitter, and Bob, the receiver, are connected via a quantum channel (QC) and a service channel (SC). The former serves for guiding the quantum encoded states and the latter for classical (public, but authenticated) communication between the parties. Each of the two apparatuses is controlled by a field-programmable gate array (FPGA), which also allows for synchronization and communication of the two parties, via the SC.

Regarding the optical elements, the transmitter encompasses a distributed feedback (DFB) laser with a filter, a photonic integrated circuit (PIC), and a dispersion compensating fiber (DCF). Phase-randomized pulses of light at a repetition rate of 2.5 GHz and a full width at half maximum of around 31 ps are generated by a gain-switched high-bandwidth DFB laser at

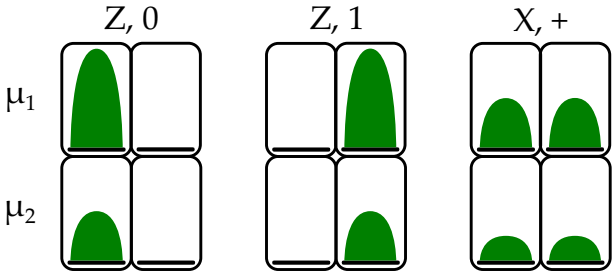

Fig. 1. Encoding of the states sent by Alice. Z and X are the bases in which the states $|0\rangle$, $|1\rangle$ and, $|+\rangle$, respectively, live. μ_1 and μ_2 correspond to the two mean photon numbers used for the one-decoy state protocol [26].

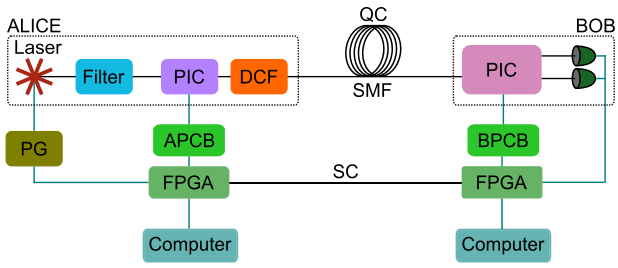

Fig. 2. Simplified schematic of the experimental setup. PIC, photonic integrated circuit; DCF, dispersion compensating fiber; QC, quantum channel; SMF, single-mode fiber; PG, pulse generator; APCB, Alice printed circuit board (PCB); BPCB, Bob PCB; FPGA, field-programmable gate array; SC, service channel. Black lines correspond to optical links, and blue lines correspond to electrical connections.

1550 nm (Gooch and Housego). The pulse train enters the integrated transmitter chip where the three states and their decoys are produced at random using the following components: imb-MZI, intensity modulator (IM), and variable optical attenuators (VOAs). The probability to select the basis Z (p_z) and X (p_x) is 0.67 and 0.33, respectively. The random numbers used to choose the states are produced by Advanced Encryption Standard (AES) cores seeded by a quantum random number generator (QRNG), Quantis from ID Quantique SA. Upon exiting the chip, light pulses travel through the DCF, which consists of specially fabricated fiber with a large negative dispersion coefficient. It will, hence, pre-compensate all the chromatic dispersion created on the trip from Alice to Bob in the QC. For example, 7 km of DCF compensates the chromatic dispersion from 50 km of SMF. The QC consists of SMF with around 0.2 dB/km losses.

On the receiver side, the integrated part consists of a passive beam splitter and an imb-MZI. The effective splitting ratio for the Z and X bases, i.e., taking into account different losses in respective optical paths, is 94/6. The imbalance of the interferometer of Bob should be ideally the same as that of Alice, i.e., 200 ps. However, due to fabrication uncertainties, a delay difference of around 1.6 ps between the two interferometers is measured using optical low-coherence interferometry. The main effect of a delay difference is on the QBER in the X basis, QBER_x, as it leads to a reduced interference of the pulses in the imb-MZI. The relative phase of their interferometers is actively adjusted by acting on the phase of Alice's interferometer in such a way that the two pulses interfere destructively in the output we monitor in the X basis. A feedback loop is locked to minimize the number of detections in this output. It should be noted that, since the occurrences are already low, the active adjustment will be more difficult with increased channel loss due to the, at that point, even lower statistics. The second output of the imb-MZI on the receiver side is not monitored.

The (off-chip) single-photon detectors (SPDs) adopted for our main experiment are InGaAs/InP negative feedback single-photon avalanche diodes (SPADs) cooled by a free-piston Stirling cooler to around −85°C [28]. The timing jitter of the SPADs is below 100 ps, the dark count rates are below 120 counts per second, and the detector efficiency is around

20%. For the characterization of our system, we also use in-house-made superconducting-nanowire single-photon detectors (SNSPDs) cooled at 0.8 K [29]. These detectors feature low timing jitter (around 40 ps), negligible after-pulsing probability, high detector efficiency (around 80 %), and low dark count rates ($d_z = 200$ Hz, $d_x = 100$ Hz). The SPADs are used for the experiment as these detectors are more mature than SNSPDs for practical real-world applications. It should be noted that the fixed 94/6 splitting ratio of the integrated beam splitter on Bob's chip is suited for intermediate distances in this proof-of-principle experiment. Indeed, for short distances, the large number of photons in the Z basis would rapidly saturate the SPADs, whereas for long distances too few detections in the X basis would give rise to non-negligible dark count contribution. However, versatility of the system could be easily increased by replacing the passive beam splitter at the receiver side with a tunable Mach–Zehnder interferometer.

