npj | Quantum Information

www.nature.com/npjqi

ARTICLE OPEN

Check for updates

Detector-integrated on-chip QKD receiver for GHz clock rates

Fabian Beutel[1,2], Helge Gehring[1,2], Martin A. Wolff[1,2], Carsten Schuck[1,2,3] and Wolfram Pernice[1,2,3]✉

Quantum key distribution (QKD) can greatly benefit from photonic integration, which enables implementing low-loss, alignment-free, and scalable photonic circuitry. At the same time, superconducting nanowire single-photon detectors (SNSPD) are an ideal detector technology for QKD due to their high efficiency, low dark-count rate, and low jitter. We present a QKD receiver chip featuring the full photonic circuitry needed for different time-based protocols, including single-photon detectors. By utilizing waveguide-integrated SNSPDs we achieve low dead times together with low dark-count rates and demonstrate a QKD experiment at 2.6 GHz clock rate, yielding secret-key rates of 2.5 Mbit/s for low channel attenuations of 2.5 dB without detector saturation. Due to the broadband 3D polymer couplers the reciver chip can be operated at a wide wavelength range in the telecom band, thus paving the way for highly parallelized wavelength-division multiplexing implementations.

npj Quantum Information (2021)7:40 ; https://doi.org/10.1038/s41534-021-00373-7

INTRODUCTION

Encryption is the basis for secure communication and becomes increasingly significant in today's digital society. At the same time, recent progress in the field of quantum computing[1,2] and long-known quantum algorithms such as Shor's[3] algorithm threaten the integrity of widespread classical algorithms for asymmetric cryptography[4]. Quantum key distrbution (QKD) has been proposed as a promising solution by allowing to generate a shared secret between two parties, Alice and Bob, in a provably secure way even in the presence of quantum computers[5,6]. Together with information-theoretically secure ciphers such as the one-time pad[7] it provides a promising means for encryption. Multiple schemes have been experimentally demonstrated, but in order to be broadly applicable, faster and more scalable systems providing higher secret-key rates than currently available are desirable.

For achieving ultrafast and highly scalable QKD systems, photonic integration is crucial in order to overcome scalability and stability limitations present in bulk optical systems. While implementations of on-chip QKD have been demonstrated in the past for continuous-variable (CV-)QKD[8] and also for discrete-variable (DV-)QKD[9–14], the integration of high-performance single-photon detectors (SPDs) in the case of DV-QKD remains a challenge.

The choice of the employed SPD technology has decisive impact on the performance of the overall DV-QKD system. Avalanche photo diodes (APDs) are commonly used, but they suffer from high dark-count rates (which requires to operate them in a gated mode) and large detector dead-times[15] at telecom wavelengths. This strongly restricts the secret-key rates especially for low-distance links for high clock rates[16] when operating at these wavelengths, which is beneficial due to their widespread use in existing fiber networks.

In the past years superconducting nanowire single-photon detectors (SNSPDs) have emerged as a superior detector technology[15,17] featuring detection efficiencies of more than 90%[18], low dark-count rates of <1 cps[18], timing jitter of <3 ps[19], and high count rates in the GHz range[20]. Due to their performance they have many applications in the field of quantum information[21] and have found their way into many QKD experiments[22–26]. However, as is the case with APDs, integration with the rest of the photonic circuit is not easily possible and hence the light has to be coupled out of the chip into a fiber before being coupled to the detector, which (in the case of SNSPDs) resides inside a cryostat at low temperatures.

We overcome these issues by employing waveguide-integrated SNSPDs[17,27] and combine them with the full photonic circuitry needed for the receiver side of the QKD setup on a single silicon nitride (Si_3N_4) chip. Thus, we maintain the benefits of high-performance superconducting nanowire detectors while eliminating the need for a separate interface between the measurement setup and the detectors. By utilizing waveguide-integrated SNSPDs we also gain additional benefits compared to traditional SNSPDs, such as shorter detector dead times[17] due to the shorter nanowire geometries. Furthermore, due to the monolithic integration of the photonic circuitry, precise temperature control, and negligible refractive-index dependence on temperature of Si_3N_4 at low temperatures[28], the receiver circuit is interferometrically stable, as desired for QKD protocols utilizing time-bin encoding.

The receiver chip utilizes 3D polymer couplers for out-of-plane coupling of incident light. As compared to grating- and edge-coupling, 3D polymer couplers simultaneously achieve high coupling efficiency over a broad spectral range in scalable two-dimensional arrays[29]. This opens the possibility of employing fully integrated wavelength-division multiplexed QKD systems at large scale.

We demonstrate the capabilities of the receiver chip by implementing a time-bin protocol with one decoy state[16,30] as illustrated in Fig. 1a. In this protocol, the key bits are encoded in the Z basis with the states $|Z_0\rangle$ and $|Z_1\rangle$, corresponding to either an early or a late weak coherent pulse. A third state $|X_+\rangle = \frac{1}{\sqrt{2}}(|Z_0\rangle + |Z_1\rangle)$ is prepared with probability p_X and is used to verify the coherence of two consecutive pulses by monitoring interference with a SPD in one output of an unbalanced Mach–Zehnder interferometer (MZI) on Bob's side (Fig. 1b). The mean photon number of a state is randomly chosen between μ_1 and μ_2 with $\mu_2 < \mu_1 < 1$ with probability p_1 and p_2 respectively in order to implement the decoy-state method. This is later used to

[1]University of Münster, Institute of Physics, Münster, Germany. [2]Center for Nanotechnology (CeNTech), Münster, Germany. [3]Center for Soft Nanoscience (SoN), Münster, Germany.
✉email: wolfram.pernice@uni-muenster.de

