Quantum cryptographic device using single-photon phase modulation

Jean-Marc Mérolla,[1] Yuri Mazurenko,[1] Jean-Pierre Goedgebuer,[2] Laurent Duraffourg,[1] Henri Porte,[2] and William T. Rhodes[1]
[1]*GTL-CNRS Telecom, UMR CNRS 6603, Georgia Tech Lorraine, 2-3 rue Marconi, 57070 Metz, France*
[2]*Laboratoire d'Optique P. M. Duffieux, UMR 6603, Université de Franche-Comté, 25030 Besançon Cedex, France*
(Received 26 October 1998)

We report a particular implementation of a quantum cryptographic device operating at 1540-nm wavelength and involving interference between phase-modulated sidebands produced by a pair of phase modulators in the transmitting and receiving modules. The principle of operation is described in terms of both classical and quantum optics. The method has been demonstrated experimentally using a strongly attenuated semiconductor laser diode. Single photon interference has been obtained with a fringe visibility greater than 90%, indicating that the system can be used for quantum key distribution. [S1050-2947(99)06608-1]

PACS number(s): 03.67.Hk, 03.67.Dd, 42.79.−e

I. INTRODUCTION

The objective of quantum key distribution is to exploit fundamental properties of quantum optics in order to share in secret a random bit sequence—the key—between two users, Alice and Bob. Once the sharing is carried out, the two parties can exchange a message over a public channel by encrypting with the key a message of equal length. If the key is used only once, the message cannot be deciphered by an eavesdropper, Eve, who does not possess the key [1]. The problem of this one-time-pad method is that the key must be transmitted without any possibility of interception. If the key distribution is effected by nonsecure transmission lines, the key can be detected by an eavesdropper without the knowledge of the legitimate users.

One of the most unexpected developments in quantum optics has been the demonstration of cryptographic key distribution schemes where security is guaranteed by fundamental laws of quantum mechanics [2,3] instead of by mathematical algorithms as in classical cryptographic methods. In quantum key distribution, the key is sent over a quantum channel. If Eve taps the line, transmission errors occur due to the quantum-mechanical nature of photons. To detect these errors, the legitimate users verify statistically a set of shared bits. If too many errors are detected in the verification process, the users discard those bits.

Such a polarization encoding method has been demonstrated in a free-space transmission in anticipation of potential applications to satellite secure communications, and in a transmission on standard optical fibers [4,5]. One of the most spectacular results in terms of systems was the demonstration performed over a 22-km-long fiber submerged in Lake Geneva [6]. Unfortunately, fiber transmission inevitably leads to problems associated with polarization preservation if standard single-mode fibers are used. Thus, in recent years, another quantum-optic method has seen increased interest. In this second method, photons with delay-coded states are used. Encoding and decoding of the bit information are implemented through optical delays introduced by a pair of fiber interferometers characterized by large optical path-length differences (typically 1 m) set in the emitter (Alice) and the receiver (Bob). The receiver can then recognize every bit sent by the sender if the pair of interferometers is closely matched in path length one to each other. However, the existence of a noninterfering signal, decreasing the maximum visibility interference of 50%, requires the use of time-gated detection and polarization division to achieve high visibility (0.99) [7]. Moreover, the interferometers must remain stable in the presence of environmental perturbations, i.e., the path-length differences in the interferometers must be held constant. Feedback loops driving piezoelectric fiber stretchers set in the interferometers have been used to compensate mechanical vibrations and thermal drift. However, despite active compensation, transmissions have been reported to be limited to some few seconds (5 sec for a slow thermal drift that occurs at a rate of 0.6 rad/min), sufficient only to demonstrate the possibility of key distribution over 30 km of standard fiber [7]. An elegant method using Faraday mirrors has been proposed to overcome the effects of polarization fluctuations in the transmission line [8]. Other approaches, based on wavelength or frequency coding, have also been proposed recently [9,10].

We describe here a system that uses single photons with phase-encoded states and operating with a nonorthogonal two-state scheme. Phase-encoded states are produced by an integrated electro-optic phase modulator set in the transmitter, which uses an attenuated semiconductor laser to produce a sequence of countable photons. Since to the best of our knowledge the method is new in the area of optical cryptography, we begin by explaining the principle of operation in a combination of classical and quantum terms. We introduce an appropriate version of a two-state protocol [3] and relate this to the ability to distribute a key in a secure fashion. We also report experimental results obtained at 1540-nm wavelength that show some interesting features of the method, especially its great simplicity.

