J. Cryptology (2000) 13: 207–220
DOI: 10.1007/s001459910007

Journal of
CRYPTOLOGY

Practical Aspects of Quantum Cryptographic Key Distribution

H. Zbinden, N. Gisin, B. Huttner, A. Muller, and W. Tittel
Group of Applied Physics, University of Geneva,
CH-1211 Geneva 4, Switzerland

Communicated by Gilles Brassard

Received 11 April 1997 and revised 21 July 1997

Abstract. Performance of various experimental realizations of quantum cryptographic protocols using polarization or phase coding are compared, including a new self-balanced interferometric setup using Faraday mirrors. The importance of detector noise is illustrated and means of reducing it are presented. Maximal distances and bit rates achievable with present day technologies are evaluated. Practical eavesdropping strategies taking advantages of the optical fiber that could open a gate into the transmitter's and receiver's offices are discussed.

Key words. Quantum cryptography, Key distribution, Interferometry, Single photon counting, Optical fibers.

1. Introduction

The use of quantum mechanical properties in cryptography has been proposed by Wiesner [24] and developed by Bennett and Brassard in 1984 [3]. In cryptography safety can be guaranteed by a common secret key, known only to the two users, Alice and Bob. Quantum cryptography (QC) provides means to establish such a key at a distance and to check its confidentiality. It is based on the fact that any measurement of incompatible quantities on a quantum system will inevitably modify the state of this system. Therefore an eavesdropper, Eve, might get information out of a quantum channel by performing measurements, but the legitimate users will detect her and hence not use the key. For convenience the quantum system is in practice a single photon (or a weak pulse) propagating through an optical fiber, and the key can be encoded either by its polarization or by its phase. A variation of the general principle based on entangled photon pairs was proposed by Ekert [8]. The first experimental demonstration of quantum cryptography was performed in 1989 over 30 cm in air with polarized photons [2]. Since then, several groups presented realizations of both the polarization [10], [21] and the phase coding scheme in optical fibers over distances of up to 30 km [19], [14].

Three parameters describe the performance of experimental quantum cryptography

systems: the transmission distance, the bit rate, and the error rate. The losses in optical fibers are typically around 2 dB/km at 800 nm, 0.35 dB/km in the 1300 nm telecom window, and 0.2 dB/km in the 1550 nm telecom window. Hence, at 1300 nm the bit rate is reducted by a factor of ten after about 30 km. At this wavelength germanium avalanche photo diodes (Ge APD) have to be used instead of commercial silicon photon counting modules. This means lower detection efficiencies, hence lower bit rates and higher dark count rates, hence higher error rates. Actually the noise of the available photon counters in the near infrared is one major problem of experimental QC that finally limits the transmission distance. Note that incompatible modes of a quantum channel cannot be amplified without noise (no cloning theorem [25]). On the one hand this is essential for the security of QC, on the other hand this limits the possible transmission distance.

Another experimental problem is that most QC systems need continuous alignment of the setup. In polarization-based QC systems, the polarization has to be maintained stable over tens of kilometers, in order to keep the polarizers at the emitter's and at the receiver's ends aligned. In fact, depending on the environment the output polarization can fluctuate randomly on time scales of hours to seconds. Therefore, these systems have to compensate actively changes of the outcoming polarization. These fluctuations are generally slow enough that automatic tracking would be feasible [21]. Interferometric QC systems are usually based on two unbalanced Mach-Zehnder interferometers, one at each end. Since two interfering pulses do not follow the same path within the two interferometers, the difference in arm lengths must be kept stable to a fraction of a wavelength for both interferometers, in order to obtain high visibility. Consequently, every few seconds, one interferometer has to be adjusted to the other by a piezoelectric transducer to compensate for thermal drifts [19].

In this article we show first that the performance of Ge APDs can be considerably improved using fast active biasing electronics. Next, we introduce an interferometric system with Faraday mirrors [20]. This phase coding setup needs no alignment of the interferometer nor polarization control, and therefore considerably facilitates the experiment. Moreover, it features excellent fringe visibility. Thirdly, we present the realization of a secret key over 23 km of installed telecom fiber. The performance of this setup is compared with polarization and phase coding setups presented before. Finally, the susceptibility of the different setups to different eavesdropping strategies is briefly discussed.

2. QC and Sources of Errors

We recall the principle of QC (based on the four-states protocol BB84 [3]) using the example of a polarization coding setup shown in Fig. 1. Experimental setups published before were based on one laser followed by a polarization rotator. The present scheme proposes using four lasers with polarizers oriented at 0°, 90°, 45°, and 135°.[1] The lasers fire at random at a rate ν. Their polarization states are adjusted to compensate for the transformation in the following fiber link with a total loss L. Bob randomly selects one

[1] The use of four laser may have experimental advantages. However, one has to make sure that Eve cannot find out which laser has fired due to differences in spectrum or timing.

