OPEN ACCESS

# A fully automated entanglement-based quantum cryptography system for telecom fiber networks

New Journal of Physics
The open-access journal for physics

# A fully automated entanglement-based quantum cryptography system for telecom fiber networks

**Alexander Treiber[1], Andreas Poppe[2], Michael Hentschel[3], Daniele Ferrini[1], Thomas Lorünser[2], Edwin Querasser[2], Thomas Matyus[2], Hannes Hübel[1] and Anton Zeilinger[1,3,4]**

[1] Quantum Optics, Quantum Nanophysics and Quantum Information, Faculty of Physics, University of Vienna, Boltzmanngasse 5, 1090 Vienna, Austria

[2] Austrian Research Centers GmbH—ARC, Donau-City-Str. 1, 1220 Vienna, Austria

[3] Institute for Quantum Optics and Quantum Information, Austrian Academy of Sciences, Boltzmanngasse 3, 1090 Vienna, Austria

E-mail: anton.zeilinger@univie.ac.at

*New Journal of Physics* **11** (2009) 045013 (19pp)
Received 17 January 2009
Published 30 April 2009
Online at http://www.njp.org/
doi:10.1088/1367-2630/11/4/045013

**Abstract.** We present in this paper a quantum key distribution (QKD) system based on polarization entanglement for use in telecom fibers. A QKD exchange up to 50 km was demonstrated in the laboratory with a secure key rate of 550 bits $s^{-1}$. The system is compact and portable with a fully automated start-up, and stabilization modules for polarization, synchronization and photon coupling allow hands-off operation. Stable and reliable key exchange in a deployed optical fiber of 16 km length was demonstrated. In this fiber network, we achieved over 2 weeks an automatic key generation with an average key rate of 2000 bits $s^{-1}$ without manual intervention. During this period, the system had an average entanglement visibility of 93%, highlighting the technical level and stability achieved for entanglement-based quantum cryptography.

[4] Author to whom any correspondence should be addressed.

## Contents



## 1. Entanglement-based quantum key distribution (QKD)

Quantum cryptography, or more specifically QKD, is the most advanced quantum information protocol, with its potential for commercial use. Since its introduction for the first time 25 years ago with the BB84 protocol [1], which, based on the single-particle encoding ideas of Wiesner, did not use entanglement yet, the field has advanced enormously both in theoretical development and experimental realizations. Most significant was the proposal [2] of entanglement-based quantum cryptography. There exists now a wide variety of different physical implementations, each with their own advantages and disadvantages. The interested reader is referred to the reviews [3, 4].

When the QKD protocols using entanglement were developed [2, 5], the use of this resource for practical QKD devices was regarded as limited because of its higher technological challenges. The onset of highly efficient down-conversion sources for entangled photon pairs [6] has changed this situation significantly. Whereas the rate and distance of early demonstrations of entanglement-based QKD [7]–[9] were still limited by the efficiency of the sources, technological advances in the meantime [10, 11] have shifted the limitations to the single photon detectors.

Although difficult to realize, there are reasons for preferring entanglement. This has been recently highlighted by the development of device-independent security proofs [12], which do not require an *a priori* trust of the QKD device. We would also like to stress that the developments in reliable and long distance entanglement-based QKD are useful not

only for the cryptographic community. Since entanglement is the resource of many other quantum communication and quantum computation protocols, these would also profit from the developments in entanglement-based QKD. We are therefore convinced that the technologies developed for entanglement-based systems will benefit the quantum information community as a whole.

To date, most entanglement systems employ free space links where a wavelength of about 800 nm is used. Inner-city links were realized [13]–[15] as well as long distance QKD over 144 km between two islands [16]. Early fiber-based implementations have also used a wavelength at 810 nm [7, 17], thereby heavily restricting the distances due to the high absorption of optical fibers in this region. The use of entanglement for QKD experiments performed at telecom wavelengths has been very sparse [18]–[20], which comes as a surprise given the multitude of entanglement distribution experiments in telecom fibers over the last years [21]–[25].

We present here an entanglement-based QKD system designed to work at 1550 nm for optimal distribution in optical fibers. Our QKD system is realized as a compact portable device offering reliable and stable key generation. The start-up and alignment process is completely automated. Stabilization routines guarantee hands-off and long-term operation. In this paper, we show the performance of our device both in the laboratory where we achieved a 50 km transmission and in the real world where we demonstrated for the first time a long-term and high-fidelity QKD based on entanglement using deployed telecom fibers [19, 20].

## 2. Description of the entangled QKD system

In this section an overview of the system, as depicted in figure 1, is given together with an explanation of some of the subsystems. The complete set-up consists of the units 'Alice' and 'Bob', two computers, a classical communication link and a quantum channel. A detailed description of the modules involved in the automation and stabilization is given in section 4.

### *2.1. Alice*

The core of Alice's unit is the polarization-entangled photon source emitting pairs with asymmetric wavelengths (810 and 1550 nm) [23]. A 532 nm cw laser pumps two ppKTP crystals for type-I spontaneous parametric down-conversion (SPDC). The two crystals are poled for collinear emission of 810 and 1550 nm. Arranged in the scheme of Kwiat *et al* [26], the polarization state after the two crystals is given by

$$|\phi\rangle = \frac{1}{\sqrt{2}}\left(|H_{810}H_{1550}\rangle + \mathrm{e}^{\mathrm{i}\phi}|V_{810}V_{1550}\rangle\right). \tag{1}$$

The pair is separated inside the source using a dichroic mirror and each photon is coupled into a single mode optical fiber. At the 810 nm side, an additional bandpass filter ($810 \pm 0.5$ nm) is placed before the fiber to limit the bandwidth of the photons.

The 810 nm photons pass an in-fiber polarization controller before entering the BB84 module. Here the photons are recollimated onto a balanced beamsplitter (BS) and then directed to two cube polarizing beamsplitters (PBS). The PBSs are rotated by 45° relative to each other to perform measurements in the 0°/90° (H/V) and in the +45°/−45° (P/M) bases. The four output ports of the PBSs are coupled into multimode fibers connected to an array of four Si-APDs (SPCM-AQ4C from PerkinElmer). The TTL outputs from the detectors are fed into an