II. PRINCIPLE OF OPERATION

In the transmission system shown in Fig. 1, the transmitter (Alice) consists of an integrated electro-optic phase modulator PM_1 powered by a single-frequency semiconductor laser operating at angular frequency ω_0, referred to subsequently as the reference frequency. The laser output is strongly attenuated by a variable fiber attenuator (this point is discussed in greater detail later, since the attenuation re-

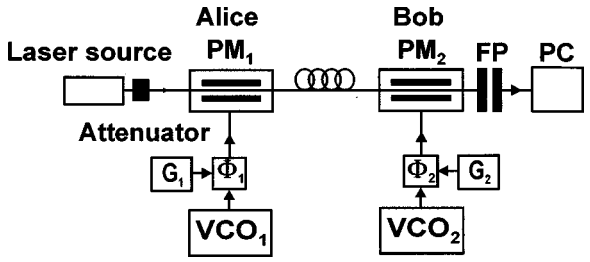

FIG. 1. Schematic diagram of the phase-modulation transmission system.

quired differs from that of previously reported methods). The reference laser beam is phase-modulated by PM_1, which is driven by a voltage-controlled oscillator VCO_1 operating at a fixed frequency Ω but with a phase Φ_1 that can be changed randomly between two states, namely 0 and π for bit ''0'' and ''1,'' respectively. These two phase states determine the basis used by Alice. A random bit generator G_1 is used by Alice to drive the phase of VCO_1. At the output of Alice's modulator, light is phase-modulated, and sideband frequencies $\omega_0+\Omega$ and $\Omega_0-\Omega$ are induced in the spectrum of light. The phase of those sideband frequencies is Φ_1. The receiver (Bob) consists of a second phase modulator PM_2 driven by a sine voltage provided by a voltage controlled oscillator VCO_2 operating at the same frequency Ω. A random bit generator G_2 switches the phase Φ_2 of that sinusoidal signal randomly between two values 0 and π. These values will be used by Bob to recognize the bits sent by Alice, as will be explained in Sec. III. When phase modulating the light, Bob also generates sidebands in the spectrum, including two with frequencies $\omega_0+\Omega$ and $\omega_0-\Omega$ with phase Φ_2. Depending on the value of Φ_2 relative to Φ_1, constructive or destructive interference can occur between the sidebands generated by Alice and Bob. To analyze such interference, Bob's receiver contains a Fabry-Pérot interferometer FP and a photon counter PC. The FP operates as a spectral filter with its transmission peak adjusted at one side frequency, e.g., $\omega_0+\Omega$. Let us now assume that Alice has sent single photons in a state Φ_1 in the sideband frequency $\omega_0+\Omega$ selected by the FP. The probability that Bob detects the photon at the FP output depends on the value he chooses for Φ_2. Assuming the transmission and the detection are ideal, i.e., lossless and error-free, the probability is 0% as $|\Phi_2-\Phi_1|=\pi$ (Alice's and Bob's modulations out of phase), and 100% as $|\Phi_2-\Phi_1|=0$ (modulations in quadrature). As Bob detects a photon with his phase set on 0 and π, he reads bit ''0'' and bit ''1,'' respectively. The working conditions yielding such specific properties of the 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 $E=E_0\exp(j\omega_0 t)$ be the light field associated with angular frequency ω_0 emitted by the laser diode and injected in Alice's modulator. The light obtained at the modulator output can be expressed as

$$E_1(t)=E_0\exp j[\omega_0 t+m_1\sin(\Omega_1 t+\Phi_1)], \tag{1}$$

where $\phi_1(t)=m_1\sin(\Omega_t t+\Phi_t)$ is the phase modulation introduced by Alice's modulator, and m_1, Ω_1, and Φ_1 its amplitude (also termed *modulation depth* in the following), angular frequency, and phase, respectively. This light field is sent to Bob's phase modulator, yielding a light field expressed as

$$E_2(t)=E_1(t)\exp j[m_2\sin(\Omega_2 t+\Phi_2)], \tag{2}$$

where $\phi_2(t)=m_2\sin(\Omega_2 t+\Phi_2)$ is the phase modulation produced by Bob's modulator, with m_2, Ω_2, and Φ_2 its amplitude, angular frequency, and phase, respectively. Setting $\Omega_1=\Omega_2=\Omega$ and $m_1=m_2=m$, we obtain