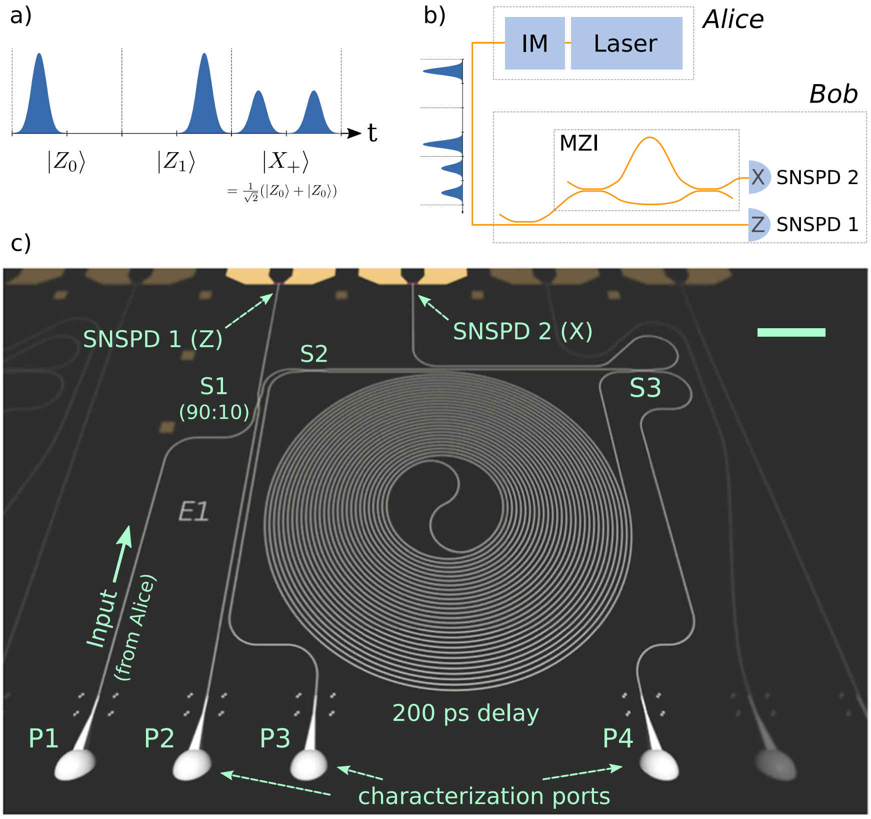

Fig. 1 Three-state time-bin QKD protocol. a For the simplified protocol, three different states from two bases are being used: $|Z_0\rangle$ and $|Z_1\rangle$ correspond to an early and a late time pulse and represent the bits 0 and 1, respectively. The third state $|X_+\rangle$ is the superposition state and is only used to estimate the phase error in the transmission. The coherent pulses are sent with two different intensity levels μ_1 and μ_2 as decoy state in order to detect photon number splitting attacks. **b** The states can be prepared by carving pulses with an intensity modulator (IM) from a CW laser on Alice's side. On Bob's side, the Z basis is measured directly using a superconducting nanowire single-photon detector (SNSPD) while the X basis is measured by placing an SNSPD at the output of an imbalanced Mach–Zehnder interferometer (MZI). **c** Rendering of the circuitry on the receiver chip. The input signal from Alice's side is coupled into a waveguide through a 3D polymer coupler P1. Approximately 90% of the light is guided directly onto SNSPD 1, while the remainder is split by a directional coupler S1 into an MZI with a long delay line in one arm. The directional coupler S2 is designed to cancel out the additional waveguide loss in one arm by the delay line. SNSPD 2 is then used to monitor one output of the MZI. Ports P2, P3, P4 are used for calibration purposes only. Scale bar corresponds to 100 μm.

check the possibility of a photon number splitting (PNS) attack being conducted.

We note that the chip itself is also suitable for other time-based protocols which feature the same photonic circuitry on the receiver side, such as the Differential Phase Shift protocol[31] and the coherent one-way protocol[32]. The photonic circuitry can also easily be adapted to protocols requiring the monitoring of both interferometer outputs by connecting the second output to a third SNSPD, which is already present on the chip presented here but was not used for the QKD measurements.

RESULTS

Receiver design and fabrication

The integrated photonic circuit of the receiver chip is fabricated on the Si_3N_4 photonic platform and the layout is designed with the open source Python-based gdshelpers toolkit[33]. As shown in Fig. 1c, the incoming light is collected by a 3D polymer coupler[29] (P1) into a Si_3N_4 waveguide with a designed width of 1.3 μm. A directional coupler is used to split ~10% of the incoming optical power into the monitoring circuit, while the remaining power is directed to a waveguide-integrated SNSPD (SNSPD 1). The monitoring circuit consists of an unbalanced MZI made of two directional couplers (S2 and S3) and a waveguide spiral in one arm, acting as delay line. The length of the delay line is selected to match the desired operating clock frequency of the QKD system. Because of the non-negligible transmission loss of the spiral compared to the reference arm of the MZI, the splitting ratio of the first directional coupler is adjusted such that the power in both arms at the second directional coupler is approximately equal, maximizing the extinction ratio of the MZI. One output of the MZI is connected to another waveguide-integrated SNSPD (SNSPD 2). The remaining outputs of the three directional couplers are connected to 3D polymer couplers (P2, P3, P4), allowing for a characterization of the MZI and the splitters.

The overall footprint of the device is 840 × 1400 μm, where the vertical dimension is mostly defined by the contact pads of the SNSPDs. The large size of the contact pads is motivated by the measurement setup involving a movable stage and an radio frequency (RF) probe with fixed pitch of 125 μm. The size of the whole device can be easily reduced to less than 800 × 850 μm when targeting a different read-out setup.

The layer stack of the photonic chip consists of 325 nm Si_3N_4 on 3300 nm SiO_2 on a Si substrate. A thin superconducting NbTiN film of 6 nm is sputter-deposited on the sample previous to fabrication.

The fabrication process consists of four steps of electron-beam lithography (Raith EBPG5150) at 100 kV. First, gold contact pads and marker structures are deposited by physical vapor deposition, after which the lithography steps for nanowire fabrication, passivation, and photonic circuitry are performed and etched using reactive ion etching (RIE).