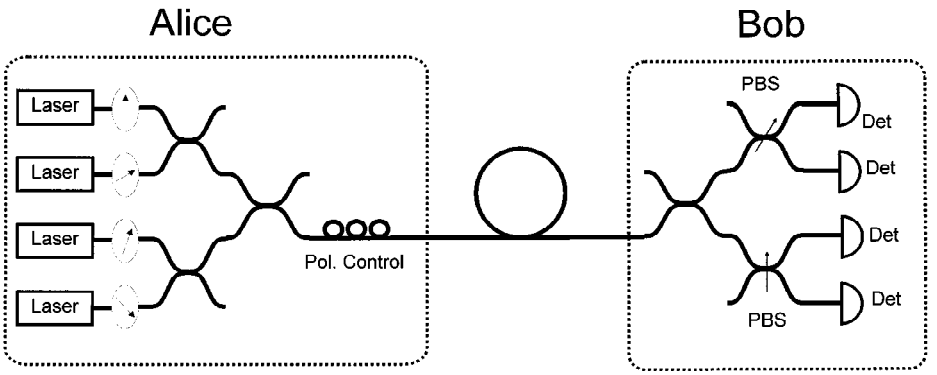

Fig. 1. Scheme of a polarization coding QC setup. PBS: polarization beam splitter.

of the two analyzers oriented at 45° (in this setup this is automatically done by a passive coupler). To prevent the simplest eavesdropping strategy, that is just splitting the pulse in two and measuring the polarization of one-half, at most 1 photon per pulse must be used. In practice the laser pulses are attenuated to an average number of photons per pulse well below 1 ($\mu = 0.1$, say), to limit the probability of obtaining more than 1 photon per pulse. The photons are then detected with a photon counter and acquisition electronics collect the data. After the measurement Alice and Bob publicly compare the chosen bases (0°/90° or 45°/135°) of emission and detection, without revealing the polarization states transmitted and measured. Incompatible measurements are disregarded. With the other results a secret key can be established by interpreting 0° and 45° as bit 1, and 90° and 135° as bit 0. If, for example, Eve uses a simple intercept–resend strategy, i.e., would just measure the polarization of every photon, she would introduce an error of 25% which can be easily detected by Alice and Bob by simply comparing a sample of their key.

For comparison, the standard phase coding setup is shown in Fig. 2. There are two unbalanced Mach-Zehnder interferometers, one at Alice's and one at Bob's side. Pulses taking the short path in Alice's and the long one in Bob's interferometers will interfere with pulses taking the long path in Alice's and the short one in Bob's interferometers. In one arm, Alice randomly applies phase shifts of 0, π, or $\pi/2$, and $3\pi/2$; Bob chooses a base by applying a phase shift of 0 or $\pi/2$. If compatible bases have been chosen, i.e., the phase difference is 0 or π, the outcome is deterministic. Hence a secret key can be established by interpreting 0 and $\pi/2$ as bit 1, and π and $3\pi/2$ as bit 0. Again incompatible measurements are disregarded.

For every QC scheme the same simple equation for the raw data rate R, i.e., the number of exchanged bits per second before any error correction, can be applied:

$$R = q\mu\nu(1 - L)\eta, \tag{1}$$

where ν is the pulse rate of the laser, μ is the average number of photon per pulse, L is the losses in the fiber lnk, η is the quantum efficiency of the detector, and q is a systematic factor smaller than (or equal to) $\frac{1}{2}$ depending on the chosen implementation. For example, in the case of the polarization scheme of Fig. 1, q equals the maximum value $\frac{1}{2}$ due to the random selection of the polarizer basis.

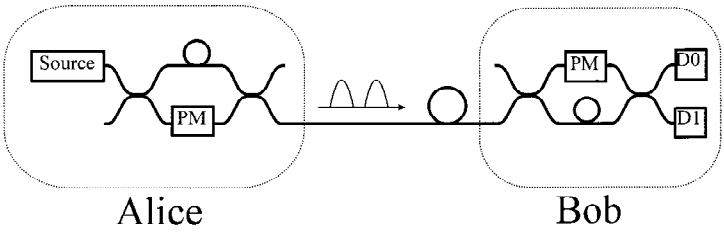

Fig. 2. Scheme of a standard phase coding QC setup. PM: phase modulator.

The error is generally expressed as the ratio of wrong bits to the total amount of detected bits (or the ratio of probability of obtaining a false detection to the total probability of detection). We call this quantity the quantum bit error rate (QBER):[2]

$$\mathrm{QBER} = \frac{p_{\mathrm{dark}} + p_{\mathrm{opt}} \cdot p_{\mathrm{phot}}}{2 \cdot p_{\mathrm{dark}} + p_{\mathrm{phot}}} = \frac{n_{\mathrm{dark}} \cdot \Delta\tau + p_{\mathrm{opt}} \cdot \mu(1-L)\eta}{2 \cdot n_{\mathrm{dark}} \cdot \Delta\tau + \mu(1-L)\eta} \cong \frac{n_{\mathrm{dark}} \cdot \Delta\tau}{\mu(1-L)\eta} + p_{\mathrm{opt}} \equiv \mathrm{QBER}_{\mathrm{det}} + \mathrm{QBER}_{\mathrm{opt}}, \quad (2)$$

where p_{dark}, p_{phot}, and p_{opt} are the probabilities of obtaining a dark count, of detecting a photon, and the probability that a photon went to an erroneous detector, respectively. n_{dark} is the dark count rate of the detector and $\Delta\tau$ is the detection time window. This formula applies for a setup with two detectors. Since a dark count will with a 50% chance not lead to an error, but just to an additional count, there is a factor two in the denominator, but not in the numerator. Of course, we do not consider dark counts when incompatible bases are used. Hence, the factor q of (1) does not appear in the denominator.

