Single-Photon Interference in Sidebands of Phase-Modulated Light for Quantum Cryptography

Jean-Marc Mérolla, Yuri Mazurenko,* Jean-Pierre Goedgebuer, and William T. Rhodes

GTL-CNRS Telecom, UMR CNRS 6603, Georgia Tech Lorraine, 2-3 rue Marconi, 57070 Metz, France
and Laboratoire d'Optique P.M. Duffieux, UMR CNRS 6603, Université de Franche-Comté, 25030 Besançon Cedex, France
(Received 15 September 1998)

We report single-photon interference in the sidebands of modulated light. The relative phase of interacting quantum states is reliably controlled by the phase of a low-frequency modulating signal. We show how this type of interference can be used to build a robust system for quantum cryptography. An experiment was implemented at 1540 nm, over a 20-km-long standard single-mode fiber, using a germanium singlephoton avalanche photodiode. [S0031-9007(99)08483-5]

PACS numbers: 03.67.Dd, 42.50.Ar, 42.79.–e

Claude Shannon is often viewed as beginning the development of cryptography as a science when, applying information theory, he demonstrated the possibility of achieving absolute confidentiality [1] with the "one-time pad" cryptographic method [2]. In that method, a signal is encrypted using a random key that has a length equal to that of the message. If such a key is used one time only, the signal is impossible to decipher without the key. The problem with this encryption method is that it is necessary to distribute the key between the transmitter (Alice) and the receiver (Bob) with complete confidentiality. This is one reason why public-key encryption methods have been developed during the past 20 years. Public-key methods rely on complexity for their security, effectively on the extremely large calculation time required to break the code. In principle, messages encrypted by public-key methods can be decrypted, and constantly increasing computing speed presents a potential threat.

Quantum cryptography offers the unique possibility of certifiably secure key distribution between transmitter and receiver by exploiting the laws of quantum mechanics combined with, in most cases, the so-called conjugate coding method defined by Wiesner [3] (a nonconjugate coding scheme is discussed in [4]). The key is sent over a quantum channel in order to benefit from the fundamental principles of quantum measurement [5]. The essential quantum property at the heart of this method is the existence of pairs of conjugate states that are chosen in such a way that if the wrong choice of measurement basis is made, the bit of information carried by a photon is necessarily randomized. Alice and Bob exploit this property to share a secret key by using such quantum states. If an eavesdropper (Eve) tries to intercept the photons emitted by Alice and resends them on to Bob after their measurement, she inevitably introduces transmission errors that can be detected through the changes in the statistics of the photons Bob ultimately receives. The key transmission is controlled by a protocol, which can be associated with a two-state or a four-state scheme [6], or with a more complicated scheme [7]. The use of orthogonal states was also discussed [8].

Two types of methods have been reported so far for preparing photons in the required quantum states. In the pioneering work of Bennett *et al.* [9], the sender uses *polarized photons* for which the linear and circular polarization states form a pair of conjugate bases that are used to represent bits "0" and "1". Decoding at the receiver is then carried out independently for each bit, using another basis with two of the polarization states used at the emission. The occurrence of a detectable photon then indicates the value of the bit. Since the first demonstration of the method in free space over a distance of 30 cm [9], progress toward transmission over 20 km of single-mode fiber [10] and over 1 km in free space [11] has been rapid. The method was also demonstrated for potential application to satellite communications [12]. The second method, due to Townsend *et al.* [13], is to use *optical delays* that encode each bit of information. In this case, the sender uses an interferometer with a large path imbalance (longer than the length of the light pulses, and typically $\approx$1 m). In a four-state scheme reported in [13], each bit is represented randomly by two values of optical delay. At the receiver, decoding is performed independently for each bit, using a second interferometer with two of the optical delays used in the transmitter. Several studies have shown the feasibility of the method for distances exceeding 30 km [14]. The great advantage of the second method is that standard single-mode fibers can be used, without concern for any polarization fluctuations that might be introduced by the transmission channel [15,16]. In another approach to interferometric realization of quantum cryptography, authors of [17] introduced the frequency shift in one of the arms of each interferometer with acousto-optic deflectors. By that means they were able to eliminate the large path imbalance of the interferometers as well as the use of very short light pulses.