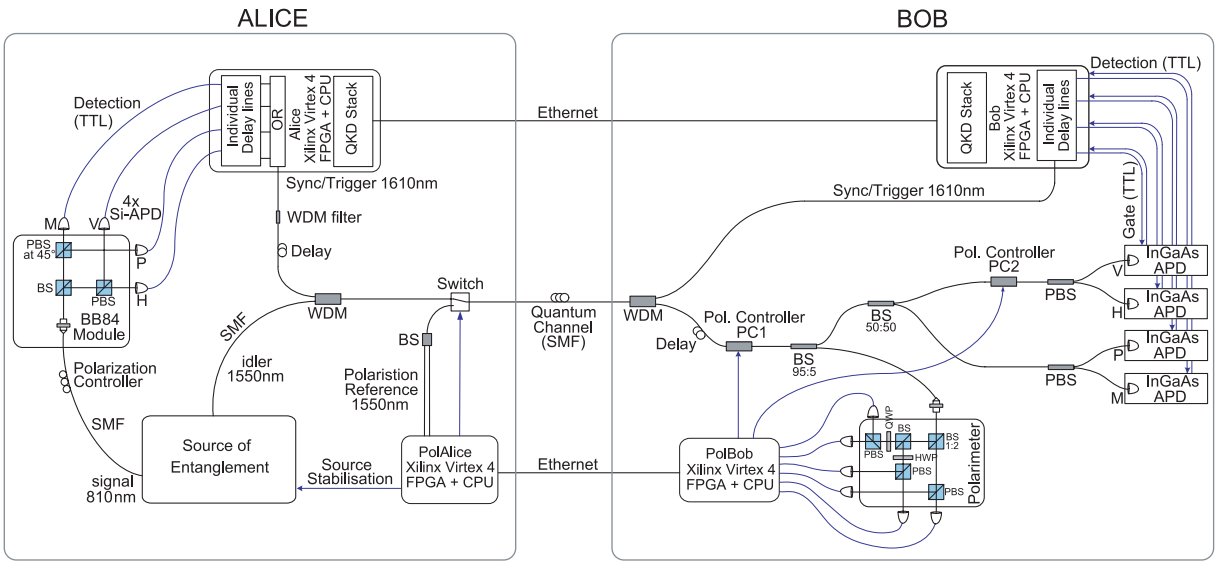


**Figure 1.** Layout of the entanglement-based QKD system. Alice contains the source of polarization entangled photons, a polarization analysis module (BB84), four Si-APDs and an electronic processing board. Furthermore, components for generation of the trigger signals and part of the polarization control module are also included in Alice (PolAlice). On Bob's side, an all-fiber BB84 module can be found together with four InGaAs detectors. The receiver part of the polarization control (Polarimeter) and the necessary electronics are also located at Bob (PolBob). A fully automated polarization alignment can be performed using the electronic polarization controllers PC1 and PC2. The necessary connections between Alice and Bob for a secure key generation are a single mode fiber and a classical network connection.

electronics board (Virtex-4 FX20 from Xilinx) for further processing. All events are logged on the embedded CPU (PowerPC 405), where the raw key is passed to a large buffer for subsequent key distillation.

Within Alice's unit, the optical fiber carrying the 1550 nm photons is first combined in a wavelength division multiplexer (WDM) with a trigger line and the fiber then passes an optical switch necessary for the operation of the polarization control. The fiber is connected at the front of Alice's case to the quantum channel, which consists of a single mode telecom fiber, allowing the 1550 nm photons to travel to Bob.

### *2.2. Bob*

At Bob's unit, only telecom wavelengths are present, so almost all optical components are fiber based. First, a WDM-demultiplexer separates the trigger signal from the single photons. After a delay line of 32 m, the photons pass through the electronic polarization controller PC1 (PolaRite II from General Photonics) after which 5% are directed to the classical polarimeter. The main fraction of 95% enters Bob's fiber-based BB84 module, where a balanced BS (50:50) randomly selects the measurement basis. One arm of the BS leads directly to a PBS, whereas the other arm is attached to another polarization controller PC2 before a second PBS. This polarization

controller allows us to rotate the measurement axis of the second basis relative to the first. The outputs of both PBSs are connected to four InGaAs-APDs (id-201 from IdQuantique). The generated detector signals are analyzed by Bob's Virtex-4 electronics.

### *2.3. Synchronization*

Since the InGaAs detectors require a gate voltage when a photon is expected, a synchronized timing channel is needed. We opted for a time and wavelength multiplexed optical trigger signal, which also runs over the quantum channel to implement a one-fiber solution. Since the SPDC is pumped with a cw-laser, timing information can only come from the pair itself. Every time a 810 nm photon is detected at Alice, a strong optical pulse at 1610 nm is generated. The sideband emission at about 1550 nm from the laser diode is sufficiently suppressed by additional filters. A WDM-multiplexer combines each 1550 nm photon with its trigger pulse, which follows the single photon by a few nanoseconds to reduce Raman scattering effects. Arriving at Bob, the trigger pulses are converted into electronic signals, which gate all four InGaAs detectors. Since the conversion takes some time, the single 1550 nm photons are delayed in order to arrive at the appropriate time at the detectors.

### *2.4. 19-inch packaging*

The system was designed for use in installed optical networks; hence further steps had to be taken to facilitate handling and installation of the devices. It was decided to comply with a standard size and the units at Alice and Bob were required to fit into a 19-inch rack, as shown in figure 2.

The unit at Alice has a two-level structure, with the entanglement source and the BB84 module on the bottom to keep the thermal effects low. To enhance the stability of the source, all optical elements were mounted on a monolithic base plate ($42 \times 26\,\mathrm{cm}^2$). On the top level, the Si-APDs, the electronics for registering the counts and the polarization control are housed.

On Bob's side, the miniaturization was helped by the fact that the whole module is fiber based with the exception of the polarimeter. All fibers are encased in plastic to prevent physical movement. Due to the fact that the four InGaAs detectors are separate devices and therefore rather bulky, an integration of the detectors inside Bob was not possible. Four fiber ports on Bob's front allow us to connect each InGaAs detector to an output of the PBSs. The corresponding trigger and detection signals are fed through eight coaxial connectors.

### *2.5. QKD protocol implementation and security considerations*

We implemented the BBM92 protocol [5] for entanglement-based QKD, a generalization of the original BB84 protocol [1] applied to entangled states [2]. Intuitively speaking, the key is just generated at both locations simultaneously. This elegantly circumvents the well-known key-transfer problem of conventional cryptography. In entanglement-based protocols, the perfect correlations in a shared entangled state are used to generate a secure key, as follows: both Alice and Bob keep track of all their detection events together with a record of their respective polarization state measurement settings; Bob communicates to Alice which of the synchronization triggers resulted in a detection event on his side and also communicates his measurement basis; Alice deletes all entries in which Bob did not detect a photon or where the bases did not match. Both parties then share a sifted key, which is further processed through the

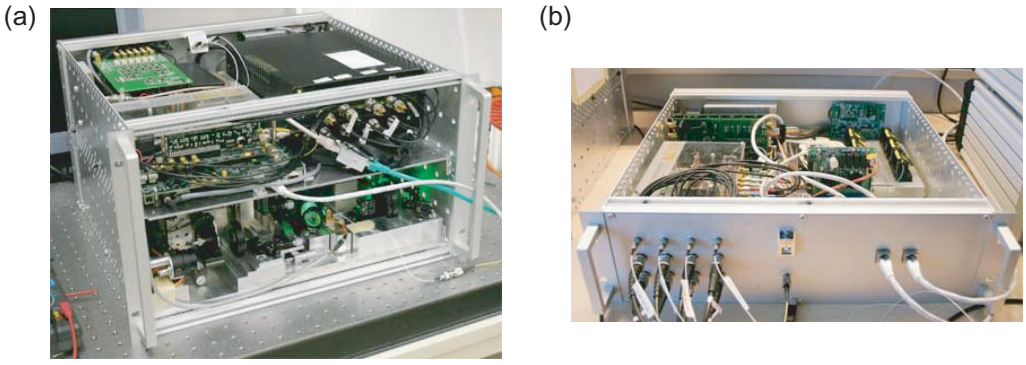


**Figure 2.** (a) The 'Alice' unit of the entangled QKD link. The entanglement source is located at the bottom together with the BB84 polarization analysis module. The Si-detector array and electronics for key generation, the trigger diode and reference diodes for the polarization control are found on top. Connections are provided by two ethernet ports and a coupler for the quantum channel. (b) The receiver unit 'Bob', containing a fiber-based BB84 module, the electronics for key generation and a polarimeter for the polarization control. Apart from the coupler to the quantum channel and two ethernet ports, Bob has also four fiber outputs and eight coaxial connectors. Those connectors are for the four InGaAs detectors, which are placed and operated outside the unit. Each unit is housed in an aluminum case ($43 \times 42\,\mathrm{cm}^2$) with Alice standing at six height units ($\sim$26 cm) and Bob at 3 HU ($\sim$13 cm).