$$E_2(t)=E_0\exp j[\omega_0 t+A\sin\{\Omega t+(\Phi_1+\Phi_2)/2\}], \tag{3}$$

with $A=2m\cos\{(\Phi_2-\Phi_1)/2\}$. Finally, the light field at the spectral filter output is the spectrum in amplitude of $E_2(t)$. It can be calculated by expressing Eq. (3) as a series of Bessel functions. Recalling that

$$\exp(jA\sin\theta)=\sum_{n=-\infty}^{\infty}J_n(A)\exp(jn\theta)\quad\text{and}$$

$$J_n(-A)=(-1)^n J_n(A),$$

where J_n is the nth-order Bessel function, Eq. (3) can also be written as

$$E_2(t)=\sum_{n=-\infty}^{\infty}J_n[2m\cos\{(\Phi_2-\Phi_1)/2\}]E_0\times\exp j[(\omega_0+n\Omega)t+n(\Phi_1+\Phi_2)/2\}]. \tag{4}$$

Assuming the modulation depth m is much smaller than 1 rad, the expression for $E_2(t)$ can be approximated as

$$\begin{aligned}E_2(t)\approx{}&J_0\{2m\cos[(\Phi_2-\Phi_1)/2]\}E_0\exp j(\omega_0 t)\\&-J_1\{2m\cos[(\Phi_2-\Phi_1)/2]\}E_0\exp j[(\omega_0-\Omega)t\\&-(\Phi_1+\Phi_2)/2]+J_1\{2m\cos[(\Phi_2-\Phi_1)/2]\}E_0\\&\times\exp j[(\omega_0+\Omega)t+(\Phi_1+\Phi_2)/2].\end{aligned} \tag{5}$$

The light field $E_2(t)$ at the output of Bob's modulator is formed by a center spectral component at frequency ω_0 and two side components at $\omega_0+\Omega$ and $\omega_0-\Omega$. The Fabry-Pérot selects the $\omega_0+\Omega$ frequency. Assuming again that the modulation depth is small ($m\ll 1$), the intensity in the center band is E_0^2 while Bob detects at his Fabry-Pérot output an intensity expressed as

$$\begin{aligned}i&=E_0^2J_1^2\{2m\cos[(\Phi_2-\Phi_1)/2]\}\\&\approx 4m^2E_0^2\cos^2[(\Phi_2-\Phi_1)/2].\end{aligned} \tag{6}$$

This intensity is maximum if $|\Phi_2-\Phi_1|=0$ and minimum if $|\Phi_2-\Phi_1|=\pi$. Note that the intensity of the center frequency component can be considered to be constant, since the modulation depth is negligibly small ($J_0\{2m\cos[(\Phi_2-\Phi_1)/2]\}\approx 1$ for $m\ll 1$). This system is formally equivalent to a system providing constructive or destructive interference between the phase-modulated sidebands generated by Alice and Bob. One of the advantages is that no optical interferometric scheme is required.

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 at time t is proportional to $P_D = {}_D\langle\Psi|E^-(t)E^+(t)|\Psi\rangle_D$, with

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

$$E^-(t) = -j\sum_\omega \xi(\omega) a_\omega^+ \exp(j\omega t), \tag{8}$$

$$\xi(\omega) = \left(\frac{\hbar\omega}{2\epsilon_0(2\pi)^3}\right)^{1/2}, \tag{9}$$

where ϵ_0 is dielectric permittivity of vacuum, a_ω and a_ω^+ are the annihilation and creation operators, and $|\Psi\rangle_D$ is the coherent state describing the field incident on the detector. Initially, the quantum field emitted by the source is $|\Psi\rangle = |\alpha_{\omega_0}\rangle|0\rangle|0\rangle$ where two zero excitations are related to the two sidebands. At Alice's modulator output, the coherent state describing the quantum field can be deduced from Eq. (2) and by considering that the modulation depth m is sufficiently small to obtain an average photon number in the sidebands much smaller than 1. The coherent state at Alice's modulator output can then be written as a superposition of coherent states:

$$|\Psi\rangle_2 = |\alpha_{\omega_0}\rangle|\exp(-j\Phi_1)\alpha_{\omega_0-\Omega}\rangle|\exp(j\Phi_1)\alpha_{\omega_0+\Omega}\rangle. \tag{10}$$