The QBER consists of two parts: The first part $\mathrm{QBER}_{\mathrm{det}}$ is due to the dark count rate of the detector, this part is proportional to $\Delta\tau$. Hence a good detector must not only be efficient and have a small dark count rate, it should also have a small time jitter, at least smaller than the pulse length of the laser diodes. The second part is what we call $\mathrm{QBER}_{\mathrm{opt}}$, that is, the fraction of photons p_{opt} whose polarization or phase is erroneously determined, i.e., the fraction of photons who end up in the wrong detector. This is mainly due to depolarization and to poor polarization alignments or due to the limited visibility of the interferometers. For example, for our first long distance experiment below Lake Geneva using polarization coding [21] we computed a $\mathrm{QBER}_{\mathrm{det}}$ of 3% and a $\mathrm{QBER}_{\mathrm{opt}}$ of 0.5%, which fitted to the measured total QBER of 3.4%. We discuss the first source of errors and have a closer look at the photon counters used.

[2] Physicists often call this quantity the bit error rate (BER). In telecommunications BER is commonly used for the total error in a transmission and is in the order of 10^{-9}. In QC the BER is in the order of 1%. Of course, this does not correspond to the final error in the message, since error correction will be applied. However, to prevent any confusion of Telecom specialists we renounce the expression BER and call it QBER. Note that in theoretical papers about eavesdropping the QBER introduced by Eve is often called the disturbance (D).

3. The Performance of Photon Counters

The photons are detected by liquid nitrogen (LN_2) cooled Ge avalanche photodiodes (NEC NDL5131) working in the passively quenched Geiger mode [22]. In this mode the diodes are driven above breakdown, i.e., the bias voltage is so high that one electron hole pair created by an absorbed photon will be able to produce an avalanche of thousands of carriers. The avalanche only stops when the current created through the resistance in series to the diode lowers the applied voltage below the breakdown value. The noise in such detectors is due to carriers generated in the detector volume by other causes than an impinging photon (dark counts). These carriers can be created thermally or by band-to-band tunneling processes, or they can be emitted from trapping levels that were populated in previous avalanches (after pulsing). The quantum efficiency and the dark count rate n_{dark} both increase with increasing bias voltage U_{bias}. To obtain a low QBER a tradeoff between high efficiency and low noise has to be found. In the early experiment mentioned above [21] we worked at $\eta = 0.2\%$ with $n_{\text{dark}} = 700$ Hz and we obtained 3% QBER_{det} (following (2), for $\mu = 0.1$ and $L = 0.9$). For $\eta = 10\%$ we would have expected more than 20% QBER_{det}.

For LN_2 cooled Ge diodes the thermal contribution can be neglected and the dark counts mainly consist of tunneled electrons and afterpulses, the latter being more important if the total charge through the device is large [17]. The afterpulse rate is decreasing almost exponentially with a time constant $(1/e)$ of about 200 ns. This fact opens the door to a further reduction of the dark count rate: If the diode is biased only immediately before a photon is expected, no spontaneous avalanches can occur before the detection and consequently no afterpulses will fall into the detection time interval. So we developed the following electronic circuit. The bias voltage of a diode is the sum of a DC part well below the threshold and a 2 ns long almost rectangular pulse of 7.5 V amplitude that pushes the diode about 1.4 V over the threshold at the time when the photon is expected. This allows us to increase considerably the efficiency without excessively increasing the noise. Moreover, the time jitter is reduced to a value below 100 ps. The short bias pulse induces a parasite signal. A discriminator in combination with a temporal coincidence window allows us to recover the true avalanche signal from this parasitic signal. A time-to-amplitude converter followed by a window-discriminator of 300 ps width, allows us to reduce the noise level further. Thanks to this technique we get 7 and 22 dark counts per 1 million pulses ($p_{\text{dark}} = 22 \cdot 10^{-6}$ and $7 \cdot 10^{-6}$) for detection efficiencies of 10% and 20%, respectively. This corresponds to a QBER_{det} of $0.72 \pm 0.13\%$ at 10% efficiency.

Recent progress in photon counting with InGaAs APDs could allow us to replace the LN_2 cooled Ge detectors [18]. A QC experiment has been performed with InGaAs detectors [14]. Performances similar to that of Ge APDs seem to be possible. Moreover, these diodes would open the second telecom window at 1550 nm.

We compare Ge detector specifications to those of commercial silicon single photon counting modules at 800 nm. These modules have about 50% efficiency with extremely low dark count rates of down to 10 Hz. The QBER_{det} and R for the different wavelengths with corresponding detector performances are summarized in Table 1 for different fiber lengths.

Note that the wavelength of 800 nm is a good choice only for distances shorter than 5 km, taking advantage of the efficient and commercially available Si detectors. The

Table 1. Quantum bit error rates (QBER) and raw data rates R for different wavelengths and detector performances for two different fiber lengths with $\nu = 10$ MHz, $\mu = 0.1$ (or as indicated), and $q = 0.5$.*

	5 km		20 km		$\text{QBER}_{\max} = 15\%$	
	QBER_{det} (%)	R (kHz)	QBER_{det} (%)	R (kHz)	$L_{\max}$ (km)	R (Hz)
800 nm, $\eta = 0.5$, $p_{\text{dark}} = 10^{-8}$	0.0022	25	0.2	0.025	29	0.3
1300 nm, $\eta = 0.1$, $p_{\text{dark}} = 7 \cdot 10^{-6}$	0.11	33	0.35	10	67	233
1300 nm, $\eta = 0.2$, $p_{\text{dark}} = 21 \cdot 10^{-6}$	0.16	67	0.53	20	62	700
1300 nm, $\eta = 0.2$, $p_{\text{dark}} = 21 \cdot 10^{-6}$ $\mu = 1$, $\nu = 1$ MHz†	0.016	67	0.053	20	90	70
1550 nm, $\eta = 0.1$, $p_{\text{dark}} = 10^{-5}$	0.13	40	0.25	20	109	333
1550 nm, $\eta = 0.1$, $p_{\text{dark}} = 10^{-5}$ $\mu = 1$, $\nu = 1$ MHz†	0.013	40	0.025	20	159	33