In whole, the practical results obtained so far show that quantum cryptography is now much more than simply a theoretical curiosity.

Here we describe a novel method of quantum cryptography in which Alice encodes each bit of information into *sidebands of phase-modulated light.* The phase of the

 0031-9007/99/82(8)/1656(4)$15.00

sidebands is induced electrically, and can be chosen randomly between a set of two values. Bob generates sidebands identical to those used by Alice, with phases that he chooses independently and randomly between the same or (possibly) another set of two values. We show that Bob can retrieve the bits sent by Alice using single-photon interference in sidebands.

Perhaps the most important parameter for a quantum cryptography system is the bit-error rate (BER), since it determines the security of the key transmission. The experimental demonstration, implemented at 1540 nm wavelength using a germanium single-photon avalanche detector (SPAD) cooled to 77 K, indicates that a BER of less than 4% can be obtained.

The basic system is illustrated in Fig. 1, which also depicts our experimental schematic. Source S emits classical monochromatic light with angular frequency ω_0. The emitted beam is intensity modulated by the electro-optic modulator EOM to produce short light pulses. This light beam at frequency ω_0 will be referred to as the reference beam. A phase modulator PM_1 (Alice) modulates the reference beam at angular frequency $\Omega \ll \omega_0$ with a modulation depth m that is chosen to be small. In modulating the reference beam, Alice uses voltage-controlled rf oscillator VCO_1 operating at frequency Ω and with phase Φ_1. She can randomly switch phase Φ_1 between two values, 0 for bit "0" and π for bit "1", using the random bit generator G_1. The light beam thus obtained at the output of Alice's transmitter contains the reference carrier ω_0 and two sidebands $\omega_0 \pm \Omega$ with phase state Φ_1 relative to the reference. Alice adjusts attenuator A such that there is much less than 1 photon/pulse (typically 0.1 photon/pulse) *in these sidebands* at the input of a standard single-mode fiber link, whereas the reference is left classical. At the receiver, the light experiences a second phase modulation with the modulator PM_2 operating also at frequency Ω but with variable phase Φ_2. To do this Bob uses rf oscillator VCO_2, which is synchronized with Alice's oscillator VCO_1. Synchronously with Alice, he drives phase Φ_2 (with the random generator G_2) to choose randomly and independently between measurement phases 0 and π. Consequently, the light leaving Bob's modulator contains the original frequencies emitted by Alice (the reference carrier ω_0 and the two sidebands $\omega_0 \pm \Omega$ with phase Φ_1) and additional sidebands, including two sidebands $\omega_0 \pm \Omega$ with phase Φ_2. Note that the sidebands created by Alice and Bob are mutually coherent. Using an appropriate spectrally selective beam splitter, Bob detects the radiation at the central frequency with a classical detector (not shown in Fig. 1) and the radiation at the sidebands by a single-photon detector. (In our demonstration Bob selects only one sideband with the Fabry-Perot interferometer FP.) The single photons thus detected result from interference of the sidebands with phase Φ_1 initiated by Alice and the sidebands produced by Bob with phase Φ_2. For instance, if $|\Phi_1 - \Phi_2| = \pi$ (sidebands of Alice and Bob are out of phase), there is destructive interference, and the probability for Bob to detect a photon is zero.

Having described how the system works, we now give further details on the process yielding single photon interference. The negative-frequency component of the electric field of the source S before modulation can be represented as $E^-(t) = E_0^- \exp(i\omega_0 t)$. In a semiclassical description, $E^-(t)$ is the classical light field, whereas in the quantum description $E^-(t)$ can be considered to be an operator. Let the optical phase, introduced by Alice or Bob with their rf oscillators, be $\varphi(t) = m\cos(\Omega t + \Phi_{1(2)})$ where m is the modulation depth assumed to be small. Note that $\varphi(t)$ changes very slowly relative to the optical oscillations. The signal obtained by Alice after modulation is

