Single-photon generation by pulsed excitation of a single dipole

Rosa Brouri, Alexios Beveratos, Jean-Philippe Poizat,* and Philippe Grangier
Laboratoire Charles Fabry de l'Institut d'Optique, UMR 8501 du CNRS, Boîte Postale 147, F91403 Orsay Cedex, France
(Received 12 July 2000; published 15 November 2000)

The fluorescence of a single dipole excited by an intense light pulse can lead to the generation of another light pulse containing a single photon. The influence of the duration and energy of the excitation pulse on the number of photons in the fluorescence pulse is studied. The case of a two-level dipole with strongly damped coherences is considered. The presence of a metastable state leading to shelving is also investigated.

PACS number(s): 42.50.Dv, 03.67.Dd, 33.50.−j

I. INTRODUCTION

The security of quantum cryptography is based on the fact that each bit of information is coded on a single quantum object, namely, a single photon. The fundamental impossibility of duplicating the complete quantum state of a single particle prevents any potential eavesdropper from intercepting the message without the receiver noticing [1]. In this context, the realization of an efficient and integrable light source delivering a periodic train of pulses containing one and only one photon would be an important advantage [2].

The purpose of this paper is to evaluate the reliability of such a source. Assuming that a smart eavesdropper can obtain the information as soon as the number n of photons in the pulse is larger than two (see Appendix A), we define a fractional information leakage f_{il} as

$$f_{il}=\frac{P_{n\geqslant 2}}{P_{n\geqslant 1}}, \tag{1}$$

where $P_{n\geqslant 1}$ and $P_{n\geqslant 2}$ are the probabilities of obtaining at least one and at least two photons, respectively. The value of f_{il} has to be close to zero, while the probability $P_e=P_{n\geqslant 1}$ to emit one photon during the sampling period should be as high as possible; we note that the probability to obtain exactly one photon is $(1-f_{il})P_e$. For a Poissonian light source, we have

$$f_{il}=1-(1-P_e^{-1})\ln(1-P_e)\simeq\frac{P_e}{2}\quad P_e\ll 1, \tag{2}$$

It is therefore possible to have a good reliability with an attenuated Poissonian light source, but P_e has to be very small, which makes the source quite inefficient. A better way to have both good reliability and a high emission probability is to design a device with fully controlled quantum properties, able to emit truly single photons [3–13]. One possibility of performing such an emission is to use the fluorescence of a single dipole (e.g., a single molecule or a single colored center). As a single dipole cannot emit more than one photon at a time, leading to antibunching in the photon statistics of the fluorescence light [14–16], a pulsed excitation of the dipole can be expected to produce individual photons on demand [3].

In previous works [4,5] the emitting dipole was generally considered to be a radiatively damped two-level system. In the present paper we will consider emitting dipoles with strongly damped coherences, as is the case for single molecules [10] or a single colored center [12,13] at room temperature. The decay time of coherences, associated with nonradiative processes which occur in the picosecond range, is thus much shorter than the population decay time, that is typically in the 10-ns range. On the other hand, systems such as molecules or colored centers often have an extra metastable state, which is very long lived and thus can induce ''shelving'' in the emission process. In order to describe these features, we will model the emitting dipole using the three-level scheme shown in Fig. 1.

Owing to the fast damping of coherences, only level populations σ_{aa} will be considered, and the system's dynamics will be described by using rate equations between the three levels. The system can be excited from ground state $|1\rangle$ to excited state $|2\rangle$ with a pumping rate r. The decay rate from level $|2\rangle$ to level $|1\rangle$ is Γ, but the system can also decay to a metastable state $|3\rangle$ at rate $\beta\Gamma$. The branching ratio $\beta/(1+\beta)$ is usually (but not necessarily) very small. The emission rate from the metastable state will be neglected (i.e., no photons are emitted from level $|3\rangle$), but we will assume that the system can go back from level $|3\rangle$ to level $|2\rangle$ with a rate r_d. This ''deshelving'' effect has been observed experimentally [17], and may be important under strong pumping conditions.

