Time coding protocols for quantum key distribution

Thierry Debuisschert* and William Boucher
THALES Research and Technology—France, Domaine de Corbeville, 91404 Orsay Cedex, France
(Received 18 December 2003; published 8 October 2004)

We propose quantum key distribution protocols based on coherent single-photon optical pulses with duration T and with minimum time-frequency uncertainty. The pulses are sent with possible delays (e.g., 0, $T/2$) that are used to code the information (e.g., bit 0, bit 1) and that are shorter than the pulse width. Therefore, the time detection of the photons may result in a ambiguity of the delay evaluation for a potential eavesdropper. The duration of the received pulses is controlled thanks to a contrast measurement using an interferometer. A quantum formalism is given, allowing us to model the transmission of the key and the consequences of a possible eavesdropping. Two protocols are proposed and discussed. The first one involves two states and is limited to channels with losses lower than 50%. The second one involves four states, which prevents the eavesdropper from exploiting the losses of the line. The security of each protocol is evaluated as a function of channel losses, quantum bit error rate, and contrast loss in the case of intercept-resend attacks. It is applied to situations where photocounters dark counts are the main limitation of the system. The resulting maximum propagation distance allowing secure communication is evaluated.

DOI: 10.1103/PhysRevA.70.042306 PACS number(s): 03.67.Dd, 03.67.Hk, 42.50.Ar

I. INTRODUCTION

The quantum key distribution (QKD) is a way, alternative to mathematical methods, to distribute a key between two parties usually called Alice and Bob. The purpose of the QKD is not to prevent a third party Eve from eavesdropping the line, but to make the eavesdropping detectable by Alice and Bob. In that case, they do not validate the key. The QKD is based on the fundamental principles of quantum mechanics. It relies on the quantum properties of photons that are used to transmit the key. The first protocols that have been proposed used a polarization basis to encode the key, with either four nonorthogonal polarization states [1] (the Bennett-Brassard 1984 protocol usually called BB84) or two nonorthogonal polarization states [2] (the Bennett 1992 protocol usually called B92). Several experimental demonstrations have been achieved based on those protocols [3]. The first one was based on polarization coding with propagation in air [4]. For telecommunication applications, a better propagation medium is an optical fiber. Polarization appeared to be unpractical due to technical limitations in optical fibers such as stress induced birefringence which transforms the initial linear polarization of the photon into an elliptical polarization [5]. Another possibility is phase coding [6]. The principle is to implement a long-arm Mach-Zender interferometer between Alice and Bob, allowing each of them to modify the dephasing between the two arms of the interferometers. This technique allows a coding similar to that of BB84 with polarization. It is also necessary to compensate for polarization modifications due to the propagation but this can be achieved with go and return techniques that allow for birefringence compensation [7,8].

An alternative protocol to polarization coding or phase coding for the quantum key distribution is to use the time-frequency uncertainty of coherent one-photon pulses [9]. The protocol we propose exploits that uncertainty and is based on a time coding technique that is expected to be robust against propagation medium disturbances. The information is coded on coherent one-photon pulses of duration T with uniform probability detection density. Alice sends the pulses at a regular frequency giving the time reference. To encode the key, an additional delay with respect to that reference can be put on each pulse (Fig. 1). The possible delays are chosen smaller than the pulse duration. Bob uses photocounters with a time resolution much better than the pulse duration. He evaluates the delay measuring the detection time with respect to the reference. He can perform only one measurement which may lead to an ambiguity on the delay evaluation. Previous use of the time domain for quantum key distribution [10,11] or quantum computation [12] made use of pulses well separated in time. The originality of our protocol is to

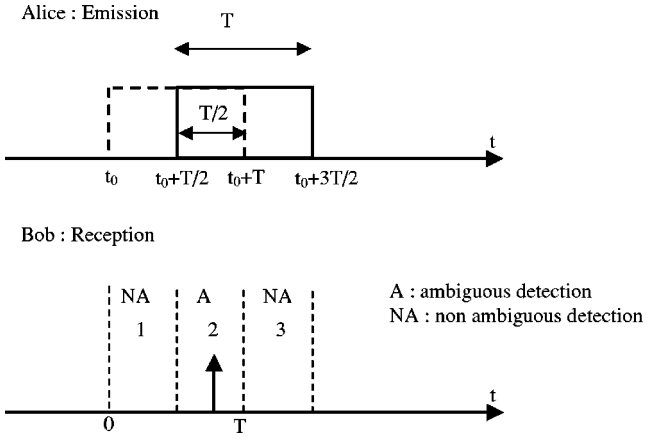

FIG. 1. Principle of the two-state protocol. Alice sends pulses of duration T with chosen delay 0 or $T/2$. Bob measures the photon detection time. The time slots 1 and 3 are nonambiguous and allow for delay determination. The time slot 2 is ambiguous and does not allow for delay determination.

*Electronic address: thierry.debuisschert@thalesgroup.com

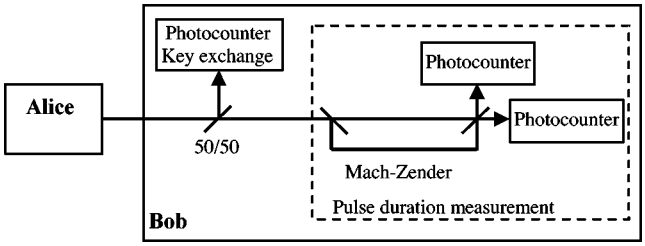

FIG. 2. Scheme of the experiment. Bob directs the pulses sent by Alice at random to a photon counter to establish the key or to a Mach-Zender interferometer that allows for duration measurement of the pulses.

explicitly exploit the possible overlap between pulses.

If a measurement is only performed in the time domain, Eve can get a perfect copy of the key after the reconciliation process. She only has to send back to Bob one photon pulses with a duration T_E much smaller than T and with a delay identical to the one she measured. Bob cannot distinguish T pulses from T_E pulses with only one measurement. To protect the transmission from that kind of attack, Alice sends coherent pulses with minimum time-frequency uncertainty product—i.e., pulses with a coherence length equal to their duration. In parallel to the measurement in the time domain, Bob does a measurement in the frequency domain thanks to an interferometer. All the protocols that are analyzed in the following require performing those two measurements at the same time. Bob sends at random the pulses he receives to a Mach-Zender interferometer with a propagation time difference equal to the delay used to encode the key and with a phase difference of π between the two arms (Fig. 2). The imbalance between the average photon number detected in each output arm of the interferometer varies with the pulse duration, thus giving a way to measure that duration. The other arm of the input beam splitter is sent to the photocounter that is used to establish the key between Alice and Bob (Fig. 2). The control of the pulse duration via a coherence measurement allows coding the information only in the time domain. In that way our protocol differs from the standard BB84 or B92 protocols where the information is coded equally between two non orthogonal basis. This removes the possibility for Eve to choose an appropriate basis combination to increase her information on the key [4]. This also has the practical advantage of avoiding for Bob to randomly switch his detection between the two basis.

From an experimental point of view, this protocol has several advantages. Available photocounters can have response time smaller than 1 ns [13]. We will thus consider pulse durations in the 10–20 ns range for which the time propagation of the pulses is only little affected by the propagation disturbances of the fiber. A low error rate requires precisions in the arrival time of about 1 ns which makes it insensitive to fiber thermal dilatation. In addition pulse spreading due to group velocity dispersion starts to be noticeable only in the ps range with usual telecommunication fibers [14]. The measurement of the arrival time of the photon does not require that the polarization of the photon be conserved. If the interferometer is made insensitive to the polarization, the whole system is potentially insensitive to the polarization. As a consequence there is no need for go and return of the pulses, which opens the way to high transmission rates. Coherent faint pulses can be produced combining a single-mode diode laser and an high-speed electro-optics amplitude modulator that can be driven with an electrical pulse generator having rise time and decay time smaller than 1 ns. These technical considerations combined with the advantages of the principle described above make the time coding protocol a realistic method for quantum key distribution.

The purpose of the paper is to give a formalism that allows describing quantum mechanically the protocols based on time coding. Then two protocols are discussed based on two or four states. The defects of the line between Alice and Bob as well as those of Bob's photocounters allow for eavesdropping. They are modeled to give a security evaluation of the protocols in the frame of intercept-resend attacks.

II. QUANTUM FORMALISM

The use of coherent one-photon pulses in the time domain can lead to many different protocols. We choose to study one class where Alice sends square pulses having all the same duration T. The delay is a multiple of $T/2$, which gives the time resolution of the problem. To describe the protocols, we divide the temporal axis in N successive time slots of duration $T/2$ labeled j. This allows introducing a discrete basis for the time coding protocols. For each time slot we introduce a characteristic function $u_j(t)$ equal to $\sqrt{2/T}$ in the interval $[(j-1)T/2, jT/2]$ and zero elsewhere. It obeys the normalization relation

$$\int dt|u_j(t)|^2 = 1. \tag{1}$$

To each time slot corresponds a one-photon state given by

$$|j\rangle = \int d\omega c_j(\omega) a^\dagger(\omega)|0\rangle. \tag{2}$$

Here, j denotes the time slot and not the number of photons of usual Fock states.

$c_j(\omega)$ has the following expression where ω_0 is the central optical frequency (see the Appendix):

$$c_j(\omega) = \frac{1}{\sqrt{2\pi}} \int dt\, u_j(t) e^{i(\omega-\omega_0)t}. \tag{3}$$

The different amplitudes are identical up to a phase shift:

$$c_j(\omega) = e^{i(\omega-\omega_0)(j-1)T/2} c_1(\omega). \tag{4}$$

To describe a protocol requiring N time slots, one considers an N-dimensional Hilbert space. The $|j\rangle$ states form a discrete basis which can be used to describe quantum mechanically that protocol.

The pulses sent by Alice are square pulses which are nonzero only on two adjacent time slots j and $j+1$. The corresponding one-photon pure state can be written

$$|j,j+1\rangle = \frac{1}{\sqrt{2}}(|j\rangle + |j+1\rangle). \quad (5)$$

In such a state, the probability to detect a photon in the time slot j or in the time slot $j+1$ is equal to $1/2$ and to 0 for other time slots. Moreover, there is a coherence between states $|j\rangle$ and $|j+1\rangle$ which allows us to observe interferences with a properly designed interferometer. In that case, the coherence is equal to $1/2$.

III. CODING PROTOCOLS

A. Principles

In all the protocols which will be analyzed in the following, Bob sends at random half of the pulses he has received to a photocounter to measure their arrival time. The other half is sent to a Mach-Zender interferometer to evaluate the average contrast which is defined as the difference between the photon numbers in the two output ports normalized to their sum. In the ideal case, a contrast of 50% should be measured.