QKD protocol stack to yield a secure key. The software implementing the QKD stack is located on two computers, one connected to Alice and the other to Bob. All classical communication between them is routed over a standard network connection. Alternatively, the QKD stack can run directly on the embedded CPU for a single-chip quantum cryptography solution [27]. This latter approach is currently limited to key rates of 1 kbit $\mathrm{s}^{-1}$ due to computational limitations of the embedded CPU.

In our implementation of the QKD stack, error correction and privacy amplification are performed using the CASCADE algorithm [28] and universal$_2$ class hash functions [29], respectively. The hash function is implemented using a Töplitz matrix approach. We are secure against individual attacks [30], which have proved sharp bounds [31]. Against coherent attacks, the proof by Koashi and Preskill [32] should be used to secure the entanglement-based QKD [33], which would reduce the secret key by $\sim$8% for our typical QBER (3–4%). Although these proofs are strictly true only in the infinite key limit [34], we currently use sifted key blocks with a size of 32 kbit due to computational limitations. To exclude a man-in-the-middle attack, all communication between Alice and Bob is authenticated by applying secure message authentication in the form of an evaluation hash [35].

In an actual realization of a QKD device, side-channel attacks have to be addressed (see section 4.2). These attacks exploit the non-ideal parts of a QKD system and have various origins [36]–[38]. In our case, the detection efficiencies of the single photon detectors are not perfectly matched. A better selection of detectors and bias adjustments can, however, be implemented.

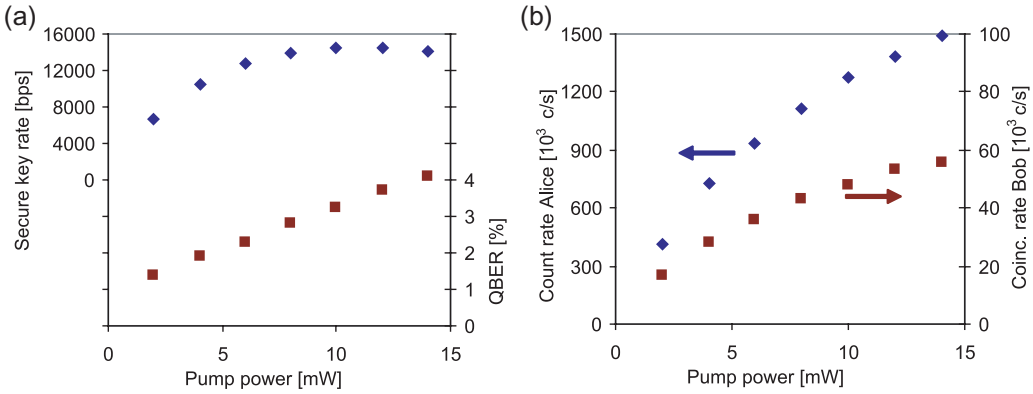


**Figure 3.** (a) The secure key rate (blue diamonds) and the QBER (red squares) produced by the entanglement-based QKD device. The data were taken at a short distance and varying pump power. (b) The total count rate of the four Si-APDs at Alice (blue diamonds) and the total coincidence rate detected by the four InGaAs-APDs at Bob (red squares) recorded at varying pump power.

Due to the nature of spontaneous down-conversion, multi-pair events are generated, which might leak information to a potential eavesdropper [39]. To counter this attack, a random measurement result should be assigned whenever double detection events occur [40]. Our electronics only process the first detection event coming from the detector array, before blanking all detectors with an artificial dead time (300 ns). This ensures a quasi-randomization of double events, since the timing jitter of the detectors (∼500 ps) is much larger than the coherence time of the photons (∼2 ps).

## 3. Results from the laboratory

With the QKD system ready in compact form, we measured the performance within the laboratory environment. Firstly, we investigated the qubit error rate (QBER) and the secure key rate as a function of the laser intensity to determine the suitable pump power. Secondly, we tested the long distance capability of the system with fiber spools.

### *3.1. Secure key rate and QBER*

The first test of the QKD system was performed at various pump power settings. The measurements presented in this section were taken with Alice and Bob connected only by a few meters of optical fiber. Data were collected at power settings ranging from 2 to 14 mW and averaged over 10 min. At 2 mW, Alice produced a trigger rate of 415 000 counts $s^{-1}$. Bob's total coincidence rate for this setting was 16 600 c $s^{-1}$, yielding a coincidence probability of ∼4%. The overall losses of coincidences can be attributed to the following: conditional fiber coupling of the 1550 nm photons at the source (50%), transmission at Alice (75%), transmission at Bob (65%) and a detector efficiency of (15%). The QBER measured at this power setting was 1.4%, yielding a secure key rate after sifting, error correction and privacy amplification of 6500 bits $s^{-1}$. Figure 3(a) summarizes the values for the other power settings.

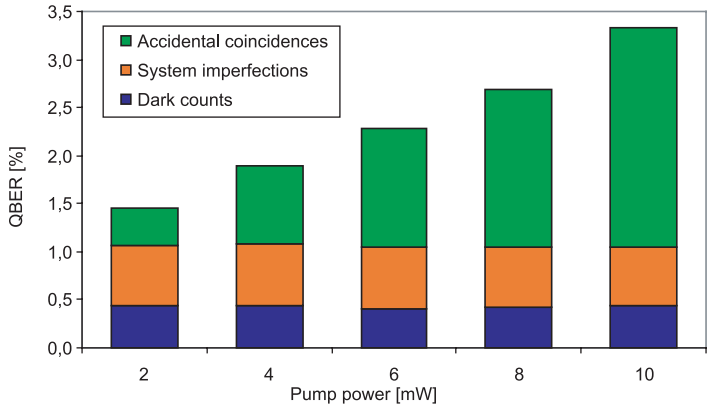


**Figure 4.** The measured error (QBER) of the entangled QKD system recorded at different power settings. The QBER was analyzed as coming from three error sources: the dark count and system QBER, caused by the dark counts of the InGaAs detectors and the non-ideal components of the system, respectively, and the accidental coincidence QBER arising from multi-pair production in the down-conversion process. Whereas the former two error contributions remain stable, the accidental coincidence QBER rises linearly with the pump power.

One can directly see in figure 3(a) that the secure key rate first rises with the pump power, then has a maximum at about 10 mW and finally decreases for even higher power. The reason for this behavior is twofold. Firstly, the raw count rates are not linear with the intensity but show a saturation behavior, see figure 3(b). This is readily understood from detector dead times and also from the gated operation of the InGaAs detectors. The minimum time difference between two consecutive gates is 250 ns. Triggers that arrive during this time are ignored. Since we did not want to overload our system, the dead time of Alice's detectors was electronically enlarged to 300 ns, suppressing the unusable events already at Alice. This leads to the saturation of Alice's counts and to the sublinear increase in Bob's coincidences with intensity. Note that the coincidence probability remains the same over the whole power range. The second and more important reason why the key rate is actually falling at higher power is the rise in QBER. The QBER increases linearly with the pump power, as shown in figure 3(a), due to multi-pair emissions from the down-conversion process. Multi-pairs from cw pumping are largely unrelated and give therefore uncorrelated results [39]. Since the multi-pairs grow quadratically with pump power as opposed to the linear increase of the single pair coincidences, the QBER increases linearly, too.

