Eur. Phys. J. D **18**, 141–146 (2002)
DOI: 10.1140/epjd/e20020017

THE EUROPEAN
PHYSICAL JOURNAL D
EDP Sciences

Integrated quantum key distribution system using single sideband detection

J.-M. Merolla[1,a], L. Duraffourg[1], J.-P. Goedgebuer[2], A. Soujaeff[1], F. Patois[1], and W.T. Rhodes[1]

[1] GTL-CNRS Telecom[b], Georgia Tech Lorraine, 2-3 rue Marconi, 57070 Metz, France
[2] Laboratoire d'Optique P.M. Duffieux[b], Université de Franche-Comté, 25030 Besançon Cedex, France

Received 13 July 2001 and Received in final form 30 November 2001

Abstract. We report a new quantum cryptographic system involving single sideband detection and allowing an implementation of the BB84 protocol. The transmitted bits are reliably coded by the phase of a high frequency modulating signal. The principle of operation is described in terms of both classical and quantum optics. The method has been demonstrated experimentally at 1 550 nm using compact and conventional device technology. Single photon interference has been obtained with a fringe visibility greater than 98%, indicating that the system can be used in view of quantum key distribution potentially beyond 50-km-long standard single-mode fiber.

PACS. 03.67.Dd Quantum cryptography – 42.79.-e Optical elements, devices, and systems

1 Introduction

The objective of quantum key distribution is to permit two parties, Alice and Bob, to exploit fundamental properties of quantum optics in order to share in secret a random bit sequence – the key –. The general procedure in quantum key distribution includes the following steps. First, Alice sends a sequence of individual photons, choosing at random the quantum state in which each photon is prepared. The state of the photons serves to encode bits of information. Upon receiving the photons, Bob performs measurements on their states. Alice and Bob retain data only from photons that have been measured in the correct basis. Should Eve tap the transmission line, intercept some of photons, and retransmit them after performing her own measurements, transmission errors occur due to the quantum-mechanical nature of photons. To detect these errors, Bob and Alice verify statistically a set of shared bits. If too many errors are detected in the verification process, the bit in that set are discarded. The security of transmission is guaranteed by a protocol: the BB84 protocol [1] if four quantum states are used, the B92 protocol if two non-orthogonal states are used [2] or one of variety of other protocols for other schemes [3,4].

Two principal methods have been used to encode information. The first is based on polarization coding [1,5,6]. The problem with this method is that it is difficult to preserve polarization over long transmission distances in standard telecommunication optical fibers. The second method is based on delay-coded quantum states [7–9]. In this latter case, each bit is encoded into an optical path difference. Two interferometers, with matched path imbalances greater than the pulse length, form the transmitter and receiver. The difficulty with delay coding is to maintain the optical delay in the interferometers constant despite inevitable mechanical vibrations and thermal drifts [9]. Systems based on Faraday mirrors have been proposed to overcome this drawback of polarization coding [10]. Other solutions have also, been proposed involving acousto-optic deflectors or multicolored photons, with wavelength now serving as the basis for encoding information [11]. Recently, we reported a new encoding method based on single-photon phase modulation. In that system, Alice encodes each bit of the transmitted key into an optical frequency by randomly selecting a modulation phase from two possible values. Bob modulates light at the same frequency carrier frequency, again selecting randomly between two phases. By means of single-photon interference experiments and an additional (possibly public) exchange of information with Alice, Bob is then able to determine the states of the photons sent by Alice [12,13]. This method of quantum key distribution can only be carried out under the B92 protocol.

In what follows, we describe an improvement of the modulation transmission scheme, based on single-sideband (SSB) detection, which allows the BB84 protocol to be used with a view to increase the transmission rate and the distance limit for secret bits distribution (the reader is referred to references [14–19] for a detailed discussion on the security aspects related with the various protocols) in a robust scheme for quantum cryptography.

[a] e-mail: merolla@georgiatech-metz.fr

[b] UMR CNRS 6603

The potential advantages expected from our new scheme compared with polarization-coding or delay-coding are:

(i) the system can be easily made polarization-independent if a polarization-independent intensity modulator is used at the receiver,
(ii) the scheme enables one to use integrated electro-optic modulators, therefore providing high stability against thermal drift as compared with a fiber Mach-Zehnder,
(iii) and, finally, the synchronization constraint can be relaxed (as will be shown below) compared with that usually required in optical interferometric systems.