The simplest configuration is a two-state protocol in analogy with the B92 protocol [2]. Alice may send two kinds of pulses. One (e.g., bit 0) is coded with zero delay, and the other one (e.g., bit 1) is coded with $T/2$ delay (Fig. 1). The photon detection can occur within three different time slots. The first one and third one are nonambiguous and allow for an exact determination of the delay. The photon detection in the second time slot leads to an ambiguity on the delay determination. At that point the raw key is established and the contrast has been measured. Then Bob announces to Alice when he has obtained a nonambiguous result and discards the others. This is the reconciliation step which results in the sifted key. Alice and Bob can then evaluate the quantum bit error rate (denoted Q) sacrifying part of the sifted key. In order to share a secret key, Alice and Bob must perform two additional steps. First they must remove the errors from the key thanks to an error correction algorithm (at the price of an increase of the information available to Eve). Then they have to cancel the information of Eve on the key thanks to a privacy amplification algorithm [3]. Those steps are required for any protocol that is considered. In the following, we will concentrate on the quantum aspect of the protocols and stop our analysis to the establishment of the sifted key.

Analyzing eavesdropping on the two states protocol, one sees that Eve cannot deduce with certainty the delay chosen by Alice for all pulses she detects. She unavoidably introduces errors in the message when she sends back pulses of duration T to Bob. Anyhow, Eve can exploit the losses of the channel between Alice and Bob. Eve resends nothing when she obtains an ambiguous result and she resends the appropriate state when she obtains a non ambiguous result. When the losses of the channel between Alice and Bob exceed 50%, Eve can measure all the pulses sent by Alice and she obtains complete information on the key. To overcome that limitation one has to go to a more sophisticated protocol involving four states as described below.

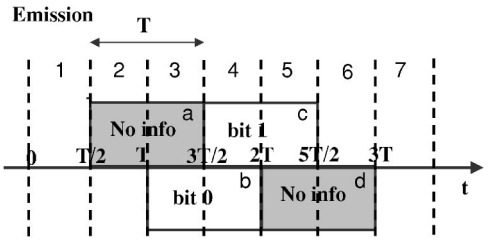

FIG. 3. Principle of the four-state protocol. Alice sends pulses of duration T with chosen delays 0, $T/2$, T, or $3T/2$. Pulses (a) and (d) carry no information. Pulses (b) and (c) encode bit 0 and bit 1, respectively. Bob measures the photon detection time. He keeps only the results corresponding to time slot 3 and time slot 5. The results are ambiguous which prevents Eve from exploiting the losses of the line.

For that protocol Alice makes use of four different states with temporal overlap between them. The protocol is illustrated on Fig. 3. Pulses (a), (b), (c), and (d) are one-photon square pulses which are nonzero only for time slots (2,3) (3,4), (4,5), and (5,6), respectively. The fact that we do not use time slot 1 at the moment will become clear when taking into account the defects of the line. Pulses (a) and (d) are auxiliary pulses which do not carry any information. Pulses (b) and (c) can be chosen to encode bit 0 and bit 1, respectively. To establish the raw key, Alice sends at random to Bob the four possible pulses with the same probability. As previously, half of the pulses are used by Bob to establish the raw key and the other half is sent to the Mach-Zender interferometer for the contrast measurement. Once the raw key has been sent, part of it can be compared publicly between Alice and Bob to make sure that the measurements at Bob are consistent with the pulses sent by Alice. To produce the sifted key, Bob announces to Alice when he has detected the result in time slot 3 or 5 without revealing the result. Alice validates the measurement if the corresponding pulse she had sent was carrying some information [pulses (b) or (c)]. Otherwise she discards the measurement. Alice and Bob can then compare publicly part of the resulting string of bits to evaluate the quantum bit error rate (Q). For a given value of the contrast, if Q is small enough, they proceed with error correction and privacy amplification to obtain a non ambiguous string of secret bits. The main difference with the previous protocol is that all measurements that allow Eve to get some information on Alice (detections in time slot 3 or 5) are now ambiguous in a way similar to the detection in time slot 4. To preserve the symmetry of the string of pulses sent by Alice, Eve has to resend pulses with the same probability whenever she detects in 3, 4, or 5. As a consequence she can no more exploit the losses of the channel to resend a pulse with a higher probability when she has detected in 3 or 5 than when she has detected in 4 as is the case in the two-state protocol. The ratio between the rate of bits in the sifted key and the rate of pulses that are sent by Alice can be evaluated considering that Bob keeps only half of the pulses he receives and sends the other ones to the interferometer. Then Alice discards half of the pulses she has sent [pulses (a) and

(d)] and only half of Bob's measurements lead to unambiguous results. Therefore the bit rate is 12.5% of the pulse rate.

B. Transmission with no eavesdropping

The formalism described below is used to give a quantitative evaluation of the protocols security. It can be used to describe the two-state protocol and the four-state protocol as well.

The states corresponding to the four possible pulses sent by Alice are defined as follows: $|a\rangle=|2,3\rangle$, $|b\rangle=|3,4\rangle$, $|c\rangle=|4,5\rangle$, and $|d\rangle=|5,6\rangle$. The states are sent at random by Alice with probabilities p_a, p_b, p_c, and p_d which are let as parameters whose values are set according to the case.

In the two-state protocol, the probabilities p_a and p_d are set to 0 when Alice sends the raw key. We will consider the symmetric case where p_b and p_c are chosen equal to $1/2$.

In the four-state protocol, they are all equal to $1/4$ (in the symmetric case), in order to simulate the launch of the raw key. To simulate the sifted key p_b and p_c are set to $1/2$ and p_a and p_d are set to zero.

In both protocols, either p_b or p_c is set to 1 the other ones being set to 0, in order to calculate the quantum bit error rate and the mutual information between Alice and Eve. Bob who does not know the choice of Alice can describe the state by a density matrix of the form

$$\rho_A = \sum_{k=a,b,c,d} p(k)|k\rangle\langle k|, \tag{6}$$

with

$$\sum_{k=a,b,c,d} p(k) = 1. \tag{7}$$

The diagonal coefficients $\rho_{A_{jj}}$ of the density matrix give the probability to detect a photon in time slot j. The off-diagonal coefficients of the density matrix are nonzero only for the two diagonals closest to the main diagonal. They are measured thanks to Bob's interferometer.

In a real system, the transmission of the signal is affected by several defects. Since the protocol is based on a precise timing of the photon detection, the system is sensitive to synchronization defects between the clocks of Alice or Bob or intrinsic fluctuations in the clocks. One could also consider a broadening of the pulses received by Bob. It can be due to the propagation in the fiber although negligible in the nanosecond range. It can also be due to imperfect pulses sent by Alice, if, for example, the pulses are produced with nonzero rise time and decay time. In that latter case this would induce errors for Bob but for Eve as well. Imperfect timing or pulse broadening would result in the possibility of detecting a photon in another time slot than the two time slots corresponding to the given state sent by Alice. In a simple model one can consider a nonzero probability to detect a photon in the two adjacent time slots—i.e., to detect a photon in time slots $j-1$ or $j+2$ for a state $|j,j+1\rangle$. This explains why we have defined the state $|a\rangle$ spanning the states $|2\rangle$ and $|3\rangle$. In a perfect transmission the probability to detect a photon in the time slots 1 would be zero, but due to the imperfect synchronization, this probability is nonzero. For the same reason, a time slot 7 must be considered accounting for the same kind of error when state $|d\rangle=|5,6\rangle$ is sent.

Another defect due to the transmission line is the unavoidable occurrence of loss. We mainly consider those occurring at the outside of Alice and Bob. Those occurring inside the apparatus of Alice and Bob can be measured and their effect corrected. The losses occurring in the transmission line are modeled with a coupler of probability transmission η that redirects the pulses to an additional auxiliary mode with probability $1-\eta$. Thus an eighth state (labeled $|0\rangle$) has to be introduced to account for the losses. Due to the losses, the state sent by Alice becomes after transmission through the line: $\eta\rho_A+(1-\eta)\pi_0$, where π_0 is the density matrix corresponding to the state $|0\rangle$ simulating the losses.

Another defect is a loss of coherence that would prevent from measuring an optimal value of the contrast at Bob's interferometer. There are unavoidable defects in the interferometer itself, but they can be measured by Bob and taken into account. Thus the contrast measurement can be corrected from proper interferometer imperfections. On the other hand, the source used by Alice cannot have a perfect coherence and decoherence may occur in the transmission line. Since the contrast measurement is an average over a large number of pulses lasting as long as the key transmission, the lack of coherence can induce phase fluctuations, resulting in a lowering of the contrast measured at Bob's interferometer. It should be mentioned that the lack of coherence of Alice's source does not affect the measurements of Eve since she only has to measure the detection time of the photon. This lack of coherence is simply modeled multiplying all the nondiagonal terms of the density matrix received by Bob by $(1-dC)$ with $0\leqslant dC\leqslant 1$ where dC accounts for the loss of coherence. $dC=0$ corresponds to the case of no loss of contrast at Bob's interferometer. The case $dC=1$ corresponds to an incoherent source at Alice or the absence of contrast measurement at Bob. It will be shown that in this last case, the transmission can never be secure.

The last defect that will be considered is the existence of dark counts in the photocounters. They consist of a triggering of the avalanche occurring without any incoming photon and due, for example, to thermal fluctuations. A signal from the detector can thus result from the detection of an effective photon or from a dark count. The dark count probability per time unit is specific from a given detector whereas the probability to detect a photon depends on several parameters such as the line losses. As a consequence, as the propagation distance increases, the probability to receive a photon decreases and the dark count probability becomes predominant. This results in an increase of the quantum bit error rate, which compromises the security of the transmission [15]. The occurrence of dark counts is one of the main limitations to single photon quantum key distribution. In order to simplify the analysis of the proposed protocols, we will first neglect the detector dark counts. Then, Sec. VIII will be devoted to the consequences of dark counts and to the resulting limitation on the secure distance of propagation.

C. Eavesdropping modeling

The four main defects that have been introduced can be used by an eavesdropper to tap some information about the

key. The purpose of Eve is to maximize her available information while being undetected by Alice and Bob. The main goal of the security evaluation of the protocol is to evaluate quantitatively the information that is made available to Eve. Numerous attacks can be considered. We limit our study to simple intercept-resend attacks. To simulate Eve's attack on the line, we suppose that she benefits from unlimited technological power. Therefore she can replace the imperfect channel between Alice and Bob with a perfect one with no loss and no error. In addition when Eve resends a pulse she uses a perfectly coherent source, which allows her to exploit the possible lack of coherence of Alice's source.