To verify this assumption, we decomposed the QBER value into three parts: system error, dark count error and accidental coincidence error. The system error comprises all the non-ideal components of the system, such as polarization splitters and polarization alignment, and also the imperfection of entanglement from the source. The dark count error is solely caused by coincidences between a dark count on Bob's InGaAs-APDs and a trigger pulse (detection event at Alice). The contribution of Alice's Si-APD dark counts to the trigger is, however, negligible. The accidental coincidence error comes from multi-pair generation within the detection window ($\sim$1.5 ns).

Figure 4 shows each error component for the power range of 2–10 mW, with the linear increase of the overall QBER clearly visible. Furthermore, the rise can be fully attributed to

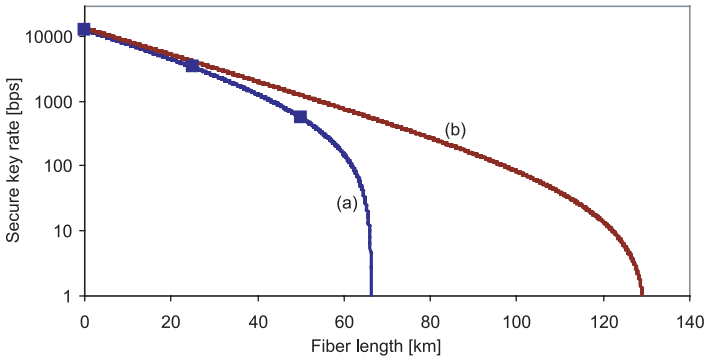


**Figure 5.** Measured secure key rate (blue squares) of the entangled QKD system as a function of fiber length at 0, 25 and 50 km. The curves are predictions for the secure key rate with distance obtained from equation (5). (a) The prediction for our actual system with a measured dark count rate per InGaAs detector of $d = 80\,\mathrm{c\,s^{-1}}$. (b) A best effort prediction using the dark count rate of the best InGaAs detector ($d = 4\,\mathrm{c\,s^{-1}}$). The following experimental parameters were used for the model: $\alpha = 0.204\,\mathrm{dB\,km^{-1}}$, $c_0 = 9000\,\mathrm{c\,s^{-1}}$, $a_0 = 240\,\mathrm{c\,s^{-1}}$ and $f(e) \approx 0.17$.

the increase in the accidental count rate. Both the system error and the dark count error remain constant for the investigated power levels. The intrinsic error of the system is very low indeed, contributing only 0.6% to the total QBER. Detector dark counts already play a role at short distance, adding 0.4% to the QBER. The error due to the accidental counts increases from just below 0.5% to more than 2%, limiting the use of larger pump powers. To decrease the accidental rate, low jitter detectors and electronics need to be used together with narrower coincidence windows, both beyond the scope of this work.

To conclude this analysis, we recognize that the optimal power level will depend on the actual fiber length, but we decided to leave the intensity at 6 mW for all subsequent measurements. This setting is a compromise between a low starting QBER and the anticipated rise of the error when longer fibers are included, due to the prominent role of dark counts.

### *3.2. Long distance measurements*

The long distance capability of the QKD system was investigated in the laboratory using spools of optical fiber. Since the bandwidth of the 1550 nm photons is about 3 nm, chromatic dispersion of a standard fiber would limit the distance. We therefore used non-zero dispersion shifted fibers with a chromatic dispersion of $4\,\mathrm{ps\,km^{-1}\,nm^{-1}}$ (TrueWave RS fiber from OFS). QKD measurements were performed at distances of 0, 25 and 50 km with a duration of 60 min each. With a pump power of 6 mW, the values for the key rate and QBER at 0 km are $12\,500\,\mathrm{bits\,s^{-1}}$ and 2.3%, respectively, as shown in figure 5. At 25 km, the QBER increased to 3.3% and the obtained key rate was $3300\,\mathrm{bits\,s^{-1}}$. At the longest distance of 50 km, a secure key rate of $550\,\mathrm{bits\,s^{-1}}$ was still observed with an overall QBER of 6%. The strong increase in QBER with distance confirmed our previous decision to start with a low QBER in order to accommodate possible rises. At larger distances, the dominant contribution to the QBER is due to detector dark counts and no secure key could be produced at distances much beyond 50 km. To show that our rates are dark count limited, we devised a simple model for our experimental data.

The average coincidences and accidental coincidences decrease exponentially with the length of the fiber ($l$):

$$c(l) = c_0 \times 10^{-\alpha \cdot l/10}, \qquad a(l) = a_0 \times 10^{-\alpha \cdot l/10}, \tag{2}$$

where $c_0$ and $a_0$ are the coincidence and accidental coincidence rates (from multi-pairs only) at 0 km per detector, respectively, and $\alpha$ is the attenuation per kilometer. The total coincidence rate is therefore $4\,c(l)$ and the total background rate is $4\,a(l)+4\,d$, where $d$ is the average dark count rate per InGaAs detector.

The QBER is defined as [4]

$$\mathrm{QBER} = \frac{n_{\mathrm{false}}}{n_{\mathrm{true}} + n_{\mathrm{false}}}, \tag{3}$$

where $n_{\mathrm{true}}$ and $n_{\mathrm{false}}$ are the true and false bits of the key, respectively. After sifting, the true bits are given by half of the coincidence rate ($2\,c(l)$) and a quarter of the total background rate ($a(l)+d$), whereas the false bits are given by just a quarter of the total background rate ($a(l)+d$). Hence, the error from the accidental coincidences and dark counts reads

$$e_{\mathrm{noise}}(l) = \frac{a(l)+d}{2\,c(l)+2\,a(l)+2\,d}. \tag{4}$$

The final secure key rate after sifting, error correction and privacy amplification is given by

$$k_{\mathrm{sec}}(l) = \frac{4\,c(l)}{2}(1-\tau(e)-f(e)\cdot h(e)) \tag{5}$$

where the factor $\frac{1}{2}$ accounts for sifting, $e$ is the overall QBER ($e = e_{\mathrm{noise}}(l) + 0.6\%$ for the system QBER), $h(e)$ is the binary entropy function, $f(e)$ is the overhead of CASCADE with respect to the Shannon limit and $\tau(e)$ is the fraction discarded by privacy amplification [30]. In our case, the overhead of CASCADE ($f(e)$) was measured to be 1.16 at 3% QBER and 1.18 at 5% QBER.

The average dark count rate per InGaAs detector was measured to be $d = 80\,\mathrm{c\,s^{-1}}$ and the expected key rate from equation (5) is plotted in figure 5(a). The prediction of the model is in very good agreement with the experimental data points and hence confirm that our long distance measurements are indeed dark count limited, since the dark count rate ($80\,\mathrm{c\,s^{-1}}$) exceeds the accidental coincidence rate ($74\,\mathrm{c\,s^{-1}}$) for distances beyond 25 km. The following question arises: What distances could be achieved with better detector technology? Our best InGaAs detector has a measured dark count rate of only $4\,\mathrm{c\,s^{-1}}$ for the given trigger rate of $950\,000\,\mathrm{c\,s^{-1}}$ and coincidence window of 1.5 ns. The prediction for the key rate in a scenario with four low-noise detectors ($d = 4\,\mathrm{c\,s^{-1}}$) is given in figure 5(b). A distance of over 100 km would therefore be possible with key rates of tens of bits $\mathrm{s^{-1}}$ at 100 km.