Bob performs the same operation as Alice but introduces a phase Φ_2. Similarly, the state describing the quantum field at his modulator output is given by

$$|\Psi\rangle_3 = |\alpha_{\omega_0}\rangle|[\exp(-j\Phi_1)+\exp(-j\Phi_2)]\alpha_{\omega_0-\Omega}\rangle \times|[\exp(j\Phi_1)+\exp(j\Phi_2)]\alpha_{\omega_0+\Omega}\rangle. \tag{11}$$

After spectral filtering, the state detected by the single photon detector is

$$|\Psi\rangle_D = |0\rangle|0\rangle|[\exp(j\Phi_1)+\exp(j\Phi_2)]\alpha_{\omega_0+\Omega}\rangle, \tag{12}$$

and the probability of photocount is proportional to

$$P_d = \langle\alpha_{\omega_0+\Omega}|(e^{-j\phi_1}+e^{-j\phi_2}) \times(e^{j\phi_1}+e^{j\phi_2})\sum_\omega \xi(\omega)a_\omega^+ e^{j\omega t} \times\sum_{\omega'} \xi(\omega')a_{\omega'}e^{-j\omega' t}|\alpha_{\omega_0+\Omega}\rangle. \tag{13}$$

Recalling that $a_\omega|\alpha_{\omega'}\rangle = \alpha_\omega\delta_{\omega\omega'}$, we finally obtain

$$P_d = 4\xi(\omega)^2\cos^2[(\Phi_2-\Phi_1)/2]\langle n_{\omega_0+\Omega}\rangle = \rho\cos^2[(\Phi_2-\Phi_1)/2], \tag{14}$$

TABLE I. Protocol for secret key transmission in the absence of an eavesdropper.

Bit sent by Alice	''0''		''1''	
Phase used by Alice	0		π	
Phase used by Bob	π	0	π	0
Photon detected by Bob	no	yes	yes	no
Bit received by Bob	?	0	1	?
Detection announced by Bob	no	yes	yes	no
Common bits shared		''0''	''1''	
Probability for photon detection	0	$\rho/4$	$\rho/4$	0

where $\langle n_{\omega_0+\Omega}\rangle = \langle\alpha_{\omega_0+\Omega}|a^+_{\omega_0+\Omega}a_{\omega_0+\Omega}|\alpha_{\omega_0+\Omega}\rangle$ is the average photon number at the detector in the sideband frequency $\omega_0+\Omega$, and ρ represents the probability of photocount per pulse, including the quantum efficiency of the detector. Equation (14) is formally equivalent to Eq. (6). Physically, Eq. (14) may be regarded as single photon interference that occurs at the FP output between the quantum fields of the side frequency $\omega_0+\Omega$ initiated by Alice and Bob. The probability of detecting a photon at the Fabry-Pérot output is 0 for $|\Phi_2-\Phi_1| = \pi$, $\rho/2$ for $|\Phi_2-\Phi_1| = \pi/2$, and ρ for $|\Phi_2-\Phi_1| = 0$. We show now how this property can be used to share a key.

III. PROTOCOL USED FOR QUANTUM KEY DISTRIBUTION

The protocol used is derived from the two-state scheme proposed by Bennett [3]. We shall describe the protocol in terms of the phase-encoded (these states should not be confused with the phase operator states of quantum optics) discussed in the preceding section. The nonorthogonal states used by Alice are formed by two states that differ by π, such as $\Phi_1 = 0$ for bit ''0'' and π for bit ''1.'' Bob makes a measurement of each state he receives by using two phases that differ by π relative to those used by Alice, such as $\Phi_2 = \pi$ (then the bit read by Bob is ''1'' as a photon is detected) and 0 (bit ''0''). The protocol can be described as follows.

(i) For each transmitted photon, Alice randomly chooses the state of transmission to be one of the two-phase states, namely 0 and π for bit ''0'' and bit ''1,'' respectively. Every photon permits the transmission of a bit of information.

(ii) Bob randomly and independently chooses his measurement state (0 or π) for each incoming photon.

(iii) Bob then tells Alice, possibly over a public channel, the results of his measurements (photon detected or not), but not the phase that he used.

(iv) Alice and Bob agree to discard all the bits for which no photon was detected. 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 four steps are summarized in Table I. For instance, when Alice sends bit ''0,'' the probability for Bob to detect a photocount is $\rho/4$, meaning that the probability to have the right bit ''0'' is also $\rho/4$.

