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, Rue de l'Ecole-de-Médecine 20, 1205, Genève, Switzerland*
[2]*ID Quantique SA, Rue Eugène-Marziano 25, 1227, Genève, Switzerland*
[3]*Institute for Photonics and Nanotechnology, CNR-IFN, 20133, Piazza Leonardo da Vinci, Milano, Italy*
[4]*Dipartimento di Fisica, Politecnico di Milano, 20133, Milano, Italy*
[5]*Sicoya GmbH, Carl-Scheele-Strasse 16, 12489, Berlin, Germany*
[*]*rebecka.sax@unige.ch*

Abstract: Quantum key distribution (QKD) is nowadays a well established method for generating secret keys at a distance in an information-theoretic secure way, as the secrecy of QKD relies on the laws of quantum physics and not 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 [1, 2].

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 up-and-rising threat is the quantum computer, which would be able to efficiently crack the current most-used encrypting techniques [3] and whose technology matures as the author is writing this article [4,5]. Hence the natural entry of quantum key distribution (QKD), which establishes an information-theoretically secure key exchange, providing long term security.

Since the first proposal of a QKD protocol in 1984 [6] and its first experimental realization in 1992 [7], more protocols and a multitude of experiments have been established. This global enthusiasm has resulted in enormous increases in the communication distance (using fiber [1,8,9], as well as free-space [10]) and in the secret key rate [11,12].

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 560 MHz clock rate, using the BB84 time-bin protocol at 20 km distance separation [13]. Subsequently, several integrated implementations have been reported for various QKD schemes [14–23]. Some

included an integrated laser [14–16] and other presented hybrid versions that maintain one of the components as non-integrated (either the transmitter or the receiver device) [15–18]. Integrated detectors on chip have also been realized [24].

Here we present a 2.5 GHz integrated QKD system, the fastest integrated system to our knowledge [25], which features a precise state preparation and a polarization independent receiver. At a distance of 151.5 km of standard single-mode fiber we obtain a secret key rate (SKR) of 1.3 kbps 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 3-state BB84 protocol using the one-decoy state method [2, 26], with time-bin encoding. The three states, and their respective decoys, prepared by Alice are shown in figure 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:

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

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

E standing 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. Qubits detected in the X basis will pass through an imbalanced Mach-Zehnder interferometer (imb-MZI) and corresponding detections will reflect the security of the exchange of the secret key.


basis, bit	state	μ_1	μ_2
Z, 0	$|0\rangle$		
Z, 1	$|1\rangle$		
X, 0	$|+\rangle$		

Fig. 1. Encoding of the states sent by Alice [2]. μ_1 and μ_2 correspond to the two mean photon numbers used for the one-decoy state protocol.

3. Experimental setup

An overview of the full QKD setup is depicted in figure 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 classic (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 FWHM of around 31 ps are generated by a gain-switched high-bandwidth DFB laser at 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 (VOA). 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 AES (Advanced Encryption Standard) cores seeded by a Quantis Quantum Random Number Generator (QRNG) from ID Quantique SA. Upon exiting the chip, light pulses travel through the DCF to pre-compensate for all the chromatic dispersion created on the trip from Alice to Bob in the QC. The QC consists of standard single-mode fibers (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 basis, 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. 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 adopted for our main experiment are InGaAs/InP negative feedback single photon avalanche diode (SPADs) cooled by a free-piston Stirling cooler to -85°C [27]. For the characterization of our system we also use in-house superconducting-nanowire single-photon detectors (SNSPDs) cooled at 0.8 K [28]. These detectors feature low timing jitter (around 40 ps), negligible after-pulsing probability, high detector efficiency (around 80 %) and low dark count rates ($dc_z = 200$, $dc_x = 100$). 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 beamsplitter 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.
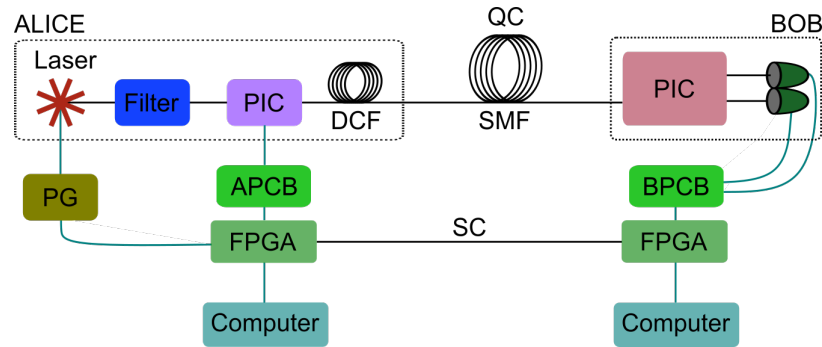
Fig. 2. Simplified schematics of the experimental setup. PIC = photonic integrated circuit, DCF = dispersion compensating fiber, QC = quantum channel, SMF = single-mode fiber, PG = pulse generator, APCB = Alice printed circuit board, BPCB = Bob PCB, FPGA = field-programmable gate array, SC = service channel. Black lines correspond to optical links and blue lines correspond to electrical connections.