4. INTEGRATED TRANSMITTER

Several challenges arise in the realization of integrated systems for QKD purposes depending on the protocol one uses. For our considerations, due to our high clock rate, we need accurate modulation of the quantum states at high frequencies on the transmitter side. Indeed, accuracy is reflected on the extinction ratio (ER) of the quantum states and consequently on the QBER. Moreover, for time-bin encoding, the platform must allow for the implementation of an MZI with high imbalance.

We developed an integrated chipset based on silicon photonics, with the formerly mentioned qualities for the transmitter, in collaboration with Sicoya GmbH. It consists of a PIC, which is as small as 4.50 mm × 1.10 mm and an adjacent electronic driver integrated circuit (EIC) 4.50 mm × 0.75 mm (see Fig. 3). It is highly advantageous to use silicon photonics for our system as now most of the expensive electronics are on-chip, hence allowing for high component density and small footprints. As can be seen in Fig. 3, the integrated circuits (ICs) are glued on and bonded to a small printed circuit board (PCB). This PCB is combined with a larger one (APCB in Fig. 2), which provides the all electronic signals necessary to control the different components of the chip. It is further connected to a computer-controlled FPGA, as shown in Fig. 2. Light is coupled to the PIC via a fiber array and a grating coupler. The chip is temperature stabilized at 45°C using a standard Peltier cooler/heater placed under the host PCB of the PIC.

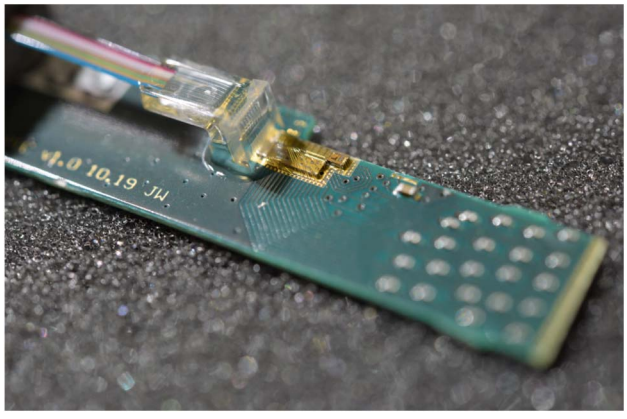

Fig. 3. Photo of the transmitter integrated circuit.

The chips were fabricated in the 0.13 μm SG25PIC SiGe bipolar-complementary metal–oxide semiconductor (BiCMOS) process at the Leibniz Institute for High Performance Microelectronics (IHP) in Frankfurt (Oder), Germany, using 200 mm silicon-on-insulator (SOI) wafers and 248 nm deep ultraviolet (DUV) lithography [30]. The nanowires are embedded within the 220 nm thick silicon device layer of the SOI substrate. The SOI rib waveguides have dimensions of 220 nm × 450 nm and are fabricated in a shallow trench process. The etching depth of the photonic structures is 170 nm, with a 50 nm high remaining slab on top of the underlying SiO_2 BOX layer with a thickness of 2 μm. The implant doping level inside the p^+- and n^+-doped regions of the electro-optic phase shifters (EOPS) is 1×10^{20} cm^{-3}. The process provides a CMOS back-end-of-line with a stack of five metal layers. For fabrication of the driver chips, the SG25H4 SiGe BiCMOS technology also from IHP was used.

Figure 4 reports a functional scheme of the transmitter device. It should be noted that the input and output are on the same side, as according to the image in Fig. 3, but drawn here on separate sides for clarity. Light entering the PIC passes first through an imb-MZI. The phase of the interferometer can be controlled via thermo-optic phase shifters (TOPSs or heaters), one in each arm, one of which is adjusted for the active phase stabilization between Alice and Bob. The shorter arm also comprises an attenuator (based on carrier absorption) to compensate for propagation loss in the longer arm. It should be highlighted that the fabrication of such a long delay line is not trivial given the size of the chip and its two-dimensional restriction, hence the specific geometry of the delay line. Light then enters an IM based on a balanced Mach–Zehnder-modulator (MZM). In the arms of the IM, there are three EOPSs based on carrier injection, which allow for a much higher electro-optic effect compared to a depletion type phase shifter, leading also to a more compact design. The bandwidth limitation is overcome by equalization schemes in the electronic driver design. Each EOPS has been fabricated with a specific size and is designed for a given amplitude of modulation. Three of them are used in order to produce our three amplitude levels independently. In addition, each EOPS is connected to the analog driver circuit on the EIC via wire-bondings. This allows us to individually actuate each EOPS and produce the full combination of quantum states. Likewise to the imb-MZI, the two arms of the IM include heaters, used to adjust its working point.