Polarization mode dispersion (PMD) was thought to prevent such distances for polarization encoding; however, modern telecom fibers are optimized to typical PMD link design values of smaller than $0.07\,\mathrm{ps\,km^{-1/2}}$. Only after 1200 km would the PMD overcome the coherence time of our entangled photons (2.5 ps) and lead to decoherence. Previous investigations [23] revealed a 100 km fiber link to have no adverse effects on polarization entanglement. Narrowband sources of entanglement [41] can be used to reliably transmit polarization qubits with coherence times (10 ps) much larger than the PMD value of a 1000 km link (2 ps). We conclude that even with current InGaAs technology, an entanglement-based QKD link of 100 km in optical fibers can be realized.

## 4. Automation and stabilization modules

As was shown in the previous section, long distance entanglement-based QKD with high key rates is possible. For a practical QKD system, one requires in addition that human intervention should be minimized. Ideally, the system should be completely automated and achieve a stable and reliable long-term key exchange. For the system presented here it is therefore necessary to distribute photonic entanglement with a stable rate and high visibility. In particular, this requires

- stable production and coupling of photons into the quantum channel
- stable synchronization to identify photons from the same entangled pair
- automated alignment of the entangled state
- compensation of polarization drifts in the quantum channel.

Most of these requirements are not necessarily specific to our QKD prototype but apply to all quantum information protocols relying on entanglement distribution, some even to other protocols as well. In the following subsections, we describe the implemented modules meeting the requirements mentioned above.

### *4.1. Source stabilization*

The entanglement source is based on free-space optics and hence is prone to mechanical drifts due to temperature fluctuations. Even small drifts will lead to misalignment and loss of fiber-coupled photons. Therefore, an active stabilization procedure was implemented. The fiber couplers (fiber tip with a fiber collimation lens) for the photons have been fixed on piezo-motor-driven optical mounts (Agilis AM-M100 series from Newport). These mounts can tilt the fiber coupler along the two axes in order to stay aligned. Another motorized mirror mount was installed just after the laser to compensate for the beam wander. All the six piezo axes are driven by the electronics at Alice and an algorithm maximizes the count rates. The source stabilization is not a fast procedure, as due to the long averaging times involved (10 s per point), it takes several minutes to complete a full cycle (all six channels). This, however, does not decrease the key rate, since the QKD continues while the source stabilization is active.

### *4.2. Delay synchronization*

As outlined in section 2.3, the synchronization channel is essential to trigger the InGaAs detectors at Bob. To have more flexibility and control over the exact synchronization, electronic delay lines were added at Alice and Bob (see figure 1). The delay lines can be addressed individually and set in steps of 10 ps for a maximum delay of 10 ns.

On Alice's side the delay lines are found between the outputs of the Si-APD detectors and the input of the FPGA electronics. This arrangement allowed us to compensate detector-dependent response times and to match the optical trigger signal to the single photon arrival irrespective of which of the four Si-APD detectors fired and therefore preventing a potential side channel attack [36].

The delay lines at Bob were inserted between the generation of the electronic trigger signal and the gate inputs on the four InGaAs detectors. With those delay lines we could precisely synchronize the gate of each InGaAs detector to the single photon, therefore also preventing a time-shift attack [37].

An automated synchronization routine is implemented for Bob's delay lines. At the start, Bob sets all delays to the minimum and then increases the delays stepwise to the maximum value. The coincidence rates are monitored during the scanning process and the optimal delay for each detector is obtained. Since temperature fluctuations also affect the delay circuits, the routine has to be repeated periodically.

The width of the coincidence peak is given by detector jitter and in longer fibers by the chromatic dispersion. The smallest gate width on the id-201 detectors leads still to the detection of more dark counts and accidental coincidences than necessary. An additional coincidence window can be defined electronically to fit the arrival-time spread of the photons tightly.

### *4.3. State alignment*

The purpose of this routine is to perform an automatic polarization alignment on the desired maximally entangled state $|\Psi^-\rangle$ to minimize the QBER. Whereas on Alice's side a free-space arrangement of the BB84 module guarantees a permanent and fixed 45° rotation between the two measurement bases H/V and P/M, on Bob's side the BB84 module is fiber based and no absolute reference exists between the two arms. Since temperature changes will influence both arms independently and any initial reference will be lost, we implemented an automated state alignment procedure using the two polarization controllers at Bob (PC1 and PC2 in figure 1). Independent bases control is achieved with the first controller acting on both bases and the second controller acting only on the H/V basis. At the start of the procedure, Alice only triggers with events coming from her P-detector (see figure 1). Bob then uses the first polarization controller (PC1) to reduce the coincidence rate in his P-detector to a minimum ($|\Psi^-\rangle$). After the P/M basis is aligned, Bob uses the second controller (PC2) to align the H/V basis by minimizing the coincidences at his V-detector, while Alice triggers with her V-detector only. The whole alignment process takes about 3–5 min for each basis (10 s averaging time for each measurement).

### *4.4. Polarization control*

Using standard optical fibers as a quantum channel for polarization-encoded photons has the disadvantage of arbitrary unitary polarization transformation. The birefringence of the fiber causes arbitrary rotations depending on environmental factors like temperature and mechanical stress. These random and dynamic changes in birefringence, which would lead to an unacceptably high QBER, need to be actively compensated for. The state alignment procedure, detailed in section 4.3, could in principle correct the drifts in the quantum channel but it is slow and would interrupt the QKD for too long. We therefore devised a fast and active control module compensating for the dynamic polarization rotation of the quantum channel.

Our implementation of the polarization control relies on time multiplexed reference pulses at the same wavelength as the entangled photon. A wavelength multiplexed version has also been shown recently [42]. When in operation, Alice sends strong pulses consecutively polarized in H and P through the fiber to Bob, where their polarization is analyzed. If a difference from a preset polarization state is found, an algorithm controlling the first polarization controller (PC1) will minimize the deviation. Two reference pulses at non-orthogonal polarizations are needed, as simply fixing a single polarization on the Poincaré sphere leaves the phase still undetermined.

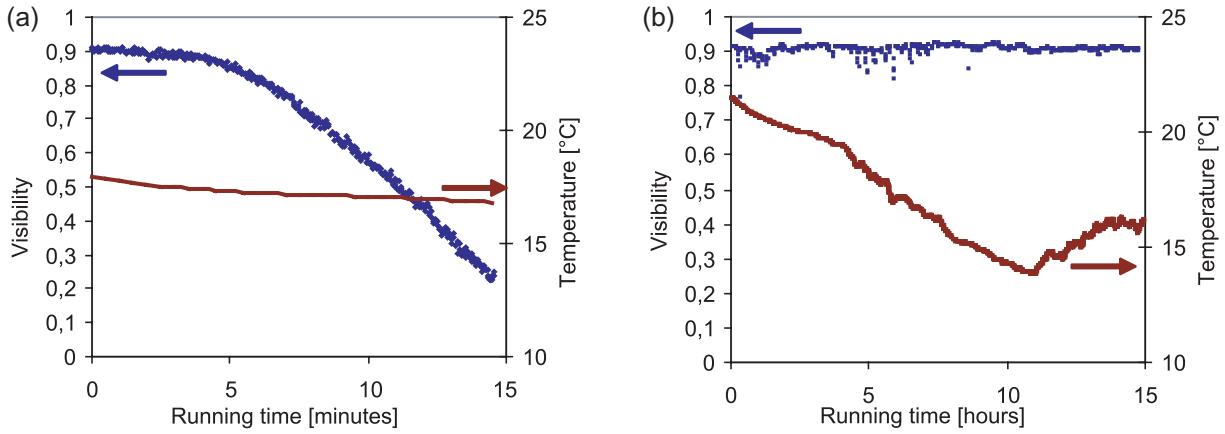


**Figure 6.** (a) Evolution of the average visibility (blue diamonds) in the H/V and P/M bases for an entanglement distribution over 25 km fiber without polarization control. The temperature at the fiber spool was measured at the same time (red line). (b) Evolution of the visibility (blue squares) over a whole night in a measurement with the active polarization control. The highly varying temperature at the fiber spool was again recorded (red line). Spikes in the visibility are caused by hysteresis effects of the polarization controller [44].