The purpose of the present calculation is to evaluate the efficiency of such a system in converting a train of classical light pulses into a train of single photon pulses (''photon gun'') [9]. We will thus assume that this system is excited by

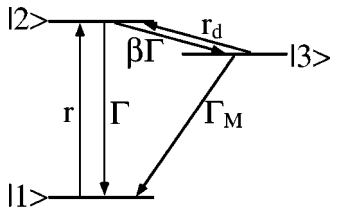

FIG. 1. Level scheme. The fluorescence is collected between levels $|2\rangle$ and $|1\rangle$. Level $|3\rangle$ is a metastable state.

*Email address: jean-philippe.poizat@iota.u-psud.fr

a train of light pulses of duration δT, such that $\Gamma \delta T \ll 1$. The separation between the pulses is denoted by T, with $\Gamma T \gg 1$. For the ideal efficiency of the source, the dipole should be coupled to a field mode in a microcavity, which is then damped to the outside world. Here we will only consider free-space emission of the dipole, assuming that the emitted light is collected by purely passive ways, such as a parabolic retroreflector [7]. The corresponding imperfect detection efficiency will be included in the present model, but the possible effect of a microcavity will not be considered here.

In Sec. II, we will introduce a useful framework for carrying out the calculation within the hypothesis discussed above: classical pump, free-space emission, and strongly damped coherences. Then we will evaluate the quantities of interest, taking into account the detection efficiency. Finally we will present numerical results illustrating the behavior of the system.

II. THEORETICAL MODEL

A. General framework

The evolution of the populations will be described using the diagonal terms of the density matrix $\sigma_{bb}(t,t_0;a)$, which denotes the population of level b at time t, starting from level a at time t_0 (where a and b may take any value from 1 to 3). For the following it will be convenient to define the probability $\sigma_{bb}^{(n)}(t,t_0;a)$ to go from state $|a\rangle$ at time t_0 to state $|b\rangle$ at time t, with the emission of exactly n photons. The quantities $\sigma_{bb}^{(n)}$ are linked to the populations σ_{bb} by the relation

$$\sigma_{bb}(t,t_0;a)=\sum_{n=0}^{\infty}\sigma_{bb}^{(n)}(t,t_0;a). \tag{3}$$

The probability density to emit one and only one photon at time t, when the system is in state $|a\rangle$ at time t_0, is given by the probability $\sigma_{22}^{(0)}(t,t_0;a)$ to be in the excited state at time t without any photon emission:

$$p_1=\Gamma\sigma_{22}^{(0)}(t,t_0;a). \tag{4}$$

The quantities $\sigma_{bb}^{(n)}(t,t_0;a)$ introduced previously can be related through the following recurrence relationship:

$$\sigma_{bb}^{(n+1)}(t,t_0;a)=\int_{t_0}^{t}\Gamma\sigma_{22}^{(n)}(t',t_0;a)\sigma_{bb}^{(0)}(t,t';1)dt'. \tag{5}$$

In other words, in order to emit $n+1$ photons, the system has to emit the photon $n+1$ at time t', and to emit no photon from t' to t. The rate equations for $\sigma_{bb}^{(0)}$ can be written

$$\frac{\partial\sigma_{bb}^{(0)}}{\partial t}(t,t_0;a)=\sum_{c}r_{cb}^{(0)}\sigma_{cc}^{(0)}(t,t_0;a), \tag{6}$$

where similar equations hold for σ_{bb}, with coefficients r_{cb}. Using Eqs. (3), (5), and (6), it can be shown (see Appendix B) that the rate coefficients $r_{cb}^{(0)}$ are related to the coefficients r_{cb} by