We introduce an appropriate version of a four-state protocol and relate this to the ability to distribute a key in a secure fashion. We also report experimental results obtained at 1 550 nm wavelength that show the possibility to transmit a key over a 50-km-long standard single-mode fiber.

2 Principle

The proposed SSB system is depicted in Figure 1. The source S, henceforth referred to as the reference source, is a pulsed laser diode operating at central frequency ω_0. An unbalanced integrated Mach-Zehnder modulator MZ_1 with a $\lambda/4$-optical path difference bias modulates the intensity of the reference beam at angular frequency $\Omega \ll \omega_0$ with a modulation depth m that is chosen to be small. Alice uses a phase-locked oscillator, PLO_1, operating at the frequency Ω with an electrical phase Φ_1. She chooses randomly the value of Φ_1 from among the four values $(0, \pi)$ or $(\pi/2, -\pi/2)$, which form a pair of conjugate bases. At the output of MZ_1, the optical signal contains the reference carrier ω_0 and two sidebands $\omega_0 \pm \Omega$ with phase Φ_1 relative to the reference. Alice adjusts the source intensity with an attenuator such that in a given pulse there is much less than one photon in these sidebands at the input of the standard single-mode transmission fiber. At the receiver, Bob uses a second unbalanced integrated Mach-Zehnder modulator MZ_2 with a $3\lambda/4$-optical path difference bias. His phase-locked oscillator, PLO_2, operates at the same frequency Ω but with an electrical phase $(\Phi_2 + \pi/2)$ relative to the reference. Classically, *i.e.*, at high light levels, the light leaving Bob's modulator contains the reference carrier ω_0 and a single sideband at frequency $\omega_0 + \Omega$ or $\omega_0 - \Omega$. when the relative phase difference $(\Phi_1 - \Phi_2)$ is 0 or π respectively. The signal contains both $\omega_0 + \Omega$ and $\omega_0 - \Omega$ when the relative phase difference $(\Phi_1 - \Phi_2)$ is $\pm\pi/2$. A Fabry-Pérot interferometer FP_1 selects the $\omega_0 + \Omega$ sideband, which is detected by photodetector D_1. The probability P_1 of detecting one photon in the sideband is governed by a cosine-squared function of the phase difference $(\Phi_1 - \Phi_2)$. The reflected signal, containing both the reference carrier and the $\omega_0 - \Omega$ sideband, is recovered thanks to a circulator C. A second Fabry-Pérot interferometer FP_2 is then used to select the $\omega_0 - \Omega$ sideband, which is detected by detector D_2. The probability P_2 of detecting a photon in that sideband is a sine-squared function of the relative phase difference $(\Phi_1 - \Phi_2)$. The BB84 scheme can then be implemented with this system, as we will explain in Section 3, which features two outputs with complementary probabilities of photon detection.

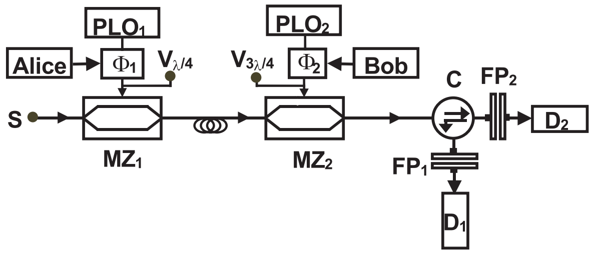


Fig. 1. Schematic diagram of the SSB modulation system.

The working conditions yielding such specific properties of the SSB system, as exploited for quantum key distribution are now explained.

Initially we assume that the laser diode operates as a classical source, not strongly attenuated. Let $E(t) = |E_0| \exp(\mathrm{j}\omega_0 t)$ represent the amplitude of the light from the source S and $m = \pi \times a/2V_\pi$ the modulation depth, a being the peak-to-peak voltage of the electrical signal, and V_π the half-wave voltage of the modulator. The light field at the output of MZ_1 can be expressed as

$$E_1(t) = \frac{1}{2} E(t) \left[1 + \mathrm{j} \exp\left\{\mathrm{j} m \cos(\Omega t + \Phi_1)\right\}\right]. \quad (1)$$

Assuming that the modulation depth m is suitable small, equation (1) can be approximated as

$$E_1(t) \approx \frac{1}{2} E(t) \Big[(1 + \mathrm{j}) - \frac{m}{2} \exp\left\{\mathrm{j}(\Omega t + \Phi_1)\right\} \\ - \frac{m}{2} \exp\left\{-\mathrm{j}(\Omega t + \Phi_1)\right\}\Big] \cdot \quad (2)$$