* The transmission losses are assumed to be 2 dB/km at 800 nm, 0.35 dB/km at 1300 nm, and 0.2 dB/km at 1550 nm. At 1550 nm, the estimated performance of InGaAs detector according to first results [14], [18].
† 1 MHz single photon production rate.

disadvantage is that fibers and modulators are generally conceived for the longer telecom wavelengths. Consequently, when Peltier cooled InGaAs counters with the expected performance are available, the telecom wavelengths will clearly be preferable, especially at 1550 nm for long distance QC. According to recent calculations QC could be performed securely with QBER up to 15% [11]. In the last column of Table 1, the maximum length of the link leading to this QBER is calculated. The limit for 1550 is around 110 km, a limit, however, that depends strongly on the performance of the detector, and its development in future. The given QBERs and $L_{\max}$ could be improved using single photon states ($\mu = 1$) [4].[3] The attainable raw data rates would be in the same order of magnitude, supposing that both a 1 MHz single photon production rate and a 10 MHz pulse rate for weak pulses are feasible.

Of course, the raw bit rates obtained will be reduced further, due to error correction and privacy amplification depending on the corresponding QBER. So the above-mentioned tradeoff between efficiency and noise of the detector depends not only on the transmission length, but also on the error correction algorithms.

With present day detector performances the QBER limit for transmission lengths

[3] The single photon source can be a two photon source (based on parametric down-conversion) where one photon serves as a trigger for the presence of its twin. The wavelength of the trigger photon is chosen in the detection range of high efficiency and low noise Si detectors. However, these are not really single photon states, because the two photon distribution is chaotic. Taking into account our time resolution the photon number can be considered as Poisson distributed as for attenuated laser pulses. For 1 MHz production rate the probability of having a second photon in a 1 ns time window pulse is 0.05%, equal to that of a laser pulse with $\mu = 0.001$.

below 20 km is set by $QBER_{opt}$ that is in the order of 0.5%. Therefore, we have a closer look at the sources of this part of the QBER.

4. Polarization Control

The fiber optic implementation of the polarimetric scheme faces three difficulties:

The first one is a topological problem related to the transport of a vector along a curve. Since the path taken by the light in the optical fiber is three-dimensional, its polarization rotates by an angle related to Berry's phase [5]. This effect does not limit the distance or the quality of the transmission if the fiber link is stable. It is clear from that consideration that an aerial cable or cable sustaining strong vibrational perturbations are not suited.

The second difficulty arises from the intrinsic birefringence of optical fibers. Changes in mechanical stress that can cause birefringence will change the state of polarization at the output of the fiber. However, these changes are usually quite slow in the order of tens of minutes depending on the mechanical and thermal stability of the environment [12]. Another effect of the birefringence is polarization mode dispersion (PMD) [13]. An optical cable behaves as a concatenation of pieces of birefringent fibers. The result of this is a spread of the pulses growing with the square root of length for long distances. This evolution is the same as a random walk. To prevent depolarization of the light pulses, lasers with a coherence time larger than the polarization mode delay must be used. This is not a real limitation since typical PMDs are between 0.1 ps/km^2 and 1 ps/km^2 and semiconductor lasers with 1 ns coherence time are available.

A third potential problem are polarization dependent losses in optical components that could arise in Passive Optical Networks (PONs). In this case the relation between the polarization state at the input and the output of the optical link is no longer unitary [16].

As for the topological effects, polarization instabilities are due to mechanical stresses and temperature variations. This requires the optical fiber to be kept as stable as possible. However, an active polarization controller is necessary to align Alice's and Bob's polarizers and keep them aligned, compensating temporal evaluation. The error rate p_{opt} can be determined simply by aligning at the receiver a polarization analyzer on the outgoing state of polarization and measure the ratio of the intensities of the two arms. In our experiments, both in the laboratory over 26 km and in the field over 23 km, we obtained a separation of the polarization of 23 dB that corresponds to an error fraction p_{opt} of 0.5%. The stability of the polarization alignment in the field experiment was excellent most of the time, and measurements could be performed for an hour without realigning the system. However, from time to time there were quite fast polarization instabilities of 2π within a few seconds. In such moments we could not of course compensate the fluctuations with our manual polarization controller. An automated polarization controller with a response time of some tens of milliseconds should be able to guarantee an uninterrupted operation.

One might think that one could spare the polarization controller by using the phase coding scheme of Fig. 2. In fact, to prevent that only every second photon chooses interfering paths (to increase q from $\frac{1}{4}$ to $\frac{1}{2}$ in (1)), a polarizing beamsplitter (PBS) is used at the receiver's end. Consequently, the phase coding scheme requires polarization controllers, too [23]. Ignoring the delay loops (which are actually no longer necessary

using PBSs) the two Mach-Zehnder interferometers with the phase shifters can simply be regarded as polarization modulators. The interferometric setup is finally equivalent to the polarization code scheme. It has just the additional inconveniences that in each Mach-Zehnder interferometer polarization has to be controlled to improve the fringe visibility and the path length differences have to be balanced every few seconds [19]. The fringe visibility obtained in phase coding is 0.99 [19], corresponding to a polarization separation of 20 dB and leading to $\mathrm{QBER}_{\mathrm{opt}} = 1\%$.