$$r_{cb}^{(0)}=r_{cb}-\Gamma\delta_{b1}\delta_{c2}, \tag{7}$$

where δ_{ai} is 1 if $a=i$, and zero otherwise. For the three-level system we consider in Fig. 1, we thus obtain the following rate equations:

$$\dot{\sigma}_{22}^{(0)}=r\sigma_{11}^{(0)}-(1+\beta)\Gamma\sigma_{22}^{(0)}+r_d\sigma_{33}^{(0)}, \tag{8}$$

$$\dot{\sigma}_{33}^{(0)}=-\Gamma_M\sigma_{33}^{(0)}+\beta\Gamma\sigma_{22}^{(0)}-r_d\sigma_{33}^{(0)}, \tag{9}$$

$$\dot{\sigma}_{11}^{(0)}=-r\sigma_{11}^{(0)}+\Gamma_M\sigma_{33}^{(0)}. \tag{10}$$

The difference between Eq. (8) and the original rate equations for populations is the missing term proportional to $\sigma_{22}^{(0)}$ in the last equation. This means that the ground level is no longer filled after the emission of one photon, and ensures the uniqueness of the emitted photon.

Equations (8)–(10), with a knowledge of the initial state, allow one to derive the different quantities of interest. In Sec. II B we first consider the ideal situation of perfect collection efficiency. Section II C deals with nonunity collection efficiency, which substantially modifies results of Sec. II B. Finally, we take into account the effect of the metastable state in Sec. II D.

B. Two-level approximation with unit quantum efficiency

We first assume that all the emitted photons are detected (unit quantum efficiency), and that the dipole is initially in its ground state $|1\rangle$. We also take $\beta=0$, so that we neglect the probability for the system to go to a metastable state in the time interval between two excitation light pulses, and set $\sigma_{33}=0$ (two-level approximation). The case $\beta\neq 0$ will be considered in Sec. II D. Equations (8)–(10) therefore reduce to the system

$$\dot{\sigma}_{22}^{(0)}=r\sigma_{11}^{(0)}-\Gamma\sigma_{22}^{(0)}, \tag{11}$$

$$\dot{\sigma}_{11}^{(0)}=-r\sigma_{11}^{(0)}, \tag{12}$$

whose solutions are, for $t\leqslant\delta T$,

$$\sigma_{11}^{(0)}(t,t_0;1)=\exp[-r(t-t_0)], \tag{13}$$

$$\sigma_{22}^{(0)}(t,t_0;1)=\frac{r}{r-\Gamma}(\exp[-\Gamma(t-t_0)]-\exp[-r(t-t_0)]), \tag{14}$$

and, for $t\geqslant\delta T$,

$$\sigma_{11}^{(0)}(t,t_0;1)=\sigma_{11}^{(0)}(\delta T,t_0;1), \tag{15}$$

$$\sigma_{22}^{(0)}(t,t_0;1)=\exp[-\Gamma(t-\delta T)]\sigma_{22}^{(0)}(\delta T,t_0;1). \tag{16}$$

The probability $P_e^{(g)}$ to emit at least one photon between two pulses (say in interval $[0,T]$) is then

$$P_e^{(g)}=\Gamma\int_0^T\sigma_{22}^{(0)}(t,0;1)dt$$

$$=1-\exp(-r\,\delta T)-\frac{r}{r-\Gamma}\exp(-\Gamma T)$$

$$\times[1-\exp((\Gamma-r)\,\delta T)]. \tag{17}$$

This probability of course increases with the period T, which has to be large compared to Γ^{-1} to assure the emission of the photon [for instance, $\exp(-\Gamma T)=5\times10^{-5}$ for a 10-MHz pulse train, and $\Gamma^{-1}\approx10$ ns]. We can therefore set