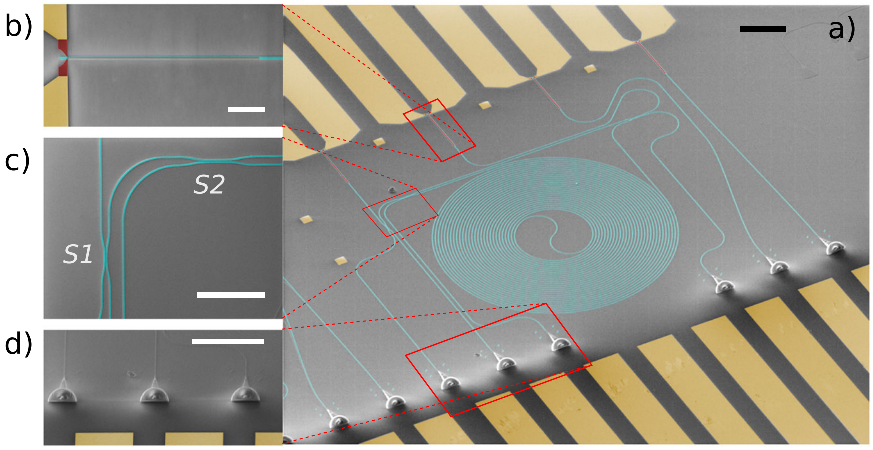

Fig. 2 SEM image of receiver chip. a Colorized scanning electron microscope (SEM) image of the receiver circuit, where the waveguide is cyan colored. Scale bar corresponds to 100 µm. **b** One of the superconducting nanowire single-photon detectors (red) on top of the waveguide (cyan). Scale bar corresponds to 20 µm. **c** The input splitter (S1) redirects ~10% of the incoming light into the MZI, where the length of splitter S2 is adjusted to account for waveguide losses in the spiral. Scale bar corresponds to 50 µm. **d** The 3D couplers allow to vertically couple light over a broad wavelength range into the waveguide. Scale bar corresponds to 100 µm.

The 3D coupling structures are fabricated using a direct laser writing (DLW) system (Nanoscribe Professional GT, ×63 objective) in drop-casted IP-Dip with a slicing and hatching distance of 100 nm. Automatic alignment of the DLW system is performed using additional marker structures which are patterned together with the photonic waveguide structures. The 3D polymer couplers are designed for a light incident angle of 12° and spaced with 127 µm pitch, thereby matching the fiber array used in the measurement setup. A false-color scanning electron microscope (SEM) image of one device on the fabricated chip is pictured in Fig. 2.

A separate fabrication run without nanowires was used to characterize the photonic circuitry and in order to find parameters for the final device. The waveguide loss was determined to be (0.6 ± 0.1) dB/cm. In order to match the target system clock rate of 2.5 GHz, we chose an MZI arm length difference of 1.50 cm, giving an approximate delay time of 200 ps, corresponding to the temporal separation of time bins for information encoding. The directional couplers (S1, S2, S3) are designed with a gap of 200 nm and lengths of $L_1 = 1.03$ µm, $L_2 = 15.66$ µm, $L_3 = 13.18$ µm corresponding to splitting ratios of 90:10, 41:59, and 50:50 respectively.

Each SNSPD consists of a superconducting nanowire with a width of 100 nm, which is placed on top of the waveguide in a single meander turn (U-shape) and is connected to the gold contact pads. The detector has an overall length of 120 µm, thereby maximizing the efficiency of absorption through the evanescent field of the waveguide.

Experimental setup

The experimental setup consists of two spatially separated units representing Alice and Bob in a typical QKD setup, as depicted in Fig. 3. On Alice's side, the sender was implemented using a tunable continuous-wave (CW) laser source (Santec TSL 710) from which pulses are carved using two electro-optic intensity modulators in series (EOM, Optilab IMC-1550-20-PM and Optilab IML-1550-40-PM-V). Both EOMs are driven by a bit-pattern generator (BPG, Agilent 81141A), where the bit rate is set to twice the protocol clock rate (since one symbol consists of two time bins). The first EOM is driven by the CLOCK output of the BPG and produces a pre-modulated signal such that the light is strongest in the center of each time bin. The actual signal modulation is done by the second EOM which is driven by the DATA output. This configuration allows for higher extinction ratios in between the time bins. Both BPG outputs are set to the maximum voltage supported by the BPG of 1.8 V_{pp}. The delay between clock and data signal is adjusted in order to match the travel time in the optical fiber between the two EOMs.

Two consecutive bits constitute one symbol, where 01, 10, and 11 correspond to $|z_0\rangle$, $|z_1\rangle$ and $\sqrt{2}|x_+\rangle$ respectively. The output is tapped and monitored such that the power of the outgoing signal can be tuned to match the desired average number of photons per pulse (μ_1 or μ_2) by a final variable optical attenuator (VOA) before being sent to Bob.

The receiver module is mounted on a movable stage inside a closed-cycle cryostat which is operated at a base temperature of 1.7 K. The optical connection was made using a fiber array held in place above the sample and consisting of single-mode fibers (9/125) with a pitch of 127 µm, while electrical contact is made using an RF probe (Cascade Microtech Unity Probe).

The electrical detector signal is enhanced using low-noise room temperature amplifiers (Mini-Circuits ZFL-1000LN+) with a gain of 50 dB and recorded with a time tagger (Swabian Instruments Time Tagger Ultra), which is connected to a PC where the data collection and evaluation takes place. The time tagger is synchronized with the signal generator on Alice's side by an electrical trigger signal.

The quantum channel between the two parties consists of a single-mode fiber together with a VOA, which is used to simulate channel loss between 0 and 45 dB, corresponding to channel lengths of up to 225 km (assuming fiber loss of 0.2 dB/cm).

Device characterization and QKD measurement

For an estimation of the system's performance, a pseudo-random 128-bit long pattern is repeated continuously by Alice's signal generator. On Bob's side, this allows for two ways of measuring the performance: The time tags can be recorded on the PC and classical cryptographic post-processing (parameter estimation, error correction and privacy amplification) as e.g. described in[34] can then take place afterwards. Alternatively, since the pattern being sent is always the same during the run of an experiment, we can utilize the histogram functionality of the time tagger: by synchronizing the histogram origin with the trigger signal from the pattern generator the resulting histogram perfectly aligns with the repeating pattern. The number of counts in the respective bins can then be used to calculate measures such as key rate and quantum bit error rate (QBER). In addition to the normal QKD pattern we also send different test states, such as multiple consecutive empty bins, which do not occur during the actual

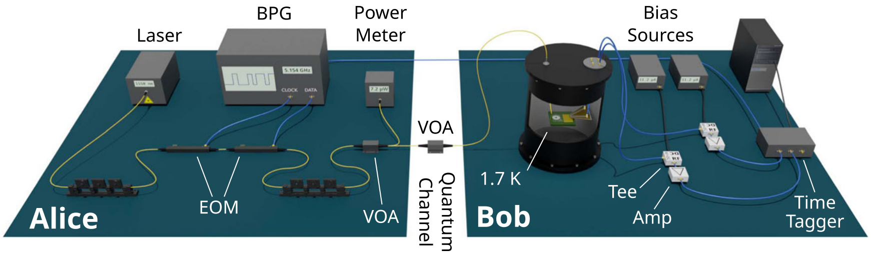

Fig. 3 Measurement setup. Simplified measurement setup for demonstrating a QKD experiment with the receiver chip. A pseudo-random bit pattern is generated on Alice's side with a CW laser and two electro-optic modulators (EOMs) driven by the bit-pattern generator (BPG). The signal is then attenuated and sent to Bob. The quantum channel is simulated by an additional variable optical attenuator (VOA). The receiver chip is hosted in a cryostat at a base temperature of 1.7 K. The electrical signal from the integrated nanowire detectors is amplified and then recorded with a time tagger. The post-processing is performed on a PC.