The electronic driver chip consists of several drivers digitally controlled by serial peripheral interface (SPI) with an input limiting amplifier for a high-speed and high-voltage swing application implemented in 250 nm BiCMOS technology. The amplification stage uses a cascode configuration to explore high bandwidth and output voltage swing. Differential input for limiting operation needs 50 mV, and the driver has a differential output swing of up to $3V_{pp}$ with a power consumption of 400 mW. The single driver consists of three active stages: a limiting amplifier, a buffer stage, and a current-mode logic (CML) output, plus a passive input matching network

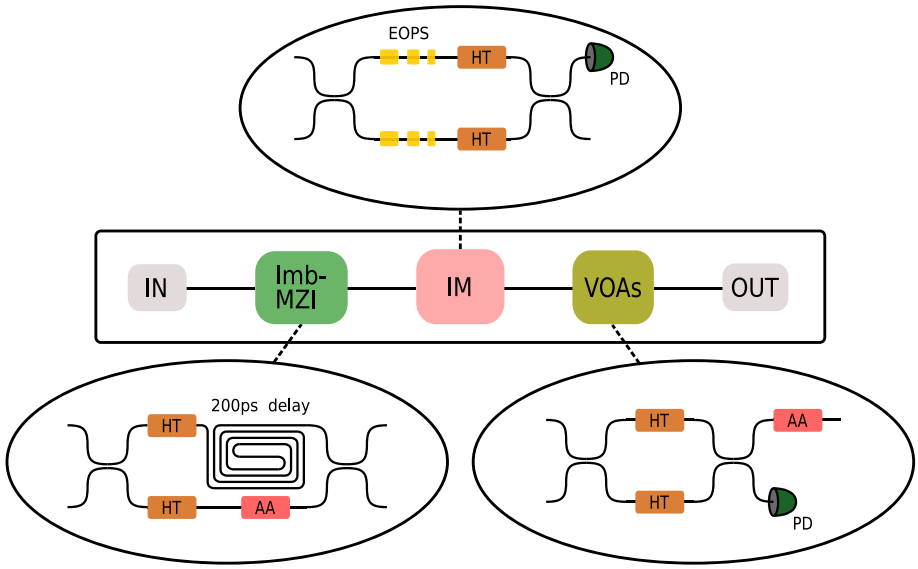

Fig. 4. Structure of the integrated transmitter circuit. Imb-MZI, imbalanced Mach–Zehnder interferometer; IM, intensity modulator; VOAs, variable optical attenuators; HT, heater; AA, absorption attenuator; EOPS, electro-optic phase shifter; PD, photodiode. The lengths of the three EOPSs are 200 μm, 400 μm, and 600 μm.

consisting of two common-base transistors. The limiting amplifier stabilizes the in-chip signal at $0.4V_{pp}$ differential, which is a compromise between the gain required at the output and the bandwidth and dissipation of the limiting amplifier itself. The buffer stage (emitter follower) partially improves the signal and brings the signal to lower DC voltages, thus allowing for higher voltage swing at the output. Finally, the output stage consists of a cascoded common-emitter amplifier with a controllable capacitive and resistive source degeneration: at low frequency, the capacitor acts as an open circuit, and the presence of the resistor causes a voltage drop that diminishes the output gain. At high frequency, the capacitor acts as a short circuit, thus restoring the full gain of the amplifier. The core of the single-channel driver is very small (order of hundred of microns) and the entire layout of the cell circuitry was kept strictly, thermally and electrically, symmetric with respect to the radio-frequency (RF) inputs and outputs. With such a configuration, the current design offers a wide range of gain and frequency compensation equivalent to two-tap digital pre-emphasis output that enables a full equalization of the low bandwidth of the phase shifters [31]. The drivers have fully differential inputs and outputs and are connected to the modulators to realize a push–pull configuration.

Before exiting the integrated chip, the light pulses are attenuated through two VOAs: one consists of a balanced-MZI with heaters in both arms in order to tune the MZI transfer function closer to a point of minimal transmission, while the other one is based on carrier absorption (the same as in the imb-MZI). Monitoring photodiodes have been placed at the outputs of the IM and the VOA-MZI. The total loss of the chip is around 25 dB. For testing purposes, it is possible to use an alternative optical input path, which is directly connected to the IM, bypassing the imb-MZI. This input has around 20 dB loss. Note that, as opposed to the receiver, loss is not an issue for the transmitter.

5. INTEGRATED RECEIVER

On the receiver side, the integrated chip is completely passive. According to our protocol, we require its polarization independence, meaning that the visibility of the integrated receiver interferometer should be high (100% ideally) for any incoming polarization state. We characterize the polarization independence by measuring the maximum and minimum visibilities depending on the incoming polarization state. Additionally, the first beam splitter should also be independent of the polarization. The former requirement is difficult to achieve in PICs due to the intrinsic birefringence of the waveguides [32–34], which is hard to control in an imb-MZI. To our knowledge, only recently, a polarization-independent receiver chip of a QKD system has been demonstrated [35,36]. However, the receiver in Ref. [35] showed a low maximum visibility (<98%) and high insertion losses (excess loss up to 6 dB) and the receiver in Ref. [36] showed a maximum visibility of 98.7%. In addition, a hybrid receiver based on a Michelson imbalanced interferometer and Faraday mirrors glued to the exterior of the chip has been recently validated [37].