$$P_e^{(g)}\approx1-\exp(-r\,\delta T). \tag{18}$$

The probability $P_n^{(g)}$ to emit exactly n photons is given by

$$P_n^{(g)}=\sum_a\ \sigma_{aa}^{(n)}(T,0;1)$$

$$=\int_0^T dt\left\{1-\Gamma\int_t^T\sigma_{22}^{(0)}(t',t;1)dt'\right\}$$

$$\times\Gamma\sigma_{22}^{(n-1)}(t,0;1), \tag{19}$$

where the second equality corresponds to the probability to emit the photon n at time t, and no photons within $[t,T]$. In the limit $\exp(-\Gamma T)\to0$, the probability $P_1^{(g)}$ is given by the following expression, which is well behaved when $r=\Gamma$:

$$P_1^{(g)}=\left(\frac{r}{r-\Gamma}\right)^2[\exp(-\Gamma\,\delta T)-\exp(-r\,\delta T)]$$

$$-\frac{\Gamma r\,\delta T}{r-\Gamma}\exp(-r\,\delta T). \tag{20}$$

C. Nonperfect collection efficiency

In practice, the dipole cannot be separated from the collection system, and the statistics of interest is the statistics of the detected events, rather than that of the emission events. Assuming again that the initial state is the ground state, and denoting η as the collection efficiency ($\overline{\eta}=1-\eta$), the probability to collect no photon between $[0,T]$ is

$$\Pi_0^{(g)}=\sum_{n=0}^{\infty}\ \overline{\eta}^n P_n^{(g)}. \tag{21}$$

Let us introduce the probability $\tilde{\sigma}_{aa}$ of reaching state $|a\rangle$ without the collection of any photon, which is given by

$$\tilde{\sigma}_{aa}=\sum_{n=0}^{\infty}\ \overline{\eta}^n\sigma_{aa}^{(n)}. \tag{22}$$

From the above definitions, we have $\Pi_0^{(g)}=\Sigma_a\tilde{\sigma}_{aa}$. Using a calculation very similar to the beginning of this section [see Eq. (7) and Appendix B], the linear differential system for $\tilde{\sigma}_{aa}$ can be shown to be

$$\dot{\tilde{\sigma}}_{22}==r\tilde{\sigma}_{11}-\Gamma\tilde{\sigma}_{22}+r_d\tilde{\sigma}_{33}, \tag{23}$$

$$\dot{\tilde{\sigma}}_{33}=-\Gamma_M\tilde{\sigma}_{33}+\beta\Gamma\tilde{\sigma}_{22}-r_d\tilde{\sigma}_{33}, \tag{24}$$

$$\dot{\tilde{\sigma}}_{11}=-r\tilde{\sigma}_{11}+\Gamma_M\tilde{\sigma}_{33}+\overline{\eta}\Gamma\tilde{\sigma}_{22}. \tag{25}$$

The correction introduced here, compared to Eqs. (8)–(10), consists in the addition of a term filling the ground state with a rate corresponding to the probability density $\overline{\eta}\Gamma$ to emit one photon but not to collect it. This term ensures the collection of one and only one photon. If the initial state is the ground state, and within the approximations of Sec. II B ($\beta\ll1$, $\tilde{\sigma}_{33}=0$), this system can be rewritten

$$\dot{\tilde{\sigma}}_{22}=r\tilde{\sigma}_{11}-\Gamma\tilde{\sigma}_{22}, \tag{26}$$

$$\dot{\tilde{\sigma}}_{11}=-r\tilde{\sigma}_{11}+\overline{\eta}\Gamma\tilde{\sigma}_{22}. \tag{27}$$