Light field $E_1(t)$ is transmitted to modulator MZ_2 *via* a standard single-mode fiber. Bob modulates the arriving light signal at the same frequency Ω and with the same modulation depth m as used by Alice. Introducing the same approximations used in obtaining equation (2) and dropping terms of order m^2 and higher yields the following expression for the output of MZ_2:

$$E_2(t) = \frac{1}{2} E_1(t) \left[1 - \mathrm{j} \exp\left\{\mathrm{j} m \cos(\Omega t + \Phi_2 + \frac{\pi}{2})\right\}\right] \quad (3)$$

$$\begin{aligned} E_2(t) &\approx \frac{1}{2} E_1(t) \Big[(1 - \mathrm{j}) + \mathrm{j}\frac{m}{2} \exp\left\{\mathrm{j}(\Omega t + \Phi_2)\right\} \\ &\quad - \mathrm{j}\frac{m}{2} \exp\left\{-\mathrm{j}(\Omega t + \Phi_2)\right\}\Big] \\ &\approx \frac{1}{2} E(t) \Big[-\mathrm{j} + \frac{m}{4}(\mathrm{j} - 1) \exp(\mathrm{j}\Omega t) \\ &\quad \times \left\{\exp(\mathrm{j}\Phi_1) + \exp(\mathrm{j}\Phi_2)\right\} \\ &\quad + \frac{m}{4}(\mathrm{j} - 1) \exp(\mathrm{j}\Omega t) \left\{\exp(-\mathrm{j}\Phi_1) - \exp(-\mathrm{j}\Phi_2)\right\}\Big] \cdot \end{aligned}$$

The spectrum of $E_2(t)$ contains a central peak at frequency ω_0 with the intensity $I = |E_0|^2/4$ and two sideband peaks at $\omega_0 \pm \varOmega$ with intensities:

$$i_{\omega_0+\varOmega} = \frac{1}{8} m^2 |E_0|^2 \cos^2\left[(\varPhi_2 - \varPhi_1)/2\right], \qquad (4)$$

$$i_{\omega_0-\varOmega} = \frac{1}{8} m^2 |E_0|^2 \sin^2\left[(\varPhi_2 - \varPhi_1)/2\right]. \qquad (5)$$

Note that the sideband intensities depend on the difference of the phases $\varPhi_1$ and $\varPhi_2$ chosen by Alice and Bob. For $|\varPhi_1 - \varPhi_2| = 0$, $i_{\omega_0-\varOmega}$ is minimum, $i_{\omega_0+\varOmega}$ is maximum and for $|\varPhi_1 - \varPhi_2| = \pi/2$, the two sideband intensities are equal with a value one-half that the previous maximum. The intensity of the center peak can be considered constant because the modulation depth is small.

The Fabry-Pérot interferometers FP_1 and FP_2 are adjusted to transmit only the upper or the lower sideband, respectively, all other spectral components of the light being blocked.

This system is formally equivalent to an interferometric system with two complementary outputs, providing constructive or destructive interference between the side bands generated by Alice and Bob.

Let us now consider the system operation when the laser diode is strongly attenuated. The output from a laser operating well above threshold can be described by a coherent state. The probability of observing a photocount with a detector of efficiency ρ at time t is proportional to $P = \rho_D \langle \varPsi | E^-(t) E^+(t) | \varPsi \rangle_D$, with

$$E^+(t) = \mathrm{j} \sum_{\omega} \xi(\omega) a_\omega \exp(-\mathrm{j}\omega t), \qquad (6)$$

$$E^-(t) = -\mathrm{j} \sum_{\omega} \xi(\omega) a_\omega^+ \exp(\mathrm{j}\omega t), \qquad (7)$$

$$\xi(\omega) = \sqrt{\frac{\hbar\omega}{2\varepsilon_0 (2\pi)^3}}, \qquad (8)$$

where ε_0 is dielectric permittivity of vacuum, a_ω and a_ω^+ are the annihilation and creation operators, and $|\varPsi\rangle_D$ is the coherent state describing the field incident on a detector. Initially, the quantum field emitted by the source is $|\varPsi\rangle_1 = |\alpha_{\omega_0}\rangle |0\rangle |0\rangle$ where two zero are related to the two sidebands. At Alice's modulator output, the coherent state describing the quantum field can be deduced from equation (2). The coherent state at Alice's modulator output can then be written as a superposition of coherent states:

$$|\varPsi\rangle_2 = |\alpha_{\omega_0}\rangle |\exp(-\mathrm{j}\varPhi_1)\alpha_{\omega_0-\varOmega}\rangle |\exp(\mathrm{j}\varPhi_1)\alpha_{\omega_0+\varOmega}\rangle \cdot \qquad (9)$$