In the present experiment, we make use of a polarization-independent PIC produced by the femtosecond laser micromachining technique [38]. Waveguides with low propagation loss (<0.2 dB/cm) and low birefringence ($<3\times10^{-5}$, due to residual stress in the material induced by the laser writing process) were inscribed in an aluminum borosilicate glass (EAGLE XG, Corning Inc.). Polarization independency of the directional couplers was achieved by exploiting the multiscan inscription technique, followed by a thermal annealing process, as described in Ref. [39]. Furthermore, at room temperature, a careful control of the waveguides' birefringence, by fabricating compensation tracks around the waveguide of the longer arm of the imb-MZI [39,40], as well as by finely tuning the temperature of the chip, allowed for the same polarization

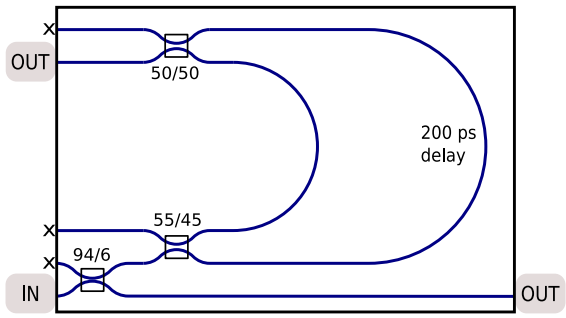

Fig. 5. Structure of the receiver integrated circuit. X means non-fiber-coupled ports. Fibers are butt-coupled to the waveguides and permanently pigtailed with UV-curing, index-matching glue. Fiber to waveguide coupling losses are better than 0.3 dB/facet.

rotation in both arms. We achieve temperature stabilization using, as on the transmitter side, a Peltier cooler/heater. At ambient temperature (around 20°C) as good as perfect birefringence compensation occurs, giving rise to a minimum visibility as high as 98.9%. It is important to note that this is the visibility corresponding to the case of the most unfavorable input polarization state; hence, the average visibility is higher. To compare our results with the values provided above in other implementations, our maximum visibility is 99.7%. The additional loss in the longer arm is compensated by adjusting the coupling ratio of the first coupler of the imb-MZI (around 55/45). The relationship of the visibility and QBER_x is given by $\mathrm{QBER}_x = (1 - V)/2$, and so, at the optimum temperature, its contribution to the QBER_x is minor.

Figure 5 shows a scheme of the receiver device. When entering the PIC, the light passes first through a 94/6 beam splitter. The majority of the light passes straight through the chip and out to an SPD. The lesser amount of light goes to the imb-MZI where another SPD at one of the outputs of the interferometer detects the exiting light. The footprint of Bob is around 6 cm × 8 cm. The total loss of the chip is notably low, something that is much desired on the receiver side. In fact, we measure the excess loss for the Z and X bases, using a low-coherence light source, to be around 2.75 dB and 3.50 dB, respectively. This is excluding the splitting ratios of the first and last beam splitters but including input/output coupling.

6. RESULTS

We performed complete secret key exchanges for different emulated distances and also employed standard SMF, using first the SNSPDs and then the InGaAs SPADs. We applied real-time error correction using a cascade algorithm with a block size of 8192 bits [41]. After 1000 error correction blocks, privacy amplification was executed. Thus, the total privacy amplification block size is 8.192×10^6 bits. In order to calculate the obtained SKR, we followed the security analysis of the one-decoy state protocol [26], where the SKR per privacy amplification block is given by

$$\mathrm{SKR} = \frac{1}{t}\{s_0 + s_1[1 - h(\phi_z)] - \lambda - 6\log_2(19/\epsilon_{\mathrm{sec}}) - \log_2(2/\epsilon_{\mathrm{corr}})\},$$

where t is the block acquisition time, s_0 is the lower bound on the number of vacuum events in the Z basis, s_1 is that of the single-photon events, $h(\cdot)$ is the binary entropy, ϕ_z is the upper bound on the phase error rate, λ is the leakage of the bits during the error correction process, and $\epsilon_{\mathrm{sec}} = 10^{-9}$ and $\epsilon_{\mathrm{corr}} = 10^{-9}$ are the secrecy and correctness parameters, respectively.

The first set of measurements was done with the main aim to understand the maximum performance of the integrated QKD system; hence, we employed the SNSPDs (see Section 3). In Table 1, we present the results obtained using different emulated fiber distances and using a 202.0 km long SMF. The emulated fiber distances were realized using an external VOA.

At 30 dB attenuation, the number of raw detections was too large for the real-time cascade error correction to be performed (this problem could be overcome by implementing a low-density parity check error correction on the FPGA [11]). Extremely low QBER_z values for all measurements with the SNSPDs were recorded. The main contribution to the QBER_z is estimated to come from the timing jitter of the SNSPD (see Section 3). A small contribution to the QBER_z could also come from the ER of the IM. In a static mode, it is above 40 dB, and it is estimated to be slightly lower in an active mode. Regarding the phase error rate, ϕ_z, it will depend on the visibilities of the interferometers at Alice's and Bob's sides and the active phase stabilization between them. Thanks to the high visibilities, ϕ_z is noticeably low. This is the case especially for the 30 dB attenuation due to the large number of counts, giving rise to a high raw key rate (RKR) and, therefore, a significant SKR. At higher attenuations, ϕ_z increases due to the smaller number of counts in the X basis detector, making it harder to stabilize the phase (for further discussion, see Section 3). For the measurement using 202.0 km of standard SMF placed in between the transmitter and the receiver, active time-tracking was performed in order to compensate for length fluctuations in the fiber.

Table 1. Parameters and Results of Secret Key Exchanges When Using SNSPDs[a]

Length [km]	Attenuation [dB]	Block Time [s]	RKR [kb/s]	QBER_z [%]	ϕ_z [%]	SKR [kb/s]
-	30	37	216	0.9	1.0	91.0*
-	36	124	66	0.8	1.1	28.3
-	38	168	42	0.8	1.4	17.2
-	40	306	27	0.8	2.1	10.6
202.0	39.5	351	25	0.9	2.2	9.4
251.7	42.7	720	12	0.5	2.2	4.9

[a]The asterisk * signifies estimated SKR from raw data. For comparison, the last line presents data from Ref. [1], which used a fiber-based setup with SNSPDs.