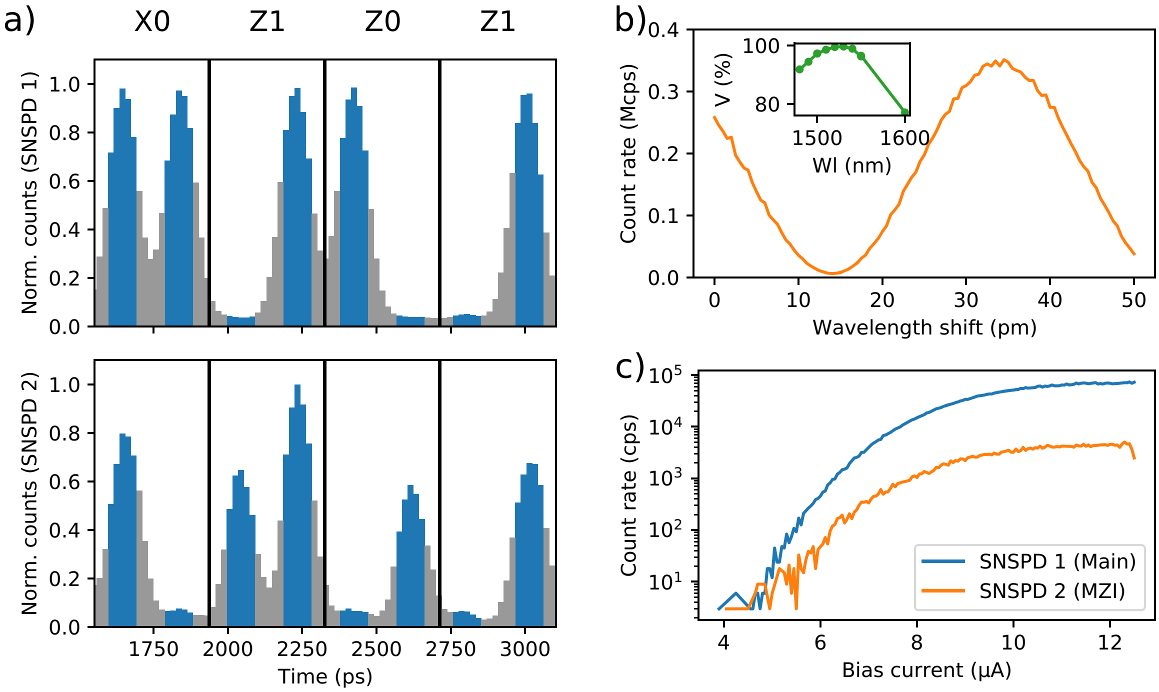

Fig. 4 Detector characterization and histogram. a Excerpt of a histogram of the clicks of the main detector (top) and the monitor detector after the MZI (bottom) when sending a pseudo-random pattern. During the post-processing phase, a gating window is applied such that only the counts in the center of each time bin are counted (blue), while the other counts are ignored (gray). This reduces both the count rate and the error rate and maximizes the secret-key rate when the optimized window width is chosen. **b** Count rate vs. wavelength around a center wavelength of 1550 nm for SNSPD 2, measured with an incident flux of 10^8 photons per second. The MZI visibility was determined to be 96.4% at 1550 nm and 99.6% at 1530 nm. Inset: The visibility V of the MZI over different wavelengths. **c** Countrate vs. bias current of both SNSPDs with an incident flux of ~10^6 photons per second at 1550 nm through input port P1. SNSPD 2 shows a considerably lower count rate due to the splitting ratio of S1 and the MZI in front of the detector.

QKD transmission. This can be used to gain a better understanding of the contributions of the different error sources and to bound the influence of the receiver chip on the error rate, as described in the next section. For each level of attenuation in the quantum channel we integrate over a time span of 5 min.

The histogram is recorded with a bin width of 19 ps, such that ~10 bins correspond to a protocol time-bin and are resampled to match the protocol bins during the post-processing step. Although the SNSPDs are operated in a free-running mode, post-selecting events which are centered in the respective time bins can be advantageous for the resulting secret-key rate. This is implemented in software on Bob's side by only choosing a subset of the recorded histogram bins and the resulting bin size is tuned depending on the results of the parameter estimation. This is also exemplarily illustrated in Fig. 4a, where the histogram bins in blue are considered in the evaluation, while counts in the gray bins are omitted.

While the delay line in the receiver is designed for a delay of 200 ps, a slight deviation in the pulse delay of the fabricated device is expected since the effective group index is impacted by uncertainties in the wafer material composition and fabrication process as well as the experimental temperature and environment. By observing a single femtosecond pulse going through the fabricated MZI in the cryogenic environment, a more precise estimation of the actual delay can be determined. The pulse is generated by a Pritel 1550 nm Femtosecond Laser, coupled into P4, measured with a fast photo diode through P3 and observed with a 13 GHz oscilloscope. The actual pulse delay is determined to be 194(5) ps, corresponding to a clock rate of $R = 2.6$ GHz.

Because the visibility of the MZI is later used to estimate the phase-error rate, it is important to properly characterize the MZI in advance. A visibility of 99.6% was measured by illuminating P1 with a tunable CW laser source and recording the count rates around a center wavelength of 1530 nm. At a center wavelength of 1550 nm the visibility drops to 96.4% (Fig. 4b). The wavelength-dependence of the visibility is plotted in Fig. 4b (inset) and can be attributed to the wavelength-dependence of the MZI input splitter (directional coupler) S2. Only when the splitting ratio matches the optical loss in the delay line can a high visibility be achieved. While this can be seen as a limitating factor on the broadband operation of a single device, we note that for the use case of a highly wavelength-division multiplexed application this does not pose a limitation as the input splitter can be individually adjusted for each channel. Alternatively, one can use the existing characterization ports before and after the MZI to fully characterize the visibility and include this in the calculation of the phase-error rate.