To summarize, polarization separation of 23 dB over 23 km can be achieved, leading to $\mathrm{QBER}_{\mathrm{opt}} = 0.5\%$. For a practical system, however, the main drawback is the need for active polarization controllers to compensate for fluctuations due to thermal and mechanical disturbances of the fiber. In the next section we present a novel QC setup that at the same time needs no alignment and reduces $\mathrm{QBER}_{\mathrm{opt}}$ further.

5. QC Using Faraday Mirrors

5.1. *An Interferometer with Faraday Mirrors*

Let us have a closer look at the QC scheme depicted in Fig. 3 [20], [26], disregarding the Faraday rotators (FR) for the moment, their crucial effect will be explained later. In principle Bob has a very unbalanced Michelson interferometer (beamsplitter C2) with one long arm going all the way to Alice. The laser pulse impinging on C2 is split in two pulses P1 and P2. P2 propagates through the short arm first (mirror M2 then M1) and then travels to Alice and back, whereas P1 propagates first to Alice and next passes through the short arm. As both pulses run exactly the same path length, they interfere maximally at C2 (disregarding polarization for the time being). To encode their bits, Alice acts with her phase modulator (PM) only on P2 (phase shift φ_a), whereas Bob lets pulse P2 pass unaltered and modulates the phase of P1 (phase shift φ_b). If no phase shifts

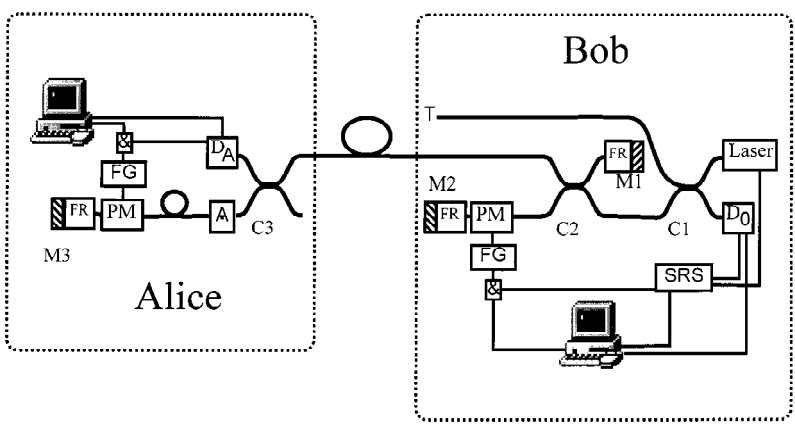

Fig. 3. Experimental setup of an interferometric QC system with Faraday mirrors. C1, C2, and C3: fiber optic couplers; M1, M2, and M3: Faraday mirrors (ordinary mirrors in combination with Faraday rotators, FR); PM: phase modulator; A: Attenuator; D_0: photon counter; D_A: photodiode; T: optional trigger output; SRS: delay generator; FG: function generator; &: and-gate.

are applied or if the difference $\varphi_a - \varphi_b = 0$, then the interference will be constructive. On the contrary, when $\varphi_a - \varphi_a = \pi$ the interference will be destructive and no light will be detected by detector D_0. Since the interfering pulses travel the same path, the interferometer is automatically aligned. The visibility of the fringes is also independent of the splitting ratio of C2.

However, visibility depends also strongly on the polarization states of the interfering pulses. Let $\mathcal{M}_{\text{in}}$ be the vector representing the polarization state of the incoming laser pulse at C2 on the Poincaré sphere, then the polarization states of the interfering pulses P1 and P2 are

$$\mathcal{M}1_{\text{out}} = R_2 R_1 R_3 \mathcal{M}_{\text{in}} \quad \text{and} \quad \mathcal{M}2_{\text{out}} = R_3 R_1 R_2 \mathcal{M}_{\text{in}},$$

where R_i is the matrix describing the polarization rotation in a round trip path to mirror M_i. Because rotation operators do not commute, these two operations are in general not identical, hence the two outcoming polarizations are not parallel. This is where the Faraday mirrors (FM) enter the game. An FM is composed of a 45° Faraday rotator and a mirror. A light pulse injected in any arbitrary polarization into a fiber terminated by an FM will come back exactly orthogonally polarized, regardless of the polarization transformations in the fiber due to induced birefringence.[4] Hence a round trip path in any fiber terminated with an FM will lead to a polarization transformation $R = -1$. This is true since there are no significant mechanical or thermal variations during the time of flight of the photons [21], which is 300 μs for a 30 km link. However, this applies only if there is no Faraday rotation inside the fiber. In fact, although the Verdet constant of a standard optical fiber is low, Faraday rotation due to the geomagnetic field may not be completely neglected for optical fibers of several tens of kilometers,[5] hence $R_3 \neq -1$. However, with $R_1 = R_2 = -1$ we obtain $\mathcal{M}1_{\text{out}} = R_3 \mathcal{M}_{\text{in}} = \mathcal{M}2_{\text{out}}$. To quantify the performance of our interferometer, we measure the ratio of the count rates for constructive and destructive interference. In practice, we change the attenuation (A) at Alice to obtain the same count rate with and without phaseshift. When we apply a phaseshift at Bob's piezo-optic modulator we obtain an attenuation of 30 ± 1 dB, while when we apply the phaseshift at Alice's $LiNbO_3$ integrated optic phase modulator the extinction is 27 ± 1 dB. Obviously the integrated phase shifter is slightly less precise. These values were reproducible within the given errors over weeks. An extinction of 30 dB corresponds to a classical fringe visibility $V = (I_{\max} - I_{\min})/(I_{\max} + I_{\min})$ of 99.8%. The measured values of 30 dB and 27 dB result in a QBER_{opt} of 0.1% and 0.2%, respectively. The average, decisive for key creation, is therefore 0.15%. Replacing one Faraday mirror by an ordinary mirror, the extinction is strongly fluctuating and can be reduced to 20 dB. If two Faraday mirrors are removed, essentially no interference is visible.