If Eve is tapping the channel, because Eve cannot know which phases Alice and Bob will choose, there will, with certainty approaching unity, be times when Eve's choice re-

TABLE II. Transmission in the presence of an eavesdropper. The phase used by Eve for detecting the bit sent by Alice is either 0 or π. The phase used by Eve for resending the photon on to Bob is 0 or π.

Phase used by Alice	0		π		0		π	
Phase used by Eve for detection	0		π		π		0	
Probability for photon detection by Eve	$\rho/4$		$\rho/4$		0		0	
Phase detected by Eve	0		π		?			
Phase used by Eve for resending the photon on to Bob	0		π		0		π	
Probability for this event	$\rho/4$		$\rho/4$		$1/2-\rho/4$		$1/2-\rho/4$	
Phase used by Bob for detection	0	π	0	π	0	π	0	π
Detection announced by Bob	yes	no	no	yes	yes	no	yes	no
Probability for photon detection by Bob	$\rho^2/8$	0	0	$\rho^2/8$	$\rho/4-\rho^2/8$	0	0	$\rho/4-\rho^2/8$

sults 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 infer her presence. A thorough eavesdropping analysis is very lengthy and so we shall restrict ourselves to some illustrative examples. We assume Eve has the same equipment as Bob to perform the measurements on the photons sent by Alice and that she can resend the photons on to Bob after her measurements. Since she has no *a priori* knowledge of Alice's phase states, her possible strategies are as follows.

(i) She can decide to resend the reference light field only, i.e., the center frequency ω_0, hoping Bob will detect no error. In that case, Bob's phase modulator will generate inevitably a photon in the sideband frequency with a unit probability even if Alice and Bob's modulators are out of phase. Then the photon-counting statistics are modified and Eve's presence is revealed directly.

(ii) She can decide to suppress the reference light field. In that case, Bob does not detect it with a classical detector.

(iii) If Eve uses the same coupled phases as Bob for detecting the photons sent by Alice, there is a probability that she resends the photons on to Bob with incorrect phases, as shown in Table II. This scheme also results in a modification of the error statistics calculated by Bob and Alice. For instance, when Alice sends bit ''0,'' the probability for Bob to detect a photocount when his phase is 0 is $\rho^2/8+\rho/4-\rho^2/8=\rho/4$ (see Table II). This probability is the same as that when the line is not tapped. However, if Bob calculates the probability of having photocounts when his phase differs from that of Alice, he finds $\rho/4-\rho^2/8+\rho/4-\rho^2/8+=\rho/2-\rho^2/4$, a value which is different from that found (0) in the absence of an eavesdropper. Such a modification of the statistics allows Alice and Bob to infer Eve's presence. A complete discussion in the general case of a nonorthogonal two-state protocol with single and coherent states is given in [11–14].

IV. EXPERIMENTAL RESULTS

Working with the system illustrated in Fig. 2, we checked the validity of the modulation scheme and of the working conditions yielding single photon interference. The source was a cw distributed feedback (DFB) laser diode from Alcatel operating at 1540-nm wavelength with a linewidth of 1 MHz and a power of -10 dBm. The temperature-induced wavelength drift was stabilized to about 15 MHz, which was of the same order of the spectral resolution of the Fabry-Pérot used. We inserted a fiber variable attenuator to adjust the power of the source launched in the input modulator. Modulators PM_1 and PM_2 were pigtailed $LiNbO_3$ integrated phase modulators. Their half-wave voltage and electrical bandwidth were 5 V and 500 MHz, respectively. Their insertion loss was 4 dB. The frequency of modulation was chosen to be 300 MHz. A high-frequency (HF) generator (1-GHz bandwidth) was used to drive the modulators (only one HF generator was available when we performed the experiment). The electrical signal of the HF generator was first attenuated independently for each modulator, using two 1-dB-increment variable electric attenuators A_1 and A_2, then amplified using two 30-dB gain amplifiers AM_1 and AM_2. This procedure allowed us to obtain nondistorted electrical modulation signals with variable amplitude that could be controlled easily and accurately. In the electrical circuit of one of the modulators, we inserted a phase shifter to introduce a variable phase difference $\Delta\Phi=\Phi_2-\Phi_1$ between the driving voltages applied to PM_1 and PM_2. The electrical bandwidth of the

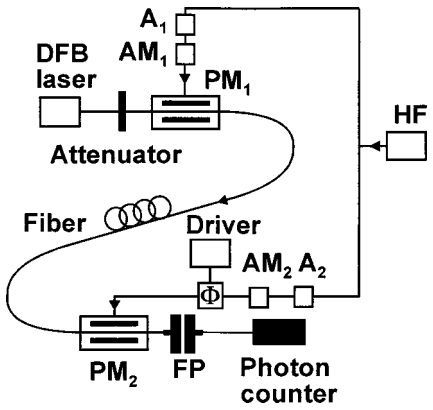

FIG. 2. Experimental setup.