Utilizing waveguide-integrated SNSPDs allows for very short dead times without jeopardizing the low dark-count rates that SNSPDs offer. This allows for much higher detection rates on the receiver side, which is especially relevant for small-distance (i.e. low-loss) channels. For our receiver, the detector dead time was measured to be lower than 20 ns, allowing for detection rates of up to 50 MHz. The switching currents of the two nanowires have been determined to be 12.7 and 12.5 µA, respectively. For the experiment, both are biased with a bias voltage of $U_b = 11.15$ V with a series resistor of 992 kΩ. With these settings, the dark-count rate was measured to be 8 and 20 Hz for SNSPD 1 and 2, respectively. Estimation of the system detection efficiency (SDE) yields 7.35% for the main SNSPD and 0.5% for the second SNSPD at the chosen bias current (Fig. 4c). We stress that these numbers include the splitter S1 and the waveguide loss in the MZI and the exact efficiencies of the detectors cannot be characterized individually, since the photonic circuitry in front of the nanowires prevents direct optical access. Further coupling losses are induced by the flexible stage setup inside the cryostat: the electrical probe and the fiber array cannot be moved independently from each other in z direction relative to the chip and thus the optimal coupling position may not be reachable. Therefore, the efficiency indications pose a lower limit and can likely be surpassed by fixing the chip to the fiber array in an optimized position, as would be done in a packaged version of the integrated photonic circuit.

With the state-preparation parameters used in this work (Table 1), the small dead times mean that the detectors will not be fully saturated even for zero loss and explains why very little detector-induced key-rate saturation is observable in Fig. 5a, where the raw-key rate and secret-key rate of the proof-of-principle experiment is plotted over the channel attenuation. We achieve high secret-key rates of up to 2.5 Mbit/s for small attenuation levels.

Table 1. Measurement parameters for the QKD transmission.

Attenuation (dB)	Length (km)	μ_1	μ_2	p_1	p_2	n_b
2.5	12.5	0.18	0.07	0.4	0.6	6
5	25	0.23	75	0.45	0.55	7
7.5	37.5	0.23	75	0.45	0.55	5
10	50	0.26	0.1	0.5	0.5	5
15	75	0.35	0.14	0.6	0.4	5
20	100	0.5	0.15	0.7	0.3	4
25	125	0.5	0.15	0.7	0.3	4
30	150	0.5	0.15	0.7	0.3	4
35	175	0.5	0.15	0.7	0.3	4
40	200	0.5	0.15	0.7	0.3	3
45	225	0.5	0.15	0.7	0.3	1

The given length is the corresponding fiber length with an assumed attenuation of 0.2 dB km^{-1}. μ_1 and μ_2 are the mean photon numbers for the two decoy-state levels which are sent with a probability of p_1 and p_2, respectively. n_b is the number of histogram time bins used in the final evaluation, as illustrated in Fig. 4c.

DISCUSSION

The actual key distribution experiment was performed at a center wavelength of 1530 nm for different levels of channel attenuation, thereby simulating transmission distances of different lengths. We note that this method does not account for potential dispersion effects and channel instabilities which would be present in field links. However, as these can be easily compensated and because

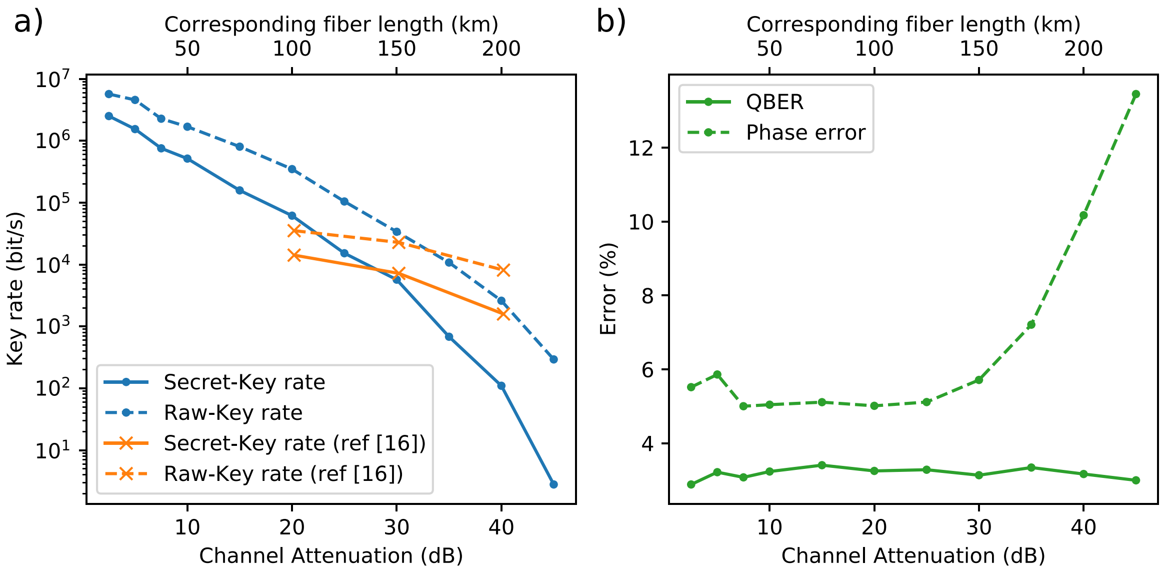

Fig. 5 Key rates and error rates. **a** Measured key rates and error rates over different levels of channel attenuation. With the demo setup we achieve 2.5 Mbit/s for an attenuation of 2.5 dB. Compared to the reference implementation[16] our setup benefits from the shorter dead times of the detectors at low attenuation. **b** Quantum bit error rate (QBER) and phase-error rates vs. channel attenuation. Due to the low dark-count rates (DCR) of the SNSPDs no increase in QBER is observable for higher attenuations. Because only a small fraction of the incoming light reaches the second SNSPD, the signal-to-noise ratio is much smaller and hence the DCR leads to an increase in the phase-error rate for channel attenuation levels higher than 25 dB.

the focus of this work is the integrated receiver chip, the results presented here should be equally reproducible in a field-deployed quantum channel.