A second non-orthogonal polarization state defines the phase, and hence all polarization states on the sphere.

The hardware needed to implement the polarization control is depicted in figure 1. On Alice's side, the electronics control two laser diodes, whose outputs are combined in a BS maintaining a relative polarization rotation of 45° between them. Alice (FGPA 'PolAlice') also controls the optical switch (Free-X from CIVCOM), which connects the quantum channel to either the entanglement source or the diodes of the polarization control. The switch also interrupts the trigger signals from Alice when the polarization control is active, preventing a saturation of Bob's detectors. At Bob, a 95:5 BS diverts a fraction of the signal to a classical polarimeter analyzing the light in the two linear H/V and P/M and in the circular R/L bases. Photo diodes at each output port measure the components along each basis and the incoming polarization state can be reconstructed from the evaluated Stoke's vectors [43].

The polarization control was tested in the laboratory using a 25 km fiber spool at varying temperatures, as shown in figure 6. We used our source of polarization entanglement to measure the average polarization visibility of the entangled state in the H/V and P/M bases after transmission of the 1550 nm photon through the fiber. The visibility in one basis is defined as $V = (\mathrm{Max} - \mathrm{Min})/(\mathrm{Max} + \mathrm{Min})$, where Max is the maximal coincidence rate as obtained for orthogonal polarizer settings for the 810 and 1550 nm photons, and Min is the coincidence rate at parallel settings. Figure 6(a) shows the measured visibility as a function of time (5 s averaging) together with the temperature of the spool. Without polarization control, even a small change in temperature ($\sim$1.2 °C) is enough to completely destroy the polarization correlations, which shows the high susceptibility of the fiber to external changes. The experiment was then repeated over a whole night (15 h) with the polarization control module. The constant visibility of the entangled state around 90%, as shown in figure 6(b), proves that the active polarization control indeed compensates polarization drifts even during large temperature changes (7 °C).

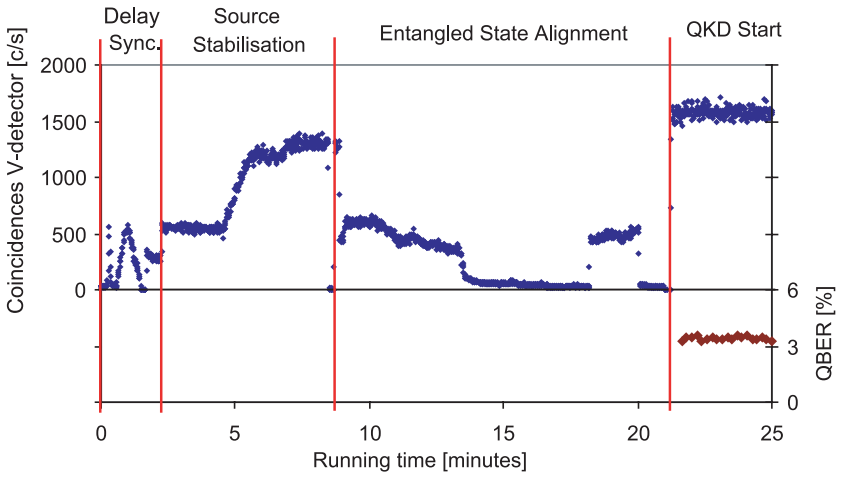


**Figure 7.** Automated start-up sequence of the QKD system after being transported. The coincidence rate (blue diamonds) of one InGaAs detector (V) is plotted over time to identify the different stages. At first, the system scans for the optimal synchronization delay (identified by the spike), then the source stabilization maximizes the coincidence rate and, finally, the state is aligned in two subsequent cycles by minimizing the V coincidences. After completion of the system start-up (21 min) the QKD is started. In this last section, the QBER is also shown (red diamonds).

### *4.5. Management module*

The management module software (MM) was developed to guarantee a seamless coordination and operation of the individual control routines. It manages the QKD system during the automated start-up and hands-off operation, and reacts to different error scenarios. During the normal QKD operation, the MM will call each of the routines sequentially to keep the whole system stable and aligned. The typical time for a single cycle, including the source stabilization, time synchronization and the polarization control, is about 10 min, after which the cycle is repeated. Within a cycle, the QKD is only interrupted for about 5 s due to the polarization control.

Interruptions of the normal cycle can be caused by several error interrupts detected by the MM: if the optical fiber linking Alice and Bob is subject to violent changes (temperature or mechanical stress), the QBER will quickly rise since the polarization control is not always active. The MM can, however, identify this error and react by starting the polarization control. If the QBER rises slowly and is not reduced by the polarization control, then the MM starts the state realignment procedure, since it is likely that parts of the fiber-based BB84 module have drifted.

An automated start-up sequence with a 25 km fiber spool between Alice and Bob is depicted in figure 7. The coincidence rates on the V-detector at Bob are shown as a function of time to identify each stage of the start-up. At first, the system searches for the appropriate delay using the delay synchronization module (section 4.2). Then the source stabilization module (section 4.1) starts and in this case increases the coincidence rate from 500 to about 1200 c $s^{-1}$ within 5 min. After that, the state alignment module (section 4.3) minimizes the coincidences

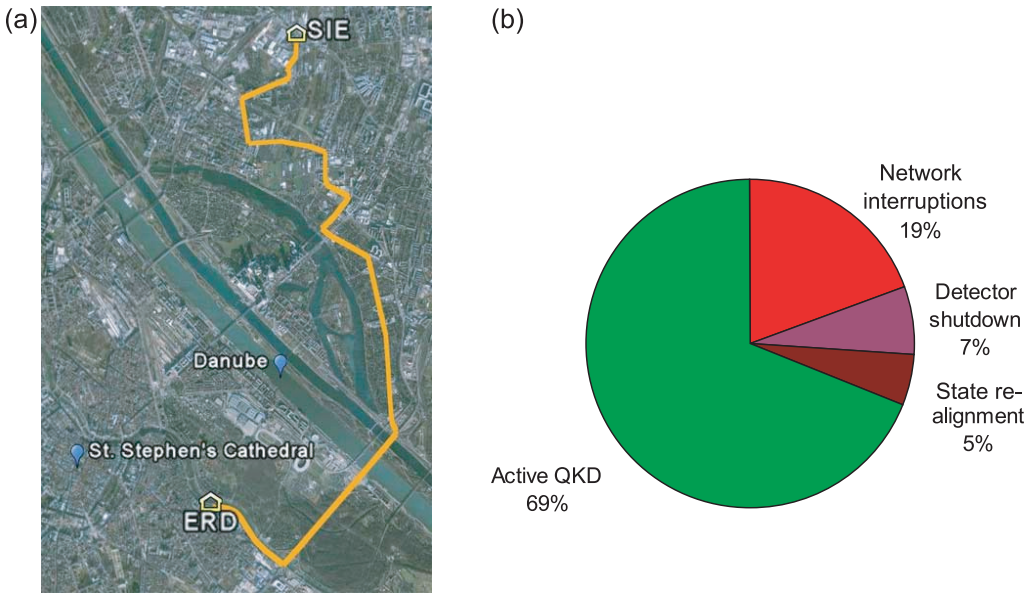


**Figure 8.** (a) Satellite image (© Google) of Vienna showing the path of the underground fiber (16 km) between the locations SIE and ERD, over which the entangled QKD link was operated. (b) Chart of the QKD availability during the 2-week network phase. The chart shows the fraction of the actual key generation (active QKD), together with the interruptions caused by SECOQC maintenance, system realignments and detector shutdowns due to high temperatures.

of the detector to align the H/V basis. The system is now fully aligned and the QKD starts with a QBER of about 3.5%. The whole start-up took about 20 min after transportation by car and a complete reinstallation of the system. The time for a routine start-up (after a temporary shutdown) takes only about 10 min.