This system can easily be solved between $[0,T]$, and for $\Pi_0^{(g)}$ we find, in the limit $\exp(-\Gamma T)\to0$,

$$\Pi_0^{(g)}=\tilde{\sigma}_{11}(\overline{\eta};T,0;1)=\overline{\eta}\tilde{\sigma}_{22}(\overline{\eta};\delta T,0;1)+\tilde{\sigma}_{11}(\overline{\eta};\delta T,0;1), \tag{28}$$

with

$$\tilde{\sigma}_{11}(\overline{\eta};\delta T,0;1)=\frac{r-\Gamma'}{r'-\Gamma'}\exp(-r'\,\delta T)$$

$$+\frac{r'-r}{r'-\Gamma'}\exp(-\Gamma'\,\delta T), \tag{29}$$

$$\tilde{\sigma}_{22}(\overline{\eta};\delta T,0;1)=\frac{r}{r'-\Gamma'}[\exp(-\Gamma'\,\delta T)-\exp(-r'\,\delta T)], \tag{30}$$

and

$$r'=\frac{1}{2}(\Gamma+r+\sqrt{(r-\Gamma)^2+4\overline{\eta}r\Gamma}), \tag{31}$$

$$\Gamma'=\frac{1}{2}(\Gamma+r-\sqrt{(r-\Gamma)^2+4\overline{\eta}r\Gamma}).$$

The probability $\Pi_0^{(g)}$ allows us to determine the probability $\Pi_e^{(g)}=1-\Pi_0^{(g)}$ to collect at least one photon. It also permits us to obtain the probability to collect one and only one photon

$$\Pi_1^{(g)}=\sum_{n=1}^{\infty}\ n\,\eta\,\overline{\eta}^{n-1}P_n^{(g)}=\eta\partial_{\overline{\eta}}\Pi_0^{(g)}. \tag{32}$$

We thus find

$$\Pi_1^{(g)}=\frac{\eta r}{r'-\Gamma'}\left(1+\frac{\Gamma(2\eta r-r-\Gamma)}{(r'-\Gamma')^2}\right)(\exp(-\Gamma'\delta T)-\exp(-r'\delta T))+\frac{\eta r\Gamma\delta T}{r'-\Gamma'}\times\left(\frac{r'-\eta r}{r'-\Gamma'}\exp(-\Gamma'\delta T)+\frac{\Gamma'-\eta r}{r'-\Gamma'}\exp(-r'\delta T)\right). \quad (33)$$

These results correspond of course to the results of Sec. II B if $\eta=1$. A simpler expression can be obtained by considering in first approximation that no more than two photons can be emitted during the light excitation pulse. We then have

$$P_0^{(g)}+P_1^{(g)}+P_2^{(g)}=1-P_e^{(g)}+P_1^{(g)}+P_2^{(g)}\approx 1. \quad (34)$$

Equation (21) can then be written as

$$\Pi_0^{(g)}=1-P_e^{(g)}+\overline{\eta}P_1^{(g)}+\overline{\eta}^2(P_e^{(g)}-P_1^{(g)}), \quad (35)$$

and Eq. (32) as

$$\Pi_1^{(g)}=\eta(P_1^{(g)}+2\overline{\eta}(P_e^{(g)}-P_1^{(g)})). \quad (36)$$

D. Influence of the metastable state

In order to study the effect of the metastable state, the three-level equations [Eqs. (8)–(10)] can be solved analytically in the general case, giving lengthy and not very illuminating expressions. In physical terms, a short intense pulse will excite the dipole as previously, but now the dipole may end up in the metastable state. Thus the emission of the single photon will be delayed by an amount depending on the time spent in the metastable state.

For definitiveness, here we shall consider the situation where the transition rate $\beta\Gamma$ to the metastable level $|3\rangle$ is weak but not completely negligible; this applies in particular to single molecules (see Sec. III). The probability to populate this level when a transition occurs from level $|2\rangle$ is $\beta/(\beta+1)\approx\beta$, so the metastable level is reached every $(\beta P_e^g)^{-1}$ light pulses in average. In a way similar to the approximations of Sec. II B, we can neglect the probability to leave the metastable state and to reach it again in the same cycle $[0,T]$. We can therefore neglect the filling term $\beta\Gamma\tilde{\sigma}_{22}$ in Eqs. (23), and the probability to stay in the metastable state in one cycle is $\exp[-(\Gamma_M+r_d)T]$, or, for q cycles