4. Integrated Transmitter

Several challenges arise in the realization of integrated systems for QKD purposes depending on the protocol one uses. For what we are concerned, due to our high clock rate, we need accurate modulation of the quantum states at high frequencies on the transmitter side. Indeed, accuracy reflects on the extinction ratio (ER) of the quantum states and finally on the QBER. Moreover, for time-bin encoding, the platform must allow for the implementation of a 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 photonic integrated circuit (PIC), which is as small as 4.5 mm × 1.1 mm and an adjacent electronic driver integrated circuit (EIC) 0.75 mm × 1.1 mm, see figure 3. It is highly advantageous to use silicon photonics for our system as now most of the expensive electronics are on-chip. Additionally, it allows for high component density and small footprints. As can be seen in figure 3, the ICs are glued on and bonded to a small printed circuit board (PCB). This PCB is combined with a larger one and connected to a computer-controlled FPGA, as shown in figure 2. Light is coupled to the PIC via a fibre array and grating couplers. The chip is temperature stabilized at 45°C using a standard Peltier cooler/heater placed under the host PCB of the PIC.

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 Ultra-Violet (DUV) lithography [29]. The nanowires are embedded within the 220 nm thick silicon device layer of the SOI substrate. The SOI rib-waveguides have dimensions of 220×450 nm^2 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 $1 \cdot 10^{20}$ 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. 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 a VOA (based on carrier absorption) to compensate for propagation loss in the longer arm. Light then enters an IM based on a balanced Mach-Zehnder-Modulator (MZM). In the arms of the IM there are
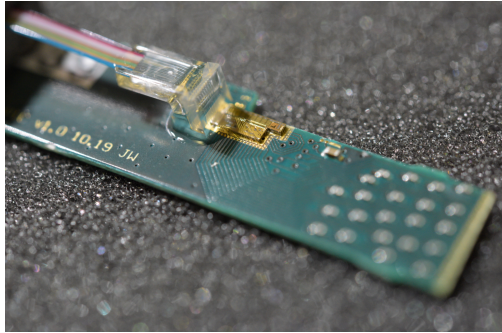
Fig. 3. Photo of the transmitter integrated circuit.

three EOPSs based on carrier injection. Each EOPS has been fabricated with a specific size and is designed for a given amplitude of modulation. In addition, each EOPS is connected to the analog driver circuit on the EIC via wire-bondings. This allows 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 driver chip is a digitally Serial Peripheral Interface (SPI) controlled driver with limiting amplifier for high bandwidth and high voltage swing applications with a 3.3 V power supply. It consists of three active stages: a limiting amplifier, a buffer stage, and a current-mode logic (CML) output driver, as well as an active input matching network consisting of two common-base transistors. The core of the single-channel driver is very small, 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. In addition, a common center-of-gravity layout and cross-coupling of the differential pair were implemented, minimizing direct-current (DC) offset and conversion between the even and odd modes without compromising RF performance. The MZM bias and driver bias currents are digitally programmed for all channels via a common control block.