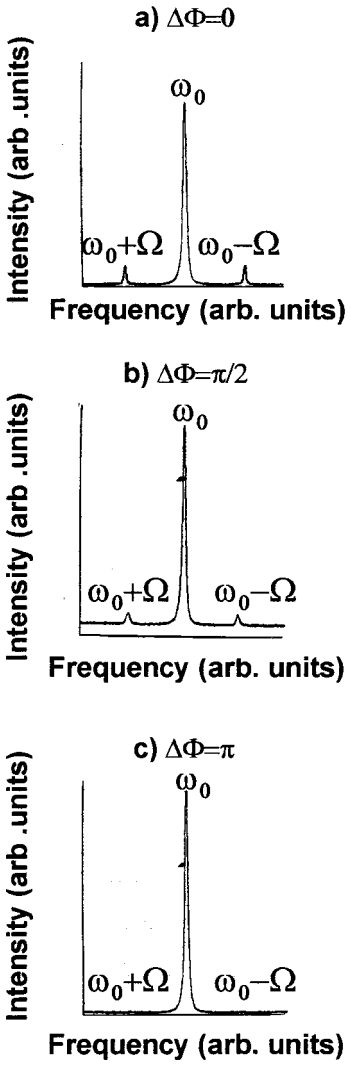

FIG. 3. Experimental power spectra obtained with a scanning Fabry-Pérot, for phase shifts $\Delta\Phi$. The sidebands $\omega_0+\Omega$ and $\omega_0-\Omega$ are spaced by 300 MHz from the reference frequency ω_0.

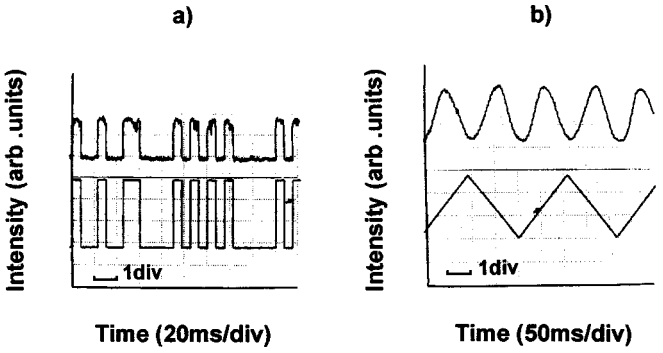

FIG. 4. Oscilloscope displays of the intensity detected in the sideband frequency vs time. In (a), $\Delta\Phi$ is randomly switched between 0 and π. In (b), $\Delta\Phi$ is linearly modulated between 0 and 2π.

driver of the phase shifter was 10 kHz. The Fabry-Pérot interferometer was operated as a scanning FP, i.e., as a spectrum analyzer, with an 800-MHz scanning range. It could also be operated as a FP with a fixed mirror spacing, i.e., as a spectral filter. Its free spectral range and its spectral resolution were 1 GHz and 18 MHz, respectively, yielding a finesse of 55.