Similarly, the state describing the quantum field at Bob's modulator output is given by

$$\begin{aligned} |\varPsi\rangle_3 = &\left| -\mathrm{j}\frac{(\mathrm{j}-1)}{2}\alpha_{\omega_0} \right\rangle \left| \frac{(\mathrm{j}-1)}{2}\big[\exp(-\mathrm{j}\varPhi_1) \right. \\ &\left. - \exp(-\mathrm{j}\varPhi_2)\big]\alpha_{\omega_0-\varOmega} \right\rangle \Big| \\ &\times \frac{(\mathrm{j}-1)}{2}\big[\exp(\mathrm{j}\varPhi_1) + \exp(\mathrm{j}\varPhi_2)\big]\alpha_{\omega_0+\varOmega} \Big\rangle \cdot \qquad (10) \end{aligned}$$

After spectral filtering, the states detected by the single photon detector 1 and 2 are respectively:

$$|\varPsi\rangle_1 = |0\rangle|0\rangle \Big| \frac{(\mathrm{j}-1)}{2}\big[\exp(\mathrm{j}\varPhi_1) + \exp(\mathrm{j}\varPhi_2)\big]\alpha_{\omega_0+\varOmega} \Big\rangle, \qquad (11)$$

$$|\varPsi\rangle_2 = |0\rangle \Big| \frac{(\mathrm{j}-1)}{2}\big[\exp(-\mathrm{j}\varPhi_1) - \exp(-\mathrm{j}\varPhi_2)\big]\alpha_{\omega_0-\varOmega} \Big\rangle |0\rangle \cdot \qquad (12)$$

Recalling that $a_\omega |\alpha_{\omega'}\rangle = \alpha_\omega \delta_{\omega\omega'}$, the probabilities of photocounts are respectively:

$$\begin{aligned} P_1 &= 2\rho\xi^2(\omega_0)\langle n_{\omega_0+\varOmega}\rangle \cos^2\left((\varPhi_1 - \varPhi_2)/2\right) \qquad (13) \\ &= 2\eta \cos^2\left((\varPhi_1 - \varPhi_2)/2\right) \\ P_2 &= 2\rho\xi^2(\omega_0)\langle n_{\omega_0-\varOmega}\rangle \sin^2\left((\varPhi_1 - \varPhi_2)/2\right) \\ &= 2\eta \sin^2\left((\varPhi_1 - \varPhi_2)/2\right) \qquad (14) \end{aligned}$$

where $\langle n_{\omega_0-\varOmega}\rangle$ and

$$\langle n_{\omega_0+\varOmega}\rangle = \langle \alpha_{\omega_0+\varOmega} | a^+_{\omega_0+\varOmega} a_{\omega_0+\varOmega} | \alpha_{\omega_0+\varOmega} \rangle = \langle n_{\omega_0-\varOmega}\rangle$$

are the average photon numbers at the detectors in the sideband frequency $\omega_0 + \varOmega$ and $\omega_0 - \varOmega$ and η represents the probability of photocount per pulse. Equations (13, 14) are formally equivalent to equations (4, 5). The probabilities of detecting a photon at the Fabry-Pérot outputs are complementary and vary respectively as a sine-squared or cosine-squared function of the relative phase difference $(\varPhi_1 - \varPhi_2)$. We show now how this property can be used to share a key.

3 Implementation of the four-state protocol

The protocol used is derived from the four-state scheme proposed by Bennett [1]. We shall describe the protocol in terms of the phase states (these states should not be confused with the phase operator states of quantum optics) discussed in the preceding section. The non-orthogonal states used by Alice is formed by four states that differ by $\pi/2$, such as $\varPhi_1 = 0$ or $\pi/2$ for bit "0" and π or $-\pi/2$ for bit "1". Bob makes a measurement of each states he receives by using two phases that differ by $\pi/2$, by example 0 and $\pi/2$. The protocol can be described as follows.