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.
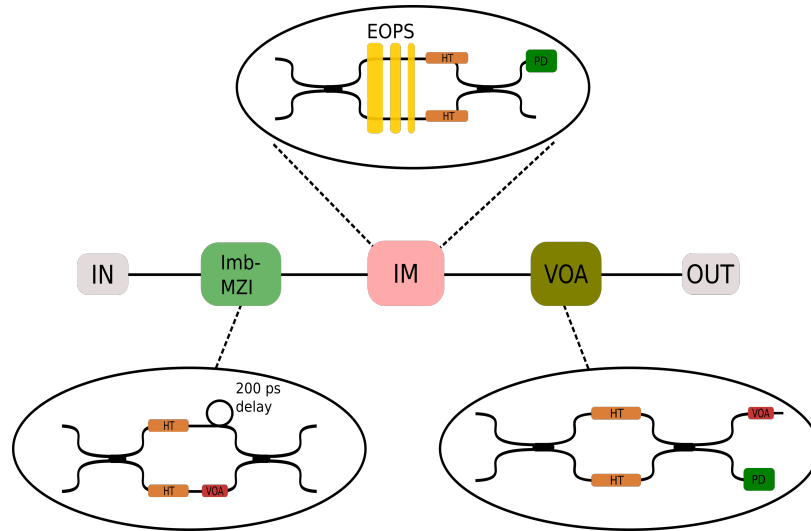
Fig. 4. Structure of the integrated transmitter circuit. Imb-MZI = imbalanced Mach-Zehnder Interferometer, IM = intensity modulator, VOA = variable optical attenuator, HT = heater, EOPS = electro-optic phase shifter, PD = photodiode.

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 [30–32], which is hard to control in an imbalanced MZI. To our knowledge, only recently, a polarization independent receiver chip of a QKD system has been demonstrated [33, 34]. However, the receiver in [33] showed a low maximum visibility (< 98%) and high insertion losses (excess loss up to 6 dB) and the receiver in [34] 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 [35].

In the present experiment we make use of a polarization independent PIC, produced by the femtosecond laser micromachining technique [36]. Waveguides with low propagation losses (< 0.2 dB/cm) and low birefringence (< $3 \cdot 10^{-5}$) 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 [37]. 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 [37, 38], as well as by finely tuning the temperature of the chip, allowed for the same polarization 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 (about 55/45). The relationship of the visibility and QBER$_x$ is given by:

$\text{QBER}_x = (1 - V)/2$ and so, at the optimum temperature, its contribution to the QBER 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 a single-photon detector (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 losses for the Z and X bases, using a low-coherent 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.
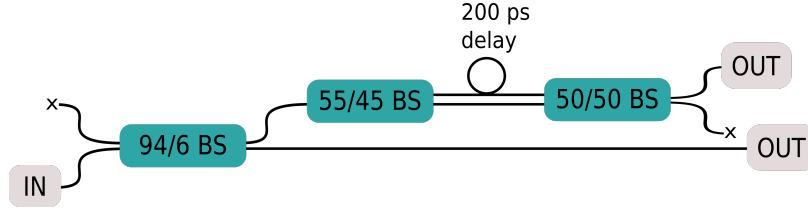

Fig. 5. Structure of the receiver integrated circuit.

6. Results

We performed complete secret key exchanges for different emulated distances and also employing standard SMF, using first the SNSPDs and then the InGaAs SPADs. We apply real-time error correction using a Cascade algorithm with a block size of 8192 bits [39]. After 1000 error correction blocks, privacy amplification is executed. Thus, the total privacy amplification block size is $8.192 \cdot 10^6$ bits. In order to calculate the obtained SKR we follow the security analysis of the 1-decoy state protocol [26] where the SKR per privacy amplification block is given by:

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

where t is the block acquisition time, s_0 is the lower bound on the number of vacuum events in the Z basis and s_1 that of the single-photon events, $h(\cdot)$ is the binary entropy, ϕ_z is the upper bound on the phase error rate, λ the leakage of the bits during the error correction process and $\epsilon_{sec} = 10^{-9}$ and $\epsilon_{corr} = 10^{-9}$ 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 single-mode fiber. The emulated fiber distances were realized using an external VOA.