First, we tested the system operating in the *classical regime*. The source was not attenuated. The detector used at the FP output was a standard photodiode. The power loss of the transmission system including the two modulators, a 20-km-long fiber (0.18 dB/km), and the FP was 15 dB. We did not try to optimize 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 $a = V_\pi/5 = 1$ V, yielding a modulation depth $m = a\pi/V_\pi = 0.3$ rad. Figure 3(a) shows the intensity thus detected at the system output for $\Delta\Phi = 0$, with the FP operating in the scanning mode. We observe clearly the two side frequencies, each spaced by 300 MHz 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 m^2, as predicted in Eq. (6). Figures 3(b) and 3(c) illustrate other cases for $\Delta\Phi = \pi/2$ and π. Constructive and destructive interference can be seen distinctly as the modulators are in phase and out of phase, respectively. Figure 4 was obtained without scanning the FP, with its mirrors spaced to select the side frequency $\omega_0+\Omega$. The value of $\Delta\Phi$ was then modulated. In Fig. 4(a), $\Delta\Phi$ is switched randomly between 0 and π with 10-ms-duration pulses (bottom trace) to simulate the phase states used in the cryptographic protocol. The intensity thus detected at the FP output is shown in the top trace. Figure 4(b) shows another example obtained by varying $\Delta\Phi$ linearly between 0 and 2π (bottom trace). The intensity detected in the side band (top trace) varies sinusoidally, in accord with the cosine-squared term of Eq. (6). We measured a visibility of 93%. This value is to be compared with the theoretical visibility, which was calculated to be 98%. The latter value is determined by the intensity of the center peak, its spacing from the side frequency, and the finesse of the FP. The discrepancy is probably due to a slight misalignment of the mirrors of the FP, resulting in a finesse lower than the specified one. We note that using a FP with a higher finesse can increase the visibility. For instance, a finesse of 100 would insure a fringe visibility higher than 99%. A second point is that the intensity at the center frequency varies slightly ($\approx$20%) with changes in the value of $\Delta\Phi$, as can be seen in Fig. 3. Such a dependence arises when the modulation depth is not sufficiently small. Such a condition would yield a detectable intensity modulation that could be used directly by an eavesdropper.

In the *quantum regime*, the situation will be different. The intensity in the side frequency will be chosen such that the probability of detecting one photon is small (typically less than 1%). This yields an average photon number per pulse of about 0.1 in the side frequency. Consequently, for the modulation depth $m = 0.3$ chosen, there will be ten times more photons in the center frequency. The source being Poissonian, the variance of the photon number in the center peak is given by the average photon number, namely 1. This value is

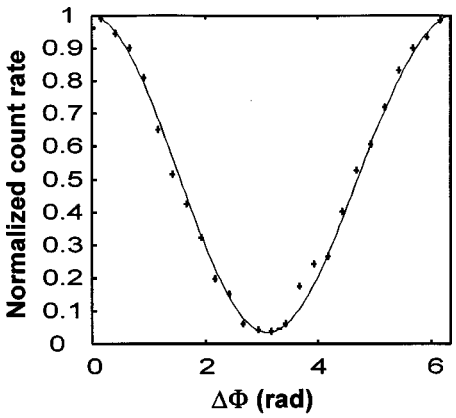

FIG. 5. Normalized single-photon count rate as a function of phase difference $\Delta\Phi$.

large compared with the intensity variation, which is 0.2, at the reference frequency component resulting from Alice's phase modulation. Hence, this intensity variation will be masked by the photon noise of the reference frequency and will not be detected by any intruder. It is then recommended to use a non-single-photon source and a very low modulation depth, instead of a single-photon source and a high modulation depth. Note that a very low modulation depth will also allow us to operate the modulators with very low driving voltages, making transmission in telecommunications systems at high bit rates easier.

Experiments in the quantum regime were performed by replacing the standard photodetector by a passively quenched germanium avalanche photodiode (APD) cooled to 77 K and operating with a photon counter in the Geiger mode. (Details of the APD characteristic will be described in another article devoted to photon counting at 1540-nm wavelength.) The DFB laser diode was modulated externally using an integrated intensity modulator to produce 50-ns-duration pulses at a repetition rate of 1 MHz. The pulses thus obtained were suitable for the photon counter we used. Note that the principle of operation described in Sec. II for a monochromatic source holds in the pulse regime, the phase difference $\Phi_2 - \Phi_1$ in Eqs. (6) and (14) being wavelength-independent. The mirror spacing of the FP was adjusted to obtain a spectral resolution of 36 MHz, a value that insures a 94% theoretical visibility. The carrier frequency Ω was 300 MHz. The DFB laser diode was attenuated to -80 dBm so that the average photon number μ of a side mode entering the transmission fiber was 0.1/pulse. The time response of the APD was 10 ns. The system was tested by measuring the visibility of the single-photon interference that occurs in the side frequency at the FP output. The visibility was measured varying $\Delta\Phi$ continuously between 0 and 2π rad with steps of 0.25 rad, and counting the photon number at the FP output. The photon counter was triggered with the initial light pulses and the duration of counting was set to be 50 ns. For each value of $\Delta\Phi$, measurement of the photon number was performed for 10^7 triggering pulses. For instance, with the modulators set in phase ($\Delta\Phi = 0$), we obtained an average number of 2500 counts, a value that corresponds approximately to 0.13 photon/pulse. Figure 5 shows the normalized average number of counts versus $\Delta\Phi$ thus obtained. The visibility calculated by subtracting dark counts is about 91%. Such a visibility corresponds to a quantum bit error rate (QBER) of 4%.