When Eve makes a measurement and detects a photon in time slot j $(2 \leqslant j \leqslant 6)$, she can decide to resend a pulse or not, thus simulating the losses of the imperfect channel. Detecting a photon in time slot j, Eve knows that the pulse she has received from Alice was $|j, j+1\rangle$ or $|j-1, j\rangle$ with equal probability (except for $j=1$ and $j=6$ where she knows exactly which pulse was sent by Alice). When she sends a pulse, she sends pure states in order to maximize the contrast in Bob interferometer. In a first step we consider that she can send any kind of state that is nonzero only on two adjacent time slots. She is not bound to square pulses and she can choose any time profile. It can be shown in fact that square pulses are the optimum choice for Eve in order to send maximum coherence pulses for given probability detections in the time slots. Let us suppose that Eve sends a pulse on time slots j and $j+1$. It can be expressed as

$$f(t) = a_j g_j(t) + a_{j+1} g_{j+1}(t), \tag{8}$$

where $g_j(t)$ are arbitrary shape functions which are nonzero only in the time slot j and which are normalized:

$$\int dt |g_j(t)|^2 = 1. \tag{9}$$

The coefficients a_j and a_{j+1} obey the relation

$$|a_j|^2 + |a_{j+1}|^2 = 1. \tag{10}$$

The contrast (A14) where $\omega_1 \tau$ is set to $2k\pi$ is given by

$$C = \frac{1}{2} \int dt f(t) f^* \left(t + \frac{T}{2} \right) + \text{c.c.}, \tag{11}$$

which reduces to

$$C = \frac{1}{2} a_j a_{j+1}^* \int dt g_j(t) g_{j+1}^* \left(t + \frac{T}{2} \right) + \text{c.c.} \tag{12}$$

The contrast is maximized choosing a_j and $g_j(t)$ real. In addition, the overlap integral between $g_j(t)$ and $g_{j+1}(t+T/2)$ is maximized to 1 when those two functions are identical. Square pulses appear to be a particular case of that condition which allows maximizing the coherence of the pulses sent by Eve. Thus one can consider that Eve sends square pulses and uses the same state basis as Alice without restricting the generality of the problem.

The state received by Bob is now the one that has transited via the perfect line of Eve. If Eve does not measure the state, she simply transmits the initial state sent by Alice ρ_A. If she performs a measurement (probability m), she intercepts the pulse with a photocounter and she determines the detection time of the photon. She then sends the state ρ_E, which allows her to minimize the possibility for Alice and Bob to detect the eavesdropping. The state received by Bob is described by a density matrix ρ_B given by

$$\rho_B = m\rho_E + (1-m)\rho_A. \tag{13}$$

The state received by Bob must be consistent with a state that could have been sent by Alice. Thus ρ_B must mimic ρ_A taking into account the defects of the line.

The density matrix received from Alice has no coherence of the form $\rho_{j-1,j+1}$. Thus the density matrix resent by Eve is a statistical mixture of states $|\psi_{j,j+1}\rangle$ and $|\psi_{j,j-1}\rangle$ with probabilities $p_{j,j+1}$ and $p_{j,j-1}$ respectively. They are of the form

$$|\psi_{j,j+1}\rangle = \sqrt{1-x_{j,j+1}}|j\rangle + \sqrt{x_{j,j+1}}|j+1\rangle, \tag{14}$$

$$|\psi_{j,j-1}\rangle = \sqrt{1-x_{j,j-1}}|j\rangle + \sqrt{x_{j,j-1}}|j-1\rangle. \tag{15}$$

The first index stands for the time slot where the photon has been detected. The second one stands for the neighboring state. $|\psi_{j,j+1}\rangle$ differs from $|j, j+1\rangle$ in the sense that $x_{j,j+1}$ is not necessarily equal to $1/2$. This parameter allows Eve to take advantage from a possible defect in the contrast measurement of Bob. Taking $x_{j,j+1}$ smaller than $1/2$ increases the probability for Bob to obtain the same measurement result than Eve (detection in time slot j).

In the case where there is no lack of coherence between Alice and Bob ($dC=0$), $x_{j,j\pm1}$ must be equal to $1/2$ to avoid a drop of the contrast in Bob interferometer that would immediately show the presence of Eve. In the limit case where $dC=1$, Eve can set $x_{j,j\pm1}$ to zero. Eve can thus intercept all the pulses and send a perfect copy to Bob without being detected.

After measurement, Eve resends a statistical mixture characterized by the following density matrix:

$$\rho_E = \sum_{j=2}^{6} \text{Tr}(|j\rangle\langle j|\rho_A|j\rangle\langle j|)[p_{j,j+1}|\psi_{j,j+1}\rangle\langle\psi_{j,j+1}| + p_{j,j-1}|\psi_{j,j-1}\rangle \times\langle\psi_{j,j-1}| + (1-p_{j,j+1}-p_{j,j-1})\pi_0]. \tag{16}$$

The detailed expression of ρ_B is obtained inserting Eqs. (6) and (16) into Eq. (13). It is complicated partly due to the different possible values of parameters $x_{j,j\pm1}$ and $p_{j,j\pm1}$. It can be greatly simplified taking into account the symmetry properties of ρ_A that ρ_B has to verify if the eavesdropper wants to remain undetected. Alice and Bob can check these properties after the raw key has been exchanged sacrifying part of that one. The main idea is that the probability detections at Bob have to be independent of the pulse (a), (b), (c), or (d) that has been sent by Alice. One evaluates the detection conditional probabilities for each time slot and for each kind of pulse sent by Alice. The conditions are the following.

(a) The probabilities to detect in j or $j+1$ when Alice has sent $|j, j+1\rangle$ must be identical and independent of j.

(b) The error probabilities must be identical. When Alice has sent $|j, j+1\rangle$, the probabilities to detect in $j-1$ or $j+2$ must be identical and independent of j.

(c) The probabilities to detect in $j+1$ must be independent of the states $|j,j+1\rangle$ or $|j+1,j+2\rangle$ that can have been sent by Alice.

Eve is free to violate these assumptions, but doing so, she will be detected when Bob will analyze part of his raw key knowing the pulses sent by Alice. Her purpose being to eavesdrop the key without being detected, we will assume in the following that these assumptions are satisfied. They will result in constraints putting an upper bound to the information available to Eve.

The consequences of those requirements differ according to the protocol that is being considered (either two states or four states). At that point we separate their study. We start considering the two-state protocol.

IV. TWO-STATE PROTOCOL

In the two-state protocol, p_a and p_d are zero. We set successively p_b and p_c to 1 in ρ_B keeping the other probability to 0. Applying the requirement on the error probability, we obtain the following condition:

$$p_{32}x_{32} = p_{43}x_{43} = p_{45}x_{45} = p_{56}x_{56}. \tag{17}$$

Applying the symmetry requirements we obtain the following conditions:

$$p_{54}x_{54} = p_{34}x_{34}, \tag{18}$$

$$p_{34} + p_{32} = p_{54} + p_{56} = p_3 = p + dp, \tag{19}$$

$$p_{43} + p_{45} = p_4 = p - dp, \tag{20}$$

$$p_{34}x_{34} = p_{32}x_{32} + \frac{p_3 - p_4}{2} = p_{32}x_{32} + dp. \tag{21}$$

The probabilities that Eve sends a pulse when she has detected in 3 or 4 (p_3 and p_4, respectively) are not necessarily identical. Thus we define their average value p and half difference dp. These parameters can be adjusted by Eve according to the defects of the real line. The possibility that dp is nonzero is specific to the two states protocol.

At that point, fulfilling the relations (17)–(21) allows Eve not to be detectable by symmetry considerations on the raw key received by Bob. The second step in the determination of ρ_B is to take into account the defects of the line admitted by Alice and Bob: quantum bit error rate (Q), relative contrast loss (dC), and line transmission (η). This will allow us to determine the remaining free parameters in the density matrix. In addition we calculate at that point the mutual information between Alice and Eve (I_{AE}), since it will appear that the contrast of the interferometer can be expressed directly as a function of I_{AE} and Q.

Bob keeps only the results where he has obtained a measurement in 3 or 5 (without revealing the result). The pulses are sent by Alice with the same probabilities (1/2); thus the quantum bit error rate can be calculated considering one or the other of the two pulses. It can thus be defined as the ratio between the probability for Bob to detect in 5 when a pulse (b) has been launched by Alice divided by the total probability for Bob to detect in 3 or 5 when a pulse (b) has been launched by Alice. Setting p_b to 1 in ρ_B, one obtains the relation

$$Q = \frac{\rho_{B_{55}}(p_b = 1)}{\rho_{B_{55}}(p_b = 1) + \rho_{B_{33}}(p_b = 1)} = \frac{mp_{32}x_{32}}{1 - m + mp}. \tag{22}$$

The same expression would have been obtained considering that Alice had sent a pulse (c). The existence of the quantum bit error rate is directly proportional to the probability that Eve resends a pulse that spans the neighboring time slots when detecting a photon in time slot j.

To calculate the information of Eve on Alice we consider only the case where Bob detects in time slot 3. Due to the equal probabilities for Alice to send a pulse (b) or a pulse (c) the consideration of a detection in 5 by Bob would lead to the same result.

Knowing that Bob has detected a photon in time slot 3, one has to calculate the probability that Eve has detected a photon in time slot 3 in which case she knows with certainty which pulse was sent by Alice and she gets one bit of information. The case where Eve has detected in 4 does not bring any information to her. The case where Eve detects in 5 and Bob detects in 3 is impossible in the limit of our starting hypothesis. The calculation is done calculating the probability that Bob detects in time slot 3 when Eve has detected in time slot 3 and using Bayes theorem. Using Eqs. (18) and (21), one gets

$$\begin{aligned} I_{AE} &= \frac{P(B=3|E=3)P(E=3)}{P(B=3)} \\ &= \frac{(p_{32}(1-x_{32}) + p_{34}(1-x_{34}))m}{1-m+mp} \\ &= \frac{m(p - 2x_{32}p_{32})}{1-m+mp}. \end{aligned} \tag{23}$$

In the case where Eve is not allowed to induce any error, x_{32} is zero. Then the information is equal to the rate of pulses that are intercepted and resent by Eve. Each time she detects a photon in time slot 3, she has to resend a pulse corresponding to the state $|3\rangle$. She thus knows for sure that Bob will detect in time slot 3 and will validate the measurement [if Alice has sent a pulse (b)], but doing that she induces a strong drop of contrast on Bob's interferometer.