$$E_1^-(t) = E_0^- \exp[i\omega_0 t + im\cos(\Omega t + \Phi_1)] \approx E_0^- \exp(i\omega_0 t) + (im/2)E_0^-\{\exp[i(\omega_0 + \Omega)t + i\Phi_1] + \exp[i(\omega_0 - \Omega)t - i\Phi_1]\} \quad (1)$$

for $m \ll 1$. Two sidebands, with frequencies $\omega_0 \pm \Omega$ and phases $\pm\Phi_1$, are produced. Applying recurrently the formula (1) but with Bob's phase Φ_2, we easily obtain the light field at the output of Bob's modulator:

$$E_2^-(t) \approx E_0^- \exp(i\omega_0 t) + im\cos[(\Phi_1 - \Phi_2)/2]E_0^-\{\exp[i(\omega_0 + \Omega)t + i(\Phi_1 + \Phi_2)/2] + \exp[i(\omega_0 - \Omega)t - i(\Phi_1 + \Phi_2)/2]\}. \quad (2)$$

The cosine factor in (2) is due to the interference of light generated at the sidebands by Alice and Bob. Calculating the resulting photon flux at the sidebands, we easily see that the probability P of photon detection by Bob in the sidebands is

$$P = 4\eta\mu\cos^2[(\Phi_1 - \Phi_2)/2]. \quad (3)$$

Here $\mu \ll 1$ is the average number of photons per pulse in sidebands emitted by Alice device, and $\eta \leq 1$ is the efficiency of the photon detection. If photons are detected in only one of the sidebands, this probability is reduced by a factor of $\frac{1}{2}$.

The protocol for quantum key distribution is analogous to one proposed by Bennett [6] if we identify the central frequency and the sidebands with the strong and dim pulses in his method. Alice announces publicly that she will use the values of phase Φ_1 equal to 0 and π to represent "0" and "1", respectively. Then she introduces these phases in her modulator in a random way. Bob also introduces randomly phases Φ_2 equal to 0 and π and

detects the result of interference. According to Eq. (3) Bob can detect a photon in the sidebands only if $\Phi_1 = \Phi_2$. Therefore when Bob detects a photon he reliably determines the value of the bit sent by Alice. If Alice uses N laser pulses, then, taking into account that the probability of coincidence for Alice's and Bob's phases is $\frac{1}{2}$, Bob detects in average $2\mu\eta N$ bits, a number much smaller than N. After conclusion of the transmission, Bob announces publicly in which signals he detected a photon but not, of course, the phases he used. Alice and Bob agree to keep only these signals as a secret key.

The aforesaid is true only if an eavesdropper (Eve) does not monitor the quantum communication channel. To check for Eve's presence, Alice and Bob disclose some part of their protocols and publicly compare the launched and detected signals. Eve intercepts the transmitted photon sequence and, using the same equipment as Bob, detects $\approx 2\mu\eta N$ bits sent by Alice. Imitating Alice, Eve can safely resend corresponding signals on to Bob. As to the remaining $\approx(1 - 2\mu\eta)N$ signals, of which she has no information, she can either suppress the sidebands or suppress both the sidebands and the reference. In any case the legitimate users will inevitably detect her, as explained in [6]. Note that the detection of the classical reference spectral component by Bob is necessary to catch an eavesdropper.