$$P_c=\exp[-(\Gamma_M+r_d)qT]. \quad (37)$$

When the system reaches the metastable level, it therefore remains shelved during a mean time $(\Gamma_M+r_d)^{-1}$, that will be assumed to be much larger than T. The probability to reach this level is approximately $\beta P_e^{(g)}$ for each excitation pulse, so the average time it takes for the system to find itself in the metastable state is $T(\beta P_e^{(g)})^{-1}$. The number of emitted photons is thus decreased by a factor

$$M=\frac{T(\beta P_e^{(g)})^{(-1)}}{T(\beta P_e^{(g)})^{-1}+(\Gamma+r_d)^{-1}}=\frac{(\Gamma+r_d)T}{\beta P_e^{(g)}+(\Gamma+r_d)T}. \quad (38)$$

Even if β is small, the factor M can thus induce a reduction of the photon flux. Obviously this decrease in the number of emitted photons has different statistical properties than the random deletion considered in Sec. II C [18]. One now obtain alternative periods where the source is ''on,'' and periods where it is ''off.'' In a practical system, one may consider using a ''deshelving'' laser [17] in order to increase r_d, and thus to maximize the duty cycle of the dipole.

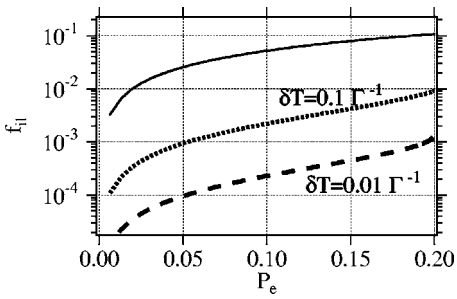

FIG. 2. Fractional information leakage f_{il} vs the probability P_e of emitting at least one photon for $\eta=0.2$. The dashed and dotted lines correspond to the fluorescence of a single emitter, as described in the text, for different excitation pulse durations $\delta T=0.01\Gamma^{-1}$ (dashed line) and $\delta T=0.01\Gamma^{-1}$ (dotted line). The thin solid line is the fractional information leakage f_{il} for a Poissonian source.

III. DISCUSSION

In this section the above model is used to demonstrate the potentiality of a single emitter to produce single photons when excited by a light pulse. This potentiality is evaluated by the fractional information leakage f_{il} defined in Eq. (1). In particular, the influence of the duration and the energy of the pulse are investigated. The parameters considered in the following corresponds to commercially available laser systems for typical emitters such as terrylene in *p*-terphenyl [10] or nitrogen-vacancy colored centers in diamond [12,13], with a saturation intensity of the order of 1 MW/cm^2. Note also that in all the plots discussed below the collection efficiency is taken as $\eta=0.2$, which is a realistic value for an optimized passive collection system at room temperature.

In Fig. 2 the ability of the single emitter source to deliver truly single photons is compared to an attenuated Poissonian source with the same number of empty pulses. The fractional information leakage f_{il} is plotted as a function of the probability P_e of emitting at least one photon. The quantity P_e is varied by changing the pulse power while the pulse duration is kept constant. When the pulse duration δT is ten times shorter than the emitter's lifetime, it appears that the occurence of pulses with two photons or more is reduced by one order of magnitude when a single emitter is used instead of an attenuated Poissonian source. Reducing further the

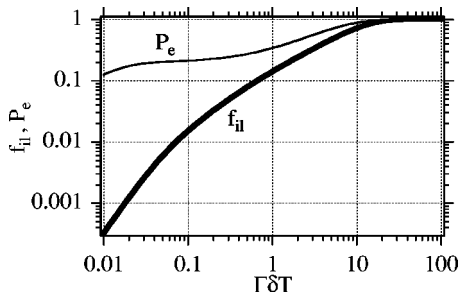

FIG. 3. Influence of the pulse duration with $\eta=0.2$. The pumping rate is kept constant, $r=100\Gamma$. The thick line is the fractional information leakage f_{il}. The thin line is the probability P_e of emitting at least one photon. Both quantities are plotted vs the normalized duration of the exciting light pulse $\Gamma\delta T$.

pulse duration to 1% of the emitter's lifetime improve the fractional information leakage by another factor of 10.