## 5. Long-term results from the SECOQC network

The final test of our entanglement-based QKD device came with the implementation of the link into the telecom fiber network provided by Siemens Austria as used by SECOQC [45]. Alice's unit was placed in an office room at the Siemens headquarters (SIE) in Vienna, Austria. Bob's unit was installed in another part of the city at a branch office of Siemens (ERD). The two locations were connected via a standard telecom fiber (G.652) of 16 km length with a total attenuation of 4.1 dB. In figure 8(a), the actual path of the fiber between SIE and ERD is depicted. Note that the fiber crosses the Danube river by means of a bridge, runs along major train tracks and along a motorway. External influences on the fiber were, however, not the only problem. Since the offices that housed the QKD devices and several computers for the network had no air conditioning, a more archaic method had to be used to 'control' the temperature. An open window allowed a capping of the temperature to prevent devices from shutting down, but resulted in large temperature variations inside the room. In figure 9(d), the actual room temperature at ERD is shown for the whole phase of operation. The difference between day and night cycles are clearly visible with fluctuations in temperature up to 12 °C.

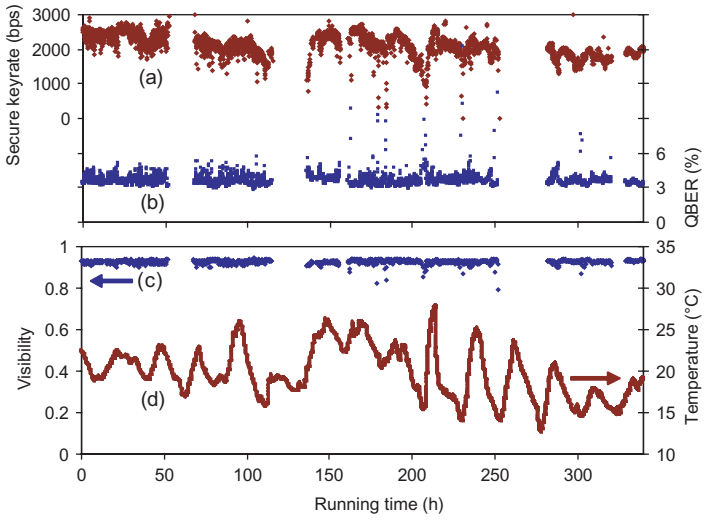


**Figure 9.** Data obtained during the 2-week network phase (336 h) using the 16 km-long deployed fiber. (a) Secure key rate (red diamonds) and (b) QBER (blue squares) of the entanglement-based QKD link. Fluctuations in the key rate are caused by temperature dependencies of the InGaAs detectors. (c) Average polarization visibility (blue diamonds) of the entangled state measured during the network phase. (d) The room temperature (red line) at the ERD office (Bob) as measured throughout the network phase. The large day/night changes are caused by an open window.

The data in figure 9 show both the secure bit rate and the QBER of the link during the 336 h run (2 weeks). Each point was averaged for about 1 min. The key rate, shown as (a), lies at about 2000 bits $s^{-1}$ for the whole duration. Fluctuations in the key rate are caused by unexpected temperature dependencies of Bob's detectors (e.g. at hour 220 in figure 9). Note that the trigger rate at Alice (not shown here) was stable at 750 000 c $s^{-1}$ throughout the 2 weeks. Bob's total coincidences decreased from 8500 to 6800 c $s^{-1}$ during this time, resulting in the decline of the key rate. We believe that this is also linked to the temperature dependence of Bob's detectors.

The QBER, shown as (b), remains very stable over the whole duration of the experiment with an average value of 3.5%. The apparent noise in the QBER plot is not caused by random fluctuations but is due to the polarization drifts not compensated by the polarization control procedure. As explained in section 4.3, certain drifts can only be corrected using the state alignment procedure. It is triggered when the QBER grows by an additional percentage point from its initial value. Depending on the temperature changes the state alignment module operates at intervals ranging from 30 min to several hours. In terms of entanglement visibility, shown as (c), we achieved a 2-week entanglement distribution with an average visibility of 93%. For 99.9% of the active time, the visibility was larger than 90%, showing the high reliability of the entanglement distribution.

For 2 weeks, the QKD system was running continuously without manual interference. The only times when no keys were produced were during interruptions of the QKD network, where the link was embedded. These periods lasted usually a day or so and can be clearly seen in figure 9. After the restart of the network, the QKD link was also started automatically and both QBER and key rate resumed from their previous values. Out of the total 336 h of recorded

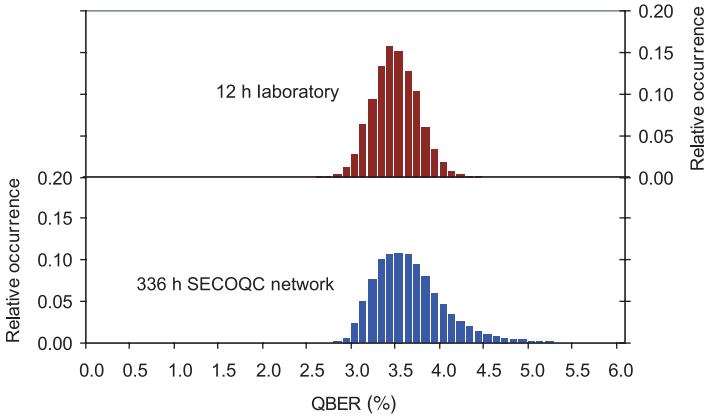


**Figure 10.** Histogram of the measured QBER (a) during a typical 12 h run under laboratory conditions using a 25 km fiber spool and (b) during the complete 2-week network phase (336 h) using the 16 km-long deployed fiber.

data, the QKD was active for 232 h (69%), as depicted in figure 8(b). The non-operating times were mainly caused by network interruptions, which amounted to 64 h (19%) and detector shutdowns accounting for 23 h (7%). The remaining 17 h (5%) were spent realigning the state. It is reasonable to assume that with a mature network infrastructure and air-conditioned rooms, the operational up-time could easily be 95%. A temperature stabilized environment would also reduce recurrence of the automated state alignment, which could bring the overall up-time to about 98%.

The high degree of robustness of the QKD system can be seen in figure 10. The QBER histogram shown on top was recorded during the 12 h run in the laboratory using a 25 km fiber, while the lower histogram incorporates the QBER of the 336 h run using the deployed fiber of the network. The two distributions have nearly the same spread with 0.6% FWHM in the laboratory compared with 0.8% FWHM in the network. The QBER distribution in the network is slightly skewed to higher values, since we allow for a QBER increase due to indoor temperature changes before the state alignment corrects the drift. The similarity of the distributions indicates, however, that our system can manage perfectly the change from a stable laboratory environment to long-term operation in a deployed fiber network.