In order to show the feasibility of the method proposed, we investigated experimentally the single-photon interference in the sidebands of modulated light using the apparatus of Fig. 1. The source S was a DBR laser diode from Alcatel operating at 1540 nm wavelength and with a 1 MHz linewidth. The source was temperature stabilized against wavelength drifts. For practical reasons related to photon counting, the laser emission was intensity modulated by the integrated electro-optic modulator (EOM) to produce 50-ns-duration pulses with a 1 MHz clock rate. We used two $LiNbO_3$ integrated phase modulators PM_1 and PM_2, operating at frequency $\Omega/2\pi = 300$ MHz. The modulation depth was chosen to be $m \approx 0.3$ rad. In this case, following the second modulator, the maximum intensity in one sideband was 10 times lower than the intensity of the central frequency. The laser diode was attenuated to -80 dB m, so that, with the chosen value of the modulation depth, the average photon number in each sideband launched in the fiber was approximately 0.1 photon/pulse. The transmission channel was a 20-km-long standard single-mode fiber. The Fabry-Perot interferometer FP was a bulk device with its mirrors designed to operate at 1540 nm wavelength. Its finesse was 55. The mirror spacing was adjusted to obtain a resolution of 36 MHz. The resulting transmission of the interferometer was about 100% at a sideband and 0.2% at the central frequency. The single-photon detector was a 77 K, liquid-nitrogen-cooled germanium avalanche photodiode (SPAD), passively quenched to operate in Geiger mode and connected to a low-noise high-gain amplifier, a discriminator, and a photon counter. The time response of the avalanche photodiode was 10 ns. As an example, Fig. 2 shows a photocount obtained after amplification. (We note that this appears to be the first time that single photon counting at 1540 nm wavelength with a germanium avalanche photodiode has been reported for quantum cryptography.)

We changed Φ_1 and Φ_2 so that the difference $\Delta\Phi = |\Phi_1 - \Phi_2|$ could vary between 0 and 2π with 10-s-duration steps of 0.25 rad. For each value of $\Delta\Phi$, the photon number was determined using 10^7 triggering pulses from the source; the receiver electronics being gated with 50-ns-wide window pulses (the procedure for photon counting will be explained elsewhere). The total number of counts for $\Delta\Phi = 0$ was about 5×10^3; dark counts were estimated to be about 200. The latter value was subtracted from the measured number of counts. In Fig. 3 the normalized dependence of photocount number on $\Delta\Phi$ is shown. The solid line shows a sinusoidal fit to the data. The experimental results correspond to Eq. (3) except for the fact that the minimum of the experimental

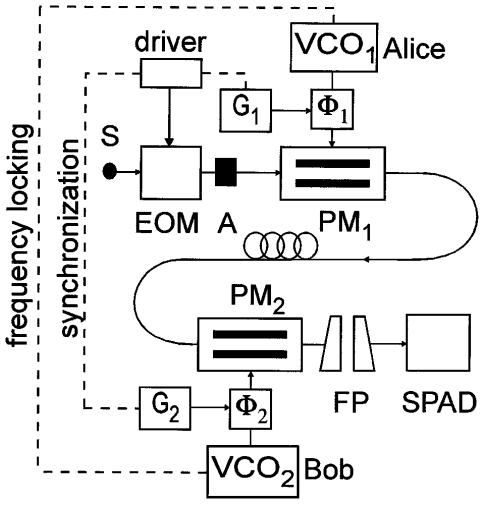

FIG. 1. Schematic diagram of the phase modulation transmission system.

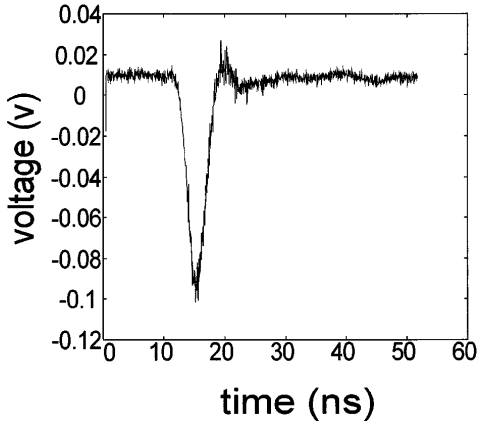

FIG. 2. Typical photocount obtained with the germanium SPAD operating at 1540-nm wavelength.