- For each transmitted photon Alice randomly chooses the state of transmission to be one of the four-phase states, namely 0 and $\pi/2$ for bit "0" and π and $-\pi/2$ for bit "1" respectively. Every photon permits the transmission of a bit of information.
- Bob randomly and independently chooses his measurement state (0 or $\pi/2$) for each incoming photon.
- Bob then tells Alice, possibly over a public channel, the results of his measurements, photon detected or not and the phase that he used.
- Alice and Bob agree to discard all the bits for which no photon was detected and for which the phase shift between the emitter and the receiver is equal to $\pi/2$. For

Table 1. Four-state protocol for secret key transmission in the absence of an eavesdropper.

Phase used by Alice	0		π		$\pi/2$		$-\pi/2$	
Bit sent by Alice	0		1		0		1	
Phase used by Bob	0	$\pi/2$	0	$\pi/2$	0	$\pi/2$	0	$\pi/2$
Photon destination	D_1	D_1 or D_2	D_2	D_1 or D_2	D_1 or D_2	D_1	D_1 or D_2	D_2
Common bits	0	no	1	no	no	0	no	1

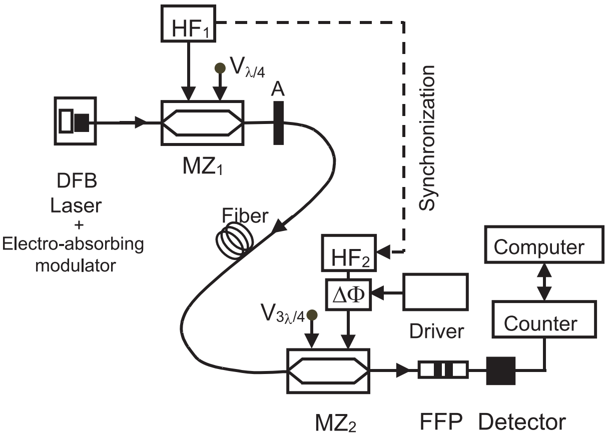


Fig. 2. Experimental setup.

this latter case, the result of the measurement realized by Bob is not concluding because the probability of detecting a photon in the two sidebands are equal (*cf.* Eqs. (14, 15)). When the phase shift $(\Phi_1 - \Phi_2) = 0$ (π) the photon can be detected only by the detector 1 (2). In that case Bob can infer the phase chosen by Alice and then the bit sent by her. In the absence of an eavesdropper, they now possess a shared random sequence of bits, which they could use as a secret key. Those first steps are summarized in Table 1. If Eve is tapping the channel, because Eve cannot know *a posteriori* which phases Alice and Bob will choose, there will, with certainty approaching unity, be times when Eve's choice results in irreducible errors in the sequence of photons that she resends on to Bob. Those errors allow Alice and Bob, through examination of the photon-count statistics, to estimate the fraction of information known by Eve. This leakage of information to Eve can be accommodated within the privacy amplification procedure [7,15]. A thorough eavesdropping analysis is very lengthy and a more complete discussion of different attacks in the case of coherent states is given in [15–18].