In the case where no drop of contrast is allowed, x_{32} is one-half. Then the information rate is half the rate of pulses that are detected in time slot 3 and resent by Eve. If Eve detects a photon in time slot 3, she has to resend a pulse corresponding to the state $|3,2\rangle$ or $|3,4\rangle$. The probability that Bob validates the measurement is one-half.

Combining Eqs. (22) and (23) one obtains the quantity A which has the following expression:

$$A = I_{AE} + 2Q = \frac{mp}{1-m+mp}. \tag{24}$$

It represents the rate of pulses that are intercepted and resent by Eve over the total number of pulses detected by Bob. It is always smaller than 1 and is equal to one only in the case

where $m=1$, which means that Eve has intercepted all pulses sent by Alice. This results in a physical upper limit on the information that Eve can obtain on Alice through intercept-resend attack which is given by

$$I_{AE} \leqslant 1 - 2Q. \tag{25}$$

In particular, Eve can obtain complete information on the key (i.e., one bit per pulse) only in the case where she does not induce any error at Bob'site and the quantum bit error rate is zero.

The following quantity that has to be calculated to evaluate the security of the protocol is the contrast of Bob's interferometer and the effect of Eve interception of the original message. Since we are considering real probability amplitudes the contrast is given by Eq. (A21) where we have to take into account the losses induced by Eve. We obtain

$$C_{AEB} = \frac{\sum_{j=1}^{6} \rho_{B_{j,j+1}}}{1 - \rho_{B_{0,0}}}. \tag{26}$$

The contrast is an average measurement performed on the raw key sent by Alice. Pulses (b) and (c) have the same probability to be launched and thus one has to set $p_b = p_c = \frac{1}{2}$ in the expression of C_{AEB}. Inserting the relations (22) and (23) in Eq. (26), one obtains the expression for the contrast in the two-state protocol as a function of I_{AE} and Q, and of the various probabilities for Eve to resend a pulse:

$$\begin{aligned} C_{AEB_2} = {} & \frac{1}{4}\sqrt{Q}\sqrt{A\frac{p_{32}}{p} - Q} \\ & + \frac{1}{4}\sqrt{Q + A\frac{dp}{p}}\sqrt{A\frac{p_{34}}{p} - Q - A\frac{dp}{p}} \\ & + \frac{1}{2}\sqrt{Q}\sqrt{A\frac{p_{43}}{p} - Q} + \frac{1}{4}\sqrt{Q}\sqrt{A\frac{p_{56}}{p} - Q} \\ & + \frac{1}{4}\sqrt{Q + A\frac{dp}{p}}\sqrt{A\frac{p_{54}}{p} - Q - A\frac{dp}{p}} \\ & + \frac{1}{2}\sqrt{Q}\sqrt{A\frac{p_{45}}{p} - Q} + \frac{1}{2} - \frac{1}{2}A, \end{aligned} \tag{27}$$

where A is given by Eq. (24).

In the absence of eavesdropping, the contrast in the ideal case is $1/2$. Taking into account the possible loss of contrast, it becomes

$$C_{AB} = \frac{1}{2}(1 - dC). \tag{28}$$

Expressing that the minimum value of C_{AEB_2} is equal to C_{AB}, one obtains an implicit relation defining the mutual information I_{AE} as a function of variables $p_{j,j-1}$, $3 \leqslant j \leqslant 5$, Q and dC being parameters. The extremum of I_{AE} is obtained when the partial derivatives of C_{AEB_2} with respect to $p_{j,j-1}$ are zero. This mathematical derivation of I_{AE} may lead to values that are not physically attainable which means that Q and dC are not compatible. One has to bear in mind that the value of I_{AE} has to fulfill the condition (25), which will be implicitly assumed in the following. Taking into account relations (19) and (20), one obtains the following relations:

$$p_{34} - p_{32} = p_{54} - p_{56} = \frac{Adp(p + dp)}{2Qp + Adp}, \tag{29}$$

$$p_{45} = p_{43}. \tag{30}$$

Inserting Eqs. (29) and (30) into Eq. (27) greatly simplifies the expression of C_{AEB_2}, which becomes

$$C_{AEB_2} = \frac{1}{2}\left[\sqrt{2Q + A\frac{dp}{p}}\sqrt{I_{AE}} + \sqrt{2Q}\sqrt{I_{AE} - A\frac{dp}{p}} + 1 - A\right]. \tag{31}$$

The purpose of Eve is to maximize its information on Alice for a given value of Q, dC, and the line transmission η respecting the relation $C_{AEB_2} = C_{AB}$. Here p and dp are two adjustable parameters that Eve can choose to optimize I_{AE}. Expressing that the probability to detect a photon has to be equal to η in order to mimic the losses of the line, one finds that

$$\eta = 1 - \rho_{B_{0,0}} = 1 - m + mp. \tag{32}$$

The resulting expression of m is combined with Eq. (24) to obtain the following expression:

$$A = I_{AE} + 2Q = \left(\frac{1 - \eta}{\eta}\right)\left(\frac{p}{1 - p}\right). \tag{33}$$

It shows that I_{AE} is an increasing function of p for given values of η and Q. Intercepting the pulse sent by Alice without resending a pulse to Bob is of no interest for Eve. Thus she has to resend a pulse as often as possible, maximizing the value of p. With the constraint that A be smaller than 1, the maximum value of p is η. Eve can obtain two measurement results. If she detects a photon in time slot 3, she knows which pulse Alice sent and she has no risk to induce a bit error in the sifted key. If she detects a photon in time slot 4, she does not know which pulse Alice sent and she may induce an error in the sifted key with probability 0.5. The best strategy for Eve is thus to resend a pulse each time she detects in 3 and to avoid resending a pulse when she detects in 4. With the definition of p and the fact that its maximum value is η, this is possible as soon as $\eta \geqslant \frac{1}{2}$. From now on, we assume that this relation is fulfilled. Eve can then resend a pulse each time she detects in 3 and set p_3 to 1. As a consequence there is only one free parameter p_4, and one finds that p is equal to $1 - dp$. From Eq. (33), one gets

$$A\frac{dp}{p} = \frac{1 - \eta}{\eta}. \tag{34}$$

Inserting Eq. (34) into Eq. (29) shows that p_{34} is always greater than p_{32}. The coherence of state $|\psi_{32}\rangle$ is limited by the amount of error that is allowed in the transmission. On the opposite, $|\psi_{34}\rangle$ does not induce any error for Bob. Therefore its coherence can be higher, which means that when Eve detects a photon in 3, she has to send more likely states $|\psi_{34}\rangle$ than states $|\psi_{32}\rangle$. In the limit case where Q is zero, Eve sends

only states $|\psi_{34}\rangle$ since $|\psi_{32}\rangle$ is equal to $|3\rangle$ and has no coherence. The same situation occurs comparing p_{54} and p_{56}. When Eve detects a photon in 4 she sends $|\psi_{43}\rangle$ or $|\psi_{45}\rangle$ with the same probability since the effect on the error and on the contrast is the same in both cases.

With Eq. (34) inserted into Eq. (31), the relation $C_{AEB_2} = C_{AB}$ entirely defines I_{AE} as a function of Q, dC, and η. In the general case it gives a fourth-order polynomial that can be solved numerically. In any case, in order for Eq. (31) to be defined, it is necessary to fulfill the following requirement:

$$I_{AE} \geqslant \frac{1-\eta}{\eta}. \tag{35}$$

This appears explicitly in two limit cases where the expression of I_{AE} can be calculated analytically. When no decrease of contrast is allowed ($dC=0$), one obtains

$$I_{AE} = \frac{1-\eta}{\eta} + 2Q. \tag{36}$$

When no errors are allowed ($Q=0$), one gets

$$I_{AE} = \frac{1-\eta+2\eta dC+\sqrt{1-\eta}\sqrt{1+4\eta dC-\eta}}{2\eta}. \tag{37}$$

Equations (36) and (37) are valid in the limit of the constraint imposed by Eq. (25). This lower limit on I_{AE} shows that Eve can exploit the losses of the channel to tap some information on Alice without being detected. In particular, when the channel losses exceed 50%, Eve can have complete information on the key. In that case she never sends any pulse when she detects in 4 and she resends a pulse when she detects in 3 or 5 with probability p_3. This confirms the intuitive approach given previously and shows that the use of the two-state protocol is limited in practical to channels with very low transmission losses.

V. FOUR-STATE PROTOCOL

The goal of the four-state protocol is to overcome the limitations of the two-state protocol that have been analyzed in the previous part. The main drawback is that Eve obtains measurement results that are not ambiguous when she detects a photon in 3 or in 5. She can then choose to send states which do not induce errors such as $|\psi_{34}\rangle$ and $|\psi_{54}\rangle$. The additional states of the four states protocol make the detection in 3 and 5 ambiguous. Thus, when sending $|\psi_{34}\rangle$ or $|\psi_{54}\rangle$, Eve induces errors at Bob. When a photon has been detected in 3, states $|\psi_{32}\rangle$ and $|\psi_{34}\rangle$ play the same role and have to be sent with the same probability.

The analysis of the protocol is performed in a very similar way as before. Calculating the different conditional probabilities [setting p_a, p_b, p_c, and p_d to 1 successively in Eq. (13)] one obtains that the following relations have to be fulfilled:

$$p_{j,j\pm1}x_{j,j\pm1} = p_{32}x_{32}, \tag{38}$$

$$p_{j,j+1} + p_{j,j-1} = p. \tag{39}$$

Those relations are a particular case of relations (17)–(21) where dp is set to zero and they are much more symmetric. p is thus the probability that Eve resends a pulse when she has measured the pulse received from Alice whatever the result of the measure. The last relation guarantees that the losses are independent of the pulse sent by Alice.

At that point, fulfilling the relations (38) and (39) allows Eve not be detectable by symmetry considerations on the raw key received by Bob. As previously, the second step in the determination of ρ_B is to calculate the quantum bit error rate and the mutual information between Alice and Eve. Those two quantities are calculated on the sifted key that results from the second part of the key exchange process. Bob keeps only the results where he has obtained a measurement in 3 or 5 (without revealing the result). Alice validates only the measurements corresponding to the launch of a pulse (b) or (c). Those pulses are sent with the same probabilities $(1/2)$. We are thus brought back to the case of the two-state protocol and we obtain similar results. Q is given by Eq. (22) and I_{AE} by Eq. (23). The influence of the parameter x_{32} is the same. The maximum value of I_{AE} is given by Eq. (25).