Table 2. Parameters and Results of Secret Key Exchanges When Using InGaAs Detectors[a]

Length [km]	Attenuation [dB]	Dead Time [μs]	Temperature [K]	Block Time [s]	RKR [kb/s]	$QBER_z$ [%]	ϕ_z [%]	SKR [kb/s]
-	30	20	188	453	18.0	3.6	2.1	2.9
-	35	32	183	858	9.6	3.1	4.5	1.3
-	40	20	188	1590	4.0	4.4	6.0	0.2
151.5	29.7	40	188	716	11.0	3.3	2.7	1.3
151.6	30.2	19	183	360	22.8	3.2	2.1	7.2

[a]For comparison, the last line presents data of the fiber-based setup using also InGaAs detectors [25].

It is interesting to note how the integrated version of the three-state BB84 protocol compares with a similar fiber-based setup employing SNSPDs, described in Ref. [1]. Its performance with 251.7 km of ultra low-loss SMF is shown in the last line of Table 1. It can be concluded that, with similar mean photon numbers, the same block size, and around 3 dB less attenuation than the measurement performed in the fiber-based setup, the integrated setup is practically as good as its fiber-based counterpart in terms of performance. However, in terms of practicality and cost, the integrated setup is more attractive.

In the following, we present measurements using the practical SPADs. On one hand, these detectors are considered more qualified than the SNSPDs for industrial implementations as they are uncomplicated to cool down. On the other hand, they present higher dark count rates, after-pulsing probabilities, and timing jitters, as well as lower efficiencies. The results obtained using the InGaAs SPADs are shown in Table 2.

Similar conclusions as for the results of Table 1 can be drawn. Compared to the results with the SNSPDs, a lower RKR is observed, which is reasonable as the detector efficiency is around 20% (a fourth of the efficiency of the SNSPDs). The increased values of $QBER_z$ are due to the higher timing jitters and after-pulsing probabilities of the InGaAs SPADs. The non-optimal 94/6 splitting ratio generates a faster saturation of the detector in the Z basis, hence a high $QBER_z$ at 30 dB attenuation, as well as non-negligible dark count rates for higher attenuations in the X basis. 151.5 km standard SMF was also placed in between the transmitter and the receiver. Due to the lower number of counts and, therefore, increased difficulty to perform perfect time-tracking and active phase tracking (see Section 3), ϕ_z is slightly higher than its attenuated analogue. The $QBER_z$ and ϕ_z at 40 dB attenuation are higher than at lower attenuations due to a smaller amount of counts, and so there is a worse signal-to-noise ratio.

Again we compare these results with those obtained using the same detectors and protocol in a fiber-based setup, more precisely, the one in Ref. [25]. At a distance of 151.6 km, with half of the mean photon numbers and the same block size, the fiber-based setup seems to perform better in terms of RKR and SKR than the integrated one with these detectors; however, this difference can be attributed mainly to the fact that the detectors were operated with different parameters. In fact, the fixed, yet non-optimal, splitting ratio at the receiver side of the integrated QKD setup forced a lower bias voltage and higher dead time in the X basis to minimize the dark counts (while lowering the detector efficiency) and maximize the number of counts, respectively. However, the comparable values of $QBER_z$ and ϕ_z make the employment of the integrated devices still attractive. In particular, the replacement of the first beam splitter with a tunable MZI, a device already well-optimized on the same platform [42], will allow for an optimal splitting ratio at the receiver side with a negligible cost in terms of loss and device complexity.

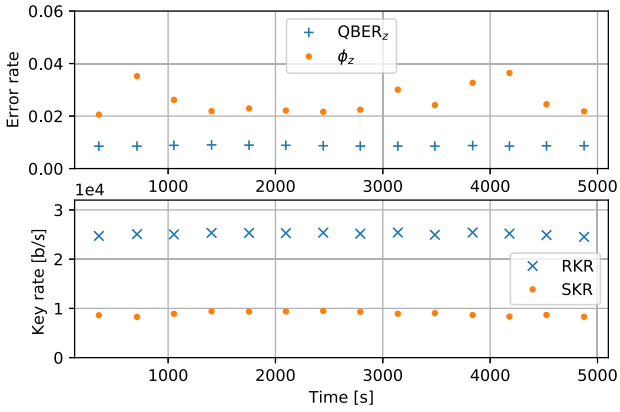

Fig. 6. $QBER_z$, ϕ_z, RKR, and SKR during several secret key exchanges over 80 min using SNSPDs at a distance of 202.0 km SMF.

Lastly, we present the complete results of the integrated QKD setup with 202.0 km of standard SMF and SNSPDs as detectors with a secret key exchange run for around 80 min. In Fig. 6, the RKR, SKR, $QBER_z$, and ϕ_z are shown as a function of time. We observe stable RKR and SKR, around 25 kb/s and 9 kb/s, respectively. The same goes for the $QBER_z$, around 0.9 %, thanks to the large number of detections in the Z basis, and so there is excellent time-tracking. Concerning ϕ_z, as previously mentioned, more fluctuations are observed due to a lower detection rate in the X basis, and so there is a more complicated time-tracking and active phase adjustment (refer to Section 3).