[4] This description of Faraday mirrors requires that after a reflection one switches from a right-handed to a left-handed reference frame, or vice versa. This is no problem as long as the interfering paths each undergo the same (the same parity of) numbers of reflections.

[5] The horizontal component of the geomagnetic field $H = B/\mu_0$ is 17 A/m in Geneva, the Verdet constant is ca. $0.6 \cdot 10^{-4}$ °/A at 1300 nm. Therefore the polarization is turned by about twice 1° per km displacement in the north–south direction. However, polarization mode coupling strongly reduces this effect.

5.2. *Key Creation*

For the key exchange we used the two-states protocol B92 [1], because our driving electronics for the phase modulators could not be used for the four-states protocol [3]. In principle, our setup could be quite easily adapted to the latter protocol by inserting another coupler and detector. We tested that using also $\pi/2$ and $3\pi/2$ phase shifts the same excellent performances of the interferometer are obtained. Alice and Bob choose at random 0 or π phase shifts, defined as bit values 0 and 1. Since very weak pulses are used, in most cases no photon will be detected in D_0. If a detection, i.e., constructive interference occurred, Alice and Bob know that they applied the same phase shift, and they register the same bit value. In our interferometric setup the pulses leaving Bob carry no phase information. The information is in the phase difference of the two pulses P1 and P2 leaving Alice. The attenuator (A) is set such that the weaker pulse P2 that already passed through Bob's delay line has 0.05 photons on average when leaving Alice. The information that Eve could obtain depends on the number of photons in the weaker pulse. Therefore, to measure the phase difference, she must attenuate P1 to the intensity of P2 in order to obtain complete interference. She actually performs the same measurement as Bob does. More generally, such a kind of measurement can be called a Loss Induced Generalized Measurement [16]. Consequently, 0.05 photons in the weaker pulse is equivalent to an average number of $\mu = 0.1$ for the pulse pair. Of course, this reasoning applies also for the standard time multiplexed interferometer setup (Fig. 2), where the two pulses may also have different intensities.

5.3. *Experimental Realization*

The heart of our experiment is a delay generator (SRS 535) at Bob (see Fig. 3). It beats at 1 kHz and triggers the laser, Bob's phase modulator (PM), the actively biased photon counter (D_0), and Bob's computer. The 1300 nm DFB-laser (Fujitsu, driven by an Avtech pulser) delivers 300 ps pulses. The phase modulator is a fiber wrapped around piezoelectric-tube. It is driven by a sinus function from a function generator (SRS DG 345). The modulation frequency of the piezo of about 10 kHz is high enough since the time delay between the two pulses is about 230 μs. Only if the computer gives a logical 1 to the and-gate at the external trigger input of the function generator is a phase applied. The optical fiber is a 22.8 km long telecom link between Geneva and Nyon, Switzerland, featuring 8.6 dB loss. The pulse P1 detected at Alice by D_A (Newport AD-300/AC) triggers Alice's phase modulator and Alice's computer. At Alice the delay between the two pulses is smaller, hence a 1 GHz $LiNbO_3$ waveguide phase modulator is used. Again this modulator is driven by a function generator, in case Alice's computer supplies a logical 1. Back at Bob's, the interfering photon directly runs to the detector D_0 via the 10 dB coupler C1 to limit the losses. The photon counter electronics are precisely triggered to coincide with the arrival of the photon at Bob and the biasing of diode. The adjustment must be precise within 100 ps, which can be easily obtained with the delay generator. Every detection is registered by Bob and assigned to the number of the pulse after the beginning of the measurement. Alice and Bob disposed of 100 files of 65,536 bits of random numbers. These numbers have been generated by an apparatus based on thermal noise of an electrical resistor [7].

Table 2. Results of the key distribution with a QC setup with Faraday mirrors.

Photons per pulse μ	Measured QBER (%)	$QBER_{det}$ (%)	$QBER_{opt}$ (%)	Length of key (bit)	Bit rate (Hz)
0.2	0.5 ± 0.1	0.40 ± 0.07	0.15 ± 0.03	2,980	0.9
0.1	1.35 ± 0.08	0.81 ± 0.14	0.15 ± 0.03	20,142	0.5

5.4. *Results and Discussion*

After having registered the results of the measurement, Alice and Bob compare their random lists in order to determine the QBER. The results are summarized in Table 2.

To our knowledge, these QBER rates are the lowest ever obtained for the corresponding numbers of photons per pulse and over a distance of more than 20 km. The measurement for $\mu = 0.1$ lasted more than 11 hours and no realignment was performed, hence the stability of the setup was extraordinary. However, we notice that the measured QBER is higher than the sum of the detector and interferometer noise. We believe that the increase in the error rate is not due to any fluctuations of the interferometer, but rather due to an increasing $QBER_{det}$ in the course of the measurement. Variations in the photon counter, its electronics and timing, which proved to be quite delicate, might be the reason for this increase. We also tried to trigger the photon counter by the strong laser pulse at the trigger output (T) running down another fiber to Alice and back, in order to obtain less time jitter and to be less sensitive to changes in the optical path length due to temperature variations. We gave up this optical trigger signal, because it did not improve the results for short time measurements (tens of minutes) significantly enough to justify the need of an additional fiber. Under difficult environmental conditions with large temperature fluctuations, however, the use of an auxiliary fiber for timing improvements might be appropriate, or periodical readjustments of the detector timing could be envisaged.