The following quantity that has to be calculated to evaluate the security of the protocol is the contrast of Bob's interferometer and the effect of Eve interception of the original message. We proceed the same way as previously. The contrast is an average measurement performed by Bob on the raw key. Pulses (a), (b), (c), and (d) have the same probability to be launched and thus one has to set $p_a=p_b=p_c=p_d=\frac{1}{4}$ in the expression of C_{AEB}. Inserting the relations (22) and (23) into Eq. (26), one obtains the following expression for the contrast:

$$\begin{aligned} C_{AEB_4} = \frac{1}{4}\sqrt{Q}\Bigg\{ & \frac{1}{2}\left(\sqrt{A\frac{p_{21}}{p} - Q} + \sqrt{A\left(1-\frac{p_{21}}{p}\right) - Q} \right) \\ & + \frac{1}{2}\left[\sqrt{A\frac{p_{65}}{p} - Q} + \sqrt{A\left(1-\frac{p_{65}}{p}\right) - Q} \right] \\ & + \sum_{j=3}^{5} \left[\sqrt{A\frac{p_{j,j-1}}{p} - Q} + \sqrt{A\left(1-\frac{p_{j,j-1}}{p}\right) - Q} \right] \Bigg\} \\ & + \frac{1}{2} - \frac{1}{2}A. \end{aligned} \tag{40}$$

Expressing that the minimum value of C_{AEB_4} is equal to C_{AB}, one obtains an implicit relation defining the mutual information I_{AE} as a function of variables $p_{j,j-1}$, $2 \leqslant j \leqslant 6$, Q and dC being parameters. The extremum of I_{AE} is obtained when the partial derivatives of C_{AEB_4} with respect to $p_{j,j-1}$ are zero. As previously, the physically possible values of I_{AE} are limited by Eq. (25). This results in the relations

$$p_{j,j+1} = p_{j,j-1} = \frac{1}{2}p. \tag{41}$$

The information of Eve on Alice is maximum when the probabilities to resend states $|\psi_{j,j+1}\rangle$ and $|\psi_{j,j-1}\rangle$ are identical. This results in a maximization of the coherence of the result-

ing mixed state which is consistent with the intuition that Eve has to maximize the coherence of the states she resends. In addition, the probabilities defined by Eq. (41) are consistent with the identity of the conditional probabilities for Eve to have received $|j,j+1\rangle$ or $|j-1,j\rangle$ when she detects a photon in time slot j $(3 \leqslant j \leqslant 5)$. As a consequence, one gets from Eq. (38) that all the x_{ij} are equal to x.

Inserting Eq. (41) into Eq. (40) greatly simplifies the expression of C_{AEB_4} which becomes

$$C_{AEB_4} = \sqrt{2}\sqrt{Q}\sqrt{I_{AE}} + \frac{1}{2} - \frac{1}{2}I_{AE} - Q. \tag{42}$$

C_{AEB_4} appears to be a particular case of C_{AEB_2} where dp has been set to zero. It can also be expressed as a function of m, p, and x:

$$C_{AEB_4} = \frac{mp\sqrt{x}\sqrt{1-x} + \frac{1}{2}(1-m)}{1-m+mp}. \tag{43}$$

$\sqrt{x}\sqrt{1-x}$ is the contrast of the pulse resent by Eve. In the case of no eavesdropping, the contrast is $1/2$.

Equating (28) and (42), one obtains the relation defining I_{AE}:

$$I_{AE} = 2Q + dC + \sqrt{8QdC}. \tag{44}$$

This expression depends only on the quantum bit error rate Q and on the contrast loss dC. In particular it does not involve anymore any dependence on the losses of the channel, which shows that Eve cannot exploit the losses of the channel to select the pulses she resends depending on the time where she has detected the photon. Any loss of contrast increases the available information for Eve. In the case of a perfect interferometer, dC is zero and necessary x is equal to $1/2$. Setting m to 1 in Eq. (22), one obtains that each pulse intercepted and resent by Eve induces a probability error of 0.25. From Eqs. (44) and (25), the maximum information gained by Eve is equal to 0.5 bit and is twice the error probability. This is a result similar to what is obtained with BB84 when Eve intercepts and resends all photons sent by Alice. In the case where $dC=1$ (Bob does not measure the contrast), Eve does not have anymore to exploit the errors and she can set x to zero resulting in no induced error. The information gained by Eve is then equal to 1 bit per pulse. Eve knows completely the sifted key. Thus the security of the transmission cannot be guaranteed. This corresponds in practical to the case where Eve resends square pulses of duration $T/2$ in the time slot corresponding to her measurement result. Eve can get a perfect copy of the key without being detected.

After having found the expression of I_{AE}, one can calculate the three free parameters in ρ_B: x, p, and m, assuming that Eve mimics the transmission of the line (32), which is identical than in the two-state protocol.

From the definition of I_{AE}, Eq. (23), combined with its expression (44), one gets the expression of m:

$$m = 1 - \eta + \eta(4Q + dC + 2\sqrt{2QdC}). \tag{45}$$

The first part of the equation simply means that some measurements have to be made and no pulse resent in order mimicking the losses of the channel. The other part concerns the useful measurements where pulses are resent from Eve to Bob.

Similarly to m, one can then deduce the expression of p:

$$p = \frac{\eta(4Q + dC + 2\sqrt{2QdC})}{1 - \eta + \eta(4Q + dC + 2\sqrt{2QdC})}. \tag{46}$$

In the case where η is equal to 1, p has to be equal to 1. As soon as a measurement is performed, Eve has to resend a pulse to Bob. In the general case, p decreases in order to simulate the channel losses. Finally, from Eqs. (22), (45), and (46), one can express x as

$$x = \frac{2Q}{(4Q + dC + 2\sqrt{2QdC})}. \tag{47}$$

In the case of perfect contrast, whatever the value of Q, one finds $x=\frac{1}{2}$, which means that Eve has to send square pulses corresponding to states of the form $|j,j+1\rangle$ or $|j-1,j\rangle$. When there is a loss of contrast, x is smaller than $1/2$, which allows Eve to increase the probability that Bob obtains the same measurement result that she has obtained, thus increasing the information she obtains on the key. If dC is equal to 1, Eve can set Q to 0. As a result x is 0 and Eve resends square pulses of duration $T/2$ in the time slot corresponding to her measurement result.

VI. MUTUAL INFORMATION OF BOB ON ALICE

To evaluate the security of the protocol, one has to calculate the mutual information between Alice and Bob, I_{AB}, in the case of an eavesdropping of the line and to compare it to I_{AE}. The security of the key transmission can be guaranteed if $I_{AB} \geqslant I_{AE}$ [16]. I_{AB} is evaluated on the sifted key. Bob keeps only the results corresponding to a detection in 3 or 5 and Alice validates them only if it corresponds to a launch of pulse (b) or (c). As previously, the probabilities evaluated for detections in 3 or 5 are identical. It is thus sufficient to evaluate the conditional probabilities in the case where Bob detects in 3 for example. They are given by the relations

$$P(A=b|B=3) = \frac{P(B=3|A=b)P(A=b)}{P(B=3)}$$

$$= \rho_{B_{33}}(p(b)=1, p(c)=0) = 1 - Q, \tag{48}$$

$$P(A=c|B=3) = \frac{P(B=3|A=c)P(A=c)}{P(B=3)}$$

$$= \rho_{B_{33}}(p(b)=0, p(c)=1) = Q. \tag{49}$$

Those expressions allow calculating the *a posteriori* entropy of Alice knowing Bob's results. Since pulses (b) and (c)

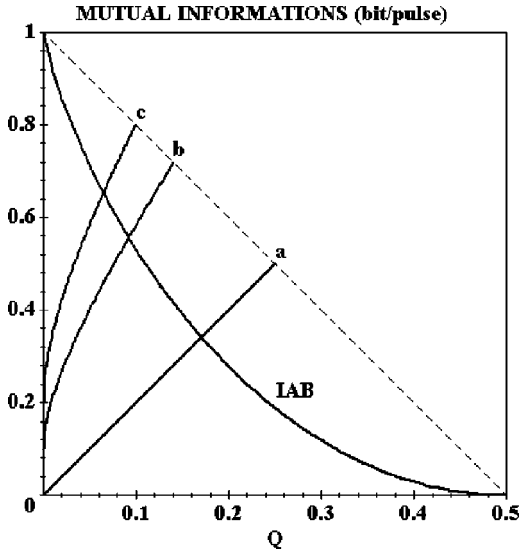

FIG. 4. Information of Bob on Alice (I_{AB}) and Eve on Alice for a relative contrast loss of 0% (a), 10% (b), and 20% (c) as a function of the quantum bit error rate (Q). Eve sends pulses spanning only two time slots. For each curve, the maximum information of Eve on Alice is obtained when Eve intercepts all pulses (dashed line). For no loss of contrast, the maximum allowed value of Q is 17%. For a relative contrast loss of 10%, the maximum allowed value of Q is 9%.

are sent with equal probability, the *a priori* entropy is 1 bit/pulse. The information of Bob on Alice is thus given by

$$I_{AB} = H_{a\ priori} - H_{a\ posteriori} = 1 + (1-Q)\log_2(1-Q) + Q\log_2(Q). \quad (50)$$

This is the classical expression of the information rate of a binary channel with cross talk. I_{AB} is a decreasing function of Q. It does not depend on other parameters such as η or dC, since only the detected photons can be taken into account and since the off-diagonal elements of the density matrix play no direct role in the information transmission between Alice and Bob.

I_{AB} and I_{AE} can be plotted as a function of Q, dC being a parameter (Fig. 4). The possible values of I_{AE} are limited by relation (25). In the ideal case with no contrast loss in Bob's interferometer ($dC=0$), the maximum quantum bit error rate compatible with the security of the transmission is 17%, which is comparable with the BB84 protocol [3]. When there is a loss of contrast at Bob's interferometer, the maximum acceptable quantum bit error rate decreases. Anyhow the protocol can tolerate quite large contrast losses. For example a contrast of 45% instead of 50% corresponds to $dC=0.1$. In that case the maximum value of Q is 9%. This tolerance is quite high. In any case, it is of first importance to minimize the quantum bit error rate since this allows to maximize the difference between I_{AB} and I_{AE} whatever the value of the contrast loss.