7. CONCLUSION

An integrated QKD system has been presented and shown to perform as well as its fiber-based analogue and, most importantly, as the state-of-the-art of integrated QKD systems [24]. Its transmitter is practical and with low cost thanks to the integration of the imb-MZI and, especially, the IM and corresponding electronics. Additionally, its receiver features low loss and is polarization-independent, which is typically complicated to achieve in integrated platforms.

Even though polarization fluctuations of QKD systems are nowadays very well controlled and compensated in laboratory

conditions [43,44], it might still be demanding to compensate for particularly rapid fluctuations in polarization that could occur in real-world fiber-optic lines, e.g., because of trains passing or lightning strikes [45]. Thus, the integrated QKD system here suggested, based on time-bin encoding and polarization insensitivity, testifies for effortless integration in present-day fiber-optic networks.

We believe that the integrated high-speed QKD system gives an important contribution to the advancement of integrated quantum technologies and simultaneously reflects their maturity. Future investigations could cover how to integrate all components on-chip (meaning the laser on the transmitter side and the SPDs on the receiver side), which has the risk of being costly due to the active materials required, such as InP, and further complicated due to the need of interfacing different active and non-active materials via gluing or bonding. Several works have already examined the merge of InP platforms with silicon platforms [46,47]. On the transmitter side of the present integrated platform, the PIC, the driver EIC, and all DC control loops could be monolithically integrated in a single electronic and photonic IC (EPIC) chip. The EPIC technology [48] for this approach is mature and already in use for data center applications. An adaptation to QKD applications is only a matter of chip design rather than process development. Furthermore, EPIC and even PIC/EIC solutions can be scaled to significantly higher modulation rates, however limited by the achievable ER. Thanks to the small dimensions of the introduced integrated platforms, it is rather straightforward to integrate the current QKD system in two rack-mountable enclosures, ready for usage in a real-work network.

Funding. Eurostars Projects (E!11493); European Quantum Flagship project openQKD (857156); Italian Ministry for University and Research (PRIN2017-SRNBRK, PNRR-NQSTI); European Research Council (742745).

Acknowledgment. We thank Claudio Barreiro for providing the electronic cards and Federico Bassi for his preliminary work on the fabrication and characterization of the receiver. We thank the Eurostars project E!11493 QuPIC for financial support. SA and AC acknowledge funding by the PRIN2017 program, QUSHIP project. RO acknowledges funding by the European Union through the ERC Advanced Grant CAPABLE, and the Italian Ministry for University and Research through the PNRR project PE0000023-NQSTI.

Disclosures. The authors declare no conflicts of interest.

Data Availability. Data underlying the results presented in this paper are not publicly available at this time but may be obtained from the authors upon reasonable request.