Length [km]	Attenuation [dB]	Block time [s]	RKR [kbps]	QBER$_z$ [%]	ϕ_z [%]	SKR [kbps]
-	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
[1]: 251.7	42.7	720	12	0.5	2.2	4.9

Table 1. Parameters and results of secret key exchanges when using SNSPDs. * signifies estimated SKR from raw data. For comparison, the last line presents data from reference [1] which used a fiber-based setup with SNSPDs.

At 30 dB attenuation the number of raw detections were too high 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 [12]). 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 extinction ratio 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 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 secret key rate (SKR). At higher attenuations, ϕ_z increases due to the lower 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.

It is interesting to note how the integrated version of the 3-state BB84 protocol compares with a similar fiber-based setup employing SNSPDs, described in reference [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 with 251.7 km of standard SMF, 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.

Length	Attenuation	Dead time	Temperature	Block time	RKR	QBER$_z$	ϕ_z	SKR
[km]	[dB]	[μs]	[K]	[s]	[kbps]	[%]	[%]	[kbps]
-	30	20	188	453	18.0	3.6	2.1	2.9
-	35	32	182	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
[2]: 151.6	30.2	19	183	360	22.8	3.2	2.1	7.2

Table 2. Parameters and results of secret key exchanges when using InGaAs detectors.
For comparison, the last line presents data of the fiber-based setup using also InGaAs
detectors [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 afterpulsing probabilities of the InGaAs SPADs. The non-optimal 94/6
splitting ratio generates a faster saturation of detections in the Z basis, hence the consecutive
increase in QBER$_z$ 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.

Again we compare these results with those obtained using the same detectors and protocol in a
fiber-based setup, more precisely, the one in reference [2]. 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 maximise the number of counts, respectively.
However, the comparable values on QBER$_z$ and ϕ_z makes 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 [40], will allow for an optimal splitting
ratio at the receiver side with a negligible cost in terms of losses and device complexity.

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 let run for around 80 min. In figure 6
the RKR, SKR, QBER$_z$ and ϕ_z are shown as a function of time. We observe a stable RKR
and SKR, around 25 kbps and 9 kbps, respectively. The same goes for the QBER$_z$, around
0.9 %, thanks to the high number of detections in the Z basis and so an 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 a more complicated time-tracking and active phase adjustment (refer to
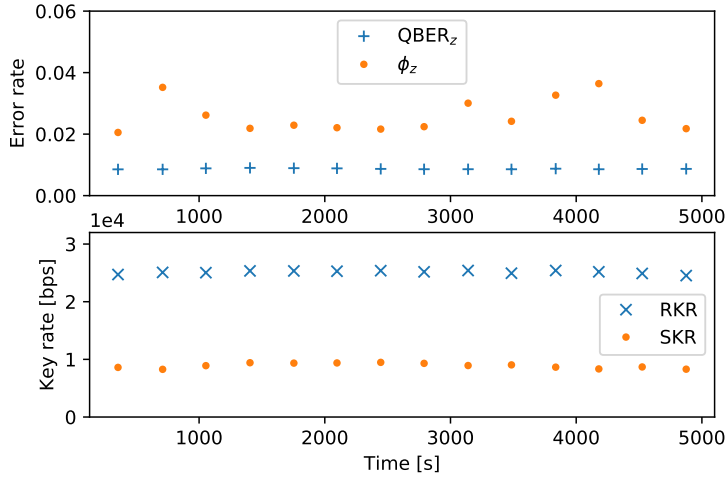section 3).

Fig. 6. QBER_z, ϕ_z, RKR and SKR during several secret key exchanges over 80 min.