VII. EVE ATTACK WITH MAXIMUM COHERENCE PULSES IN THE FOUR-STATE PROTOCOL

As seen previously, the ideal solution for Eve is to maximize the coherence of the state she resends in order to fully exploit the loss of contrast of the interferometer. Therefore, she would resend a pure state instead of a statistical mixture. Considering that when she detects a photon in time slot j she can induce errors only in the two closest neighbors, the pure state that she can resend has the following expression:

$$|\psi_j\rangle = \sqrt{\frac{x}{2}}|j-1\rangle + \sqrt{1-x}|j\rangle + \sqrt{\frac{x}{2}}|j+1\rangle. \quad (51)$$

We have supposed a state symmetric in $j-1$, $j+1$ to respect the symmetry of the problem. The density matrix sent by Eve is the following:

$$\rho_E = \sum_{j=2}^{6} \mathrm{Tr}(|j\rangle\langle j|\rho_A|j\rangle\langle j|)[p_j|\psi_j\rangle\langle\psi_j| + (1-p_j)\pi_0]. \quad (52)$$

The density matrix received by Bob is given by

$$\rho_B = m\rho_E + (1-m)\rho_A \quad (53)$$

where m is the probability for Eve to do a measurement.

Exploiting the same symmetry argument on the errors introduced in the raw key as previously, one finds the necessary condition on the probabilities:

$$p_j = p. \quad (54)$$

From the resulting expression of ρ_B, one can calculate the expression of the quantum bit error rate Q and that of the mutual information between Alice and Eve I_{AE}. One finds the expressions

$$Q = \frac{\frac{1}{2}mpx}{1-m+mp}, \quad (55)$$

$$I_{AE} = \frac{mp(1-x)}{1-m+mp}. \quad (56)$$

Those expressions are the same as for the attack on two adjacent states in the case of the four-state protocol. In particular the same limit on physically attainable values of I_{AE}, Eq. (25), still holds.

The contrast defined as previously has the following expression which only slightly differs from that of the previous case (43):

$$C_{AEB_{\max}} = \frac{2mp\sqrt{\frac{x}{2}}\sqrt{1-x} + \frac{1}{2}(1-m)}{1-m+mp}. \quad (57)$$

Here the contrast measurement of a pulse sent by Eve is $2(\sqrt{x/2})\sqrt{1-x}$. $C_{AEB_{\max}}$ can also be expressed as a function of I_{AE} and dC:

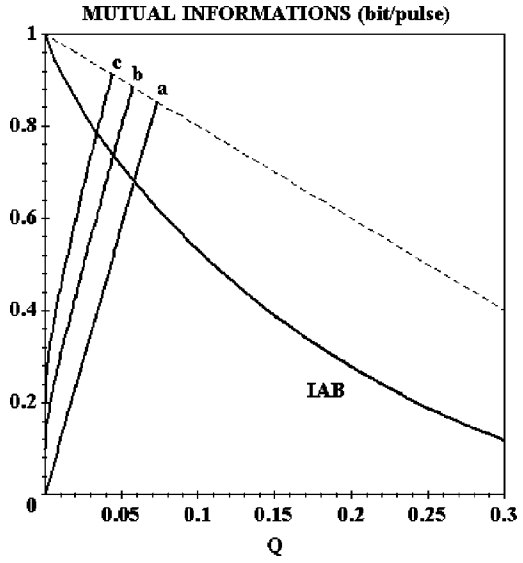

FIG. 5. Information of Bob on Alice (I_{AB}) and Eve on Alice for a relative contrast loss of 0% (a), 10% (b), and 20% (c) as a function of the quantum bit error rate (Q). Eve sends maximum coherence pulses (spanning three time slots). For each curve, the maximum information of Eve on Alice is obtained when Eve intercepts all pulses (dashed line). For no loss of contrast, the maximum allowed value of Q is 5.8%. For a relative contrast loss of 10%, the maximum allowed value of Q is 4.4%.

$$C_{AEB_{\max}} = 2\sqrt{Q}\sqrt{I_{AE}} + \frac{1}{2} - \frac{1}{2}(I_{AE} + 2Q). \tag{58}$$

As previously I_{AE} can be expressed as a function of dC and of Q [in the limit of the constraint (25)]:

$$I_{AE} = 6Q + dC + 4\sqrt{Q(2Q + dC)}. \tag{59}$$

In that case the available information for Eve is higher than that of the previous case for given values of Q and dC. The mutual information between Alice and Bob has the same expression as previously since it does not depend on the coherence of the pulses. One can plot those quantities as a function of Q (Fig. 5). In the ideal case the maximum allowed quantum bit error rate is 5.8%. With $dC=0.1$ it is 4.4%.

As previously, the parameters m, p, and x can be calculated as a function of the characteristic parameters of the lines η, Q, and dC:

$$m = 1 - \eta + \eta[8Q + dC + 4\sqrt{Q(2Q + dC)}], \tag{60}$$

$$p = \frac{\eta[8Q + dC + 4\sqrt{Q(2Q + dC)}]}{1 - \eta + \eta[8Q + dC + 4\sqrt{Q(2Q + dC)}]}, \tag{61}$$

$$x = \frac{2Q}{8Q + dC + 4\sqrt{Q(2Q + dC)}}. \tag{62}$$

In principle, Alice and Bob can detect that kind of attack since the pulses resent by Eve induce coherences between nonadjacent time slots. It can be measured with an additional interferometer with two arms having a time propagation difference of T. In case of no eavesdropping, the contrast is zero. In case of eavesdropping, the contrast is defined by

$$C_T = \frac{\sum_{j=1}^{5} \rho_{B_{j,j+2}}}{1 - \rho_{B_{0,0}}}. \tag{63}$$

Alice sends the pulses with probabilities $p_a=p_b=p_c=p_d=\frac{1}{4}$. The expression of the contrast is thus

$$C_T = \frac{\frac{1}{2}mpx}{1 - m + mp} = Q. \tag{64}$$

This is a value in the order of a few percent, which may be difficult to measure in practice. Therefore, Alice and Bob have two alternatives. Either keep the simplicity of the initial scheme with only one interferometer at the price of restriction of the acceptable quantum bit error rate to ensure security or increase the complexity of the system introducing an additional interferometer in order to allow higher values of the quantum bit error rate without compromising the security. On the other hand, Eve does not know which solution Alice and Bob choose. To be certain not to be discovered she should only choose the first case where pulses are sent only on two adjacent time slots.

VIII. CONSEQUENCES OF THE DARK COUNTS ON THE PROTOCOLS

After having analyzed the security in a general way, we focus on a particular limitation which is due to photocounters dark counts and which is very important in practical implementations. Dark counts result from the probability to trigger the avalanche in the photocounter even without any incident photon. It is not possible to separate effective photodetections from dark counts. Therefore all the triggerings of the photocounter are considered resulting from an incident photon. For a given kind of photocounter, the dark counts are characterized by a probability of occurrence per second. They are typically of 300 s^{-1} for Perkin Elmer SPCM14 Silicium photocounters and of 40 000 s^{-1} for InGaAs photocounters [3]. To extend our model we define p^{dark} as the probability of a dark count during a time slot of duration $T/2$. Then we simply add p^{dark} to each probability detection calculated during the same time slot and derived from the previous calculations. The dark counts become predominant when their probability is of the same order as the probability to detect a photon. Considering time slots of duration 10 ns and the case of InGaAs we see that the dark-count probability is typically of the order of 4×10^{-4}. The probability to detect a photon is mainly of the order of the line transmission η. We have seen previously that the two-state protocol is limited to transmissions greater than 0.5. In that case dark counts are not the limitation since their probability is several orders of magnitude smaller than the probability to detect a photon. We can thus conclude that, within its domain of validity, the two-state protocol is not affected by dark counts.

In Sec. V we have seen that the four-state protocol is not affected by the losses of the line when perfect photodetectors

with no dark counts are used. It is thus possible to consider low transmissions (or long propagation distances) that can be of the same order of the dark-count probability. Then those latter play a crucial role and induce a limitation to the range of the system. We will thus focus on the consequences of dark counts on the four-state protocol.

The main advantage of the four-state protocol as compared to the two-state protocol is to impose symmetry conditions that Eve has to fulfill if she wants to remain undetected. These conditions are enounced in Sec. III C and rely on equalities of conditional probabilities knowing the state sent by Alice. The result of the dark counts is to add an identical probability p^{dark} to all of those conditional probabilities. Therefore the requirement on their equality remains valid and Bob can still check the symmetry of the results on part of his raw key. As a consequence Eve still has to fulfill the symmetry relations (38) and (39) and the derivation of Sec. V is still valid.

To proceed, we first start evaluating the quantum bit error rate in the presence of dark counts, denoted Q', in the case of the imperfect line between Alice and Bob with no eavesdropping. In the previous parts we have considered a quantum bit error rate resulting only from the propagation of the pulses in the line or from the shape of the pulses themselves. We have introduced it as an external parameter given by the experiment without analyzing the precise process that is at its origin. This would be a tricky task very dependent on the chosen model. To avoid that, we can go back to the definition of Q:

$$Q = \frac{\rho_{B_{55}}(p_b = 1)}{\rho_{B_{55}}(p_b = 1) + \rho_{B_{33}}(p_b = 1)}. \tag{65}$$

In the range allowing secure communication, Q is always small compared to one which allows one to develop Eq. (65) at first order in Q. Therefore $\rho_{B_{55}}(p_b=1)$ is a term at first order in Q whereas $\rho_{B_{33}}(p_b=1)$ is a term at zero order in Q whose value is given by the probability to detect a photon in time slot 3 knowing that Alice has sent a pulse (b). Taking into account the line transmission η, the beam splitter transmission η_b, and the photocounter efficiency η_c we obtain

$$\rho_{B_{33}}(p_b = 1) = \frac{\eta_c \eta_b \eta}{2}, \tag{66}$$

$$\rho_{B_{55}}(p_b = 1) = \frac{\eta_c \eta_b \eta Q}{2}. \tag{67}$$

The expression of Q', in the presence of dark counts, is obtained adding p^{dark} in the numerator of Eq. (65) and developing at first order, leading to

$$Q' = Q + \frac{\beta}{\eta}, \tag{68}$$

where β is a parameter which is specific from Bob's setup and has the expression

$$\beta = \frac{2p^{dark}}{\eta_c \eta_b}. \tag{69}$$

In addition to its intrinsic part due to the transmission through the line, the quantum bit error rate has a new contribution due to the dark counts which introduces a dependence with the line transmission.