4 Experimental results

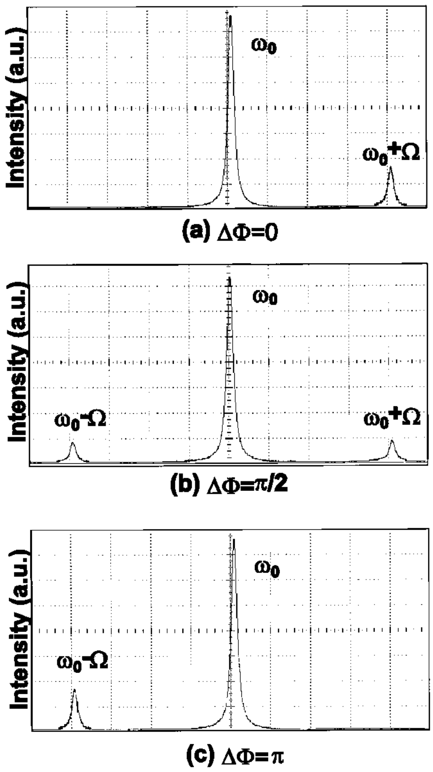
Working with the system illustrated in Figure 2, we checked the validity of the SSB modulation scheme and of the working conditions yielding single photon interference. The source was a DFB laser diode operating at 1 550 nm and with a linewidth of 30 MHz and a power of 0 dBm. The source was temperature stabilized against wavelength drift. An electro-absorbing modulator, set on the same wafer, generated 5-ns-duration optical pulses with a repetition rate of 100 kHz. We inserted a fiber variable attenuator to adjust the power of the beam launched in the transmission fiber. Intensity modulators MZ$_1$ and MZ$_2$ were pigtailed LiNbO$_3$ integrated phase modulators including DC bias electrodes. Their half-wave voltage and electrical bandwidth were 5 V and 5 GHz, respectively. Their insertion loss was 4 dB. The frequency of modulation was chosen to be 2.5 GHz. Two high-frequency (HF$_1$ and HF$_2$) generators (4 GHz bandwidth) were used to drive the modulators. The generators were phase- locked thanks to a clock signal produced by one of the generators. The electrical signal of the HF generators was first adjusted independently for each modulator to obtain the same modulation depth. In the electrical circuit of one of the modulators we inserted a phase shifter $\Delta\Phi$ to introduce a variable phase difference $\Delta\Phi = (\Phi_1 - \Phi_2)$ between the driving voltages applied to MZ$_1$ and MZ$_2$. The electrical bandwidth of the driver of the phase shifter was 10 kHz. The Fiber Fabry-Pérot (FFB) interferometer was operated as a scanning FP, *i.e.*, as a spectrum analyzer, with a 5 GHz scanning range. It could also be operated as a spectral filter. Its free spectral range and its spectral resolution were 10 GHz and 100 MHz respectively, yielding a finesse of 100.

First, we tested the system operating in the *classical regime.* The source was not attenuated and not pulsed. The detector used at the FP output was a standard photodiode. The power loss of the transmission system including modulator MZ$_2$, a 20-km long fiber (0.2 dB/km), and the FP was 9 dB. We did not try to optimize the power efficiency with the available components. Although the system did not operate in the quantum regime, we checked easily the principle of operation. Normally, the peak-to-peak amplitude a of the driving voltage of the modulators should be much smaller than the half-wave voltage of the modulators to meet the condition of a weak modulation depth $(m \ll 1)$, as defined earlier. In fact, to obtain illustrative figures, we let $a = 0.7$ V, yielding a modulation depth $m = a\pi/2V_\pi = 0.2$ radian. The bias voltages $V_{\lambda/4}$ and $V_{3\lambda/4}$ of each modulator were chosen such that $3\lambda/4$-optical path difference bias and $3\lambda/4$-optical path difference bias were introduced respectively for MZ$_1$ and MZ$_2$. Figure 3b shows the intensity thus detected at the system output for $\Delta\Phi = \pi/2$, with the FFP operating in the scanning mode. We observe clearly the two side frequencies, each spaced by 2.5 GHz from the center peak The ratio between the intensity of the center frequency and that of the side frequency was measured to be 10%, which is in good accord with $2m^2$, as predicted in equations (4, 5). Figures 3a and 3c illustrate other cases for $\Delta\Phi = 0$ and π. Complementarities of the upper and lower sideband intensities can be seen distinctly as the modulator phase shift varies between 0 and π. Figure 4 was obtained without scanning the FFP, but using the FFP as a filter to select (1) the upper sideband and (2) the lower sideband. The value of $\Delta\Phi$ was then modulated and the intensity thus detected at the FFP output in the upper and lower sidebands is shown in the bottom trace (1) and (2). In Figure 4a, $\Delta\Phi$ varies linearly between 0 and π (top trace). The intensity detected in the sideband (bottom traces) vary respectively as a cosine-squared and sine-squared function of the phase shift $\Delta\Phi$, in accord with equations (4, 5). Figure 4b shows another example obtained by switching $\Delta\Phi$ randomly between 0 and π with 1 ms-duration pulses (top trace) to simulate the phase states used in the cryptographic protocol.

Finally the visibility of the interference between the sidebands was measured be 99%, a value to be compared with the theoretical visibility of 99.2% as calculated from the Fabry-Pérot finesse, the modulation depth m and the modulation frequency.

Note that, in our demonstrator, phase-locking the two generators is necessary to drive the emitter and the receiver. An alternative solution would be to use a second optical signal (S2) at a different wavelength modulated at the same frequency Ω. At Bob's premises, this second signal is separated from the quantum signal (S1) (*e.g.* by use of a wavelength demultiplexer) and serves as the input electrical signal of Bob's modulator. In that case, synchronization of Bob's and Alice's modulators is obtained directly. As a bonus, propagation effects in the transmission link between Alice and Bob such as the propagation time attached to the group velocity and the dispersion related to phase velocity are directly taken into account and therefore allow full synchronization.