The obtained bit rates are quite low, in agreement with the expected values following (1). This is simply due to the low pulse rate and could be increased by replacing the piezoelectric modulator and adapting the computer steering. We have noticed that the noise of our detector increases if a relatively strong light pulse is impinging before the detection window. This might cause a problem going to higher frequencies, since in our setup we have to deal with different parasite pulses.

It is noteworthy that the timing of Alice's apparatus can be preadjusted in the laboratory and will not change, even if the apparatus is plugged into another fiber to communicate with a third party. The timing of Bob's apparatus, especially of his photon counter, has to be adjusted once for every link, this could be done using an Optical Time Domain Reflectometer (OTDR).

6. Practical Eavesdropping

We have seen that the simplest attack of Eve can be prevented using weak pulses with, e.g., $\mu = 0.1$. More elaborated strategies are analyzed in [2], [11], [15], [6], and [9]. However, in practice, Eve could follow another strategy: She could chop the fiber and try to measure actively the phase or polarization settings applied by Alice. Eve could

mount an interferometer similar to Bob's one and measure with intense light pulses the phase shifts applied by Alice. Then she can apply the same phase shifts to the pulses received from Bob and send them back to him, as if she was Alice. However, as Alice attenuates the incoming pulses by more than 40 dB down to the 0.1 photon level before sending them back, Eve is forced to send intense pulses to Alice, which can be detected by the detector D_A, inserted for this purpose. However, by assumption, Eve has perfect technology at her disposal. Therefore, she could for example try to sense Alice's phase with a very short pulse beyond the bandwidth of D_A. Alice, in return, could prevent such an intrusion with a narrow line filter. Probably any kind of intrusion could be prevented with the appropriate means, but security would no longer be guaranteed solely by the fundamental laws of quantum mechanics. In fact, all other QC schemes face the same problem. In the standard phase scheme the position of the phase shifter could be sensed interferometrically using small reflections at Alice's or Bob's ends. Hypothetically, Eve might find an optical technique to find out which laser fired or which detector clicked in the polarization scheme proposed above. In these setups optical isolators could be introduced in contrast to the Faraday mirror setup. We cannot discuss all possible strategies of Eve and the technical means to fight them. A general assumption implicit in all discussions of QC security is that Alice's and Bob's offices are absolutely safe. This is a reasonable assumption, necessary also for all other cryptosystems. However, as illustrated by the above discussion, care should be given to the fact that the fiber-obtic quantum channel provides a potential entrance gate for malevolent intruders.

In yet another eavesdropping strategy, that applies to the two-states system only [1], Eve interrupts the transmission and measures as many pulses as possible. She sends to Bob only the pulses for which she obtained the phase or the polarization. To prevent this, Bob has to introduce another detector to monitor the stronger pulse P1 to make sure that Eve cannot suppress this pulse. If Eve suppresses only the weak one, because she did not get the phase information, the strong pulse alone will introduce 50% error on detector D_0. To render the power of P1 measurable by a conventional detector, the losses of Bob's delay line could be increased and the attenuation applied at Alice's side reduced by the same amount. The attenuation at Alice applies also to pulses needed by Eve to spy on Alice's phase, following the strategy mentioned above. With the laser power and the detectors at our disposal, it is not possible to monitor P1 at Bob's and P2 at Alice's (hence Eve's spying pulse) at the same time (also with appropriate choice of the splitting ratio of the couplers C2 and C3, presently 3 dB couplers). So, the present implementation of the B92 protocol is insecure, and the BB84 protocol should be applied.

In the four-states protocol BB84 [3] the eavesdropping strategy mentioned in the previous paragraph fails because Eve would introduce errors when she chooses the wrong basis. However, suppose that Eve has a lossless line and a way to sense how many photons are in the pulse. For $\mu = 0.1$ there is about a 6% chance of having two photons in a nonempty pulse. In these cases Eve could let one photon pass and store the other until Alice and Bob publicly communicate their bases and get full information on this bit. Eve would then send only these pulses to Bob, and block the others. Bob would not notice Eve's presence, since he expects considerable losses in his line. Therefore, Eve could obtain 100% of the information if the line had, e.g., just 6% transmission. In conclusion, as a function of μ and the losses in the line Eve could win a considerable

fraction of the information. Again this could be prevented by measuring the intensity of a stronger pulse, to force Eve to send a pulse every time [15].

QC with correlated photon pairs would have the advantage that, since in this case real single photon states are used, all strategies dealing with the fraction of pulses containing more than one photon must fail. Unfortunately, the self-aligning setup with Faraday mirrors is not suited for such a photon source, due to the high losses in a complete round trip.

In practice, a tradeoff has to be found between the complexity, hence the price, and the absolute security of the setup. We mention in this context that since the interferometer in the Faraday mirror setup is not stabilized, the absolute phase difference between the pulses P1 and P2 will randomly fluctuate, rendering Eve's job very hard. This contrasts with the standard phase coding setup, where the intense pulses sent by Alice to adjust Bob's interferometer can also be used by Eve to adjust hers.