REFERENCES

1. P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," SIAM J. Comput. **26**, 1484–1509 (1997).
2. M. Amico, Z. H. Saleem, and M. Kumph, "Experimental study of Shor's factoring algorithm using the IBM Q experience," Phys. Rev. A **100**, 012305 (2019).
3. K. Wright, K. M. Beck, S. Debnath, J. M. Amini, Y. Nam, N. Grzesiak, J.-S. Chen, N. C. Pisenti, M. Chmielewski, C. Collins, K. M. Hudek, J. Mizrahi, J. D. Wong-Campos, S. Allen, J. Apisdorf, P. Solomon, M. Williams, A. M. Ducore, A. Blinov, S. M. Kreikemeier, V. Chaplin, M. Keesan, C. Monroe, and J. Kim, "Benchmarking an 11-qubit quantum computer," Nat. Commun. **10**, 5464 (2019).
4. C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," in *International Conference on Computers, Systems & Signal Processing* (1984), pp. 175–179.
5. C. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," J. Cryptol. **5**, 3–28 (1992).
6. A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, "Secure quantum key distribution over 421 km of optical fiber," Phys. Rev. Lett. **121**, 190502 (2018).
7. M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Overcoming the rate–distance limit of quantum key distribution without quantum repeaters," Nature **557**, 400–403 (2018).
8. S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, R.-Q. Wang, P. Ye, Y. Zhou, G.-J. Fan-Yuan, F.-X. Wang, W. Chen, Y.-G. Zhu, P. V. Morozov, A. V. Divochiy, Z. Zhou, G.-C. Guo, and Z.-F. Han, "Twin-field quantum key distribution over 830-km fibre," Nature **16**, 154–161 (2022).
9. S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, F.-Z. Li, X.-W. Chen, L.-H. Sun, J.-J. Jia, J.-C. Wu, X.-J. Jiang, J.-F. Wang, Y.-M. Huang, Q. Wang, Y.-L. Zhou, L. Deng, T. Xi, L. Ma, T. Hu, Q. Zhang, Y.-A. Chen, N.-L. Liu, X.-B. Wang, Z.-C. Zhu, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, "Satellite-to-ground quantum key distribution," Nature **549**, 43–47 (2017).
10. Z. Yuan, A. Plews, R. Takahashi, K. Doi, W. Tam, A. W. Sharpe, A. R. Dixon, E. Lavelle, J. F. Dynes, A. Murakami, M. Kujiraoka, M. Lucamarini, Y. Tanizawa, H. Sato, and A. J. Shields, "10-Mb/s quantum key distribution," J. Lightwave Technol. **36**, 3427–3433 (2018).
11. F. Grünenfelder, A. Boaron, M. Perrenoud, G. V. Resta, D. Rusca, C. Barreiro, R. Houlmann, R. Sax, L. Stasi, S. El-Khoury, E. Hänggi, N. Bosshard, F. Bussières, and H. Zbinden, "Fast single photon detectors and real-time key distillation: enabling high secret key rate QKD systems," arXiv, arXiv:2210.16126 (2022).
12. P. Sibson, J. E. Kennard, S. Stanisic, C. Erven, J. L. O'Brien, and M. G. Thompson, "Integrated silicon photonics for high-speed quantum key distribution," Optica **4**, 172–177 (2017).
13. P. Sibson, C. Erven, M. Godfrey, S. Miki, T. Yamashita, M. Fujiwara, M. Sasaki, H. Terai, M. G. Tanner, C. M. Natarajan, R. H. Hadfield, J. L. O'Brien, and M. G. Thompson, "Chip-based quantum key distribution," Nat. Commun. **8**, 13984 (2017).
14. T. K. Paraïso, T. Roger, D. G. Marangon, I. De Marco, M. Sanzaro, R. I. Woodward, J. F. Dynes, Z. Yuan, and A. J. Shields, "A photonic integrated quantum secure communication system," Nat. Photonics **15**, 850–856 (2021).
15. T. K. Paraïso, I. D. Marco, T. Roger, D. G. Marangon, J. F. Dynes, M. Lucamarini, Z. Yuan, and A. J. Shields, "A modulator-free quantum key distribution transmitter chip," npj Quantum Inf. **5**, 1 (2019).
16. C. Ma, W. D. Sacher, Z. Tang, J. C. Mikkelsen, Y. Yang, F. Xu, T. Thiessen, H.-K. Lo, and J. K. S. Poon, "Silicon photonic transmitter for polarization-encoded quantum key distribution," Optica **3**, 1274–1278 (2016).
17. D. Bunandar, A. Lentine, C. Lee, H. Cai, C. M. Long, N. Boynton, N. Martinez, C. DeRose, C. Chen, M. Grein, D. Trotter, A. Starbuck, A. Pomerene, S. Hamilton, F. N. C. Wong, R. Camacho, P. Davids, J. Urayama, and D. Englund, "Metropolitan quantum key distribution with silicon photonics," Phys. Rev. X **8**, 021009 (2018).
18. L. Kong, Z. Li, C. Li, L. Cao, Z. Xing, J. Cao, Y. Wang, X. Cai, and X. Zhou, "Photonic integrated quantum key distribution receiver for multiple users," Opt. Express **28**, 18449–18455 (2020).
19. W. Geng, C. Zhang, Y. Zheng, J. He, C. Zhou, and Y. Kong, "Stable quantum key distribution using a silicon photonic transceiver," Opt. Express **27**, 29045–29054 (2019).
20. H. Semenenko, P. Sibson, A. Hart, M. G. Thompson, J. G. Rarity, and C. Erven, "Chip-based measurement-device-independent quantum key distribution," Optica **7**, 238–242 (2020).