We find a QBER between 3% and 3.5% for channel attenuation up to 45 dB, while the phase-error of around 5% for low attenuation levels grows much stronger with higher attenuation levels, reaching 13% at 45 dB.

The QBER is strongly influenced by the ratio of dark counts and real counts. Since counts in SNSPD 1 are about two orders of magnitude higher even for the highest measured attenuation of 45 dB, the effect on the QBER is relatively small and thus the dependency of the QBER on the channel attenuation as shown in Fig. 5b is small. In the phase monitoring channel, however, the real count rate is much lower due to the splitting ratio of S1, the losses in the interferometer and the fact that only the output port of the MZI with destructive interference is monitored. This leads to a much higher influence of dark counts on the phase-error rate, as can be seen in Fig. 5b for attenuation levels higher than 25 dB.

Other error sources contributing to both the QBER and phase-error rate are the imperfect state preparation on Alice's side, pulse dispersion in the quantum channel (including the circuitry of the receiver setup) and detector jitter. We determined the full width at half-maximum (FWHM) jitter of the first SNSPDs to be 59 ps. This could be further improved by employing cryogenic amplifiers[19]. With a bin width of 200 ps, events which will be detected near the edge of a time bin have a non-negligible probability to be associated with the wrong time bins, hence leading to an error.

In order to more tightly bound the effects of error sources on the QBER which originate from the receiver chip, their impact can be studied by sending multiple subsequent 0 bits, where the second EOM should be completely closed, and comparing the number of (error) clicks in the center of such a 0-series with the number of clicks in between two pulses (when sending 1–0–1). In the first case, the clicks cannot originate from detector jitter or dispersion and thus the ratio between the two numbers gives a bound on the error induced by the receiver module. With this method, the fraction of the QBER caused by the receiver module can be bound to be smaller than 13%, showing that the vast majority of the QBER is caused by the sender setup.

For the evaluation of the actual secret-key rate pictured in Fig. 5a we follow the finite-key analysis of[30] and assume a secret-key length of

$$l \leq s_{Z,0} + s_{Z,1}(1 - h(\phi_Z)) - \lambda_{\mathrm{leak}} - 6\log_2(19/\epsilon_{\mathrm{sec}}) - \log_2(2/\epsilon_{\mathrm{cor}}), \tag{1}$$

where $s_{Z,0}$, $s_{Z,1}$ are lower bounds on the number of clicks caused by vacuum and single-photon states in the Z basis respectively, h is the binary entropy function, ϕ_Z is an upper bound for the phase-error rate, ϵ_{sec} is a secrecy parameter and ϵ_{cor} the correctness parameter as defined in[35]. We set $\epsilon_{\mathrm{sec}} = \epsilon_{\mathrm{cor}} = 10^{-9}$. The number of leaked bits during error correction λ_{leak} are estimated with an assumed reconciliation efficiency of 1.16 for a block size of 10^{7}[36].

The results achieved with the proof-of-principle experiment using the receiver chip are comparable with recent publications implementing similar protocols. Compared to the reference implementation of the three-state protocol[16], we benefit from short dead times at low dark-count rates and are able to achieve higher secret-key rates at lower attenuation levels below 20 dB. Implementations such as[37] achieve even higher secret-key rates for very low attenuation levels of 2 dB by utilizing self-differencing InGaAs APDs[38] which allow for dead-times similar to the ones reported herein. However, while the main bottleneck of our implementation is the sender side, InGaAs APDs show a significantly higher dark-count rate which a substantial fraction of the measured QBER can be attributed to at low attenuation levels[37]. Because of the low dark-count rates of waveguide-integrated SNSPDs we overcome this limitation in our receiver implementation. Since our platform allows for the integration of even faster waveguide-integrated SNSPDs with similarly low dark-count rates[20] we are far from reaching the theoretical performance limits of the underlying technology in a QKD receiver unit. We note that future studies are neccessary to evaluate to which extent the waveguide-integrated SNSPDs are susceptible to attacks such as detector blinding[39,40] and to identify possible countermeasures.

Overall, in this work we show for the first time a fully integrated photonic receiver module for DV-QKD applications. The receiver is fabricated on the low-loss Si_3N_4 photonic platform and features all photonic components, including high-performance SPDs, needed for performing the quantum measurements of Bob for various time-based QKD protocols.

Because of the vertical out-of-plane coupling, realizing 2D arrays consisting of many such receiver devices on a single chip become feasible. Together with on-chip spectrometric devices, which have been demonstrated for the Si_3N_4 platform in various shapes[41–44], a fully integrated multichannel wavelength-division multiplexed receiver module, where one broadband coupler serves as input for many spectrally separated channels, each served by two individual SNSPDs, can be realized in the future. This requires many waveguide-integrated SNSPDs to be operated in parallel on a single chip, which has previously been demonstrated[45].

While the need for a cryogenic environment is common to all QKD systems employing supercoducting SPDs, the benefits of the all-integrated optical setup in terms of stability and overall complexity could be a major step towards the realization of large-scale QKD server stations[46]. The unique combination of broadband 3D polymer couplers, low-loss photonic waveguides and state-of-the-art single-photon detector technology thus paves the way for scalable and stable high-performance QKD receiver modules in the future.

METHODS

Fabrication

In order to minimize absorption loss of the Si_3N_4 waveguides, the sample is initially annealed at 1100 °C. We then deposit NbTiN thin films (6 nm) using a single Nb/Ti alloy target in an Ar/N_2 atmosphere via a DC magnetron sputter deposition process. This process is done at room-temperature while we apply a RF bias to our substrate, which has shown to enhance the growth of ultra-thin films[47].

The gold contact pads and markers are made by spin-coating a 340 nm layer of PMMA, exposing it with a dose of 1400 $\mu C\,cm^{-2}$ and developing it with a solution of methyl isobutyl ketone and isopropanol in the ratio 1:3 for 3 min. 7 nm of Cr and 70 nm of Au is then evaporated on the sample using electron-beam physical vapor deposition (EB-PVD) and lift-off is performed in acetone.

A 7 nm layer of SiO_2 is then deposited with EB-PVD as an adhesion layer for the negative-tone electron-beam resist HSQ, which is spin-coated with a thickness of 120 nm and exposed with a dose of 1900 $\mu C\,cm^{-2}$. The nanowires are developed for 10 min in MF-319 and reacitve-ion etched under an SF_6/Ar atmosphere for 290 s. Another layer of HSQ is spin-coated, patterned and developed with the same parameters around the nanowires as a protection buffer, but no etching is performed.