In the *quantum regime*, the intensity in the side frequency will be chosen such that the probability at Alice's side, of launching one photon in both sidebands is 0.1 photon per pulse (and therefore after Poisson's law a 5×10^{-3} probability of having pulses with more than one photon per pulse in both sidebands). This yields an average photon number per pulse of about 0.05 in each side frequency. Consequently, for the modulation depth $m = 0.2$ chosen, there will be ten times more photons in the center frequency. Experiments were performed by replacing the standard photodetector by an InGaAs/InP single-photon avalanche diode (SPAD) operating in the active gating mode [20] with an electrical gate width of 7 ns. The SPAD was temperature stabilized at −140 °C (±0.2 °C) to avoid quantum efficiency drift. Its quantum efficiency was 13%.



(a) ΔΦ=0

(b) ΔΦ=π/2

(c) ΔΦ=π

Fig. 3. Experimental power-spectra obtained with a scanning Fabry-Pérot interferometer for phase difference $\Delta\Phi = (\Phi_1 - \Phi_2)$. The scale of the horizontal axis is 625 MHz/division.

We studied the count-rate at the filter output as a function of the relative phase difference $\Delta\Phi$. The value of $\Delta\Phi$ was varied between 0 and 2π. For each value, the count number was determined during intervals of ten seconds. The dark count probability of the SPAD per pulse was measured to be 3×10^{-5}. Figure 5 shows the normalized photon-count rate observed at each of sidebands as a function of the relative phase difference $\Delta\Phi$ after removal of the dark-count rate from the experimental count-rate. The circled line and the asterisked line represent the photon counts detected for the lower- and upper-sideband respectively. The plain line represents the sinusoidal fit of the experimental photon-count, which is in agreement with equations (13, 14). The visibility V of the single-photon interference fringes thus obtained was 98%. The QBER, as defined in [7], depends on both the visibility and the dark-count rate P_{d} of the SPAD:

$$\mathrm{QBER} \approx \frac{(1-V)\mu\eta T T_{\mathrm{B}} + P_{\mathrm{d}}}{2P_{\mathrm{d}} + 2\mu\eta T T_{\mathrm{B}}} \tag{15}$$

where T is the attenuation of the fiber (0.2 dB/ km), T_{B} is the attenuation induced by Bob (5 dB in our case), V is the experimental visibility (98%), η is the quantum efficiency (13%) and $\mu = 0.05$ is the average photon number launched in one sideband. As shown in [17], in a system using single photon signals the transmission rate for secret bits is non-zero for QBER values less than 11%. Using this criterion in equation (15), the upper-bound of the limit distance is found to be beyond 50 km. Note however that in an experimental system with a strongly attenuated source, the distance limit can be more restrictive, as discussed in reference [17,18], due to the unavoidable presence of pulses with more than one photon per pulse

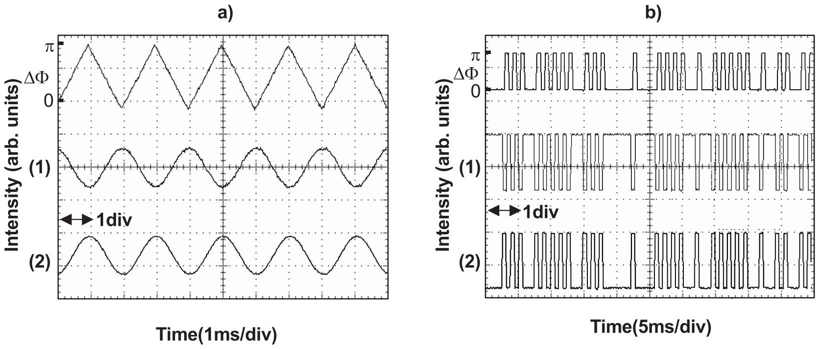


Fig. 4. Oscilloscope displays of the intensities detected in the sideband frequency $\omega_0 + \Omega(1)$ and $\omega_0 - \Omega(2)$ *versus* time (vertical axis: arbitrary units, horizontal axis: (a) 1 ms/div, (b) 5 ms/div). In (a) $\Delta\Phi$ is linearly modulated between 0 an π. In (b) $\Delta\Phi$ is randomly switched between 0 and π.