21. K. Wei, W. Li, H. Tan, Y. Li, H. Min, W.-J. Zhang, H. Li, L. You, Z. Wang, X. Jiang, T.-Y. Chen, S.-K. Liao, C.-Z. Peng, F. Xu, and J.-W. Pan, "High-speed measurement-device-independent quantum key distribution with integrated silicon photonics," Phys. Rev. X **10**, 031030 (2020).
22. G. Vest, P. Freiwang, J. Luhn, T. Vogl, M. Rau, L. Knips, W. Rosenfeld, and H. Weinfurter, "Quantum key distribution with a hand-held sender unit," Phys. Rev. Appl. **18**, 024067 (2022).
23. F. Beutel, H. Gehring, M. A. Wolff, C. Schuck, and W. Pernice, "Detector-integrated on-chip QKD receiver for GHz clock rates," npj Quantum Inf. **7**, 40 (2021).
24. Q. Liu, Y. Huang, Y. Du, Z. Zhao, M. Geng, Z. Zhang, and K. Wei, "Advances in chip-based quantum key distribution," Entropy **24**, 1334 (2022).
25. A. Boaron, B. Korzh, R. Houlmann, G. Boso, D. Rusca, S. Gray, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, "Simple 2.5 GHz time-bin quantum key distribution," Appl. Phys. Lett. **112**, 171108 (2018).
26. D. Rusca, A. Boaron, F. Grünenfelder, A. Martin, and H. Zbinden, "Finite-key analysis for the 1-decoy state QKD protocol," Appl. Phys. Lett. **112**, 171104 (2018).
27. D. Rusca, A. Boaron, M. Curty, A. Martin, and H. Zbinden, "Security proof for a simplified Bennett-Brassard 1984 quantum-key-distribution protocol," Phys. Rev. A **98**, 052336 (2018).
28. B. Korzh, N. Walenta, T. Lunghi, N. Gisin, and H. Zbinden, "Free-running InGaAs single photon detector with 1 dark count per second at 10% efficiency," Appl. Phys. Lett. **104**, 081108 (2014).
29. M. Caloz, M. Perrenoud, C. Autebert, B. Korzh, M. Weiss, C. Schönenberger, R. J. Warburton, H. Zbinden, and F. Bussières, "High-detection efficiency and low-timing jitter with amorphous superconducting nanowire single-photon detectors," Appl. Phys. Lett. **112**, 061103 (2018).
30. "SiGe BiCMOS and silicon photonics technologies," 2022, http://www.ihp-microelectronics.com/services/research-and-prototyping-service/mpw-prototyping-service/sigec-bicmos-technologies.
31. Q. Xu, S. Manipatruni, B. Schmidt, J. Shakya, and M. Lipson, "12.5 Gbit/s carrier-injection-based silicon micro-ring silicon modulators," Opt. Express **15**, 430–436 (2007).
32. D. Dai and S. He, "Analysis of the birefringence of a silicon-on-insulator rib waveguide," Appl. Opt. **43**, 1156–1161 (2004).
33. D. Dai, L. Liu, S. Gao, D.-X. Xu, and S. He, "Polarization management for silicon photonic integrated circuits," Laser Photon. Rev. **7**, 303–328 (2013).
34. L.-M. Chang, L. Liu, Y.-H. Gong, M.-Q. Tan, Y.-D. Yu, and Z.-Y. Li, "Polarization-independent directional coupler and polarization beam splitter based on asymmetric cross-slot waveguides," Appl. Opt. **57**, 678–683 (2018).
35. D. Wu, X. Li, L.-L. Wang, J.-S. Zhang, W. Chen, Y. Wang, H.-J. Wang, J.-G. Li, X.-J. Yin, Y.-D. Wu, and J.-M. An, "Temperature characterizations of silica asymmetric Mach-Zehnder interferometer chip for quantum key distribution," Chin. Phys. B **32**, 010305 (2022).
36. X. Li, M. Ren, J. Zhang, L. Wang, W. Chen, Y. Wang, X. Yin, Y. Wu, and J. An, "Interference at the single-photon level based on silica photonics robust against channel disturbance," Photon. Res. **9**, 222–228 (2021).
37. G.-W. Zhang, Y.-Y. Ding, W. Chen, F.-X. Wang, P. Ye, G.-Z. Huang, S. Wang, Z.-Q. Yin, J.-M. An, G.-C. Guo, and Z.-F. Han, "Polarization-insensitive interferometer based on a hybrid integrated planar lightwave circuit," Photon. Res. **9**, 2176–2181 (2021).
38. G. Corrielli, A. Crespi, and R. Osellame, "Femtosecond laser micromachining for integrated quantum photonics," Nanophotonics **10**, 3789–3812 (2021).
39. G. Corrielli, S. Atzeni, S. Piacentini, I. Pitsios, A. Crespi, and R. Osellame, "Symmetric polarization-insensitive directional couplers fabricated by femtosecond laser writing," Opt. Express **26**, 15101–15109 (2018).
40. L. A. Fernandes, J. R. Grenier, P. R. Herman, J. S. Aitchison, and P. V. S. Marques, "Stress induced birefringence tuning in femtosecond laser fabricated waveguides in fused silica," Opt. Express **20**, 24103–24114 (2012).
41. J. Martinez-Mateo, C. Pacher, M. Peev, A. Ciurana, and V. Martin, "Demystifying the information reconciliation protocol Cascade," arxiv, arXiv:1407.3257 (2014).
42. R. Albiero, C. Pentangelo, M. Gardina, S. Atzeni, F. Ceccarelli, and R. Osellame, "Toward higher integration density in femtosecond-laser-written programmable photonic circuits," Micromachines **13**, 1145 (2022).
43. C.-Z. Peng, J. Zhang, D. Yang, W.-B. Gao, H.-X. Ma, H. Yin, H.-P. Zeng, T. Yang, X.-B. Wang, and J.-W. Pan, "Experimental long-distance decoy-state quantum key distribution based on polarization encoding," Phys. Rev. Lett. **98**, 010505 (2007).
44. G. B. Xavier, G. V. de Faria, G. P. Tao, and J. P. von der Weid, "Full polarization control for fiber optical quantum communication systems using polarization encoding," Opt. Express **16**, 1867–1873 (2008).
45. E. I. J.-S. Tassé and G. P. C. W. Daab, "White paper: why coherent detection systems may fail at compensating for polarization mode dispersion," 2015 https://lunainc.com/sites/default/files/assets/files/resource-library/White-Paper-Coherent-Detection-Systems-PMD-Compensation.pdf.
46. G. Roelkens, L. Liu, D. Liang, R. Jones, A. Fang, B. Koch, and J. Bowers, "III-V/silicon photonics for on-chip and intra-chip optical interconnects," Laser Photon. Rev. **4**, 751–779 (2010).
47. D. Liang and J. E. Bowers, "Recent progress in heterogeneous III-V-on-silicon photonic integration," Light Adv. Manuf. **2**, 59–83 (2021).
48. D. Knoll, S. Lischke, R. Barth, L. Zimmermann, B. Heinemann, H. Rucker, C. Mai, M. Kroh, A. Peczek, A. Awny, C. Ulusoy, A. Trusch, A. Kruger, J. Drews, M. Fraschke, D. Schmidt, M. Lisker, K. Voigt, E. Krune, and A. Mai, "High-performance photonic BiCMOS process for the fabrication of high-bandwidth electronic-photonic integrated circuits," in *IEEE International Electron Devices Meeting (IEDM)* (2015), pp. 15.6.1–15.6.4.