## 6. Conclusion

We have presented a QKD system based on polarization entanglement for use in telecom fibers. The whole system is compact and can be used in standard 19-inch racks. We operated the system at a transmission distance of up to 50 km in optical fibers with a final secure key rate of 550 bits $s^{-1}$. Simulations show that with current InGaAs detector technologies, distances of up to 100 km would be possible.

In addition, a variety of control and stabilization modules were combined for the first time to demonstrate a stable distribution of entanglement with high purity and hence a reliable QKD implementation. With those extra modules, it was possible to realise a completely hands-off operation of the whole QKD system. During 2 weeks and without any manual intervention, we measured a key rate of 2000 bits $s^{-1}$ over a 16 km-long deployed fiber with a QBER of 3.5%.

These results also show that stable entanglement distribution in optical fibers is possible over long periods of time. The high visibility (93%) of the entanglement and its reliability (for 99.9% of the time higher than 90%) makes applications such as QKD feasible and hopefully stimulates the application of other quantum communication protocols in optical fiber networks.

Since an entangled QKD system needs single photon detection, in contrast to other QKD implementations, at Alice *and* Bob, the clock rate is currently restricted to the MHz region and thus limits the key rate. However, our experiment proves that entanglement-based quantum cryptography can be operated at least as reliably as simpler systems based on weak pulses. Thus the technological challenges that entanglement-based systems were facing initially have successfully been overcome. Such systems therefore offer a very secure and advanced approach to QKD.

## Acknowledgments

We thank Bernhard Schrenk, Thorben Kelling, Fotini Karinou and Bibiane Blauensteiner for their initial contributions. We also thank Michael Meyenburg and Roland Lieger for the software support of the Virtex-4 FPGA boards as well as Sebastian Sauge and Anders Karlsson for the loan of an InGaAs detector and discussions on entanglement distribution. We also acknowledge Siemens Austria for the usage of their fiber network. This work was supported by the European Commission through the integrated projects SECOQC (IST-2003-506813) and QAP (015846) and by the Austrian Science Foundation FWF (TRP-L135 and SFB-1520).

## References

[1] Bennett C H and Brassard G 1984 *Proc. IEEE* p 175
[2] Ekert A 1991 *Phys. Rev. Lett.* **67** 661
[3] Scarani V, Bechmann-Pasquinucci H, Cerf NJ, Dusek M, Lutkenhaus N and Peev M 2008 arXiv:0802.4155 [quant-ph]
[4] Gisin N, Ribordy G, Tittel W and Zbinden H 2000 *Rev. Mod. Phys.* **74** 200
[5] Bennett C H, Brassard G and Mermin N D 1992 *Phys. Rev. Lett.* **68** 557
[6] Kwiat P G, Mattle K, Weinfurter H, Zeilinger A, Sergienko A V and Shih Y 1995 *Phys. Rev. Lett.* **75** 4337
[7] Jennewein T, Simon C, Weihs G, Weinfurter H and Zeilinger A 2000 *Phys. Rev. Lett.* **84** 4729
[8] Naik D S, Peterson C G, White A G, Berglund A J and Kwiat P G 2000 *Phys. Rev. Lett.* **84** 4733
[9] Tittel W, Brendel J, Zbinden H and Gisin N 2000 *Phys. Rev. Lett.* **84** 4737
[10] Fiorentino M, Messin G, Kuklewicz C E, Wong F N and Shapiro J H 2004 *Phys. Rev.* A **69** 041801
[11] Fedrizzi A, Herbst T, Poppe A, Jennewein T and Zeilinger A 2007 *Opt. Express* **15** 15377
[12] Acin A, Brunner N, Gisin N, Massar S, Pironio S and Scarani V 2007 *Phys. Rev. Lett.* **98** 230501
[13] Hughes R J, Buttler W T, Kwiat P G, Lamoreaux S K, Morgan G L, Nordholt J E and Peterson C G 2000 *J. Mod. Opt.* **47** 549
[14] Marcikic I, Lamas-Linares A and Kurtsiefer C 2006 *Appl. Phys. Lett.* **89** 101122
[15] Erven C, Couteau C, Laflamme R and Weihs G 2008 *Opt. Express* **16** 16840
[16] Ursin R *et al* 2007 *Nat. Phys.* **3** 481
[17] Poppe A *et al* 2004 *Opt. Express* **12** 3865
[18] Fasel S, Gisin N, Ribordy G and Zbinden H 2004 *Eur. Phys. J.* D **30** 143
[19] Marcikic I, de Riedmatten H, Tittel W, Zbinden H, Legré M and Gisin N 2004 *Phys. Rev. Lett.* **93** 180502
[20] Honjo T *et al* 2008 *Opt. Express* **16** 19118
[21] Takesue H 2006 *Opt. Express* **14** 3453

[22] Liang C, Lee K F, Chen J and Kumar P 2006 *Optical Fiber Communications Conf. (OFC2006)* paper PDP35
[23] Hübel H, Vanner M R, Lederer T, Blauensteiner B, Lorünser T, Poppe A and Zeilinger A 2007 *Opt. Express* **15** 7853
[24] Zhang Q, Takesue H, Nam S W, Langrock C, Xie X, Beak B, Fejer M and Yamamoto Y 2007 *Opt. Express* **16** 5776
[25] Lim H C, Yoshizawa A, Tsuchida H and Kikuchi K 2008 *Opt. Express* **16** 14512
[26] Kwiat P G, Waks E, White A G, Appelbaum I and Eberhard P E 1999 *Phys. Rev.* A **60** R773
[27] Lorünser T, Querasser E, Matyus T, Peev M, Wolkerstorfer J, Hutter M, Szekely A, Wimberger I, Pfaffel-Janser C and Neppach A 2008 *Proc. IEEE ASAP 2008* p 37
[28] Brassard G and Salvail L 1994 *Lect. Notes Comput. Sci.* **765** 410–23
[29] Bennett C H, Brassard G and Robert J M 1995 *IEEE Trans. Inf. Theory* **41** 1915
[30] Lütkenhaus N 2000 *Phys. Rev.* A **61** 052304
[31] Herbauts I, Bettelli S, Hübel H and Peev M 2008 *Eur. Phys. J.* D **46** 395
[32] Koashi M and Preskill J 2003 *Phys. Rev. Lett.* **90** 057902
[33] Ma X, Fung C F and Lo H 2007 *Phys. Rev.* A **76** 012307
[34] Scarani V and Renner R 2008 *Phys. Rev. Lett.* **100** 200501
[35] Shoup V 1996 *Lect. Notes Comput. Sci.* **1109** 313
[36] Lamas-Linares A and Kurtsiefer C 2006 *Opt. Express* **15** 9388
Lamas-Linares A and Kurtsiefer C 2006 *Opt. Express* **16** 1867
[37] Qi B, Fung CF, Lo H and Ma X 2007 *Quantum Inf. Comput.* **7** 73
[38] Makarov V 2007 arXiv:0707.3987 [quant-ph]
[39] Dusek M and Bradler K 2000 arXiv:quant-ph/0011007
[40] Beaudry N, Moroder T and Lütkenhaus N 2008 *Phys. Rev. Lett.* **101** 093601
[41] Sauge S *et al* 2007 *Opt. Express* **15** 6926
[42] Xavier G B, Vilela de Faria G, Temporão G P and von der Weid J P 2008 *Opt. Express* **16** 1867
[43] Damask J 2005 *Polarization Optics in Telecommunications* (Berlin: Springer)
[44] www.generalphotonics.com/pdf/FAQPolariteII.pdf (question 18)
[45] Poppe A, Peev M and Maurhart O 2008 *Int. J. Quantum Inf.* **6** 209