7. Conclusion

An integrated QKD system has been presented and shown to perform as good as its fiber-based analogue, and most importantly as the state-of-the-art of integrated QKD systems [25]. Its transmitter is practical and 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 [41, 42], 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 [43]. 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 [44, 45]. 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 [46] 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 extinction ratio. Thanks to the small dimensions of the introduced integrated platforms, it is rather straight-forward to integrate the current QKD system in two 19-inch racks, ready for usage in a real-work network.

CAPABLE (742745).

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. 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** (2018).
2. 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).
3. P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," SIAM J. on Comput. **26**, 1484–1509 (1997).
4. 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).
5. K. Wright, K. M. Beck, S. Debnath, J. Amini, Y. Nam, N. Grzesiak, J.-S. Chen, N. Pisenti, M. Chmielewski, C. Collins *et al.*, "Benchmarking an 11-qubit quantum computer," Nat. communications **10**, 1–6 (2019).
6. C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *International Conference on Computers, Systems & Signal Processing, Bangalore, India, Dec 9-12, 1984,* (1984), pp. 175–179.
7. C. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," J. Cryptol. **5**, 3–28 (1992).
8. 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).
9. S. Wang, Z. Q. Yin, D. Y. He, and al., "Twin-field quantum key distribution over 830-km fibre," Nature (2022).
10. 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).
11. 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. Light. Technol. **36**, 3427–3433 (2018).
12. 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:2210.16126 [quant-ph] (2022).
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** (2017).
14. 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 (2017).
15. P. T.K., R. T., M. D.G., and al, "A photonic integrated quantum secure communication system." Nature (2021).
16. P. T.K., D. M. I., R. T., and al., "A modulator-free quantum key distribution transmitter chip." NPJ (2019).
17. 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).
18. 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).
19. 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).
20. 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 20**, 29045–29054 (2019).
21. 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).
22. 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).
23. 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** (2022).

24. 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**, 1–8 (2021).

25. Q. Liu, Y. Huang, Y. Du, Z. Zhao, M. Geng, Z. Zhang, and K. Wei, "Advances in chip-based quantum key distribution," Entropy **24** (2022).

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. 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).

28. 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).

29. "Sige bicmos and silicon photonics technologies," http://www.ihp-microelectronics.com/services/research-and-prototyping-service/mpw-prototyping-service/sigec-bicmos-technologies. Accessed: 2022-11-09.

30. D. Dai and S. He, "Analysis of the birefringence of a silicon-on-insulator rib waveguide," Appl. Opt. **43**, 1156–1161 (2004).

31. D. Dai, L. Liu, S. Gao, D.-X. Xu, and S. He, "Polarization management for silicon photonic integrated circuits," Laser & Photonics Rev. **7**, 303–328 (2013).

32. 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).

33. 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 (2022).

34. 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).

35. 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 light-wave circuit," Photon. Res. **9**, 2176–2181 (2021).

36. G. Corrielli, A. Crespi, and R. Osellame, "Femtosecond laser micromachining for integrated quantum photonics," Nanophotonics **10**, 3789–3812 (2021).

37. 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).

38. 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).

39. J. Martinez-Mateo, C. Pacher, M. Peev, A. Ciurana, and V. Martin, "Demystifying the information reconciliation protocol cascade," Quantum Inf. Comput. (2014).

40. 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** (2022).

41. 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).

42. G. B. Xavier, G. V. de Faria, G. P. T. ao, and J. P. von der Weid, "Full polarization control for fiber optical quantum communication systems using polarization encoding," Opt. Express **16**, 1867–1873 (2008).

43. E. I. Jean-Sébastien Tassé, Product Manager and G. P. C. Wajih Daab, Sales Engineer, "White paper: Why coherent detection systems may fail at compensating for polarization mode dispersion," (2015).

44. 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 & Photonics Rev. **4**, 751–779 (2010).

45. D. Liang and J. E. Bowers, "Recent progress in heterogeneous iii-v-on-silicon photonic integration," Light. Adv. Manuf. **2**, 59–83 (2021).

46. 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 *2015 IEEE International Electron Devices Meeting (IEDM),* (2015), pp. 15.6.1–15.6.4.