The second step consists in analyzing how Eve can exploit this additional term to eavesdrop the line. We make the assumption that she has no access to the apparatus of Bob. The measurements of the pulses she sends are thus affected by the same limitations: transmission of the beam splitter, efficiency and dark counts of the photocounters. As in the previous part we assume that she is able to replace the imperfect line with a perfect line with no loss and no intrinsic quantum bit error rate. She introduces a controlled quantum bit error rate called Q_E which simulates the quantum bit error rate expected by Bob and allows her to tap some information. The maximum value of Q_E allowed with her perfect line is thus given by

$$Q_E = Q + \beta\left(\frac{1}{\eta} - 1\right). \tag{70}$$

In addition to the intrinsic quantum bit error rate, Eve can exploit an additional term that is due to the dark counts and which increases as the transmission of the line decreases. As a consequence, as the propagation distance increases, the transmission can become small enough so that the term due to the dark counts is predominant. The quantum efficiency of the photocounter and the transmission of the beam splitter appear explicitly. The beam splitter is unavoidable since it is intrinsic to the protocol, but it is important to have quantum efficiency as great as possible to minimize the effect of the dark counts.

Dark counts not affect only the quantum bit error rate, but the contrast as well since similar photocounters are used to measure it. To evaluate their incidence on the contrast measurement, we proceed the same way as for the quantum bit error rate. For the sake of simplicity, we assume that the two photocounters have the same quantum efficiency and have the same probability of dark counts. An imbalance between the two photocounters would not change the main results provided it consists in a small correction. We consider that the photocounters remain activated during a time sufficient to register all possible detection events, but not much in order to keep the dark-count probability as low as possible. Depending on the protocol, the required number of time slots, n, can vary. For the four-state protocol, the detection can occur during seven successive time slots if one takes into account the possible errors. An additional time slot is necessary to take into account the delay introduced by the interferometer. A total of eight time slots is thus necessary to record all possible events. We consider the photon detection probabilities in the two output ports of the interferometer P_{2+} and P_{2-} in the ideal case with perfect detectors and a loss less channel. Their sum is equal to 1 and their difference is equal to $\frac{1}{2}(1-dC)$ which depicts the intrinsic coherence loss due to the quantum channel. Introducing the dark counts, and

TABLE I. Maximum propagation distances (in km) as a function of the kind of attack and of the type of photocounter for time slots of 10 ns.

	Attack with two time-slot pulses	Maximum coherence attack
Si photocounters	16.6	15.7
InGaAs photocounters	23.9	18.2

TABLE II. Maximum propagation distances (in km) as a function of the kind of attack and of the type of photocounter for time slots of 2.5 ns.

	Attack with two time-slot pulses	Maximum coherence attack
Si photocounters	19.6	18.7
InGaAs photocounters	46.6	39.1

assuming that they are identical for both photocounters, the new expression of the contrast becomes

$$C' = \frac{\eta_c(1-\eta_b)\eta(P_{2+}-P_{2-})}{\eta_c(1-\eta_b)\eta + 2np^{dark}} = \frac{1}{2}(1-dC)\frac{1}{\left(1+\frac{n\beta'}{\eta}\right)}, \tag{71}$$

where β' has the same expression than β with η_b replaced by $(1-\eta_b)$. Since n can be large (8 in the four-state protocol), the expansion of the denominator in first order is not necessary justified. The new expression for the relative contrast loss, defined by $C'=\frac{1}{2}(1-dC')$, is given by

$$dC' = dC + \frac{n\beta'(1-dC)}{\eta + n\beta'}. \tag{72}$$

As previously, we define the relative contrast loss dC_E that can be induced by Eve, considering a lossless channel:

$$C' = \frac{1}{2}(1-dC_E)\frac{1}{(1+n\beta')}. \tag{73}$$

We obtain

$$dC_E = dC + \frac{n\beta'(1-\eta)(1-dC)}{(\eta + n\beta')}. \tag{74}$$

Similarly to the quantum bit error rate, the dark counts allow Eve to introduce an additional decoherence which increases as the transmission of the channel between Alice and Bob decreases. It is clear from the previous analysis that the dark counts induce a dependence with the channel losses of both quantum bit error rate and contrast loss. It cancels only in the case of a perfect channel with no loss since we have assumed that Eve cannot control the detection setup at Bob's site and is affected by the partial transmission of the beam splitter and by the photocounters quantum efficiency as well. The dependence with the losses of the line imposes a limitation of the range in which the security of the transmission can be guaranteed. To evaluate that range, we assume that Q and dC are negligible in front of the terms due to the dark counts in Eqs. (70) and (74), respectively. Therefore Q_E and dC_E depend only on one variable η. Knowing the parameters characteristic of Bob's setup, one is then able to calculate the range for which the transmission is secure. In Eqs. (70) and (74), we set dC and Q to 0. The resulting relations can be inserted into Eq. (44) to obtain the dependence of the mutual information of Alice and Eve in the case of an attack using pulses spanning only to adjacent time slots (Sec. V) or in Eq. (59) in the case of an attack with maximum coherence pulses. The minimum tolerable transmission is obtained when the mutual information of Alice and Eve is equal to the mutual information of Alice and Bob. The maximum propagation length can be deduced from that value knowing the attenuation of the line α (in dB/km).

We have calculated the maximum propagation length in the case of the four-state protocol ($n=8$) for both kinds of attacks. We have considered typical implementations in the case of silicium photocounters (850 nm) or InGaAs photocounters (1550 nm). The number of dark counts per second is typically of 300 for Perkin Elmer SPCM14 silicium photocounters and of 40 000 for InGaAs photocounters [3]. Considering time slots of 10 ns, the corresponding probability of dark count per time slot is thus 3×10^{-6} for silicium photocounters and 4×10^{-4} for InGaAs photocounters. The quantum efficiency is 0.5 for Perkin Elmer SPCM14 silicium photocounters and 0.06 for InGaAs photocounters [3]. The transmission of the beam splitter is 50%. The losses of the fibers are 2 dB/km at 850 nm and 0.2 dB/km at 1550 nm. The maximum propagation lengths obtained for the different cases are gathered in the Table I. The propagation length is in the range of 15 km for Si photocounters and in the range of 20 km for InGaAs photocounters. The smallest range is obtained for the attack with maximum coherence pulses. Anyhow the difference with the attack using two time slots pulses is not very big. This can be attributed to the fact that the decrease of contrast is predominant on the quantum bit error rate since n is high. The ranges that are found can be considered as small compared to results obtained with other systems (e.g., 67 km [3]). It is worth being noticed that the dark-count probability is very dependent on the duration of the pulses and thus on the time slots which are considered. Assuming pulses with a duration of 2.5 ns, which is compatible with the performances of present modulators and photocounters, one divides by 4 the dark-count probability. The maximum ranges calculated in that case are gathered in Table II. In that case the difference between the two kinds of attacks is still not very important. One can see a range that is doubled in the case of InGaAs counters whereas it has not varied that much in the case of Si photocounters. In the case of high loss fibers (850 nm) decreasing the dark-count probability does not bring that much since the fiber losses are predominant. In the case of low-loss fibers (1550 nm) it is thus very important to decrease the dark-count probability to increase the range. The ranges obtained with both kinds of attacks are compatible with an implementation at Telecom wavelength.

IX. CONCLUSION

We have proposed quantum key distribution protocols based on coherent single-photon optical pulses with duration T and with minimum time-frequency uncertainty. The pulses are sent with possible delays (e.g., 0, $T/2$) which are used to code the information (e.g., bit 0, bit 1) and which are shorter than their width. Therefore, the time detection of the photons may result in an ambiguity of the delay evaluation for a potential eavesdropper. In parallel, pulses are sent at random by Bob to a long-arm interferometer ($T/2$ delay) allowing checking, thanks to a coherence measurement, that the received pulses have the requested duration. We have given a formalism allowing describing quantum mechanically those protocols. A first protocol has been proposed based on two different pulses with delay 0 or $T/2$. It has been shown in that case that the losses of the channel can be exploited by Eve to tap some information on the transmitted key. Even in the absence of any other defect of the line, the transmission is not secure if the channel losses exceed 50%. To overcome that limitation another protocol has been proposed with delays 0, $T/2$, T, and $3T/2$. We have shown in that case that Eve cannot exploit the channel losses (assuming perfect photocounters). Comparing the mutual information between Alice and Eve and between Alice and Bob, we have evaluated the security as a function of the quantum bit error rate and of the relative contrast loss of the interferometer. In a first part, those parameters have been considered as independent. The quantum bit error rate can be attributed to defects in the transmission line (possible pulse spreading of the pulse or time jitter of the clock) or to the dark counts of Bob's photocounters. The possible loss of contrast can be attributed to decoherence during the propagation, imperfect source linewidth, or to the dark counts of Bob's photocounters. We have first considered an attack where Eve sends pulses which are similar to those of Alice. In the case of a transmission with no decoherence the maximum allowed quantum bit error rate is 17% which is comparable to that obtained with BB84 protocol. For a realistic value of 10% relative loss of contrast in the interferometer, the allowed quantum bit error rate is still 9%. We have considered another kind of attack where Eve sends pulses which maximize the coherence for a given error value. Bob can in principle detect those pulses but this requires an additional interferometer with T time delay between the two arms and the measurement of a contrast equal to the quantum bit error rate. This may be difficult from a practical point of view, thus making that kind of attack possible. In the case of no decoherence the maximum allowed quantum bit error rate is then 5.8%. In the case of a 10% relative contrast loss it is 4.4%. Those values are much smaller than those obtained in the previous case but are still compatible with a realistic experimental setup with a quantum bit error rate in the order of a few percent. On the other hand, Eve can never be sure not to be detected in that case, which would prevent her to send pulses with maximum coherence. In any case, it is of first importance to minimize the quantum bit error rate since this allows maximizing the difference between Alice and Bob mutual information and Alice and Eve mutual information whatever the value of the contrast loss.

Those protocols have several practical advantages. The information is coded only in the time domain, which simplifies the implementation and avoids for Bob to randomly switch his detection between two bases. Their implementation in an experimental setup is realistic. Considering that the response time of available photocounters can be smaller than 1 ns leads to the use of pulse durations in the 10–20 ns range. For those duration values, the precision in the arrival time is about 1 ns. Coherent faint pulses can be produced combining a single-mode diode laser and a high-speed electro-optics amplitude modulator that can be driven with an electrical pulse generator having rise time and decay time smaller than 1 ns. The measurement of the arrival time of the photon does not require that the polarization of the photon be conserved. If the interferometer is made insensitive to the polarization, the whole system is potentially insensitive to the polarization. As a consequence there is no need for go and return of the pulses, which opens the way to high transmission rates.

In the 10 ns range, the clock can be precisely controlled. In addition pulse spreading due to propagation is negligible over long distances in this range [14]. The time propagation of the pulses is little affected by the propagation disturbances of the fiber such as fiber thermal dilatation or group velocity dispersion. The main limitation is expected from the dark counts of the photocounters which introduce a dependence of the quantum bit error rate and the relative contrast loss with the attenuation of the line. Considering standard characteristics of present photocounters and fiber optics, we have calculated secure transmission distance in the 20 km range when using 10 ns time slots. That range can be extended to 40 km when using 2.5 ns time slots and optical fibers at 1550 nm. Such small time slots are possible with present technology.