Figure 3 shows the influence of the pulse duration δT on the fractional information leakage f_{il} for a given excitation peak power (i.e., for a given r). This would correspond to an experiment where the pulses are sliced up in a continuous wave laser with fast optical modulators. Of course the shorter the pulse the better f_{il} is, but when the pulse is too short the probability P_e also decreases, since the peak power is constant. Note that P_e can exceed the collection efficiency η for δT large compared to Γ^{-1}. In this case the fluorescence pulse emitted by the dipole contains much more than one photon, so that even after the $\eta=0.2$ attenuation the probability of having more than one photon remains larger than η.

In Fig. 4 the fractional information leakage f_{il} and the probability P_e of emitting at least one photon are plotted versus the pulse power for a given pulse duration. As expected, short pulses ($\delta T=0.01/\Gamma$) require more power to reach a value of P_e around $P_e=\eta=0.2$, since P_e depends only on the pulse energy $r\delta T$. But short pulses offer a better fractional information leakage f_{il}, owing to the fact that the shorter the pulse, the lower the probability of emitting a photon and being reexcited within the same pulse.

For typical molecules or colored centers, the excited-state

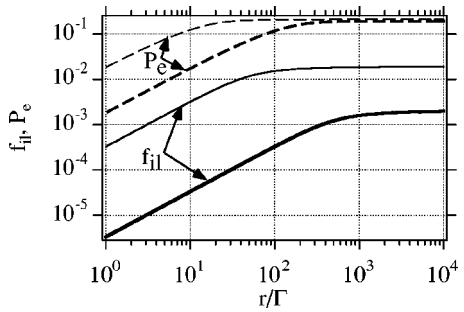

FIG. 4. Influence of the pulse power. All traces are plotted vs the normalized pumping rate r/Γ for a given pulse duration δT, with $\eta=0.2$. The solid lines correspond to the fractional information leakage f_{il}, and the dashed lines to the probability P_e of emitting at least one photon. These values are given for $\delta T=0.01\Gamma^{-1}$ (thick lines) and for $\delta T=0.1\Gamma^{-1}$ (thin lines).

lifetime is of the order of $\Gamma^{-1}=10$ ns, and typical saturation intensities when focused on a submicron spot are of the order of 1 mW. For these types of emitting dipoles-laser pulses with $\delta T=0.1$ ns and a peak power of 1 W (i.e., a pulse energy of 0.1 nJ) will already lead to good results. It has to be recalled that the incoherent model used here is valid only when the pulse duration remains larger than the coherence decay, that is, in the picosecond range. This hypothesis prevents the use of extremely short and intense pulses, but is fully compatible with the numbers just quoted.

IV. CONCLUSION

We have evaluated the efficiency of a single-photon source based upon the pulsed excitation of an individual dipole, in a regime where coherences are strongly damped and thus rate equations are relevant. This calculation applies for instance to the excitation of a single molecule [10] or a single colored center [12,13] at room temperature [12,13].

With respect to a radiatively damped two-level system, where either an exact π pulse or a fast adiabatic passage is required [5–7], the requirement for the pulse intensity is much less stringent. This type of system is thus promising for achieving an all-solid-state single-photon source operating at room temperature.

ACKNOWLEDGMENTS

This work was supported by the European IST/FET Program ''Quantum Information Processing and Telecommunication,'' Project No. 1999-10243 ''S4P,'' and France Telecom - Centre National d'Etude des Télécommunications under the ''CTI,'' Project No. 99 1B 784.