We note that the count rate, which was 250 counts/s, can be increased by using a higher modulation frequency, thereby allowing an increase in transmission rate. We did not try to optimize this parameter in these preliminary experiments.

V. CONCLUSION

In summary, we have reported a quantum cryptographic scheme involving single photon interference between phase-modulated sidebands produced by a pair of phase modulators in the transmitting and receiving modules. We conclude with some comments concerning the estimated performance and potential advantages of the scheme as compared with interferometer-based implementations.

(i) Polarization-independent behavior can be expected if the integrated $LiNbO_3$ phase modulators are replaced by intensity-modulating Mach-Zehnder interferometers [15]. When the input polarization fluctuates, the phase difference thus induced between the TE and TM modes in such modulators is shown to be small ($\approx \pi/30$). The resulting variation of the visibility of the single photon interference that occurs in the side frequency at the Fabry-Pérot output is negligibly small ($<0.5\%$), meaning that QBER is expected to be constant if the polarization fluctuates in the transmitting fiber.

(ii) Because the modulators are quite compact, high stability against environmental thermal drifts can be obtained, as compared with that provided by a fiber Mach-Zehnder. The temperature of integrated modulators can be easily controlled to within 10^{-2} degrees. The corresponding variation in fringe visibility is smaller than 0.5% and does not alter the QBER significantly.

(iii) Since the physical principle of the scheme relies essentially on interference in the frequency domain, the most serious problems that may arise come from the possible instability of the wavelength emitted by the source, and of the frequency of the electrical signals produced by the VCO's, either of which can degrade system performance. As an example, if we use the same criterion as above (variation in fringe visibility $<0.5\%$), calculations predict that a system operating with VCO's with a 5 GHz modulation frequency, and with a Fabry-Pérot with a finesse and a free spectral range of 100 and 100 MHz, respectively, requires the laser and the VCO frequency to be stabilized to within 10 and 5 MHz, respectively. Finally, it appears that the needed highly stabilized path-length differences in interferometer-based architectures translate in the proposed scheme into requirements for highly stabilized electronics devices.

(iv) The secret key is obtained by sacrificing some bits from raw data shared by Alice and Bob to improve security. The net secure throughput level of a two-state protocol is known to be smaller than with a four-state protocol [14]. We are investigating an improved version of the system to overcome this drawback.

ACKNOWLEDGMENT

We thank France Telecom for financial support.

[1] G. S. Vernam, J. Am. Inst. Electr. Eng. **XLV**, 109 (1926).
[2] C. H. Bennet and G. Brassard, *Proceedings of IEEE International Conference on Computers, Systems and Signal Proceeding* (IEEE, New York, 1984), p. 175.
[3] C. H. Bennet, Phys. Rev. Lett. **68**, 3121 (1992).
[4] B. C. Jacobs and J. D. Franson, Opt. Lett. **21**, 1854 (1996).
[5] J. D. Franson and H. Ilves, Appl. Opt. **33**, 2949 (1994).
[6] A. Muller, H. Zbinden, and N. Gisin, Europhys. Lett. **33**, 335 (1995).
[7] C. Marand and P. D. Townsend, Opt. Lett. **20**, 1695 (1995).
[8] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, Europhys. Lett. **33**, 586 (1997).
[9] P. C. Sun, Y. Mazurenko, and Y. Fainman, Opt. Lett. **20**, 1062 (1995).
[10] D. N. Klyshko, Phys. Lett. A **227**, 1 (1997).
[11] A. K. Ekert, B. Huttner, G. M. Palma, and A. Peres, Phys. Rev. A **50**, 1047 (1994).
[12] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A **51**, 1863 (1995).
[13] S. J. D. Phoenix and P. D. Townsend, Contemp. Phys. **36**, 165 (1995).
[14] B. Slutsky, R. Rao, P. C. Sun, and S. Fainman, Phys. Rev. A **57**, 2383 (1998).
[15] T. Ishikawa, Electron Lett. **28**, 566 (1992); C. C. Chen, H. Porte, A. Carenco, J. P. Goedgebuer, and V. Armbruster, IEEE Photonics Technol. Lett. **9**, 1361 (1997).