These technical considerations combined with the advantages of the principle described above make the time coding protocol a realistic method for quantum key distribution.

ACKNOWLEDGMENTS

The authors are grateful to Philippe Grangier and Ariel Levenson for helpful discussions and advice on the protocols and on the manuscript.

APPENDIX

Coherent one-photon state expression

One way to produce faint pulses which can approximate coherent single-photon pulses is to couple a single-frequency laser field through an electro-optic modulator which is driven with a voltage having the appropriate time profile. We consider a one-dimensional problem. We describe the incoming field (index 1) with a single-mode coherent state and the output (index 2) as a sum of modes initially in the vacuum state. We consider a point interaction to avoid phase-matching limitations in the coupling of the two modes. The modulator can thus be considered as a beam splitter with a time varying coupling constant. The incoming field has a high intensity which allows us to neglect its depletion and to

consider it as classical. The interaction can thus be described by a Hamiltonian of the form

$$H = \hbar\chi g(t)\alpha_1 \sum_{k_2} a_{k_2}^{\dagger} e^{-i(\omega_1-\omega_2)t} + \text{H.c.} \tag{A1}$$

χ is a coupling constant, $g(t)$ is a normalized time profile function obeying the relation

$$\int dt|g(t)|^2 = 1, \tag{A2}$$

α_1 is the incoming field amplitude, $a_{k_2}^{\dagger}$ is the creation operator on output mode k_2 with frequency $\omega_2 = ck_2$, and ω_1 is the input mode frequency.

The final state is obtained applying the evolution operator obtained from Eq. (A1) to the initial state. The evolution operator is a product of displacement operators for each mode of the output field. A product of coherent states thus describes the resulting output state. When sufficiently attenuated, this state can be approximated by an expansion limited to its first order term in χ which is a superposition of the vacuum and of a one-photon state of the form [17]

$$\sum_{k_2} c_{k_2} a_{k_2}^{\dagger}|0\rangle. \tag{A3}$$

Changing from the discrete basis to a continuous basis and using the frequency as the variable, the expression of the one-photon state becomes

$$|\psi\rangle = \int d\omega_2 c(\omega_2) a^{\dagger}(\omega_2)|0\rangle. \tag{A4}$$

$c(\omega_2)$ obeys to the normalization relation

$$\int d\omega_2 |c(\omega_2)|^2 = 1. \tag{A5}$$

Its expression deduced from the previous Hamiltonian is given by

$$c(\omega_2) = \tilde{g}(\Omega), \tag{A6}$$

where $\Omega = \omega_2 - \omega_1$ and $\tilde{g}(\Omega)$ is the Fourier transform of $g(t)$ defined by

$$\tilde{g}(\Omega) = \frac{1}{\sqrt{2\pi}} \int dt g(t) e^{i\Omega t}. \tag{A7}$$

$c(\omega_2)$ is the Fourier transform of the envelope of the pulses generated by the modulator centered at frequency ω_1. This way, coherent one-photon pulses are produced starting from a coherent single-mode incoming field. For sufficient attenuation, the output faint pulse can be approximated by a coherent one-photon state.

Detection probability

The expression of the one dimension electric field is given by

$$E^{(+)}(x,t) = \varepsilon_{\omega} \int d\omega a(\omega) e^{-i\omega(t-x/c)}. \tag{A8}$$

We have supposed that the frequency distribution of the state on which it applies is much smaller than the optical mean frequency.

The first-order count rate is defined by [17]

$$w_1(x,t) = |E^{(+)}(x,t)|\psi\rangle|^2. \tag{A9}$$

One can deduce the photon detection density probability in x and t:

$$\frac{dP}{dt}(x,t) = \frac{1}{2\pi}\left|\int d\omega c(\omega) e^{-i\omega(t-x/c)}\right|^2 = \left| g\left(t - \frac{x}{c}\right)\right|^2. \tag{A10}$$

Interferometer contrast

One key element of the setup is the interferometer that allows to detect a possible change in the pulse duration induced by the eavesdropper. We consider a perfect Mach-Zender interferometer with an equal balance of the two propagation arms that combines two input ports into two output ports introducing a delay difference in the two arms. The two output fields $E_{2-}^{out}(x_2,t)$ and $E_{2+}^{out}(x_2,t)$ can be expressed as a function of the incoming fields $E_{1-}^{in}(x_1,t)$ and $E_{1+}^{in}(x_1,t)$. We consider a one-photon state incoming into the $+$ input port of the interferometer and the vacuum in the $-$ port. Keeping only the terms with nonzero input, the output fields are given by the relations

$$E_{2-}^{out}(x,t) = \frac{1}{2}[E_{1+}^{in}(x - L_b,t) - E_{1+}^{in}(x - L_a,t)], \tag{A11}$$

$$E_{2+}^{out}(x,t) = \frac{1}{2}[E_{1+}^{in}(x - L_a,t) + E_{1+}^{in}(x - L_b,t)]. \tag{A12}$$

The origin is taken on the second beam splitter. L_a and L_b are the lengths of the two arms of the interferometer.

One can calculate the first-order count rate and deduce the photon probability detection in the two output ports P_{2+} and P_{2-}:

$$P_{2\pm} = \frac{1}{2} \pm \frac{1}{4}\left(\int dt g\left(t + \frac{L_a}{c}\right) g^*\left(t + \frac{L_b}{c}\right) e^{i\omega_1(L_a - L_b)/c} + \text{c.c.}\right). \tag{A13}$$

The sum of the probabilities is equal to 1. The contrast of the interferometer can be defined as the difference in the probabilities between arm $+$ and arm $-$. It can be expressed in the time domain as well as in the Fourier domain:

$$C = \frac{1}{2}\left(\int dt g(t) g^*(t+\tau) e^{i\omega_1\tau} + \text{c.c.}\right) = \int d\Omega |\tilde{g}(\Omega)|^2 \cos[(\Omega + \omega_1)\tau], \tag{A14}$$

where the time propagation difference between the two arms τ is given by

$$\tau = \frac{L_b - L_a}{c}. \tag{A15}$$

The expression (A14) in the time domain shows that the contrast is the real part of the autocorrelation function of a monochromatic optical field modulated by the time envelope of the pulse. In the Fourier domain the contrast is the sum of the interferograms produced at each frequency of the distribution corresponding to the pulse. In addition there is a common phase depending on τ and on the optical carrier frequency.

In our setup the interferometer is set at a constant value of τ equal to half of the pulse duration. The possible reduction of the pulse duration by the eavesdropper is measured through a measurement of the interferometer contrast. In order to maximize its value, one has to set $\omega_1\tau$ to $2k\pi$. Thus the contrast is only depending on the shape and duration of the temporal pulse.

The protocols imply the use of mixed states. It is thus important to generalize the expression of the contrast (A14) to that case. A general pulse $f(t)$ can be described as the sum of N square pulses with coefficients α_j defined by the relations

$$f(t) = \sum_{j=1}^{N} \alpha_j u_j(t), \tag{A16}$$

$$\sum_{j=1}^{N} |\alpha_j|^2 = 1. \tag{A17}$$

The corresponding state is

$$|\psi\rangle = \sum_{j=1}^{N} \alpha_j |j\rangle. \tag{A18}$$

The interferometer evaluates the autocorrelation of the received pulse for a delay equal to the propagation time difference between the two arms. When that delay is exactly equal to $T/2$, the measurement result of the interferometer is simply related to the scalar product of the incoming state and the same state where all the indices are shifted by one. Inserting Eq. (A16) and $u_j(t) = u_{j+1}(t+T/2)$ into Eq. (A14) the contrast can be expressed as a function of the α_j:

$$C = \frac{1}{2}\left[\sum_{j=1}^{N-1} \alpha_j \alpha_{j+1}^{*} e^{i\omega_1 T/2} + \text{c.c.}\right]. \tag{A19}$$

In the case where Bob receives a density matrix that is a mixture of pure states, the previous expression can be extended taking into account the linearity of the trace in the calculation of the first-order counting rate w_1. The contrast is the weighted sum of the contrast of each pure state. It writes as a function of the off-diagonal terms of the density matrix:

$$C = \frac{1}{2}\left[\sum_{j=1}^{N-1} \rho_{j,j+1} e^{i\omega_1 T/2} + \text{c.c.}\right]. \tag{A20}$$

In the particular case of our protocol, we set T to $\omega_1 T/2 = 2k\pi$, and the probability amplitudes are real. The expression of the contrast simplifies to

$$C = \sum_{j=1}^{N-1} \rho_{j,j+1}. \tag{A21}$$

[1] C.H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175.

[2] C.H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).

[3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[4] C.H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, J. Cryptology **5**, 3 (1992).

[5] J. Bréguet, A. Muller, and N. Gisin, J. Mod. Opt. **41**, 2405 (1994).

[6] P.D. Townsend, J. Rarity, and P. Tapster, Electron. Lett. **29**, 634 (1993).

[7] A. Muller *et al.*, Appl. Phys. Lett. **70**, 793 (1997).

[8] D. Bethune and W. Risk, IEEE J. Quantum Electron. **QE-36**, 340 (2000).

[9] T. Debuisschert and W. Boucher, e-print quant-ph/0309138; e-print quant-ph/0309139.

[10] G. Ribordy, J.-D. Gautier, N. Gisin, O. Guinnard, and H. Zbinden, Electron. Lett. **34**, 2116 (1998).

[11] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, Phys. Rev. Lett. **84**, 4737 (2000).

[12] E. Brainis, L.-P. Lamoureux, N.J. Cerf, Ph. Emplit, M. Haelterman, and S. Massar, Phys. Rev. Lett. **90** 157902-1 (2003).

[13] Typically 300 ps for Perkin Elmer SPCM avalanche photodiodes.

[14] A. Yariv, *Quantum Electronics* (Wiley, New York, 1988), Chap. 22, p. 642.

[15] G. Brassard, N. Lütkenhaus, T. Mor, and B.C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).

[16] I. Csiszar and J. Körner, IEEE Trans. Inf. Theory **IT-24**, 339 (1978).

[17] C. Cohen-Tannoudji, J. Dupont-Roc, and G. Grynberg, *Photons et Atomes, Introduction à l'Électrodynamique Quantique* (InterEditions/Editions du CNRS, Paris, 1987), Chap. III.