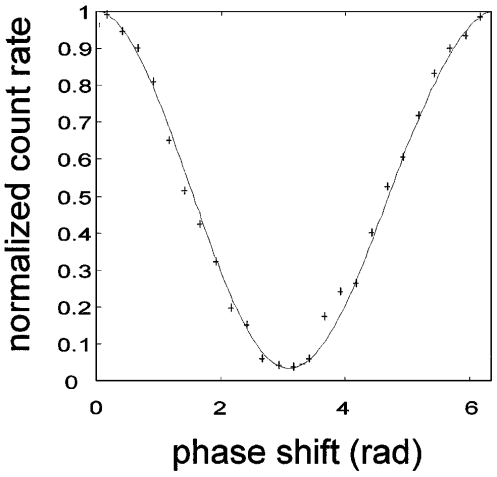

FIG. 3. Normalized single-photon count rate versus $\Delta\Phi$.

curve, positioned at $\Delta\Phi = \pi$, is not zero. In accordance with the protocol described above, this minimum value determines the relative rate of false counts (and, hence, the BER), corresponding to reasons other than photodetector dark counts. The BER was measured to be about 4%. Approximately half of this value can be attributed to the spurious transmission of the central frequency radiation through the interferometer, which was not optimized. The remaining $\approx 2\%$ are probably related to polarization dependence of the present system.

In conclusion, we have proposed a novel method of quantum key distribution that is based on single photon interference in the sidebands of phase modulated light and have demonstrated its feasibility in the 1540 nm telecommunication window. In our preliminary experiments, we did not investigate the performance limits in terms of frequency stability of the rf oscillators and the laser source, construction and finesse of the Fabry-Perot interferometer, polarization dependence, lost budget, transmission rate, transmission span, etc. However, our initial results indicate that the system features the following important advantages: (i) It requires only readily available standard telecommunication components (integrated modulators, fiber Fabry-Perot filters, voltage-controlled oscillators) that are compatible with practical fiber systems; (ii) the system can be polarization independent, if polarization-independent electro-optic modulators are used in the transmitter and in the receiver. The apparatus can then be many kilometers in length and remain stable against environmental perturbations. Finally, we note that modulation operating at a higher frequency would allow more relaxed constraints on the linewidth of the source and on the finesse of the spectral filter, thereby allowing a higher bit rate.

We acknowledge the financial support of the Délégation Générale à l'Armement (Ministry of Defense) and of France Telecom.

*Permanent address: S. I. Vavilov State Optical Institute 199034, St. Petersburg, Russia

[1] C. E. Shannon, Bell Syst. Tech. J. **28**, 656 (1948).
[2] G. S. Vernam, J. Am. Inst. Electr. Eng. **XLV**, 109 (1926).
[3] S. Wiesner, Sigact News **15**, 78 (1983).
[4] S. J. D. Phoenix, Phys. Rev. A **48**, 96 (1993).
[5] C. H. Bennet, G. Brassard, S. Breidbart, and S. Wiesner, in *Proceedings of Crypto '82: Advances in Cryptology* (Plenum, New York, 1983).
[6] C. H. Bennet, Phys. Rev. Lett. **68**, 3121 (1992).
[7] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A **51**, 1863 (1995).
[8] L. Goldenberg and L. Vaidman, Phys. Rev. Lett. **75**, 1239 (1995); Discussion: A. Peres, Phys. Rev. Lett. **77**, 3264 (1996); L. Goldenberg and L. Vaidman, Phys. Rev. Lett. **77**, 3265 (1996).
[9] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, J. Cryptol. **5**, 3 (1992).
[10] A. Muller, H. Zbinden, and N. Gisin, Europhys. Lett. **33**, 335 (1995).
[11] W. T. Buttler, R. J. Hughes, P. G. Kwiat, S. K. Lamoreaux, G. G. Luther, G. L. Morgan, J. E. Nordolt, C. G. Peterson, and C. M. Simmons, Phys. Rev. Lett. **81**, 3283 (1998).
[12] B. C. Jacobs and J. D. Franson, Opt. Lett. **21**, 1854 (1996).
[13] P. D. Townsend, J. G. Rarity, and P. R. Tapster, Electron Lett. **29**, 634 (1993).
[14] C. Marand and P. D. Townsend, Opt. Lett. **20**, 1695 (1995).
[15] J. Breguet, A. Muller, and N. Gisin, J. Mod. Opt. **41**, 2405 (1994).
[16] B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, Appl. Phys. Lett. **70**, 793 (1997).
[17] P. C. Sun, Y. Mazurenko, and Y. Fainman, Opt. Lett. **20**, 1062 (1995).