7. Conclusions

We have discussed the experimental advantages and drawbacks of different QC setups. We have seen that one major problem is the availability of good photon counters. It is essentially the noise of these detectors, in combination with the losses in the optical fiber, that limits the maximum distance of a QC link. This maximum distance would be about 100 km working at 1550 nm in combination with InGaAs photon counters. The other problem of standard polarization and phase coding setups is the need for continuous alignment. We introduced and demonstrated an interferometric QC setup using Faraday mirrors which requires no continuous alignment. It features impressive stability and a fringe visibility of 99.8%. Using this new QC setup, we produced a secret key of 20 kbit length with a QBER of 1.35% for 0.1 photon per pulse.

Acknowledgments

We would like to thank the Swiss Telecom for financial support and for placing at our disposal the Nyon–Geneva optical fiber link. We appreciate stimulating discussions with our colleagues within the TMR network on the physics of quantum information.

References

[1] C. H. Bennett, Quantum cryptography using any two non-orthogonal states, *Phys. Rev. Lett.* 68 (21), 3121–3124 (1992).
[2] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, Experimental quantum cryptography, *J. Cryptology* 5, 3–28 (1992).
[3] C. H. Bennet and G. Brassard, Quantum cryptography: public key distribution and coin tossing, *Proc. Internat. Conf. Computer Systems and Signal Processing*, Bangalore, 1984, pp. 175–179.
[4] C. H. Bennett, G. Brassard, and N. D. Mermin, Quantum cryptography without Bell's theorem, *Phys. Rev. Lett.* 68 (5), 557–559 (1992).
[5] R. Y. Chiao and Y. S. Wu, *Phys. Rev. Lett.* 57 (8), 933–936 (1986).
[6] J. Cirac and N. Gisin, Coherent eavesdropping strategies for the four state quantum cryptography protocol, *Phys. Lett. A*, in press.

[7] F. Devillard, Etude d'un générateur de bruit et de ses applications, Travail de diplôme, Ecole d'ingénieurs de Genéve, 1996.
[8] A. K. Ekert, Quantum cryptography based on Bell's theorem, *Phys. Rev. Lett.* 67 (6), 661–663, 1991.
[9] A. K. Ekert, B. Huttner, G. M. Palma, and A. Peres, Eavesdropping on quantum-cryptographical systems, *Phys. Rev. A* 50 (2), 1047–1056 (1994).
[10] J. D. Franson and B. C. Jacobs, Operational system for quantum cryptography, *Electron. Lett.* 31 (3), 232–234 (1995).
[11] C. A. Fuchs, N. Gisin, R. B. Griffiths, C.-S. Niu, and A. Peres, Optimal eavesdropping in quantum cryptography, *Phys. Rev. A* 56, 1163 (1997).
[12] N. Gisin, R. Passy, J. C. Bishoff, and B. Perny, Experimental investigations of the statistical properties of polarization mode dispersion in single mode fibers, *IEEE Phot. Technol. Lett.* 5, 819–821 (1993).
[13] N. Gisin, J. P. Pellaux, and J. P. Von Der Weid, Polarization mode dispersion of short and long single mode fibers, *IEEE J. Lightwave Technol.* 9, 821–827 (1991).
[14] R. J. Hughes, G. G. Luther, G. L. Morgan, C. G. Peterson, and C. Simmons, Quantum cryptography over underground optical fibers, *Proc. Crypto*. '96, Lecture Notes in Computer Science, vol. 1109, p. 329 (1996).
[15] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Quantum cryptography with coherent states, *Phys. Rev. A* 51 (3), 1863–1869 (1995).
[16] B. Huttner, A. Muller, J. D. Gautier, H. Zbinden, and N. Gisin, Unambiguous quantum measurements of non-orthogonal states, *Phys. Rev. A* 54 (5), 3783–3789 (1996).
[17] A. Lacaita, P. A. Francese, F. Zappa, and S. Cova, Single-photon detection beyond 1 μm: performance of commercially available germanium photodiodes, *Appl. Opt.* 33 (30), 6902–6918 (1996).
[18] A. Lacaita, F. Zappa, S. Cova, and P. Lovati, Single-photon detection beyond 1 μm: performance of commercially available InGaAs/InP detectors, *Appl. Opt.* 35 (16), 2986–2996 (1996).
[19] Ch. Marand and P. D. Townsend, Quantum key distribution over distances as long as 30 km, *Opt. Lett.* 20 (16), 1695–1697 (1995).
[20] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, "Plug and play" systems for quantum cryptography, *Appl. Phys. Lett.* 70 (7), 793–795 (1997). US patent pending.
[21] A. Muller, H. Zbinden, and N. Gisin, Quantum cryptography over 23 km in installed under-lake telecom fibre, *Europhys. Lett.* 33 (5), 335–339 (1996).
[22] P. C. M. Owens, J. G. Rarity, P. R. Tapster, D. Knight, and P. D. Townsend, Photon counting with passively quenched germanium avalanche diodes, *Appl. Opt.* 33 (30), 6895–6901 (1994).
[23] P. D. Townsend, J. G. Rarity, and P. R. Tapster, Enhanced single photon fringe visibility in a 10 km long prototype quantum cryptography channel, *Electron. Lett.* 29 (14), 1291–1293 (1993).
[24] S. Wiesner, Conjugate coding, *Sigact News* 15 (1), 77–88, 1983.
[25] W. K. Wootters and W. H. Zurek, A single quantum cannot be cloned, *Nature*, **299**, 802 (1982).
[26] H. Zbinden, J. D. Gautier, N. Gisin, B. Huttner, A. Muller, and W. Tittel, Interferometry with Faraday mirrors for quantum cryptography, *Electron. Lett.* 33 (7), 586–588 (1997).