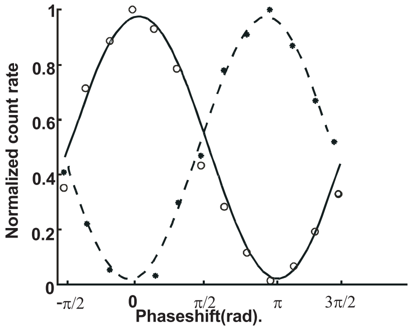


Fig. 5. Normalized single-photon count rate *versus* $\Delta\Phi = (\Phi_1 - \Phi_2)$. The white circles and the dark dots correspond to experimental photon-counts detected respectively at $\omega_0 + \Omega$ and $\omega_0 - \Omega$. The plain line and the dash line represent respectively the cosine-squared fit and the sine-squared fit.

in both sidebands. Consequently, to obtain secret bits in a 50 km fiber, the average number of photons per pulse launched by Alice should be smaller than that used in our experiment.

5 Conclusion

In summary, we have reported a new experimental configuration that allows the BB84 protocol to be employed and thereby addresses principal concerns about security and the use of modulation sidebands in quantum cryptography. We believe that the many potential advantages of SSB detection scheme and of the use of integrated optics technology make the method described a very promising alternative to other schemes. Experimentally, we have demonstrated a compact system based on single-photon interference in sidebands of modulation of light. Such a scheme provides high mechanical stability against environmental perturbations and can be made polarization-independent by use of a polarization-independent- modulator at the receiver. Current work deals with practical implementation of a quantum key distribution with full synchronization between the transmitter and receiver. It should be note finally that maintaining the bias is easily achieved by using readily available devices such as integrated x-cut Mach-Zehnder modulator.

We acknowledge the financial support of France Telecom (contract n°991B489).

References

1. C.H. Bennett, G. Brassard, *Proceeding of IEEE international Conference on computers, System and Signal Processing* (IEEE, New-York, 1984), p. 175.
2. C.H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
3. S.J.D. Phoenix, S.M. Barnett, A. Chefles, J. Mod. Opt. **47**, 507 (2000).
4. A.K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
5. J. Breguet, A. Muller, N. Gisin, J. Mod. Opt. **41**, 2405 (1994).
6. J.G. Rarity, P.M. Gorman, P.R. Tapster, Electron. Lett. **37**, 512 (2001).
7. P.D. Townsend, J.G. Rarity, P.R. Tapster, Electron. Lett. **29**, 634 (1993).
8. Ch. Marand, P.D. Townsend, Opt. Lett. **20**, 1695 (1995).
9. R.J. Hughes, G.L. Morgan, C.G. Peterson, J. Mod. Opt. **47**, 533 (2000).
10. M. Bourennane, D. Ljunggren, A. Karlsson, P. Jonsson, A. Hening, J.P. Ciscar, J. Mod. Opt. **47**, 563 (2000).
11. B.S. Shi, G.-C. Guo, J. Mod. Opt. **46**, 1011 (1999).
12. Y. Mazurenko, J.M. Merolla, J.P. Goedgebuer, Opt. Spectro. **86**, 145 (1999).
13. J.M. Merolla, Y. Mazurenko, J.P. Goedgebuer, W.T. Rhodes, Phys. Rev. Lett. **82**, 1656 (1999); Phys. Rev. A **63**, 1899 (1999).
14. T. Durt, Phys. Rev. Lett. **83**, 2476 (1999).
15. B.A. Slutsky, R. Rao, P.C. Sun, Y. Fainman, Phys. Rev. A **57**, 2383 (1998).
16. J.I. Cirac, N. Gisin, Phys. Lett. A **229**, 1 (1997).
17. N. Lutkenhaus, Phys. Rev. A **61**, 052304 (2000).
18. H. Inamori, N. Lutkenhaus, D. Mayers, `quant-ph/0107017` (2001).
19. B. Huttner, N. Imoto, N. Gisin, T. Mor, Phys. Rev. A **51**, 1863 (1995).
20. S. Cova, M. Ghioni, A. Lacaita, C. Samori, F. Zappa, Appl. Opt. **35**, 1956 (1996); D. Stucki, G. Ribordy, A. Stephanov, H. Zbinden, J. G. Rarity, T. Wall, J. Mod. Opt. **48**, 1967 (2001).