For the photonic circuitry, 350 nm of negative-tone electron-beam resist AR-N 7520.12 is spin-coated and pre-baked for 60 s at 85 °C. The pattern is exposed with a dose of 1450 $\mu C\,cm^{-2}$ and a beam current of 10 nA. Development is performed in MF-319 for 60 s and the sample is subsequently hard-baked at 85 °C for 60 s. The structures are then reactive-ion etched for 380 s in a CHF_3/ O_2 plasma and remaining resist is removed using 10 min of O_2 plasma.

Finally the 3D coupling structures are fabricated by means of DLW as described in the main text. Subsequently, the chip is developed in acetone and rinsed with IPA.

Measurement

The detectors are first characterized by recording I–V curves without light by sweeping the bias voltage from 0 to 14 V and back using a Keithley

2400 multimeter and a series resistor of 992 kΩ. The SDE is then measured by coupling light with a calibrated photon flux into port P1, where photon flux is set by measuring the laser power right before the input fiber of the cryostat and attenuating to the desired level. The count rate is then recorded during a bias voltage sweep. By performing the same procedure with the laser turned off we determine the dark-count rate. The difference then yields the SDE at different bias levels. For the jitter measurement we send a short laser pulse (Pritel 1550 nm Femtosecond Laser) through a splitter, where one half is forwarded directly to the device and the second half is recorded using a fast photo dioide (New Focus 1554-B) and an electrical oscilloscope (Agilent infiniium 54855A). The RF output of the bias tee from the detector is connected to a second channel of the oscilloscope. We determine the jitter from the FWHM of the resulting correlation histogram.

For determining the actual mean photon number per pulse on Alice's side we tap half of the outgoing light with a previously characterized 50:50 splitter and measure with a low-noise power meter (HP 8163A with HP 81635A). As variable optical attenuators we use cascaded fiber-coupled MEMS attenuators driven by a 12-bit DAC which we calibrate individually for wavelengths in the range from 1480 to 1610 nm. Two attenuators are used to set the output power from Alice and two further attenuators are used to simulate the channel attenuation.

The polarization is optimized on Alice's side to maximize the count rate for SNSPD 1 on Bob's side. No additional polarizers are used on Bob's side in our setup.

The parameters for the state preparation at different attenuation levels are listed in Table 1. The pseudo-random symbol pattern used for the transmission is generated once and uploaded to the BPG. The same pattern was used for all levels of attenuation.

Post-processing

The histogram data recorded by the time tagger is processed using a Python interface. One recording session consists of 5 min measurement time after which the histogram data is read and evaluated. The delay between the trigger signal and the click events is determined for both SNSPDs individually by sending a repeating signal pattern consisting mostly of 0 pulses and aligning the resulting histograms. The optimal number of histogram time bins to be included in the key-rate calculation (see Fig. 4c) is determined individually for each channel attenuation such that the optimal secret-key rate is achieved for that attenuation level.

DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author upon reasonable request.

Received: 14 September 2020; Accepted: 13 January 2021;
Published online: 23 February 2021

REFERENCES

1. Soeken, M., Haener, T. & Roetteler, M. Programming quantum computers using design automation. in 2018 Design, Automation & Test in Europe Conference & Exhibition (DATE), 137–146 https://doi.org/10.23919/DATE.2018.8341993 (2018).
2. Arute, F. et al. Quantum supremacy using a programmable superconducting processor. *Nature* **574**, 505–510 (2019).
3. Shor, P. W. Algorithms for quantum computation: discrete logarithms and factoring. In Proceedings 35th Annual Symposium on Foundations of Computer Science 124–134 https://doi.org/10.1109/SFCS.1994.365700 (IEEE Comput. Soc. Press, 1994).
4. Mavroeidis, V., Vishi, K., Zych, M. D. & Jøsang, A. The impact of quantum computing on present cryptography. *Int. J. Adv. Comput. Sci. Appl.* 9, (2018).
5. Bennett, C. H. & Brassard, G. Quantum cryptography: quantum key distribution and coin tossing. *Proc. IEEE Int. Conf. Comput. Syst. Signal Process.* 175–179 (1984).
6. Bennett, C. H., Bessette, F., Brassard, G., Salvail, L. & Smolin, J. Experimental quantum cryptography. *J. Cryptol.* **5**, 3–28 (1992).
7. Shannon, C. E. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **28**, 656–715 (1949).
8. Zhang, G. et al. An integrated silicon photonic chip platform for continuous-variable quantum key distribution. *Nat. Photonics* **13**, 839–842 (2019).
9. Orieux, A. & Diamanti, E. Recent advances on integrated quantum communications. *J. Opt.* **18**, 083002 (2016).
10. Ding, Y. et al. High-dimensional quantum key distribution based on multicore fiber using silicon photonic integrated circuits. *npj Quantum Inf.* **3**, 1–7 (2017).
11. Ma, C. et al. Silicon photonic transmitter for polarization-encoded quantum key distribution. *Optica* **3**, 1274–1278 (2016).
12. Sibson, P. et al. Chip-based quantum key distribution. *Nat. Commun.* **8**, 13984 (2017).
13. Sibson, P. et al. Integrated silicon photonics for high-speed quantum key distribution. *Optica* **4**, 172–177 (2017).
14. Semenenko, H. et al. Chip-based measurement-device-independent quantum key distribution. *Optica* **7**, 238–242 (2020).
15. Hadfield, R. H. Single-photon detectors for optical quantum information applications. *Nat. Photonics* **3**, 696–705 (2009).
16. Boaron, A. et al. Simple 2.5 GHz time-bin quantum key distribution. *Appl. Phys. Lett.* **112**, 171108 (2018).
17. Ferrari, S., Schuck, C. & Pernice, W. Waveguide-integrated superconducting nanowire single-photon detectors. *Nanophotonics* **7**, 1725–1758 (2018).
18. Marsili, F. et al. Detecting single infrared photons with 93% system efficiency. *Nat. Photonics* **7**, 210–214 (2013).
19. Korzh, B. et al. Demonstration of sub-3 ps temporal resolution with a superconducting nanowire single-photon detector. *Nat. Photonics* **14**, 250–255 (2020).
20. Münzberg, J. et al. Superconducting nanowire single-photon detector implemented in a 2D photonic crystal cavity. *Optica* **5**, 658–665 (2018).
21. You, L. Superconducting nanowire single-photon detectors for quantum information. *Nanophotonics* **9**, 2673–2692 (2020).
22. Hadfield, R. H., Habif, J. L., Schlafer, J., Schwall, R. E. & Nam, S. W. Quantum key distribution at 1550nm with twin superconducting single-photon detectors. *Appl. Phys. Lett.* **89**, 241129 (2006).
23. Takemoto, K. et al. Quantum key distribution over 120 km using ultrahigh purity single-photon source and superconducting single-photon detectors. *Sci. Rep.* **5**, 14383 (2015).
24. Liu, Y. et al. Experimental twin-field quantum key distribution through sending or not sending. *Phys. Rev. Lett.* **123**, 100505 (2019).
25. Wang, S. et al. Beating the fundamental rate-distance limit in a proof-of-principle quantum key distribution system. *Phys. Rev. X* **9**, 021046 (2019).
26. Fang, X.-T. et al. Implementation of quantum key distribution surpassing the linear rate-transmittance bound. *Nat. Photonics* **14**, 422–425 (2020).
27. Pernice, W. H. P. et al. High-speed and high-efficiency travelling wave single-photon detectors embedded in nanophotonic circuits. *Nat Commun* **3**, 1325 (2012).
28. Elshaari, A. W., Zadeh, I. E., Jons, K. D. & Zwiller, V. Thermo-optic characterization of silicon nitride resonators for cryogenic photonic circuits. *IEEE Photonics J.* **8**, 1–9 (2016).
29. Gehring, H., Eich, A., Schuck, C. & Pernice, W. H. P. Broadband out-of-plane coupling at visible wavelengths. *Opt. Lett.* **44**, 5089 (2019).
30. Rusca, D., Boaron, A., Grünenfelder, F., Martin, A. & Zbinden, H. Finite-key analysis on the 1-decoy state QKD protocol. *Appl. Phys. Lett.* **112**, 171104 (2018).
31. Inoue, K., Waks, E. & Yamamoto, Y. Differential phase shift quantum key distribution. *Phys. Rev. Lett.* **89**, 037902 (2002).
32. Stucki, D., Brunner, N., Gisin, N., Scarani, V. & Zbinden, H. Fast and simple one-way quantum key distribution. *Appl. Phys. Lett.* **87**, 194108 (2005).
33. Gehring, H., Blaicher, M., Hartmann, W. & Pernice, W. H. P. Python based open source design framework for integrated nanophotonic and superconducting circuitry with 2D-3D-hybrid integration. *OSA Contin.* **2**, 3091 (2019).
34. Ma, X., Fung, C.-H. F., Boileau, J.-C. & Chau, H. F. Practical post-processing for quantum-key-distribution experiments. *Comput. Secur.* **30**, 172–177 (2011).
35. Rusca, D., Boaron, A., Curty, M., Martin, A. & Zbinden, H. Security proof for a simplified BB84-like QKD protocol. *Phys. Rev. A* **98**, 052336 (2018).
36. Martinez-Mateo, J., Pacher, C., Peev, M., Ciurana, A. & Martin, V. Demystifying the information reconciliation protocol cascade. *Quantum Inf. Comput.* **15**, 453–477 (2015).
37. Yuan, Z. L. et al. 10-Mb/s quantum key distribution. *J. Light. Technol.* **36**, 3427–3433 (2018).
38. Yuan, Z. L., Kardynal, B. E., Sharpe, A. W. & Shields, A. J. High speed single photon detection in the near infrared. *Appl. Phys. Lett.* **91**, 041114 (2007).
39. Lydersen, L. et al. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nat. Photonics* **4**, 686–689 (2010).
40. Tanner, M. G., Makarov, V. & Hadfield, R. H. Optimised quantum hacking of superconducting nanowire single-photon detectors. *Opt. Express* **22**, 6734 (2014).
41. Hammood, M. et al. Compact, silicon-on-insulator, series-cascaded, contradirectional-coupling-based filters with >50 dB adjacent channel isolation. *Opt. Lett.* **44**, 439–442 (2019).
42. Cheng, R. et al. Broadband on-chip single-photon spectrometer. *Nat. Commun.* **10**, 4104 (2019).
43. Schuler, L. P., Milne, J. S., Dell, J. M. & Faraone, L. MEMS-based microspectrometer technologies for NIR and MIR wavelengths. *J. Phys. Appl. Phys.* **42**, 133001 (2009).

44. Hartmann, W. et al. Waveguide-integrated broadband spectrometer based on tailored disorder. *Adv. Opt. Mater.* **8**, 1901602 (2020).
45. Wolff, M. A. et al. Waveguide-integrated superconducting nanowire singlephoton detector array for ultra-fast quantum key distribution. in Conference on Lasers and Electro-Optics SM4O.5 https://doi.org/10.1364/CLEO_SI.2020.SM4O.5 (OSA, 2020).
46. Zhang, P. et al. Reference-frame-independent quantum-key-distribution server with a telecom tether for an on-chip client. *Phys. Rev. Lett.* **112**, 130501 (2014).
47. Dane, A. E. et al. Bias sputtered NbN and superconducting nanowire devices. *Appl. Phys. Lett.* **111**, 122601 (2017).

ACKNOWLEDGEMENTS

This work was supported by the Federal Ministry of Education and Research of Germany through QuPAD and SINPHOSS. We also gratefully acknowledge support by the European Research Council through grant 724707. H.G. thanks the Studienstiftung des deutschen Volkes for financial support. C.S. acknowledges support from the Ministry for Culture and Science of North Rhine-Westphalia (421-8.03.03.02-130428).

AUTHOR CONTRIBUTIONS

F.B. developed the device layout and the experiment. M.A.W. deposited the NbTiN layer. H.G. fabricated the 3D polymer couplers. F.B. fabricated the sample, implemented the experiment, and evaluated the data. C.S. and W.P. supervised the research and experiment. All authors contributed to the writing of the manuscript.

FUNDING

Open Access funding enabled and organized by Projekt DEAL.

COMPETING INTERESTS

The authors declare no competing interests.

ADDITIONAL INFORMATION

Correspondence and requests for materials should be addressed to W.P.

Reprints and permission information is available at http://www.nature.com/reprints

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