APPENDIX A: LOSS OF INFORMATION OWING TO PULSES CONTAINING TWO PHOTONS OR MORE IN A QUANTUM CRYPTOGRAPHIC SCHEME

We emphasize that f_{il} defined by Eq. (1) clearly gives a physically meaningful evaluation of the single-photon character of the pulse. We note in particular that when $P_{n\geqslant 1}\ll 1$, the condition $f_{il}<P_1/2$ is equivalent to the ''anticorrelation'' criterion $\alpha<1$ that was introduced in Ref. [19]. Below we give a few examples that suggest a heuristic conjecture that f_{il} also gives a good indication of the information leakage due to the multiphotonic character of the light pulses. The quantitative evaluation of f_{il}, which is the main result of this paper, obviously does not depend on the arguments given below.

For the sake of illustration, the information is supposed to be coded in the photon polarization, but the following discussion remains valid for all types of information encoding. A simple strategy for Eve to exploit photon pairs is to tap a fraction $\bar{\eta}=1-\eta$ of the beam, and to store the corresponding photons. The polarization of the stored photons is measured later on, when Alice and Bob have disclosed the relevant basis information. Assuming that the probability to obtain more than two photons per pulse is negligible, the

probability for Eve to catch the information is then $2\eta\overline{\eta}P_2$, which is at a maximum for $\eta=0.5$, and takes a value $P_2/2$. The relative fraction of Bob's information which is known to Eve is then $P_2/P_{n\geqslant 1}$, which is just f_{il}. For attenuated light pulses, one obtains $f_{il}\approx P_2/P_1\approx P_1/2$. The action of Eve creates no polarization errors, and cannot be distinguished from a 50% random loss in the transmission between Alice and Bob.

Another possible, more sophisticated, strategy for Eve is to use a fast polarization-insensitive quantum-nondemolition measurement (QND) [20] of the number of photons in each pulse, and to deflect every second photon. The polarization of the deflected photons is measured later on, as stated above. The fraction of useful bits is thus $P_{n\geqslant 1}$ for Bob and P_2 for Eve, and the information leakage is again $f_{il}=P_2/P_{n\geqslant 1}$. This scheme introduces neither polarization errors nor apparent loss. It can nevertheless be detected by Bob if he analyzes the photon statistics of the light pulses he receives.

In the presence of high transmission losses between Alice and Bob, for instance, in long-distance or free-space quantum cryptography, both methods can be combined to give even more powerful attacks [21,22]. For instance, let us assume that Eve is able to catch the light pulses before they go through the transmission line, and to distribute them to Bob through her own lossless line. Using the QND setup, Eve identifies the pulses with more than one photon, keeps one of them, and redistributes the remaining photons to Bob in order to simulate the low efficiency η_L of the original line between Alice and Bob. In this case, as soon as $\eta_L<f_{il}$, Eve receives essentially all the information and remains undetected. Though some countermeasures are possible, it is now clear that attenuated light pulses and high transmission losses are a deadly combination for quantum cryptography [21,22].

As a numerical example, when using attenuated light pulses with a typical value $P_1=0.2$, a fraction $f_{il}=0.1$, i.e., at least 10% of the information may leak to Eve. By comparison, the single-photon source described in this paper will give $P_1=0.1$ and $f_{il}=0.002$ for experimentally reachable operating conditions ($\Gamma\delta T=0.01$, $r=1000\Gamma$, and the overall efficiency 20%; see the text for definitions). In the cryptographic situations discussed above, the information leakage to Eve is thus reduced by a factor 50 when using a single-photon source.

APPENDIX B: DERIVATION OF THE EQUATION FOR $\tilde{\sigma}_{bb}$

Here we will derive the rate equations for the quantity $\tilde{\sigma}_{bb}(\overline{\eta};t,t_0;a)$, which has been defined as

$$\tilde{\sigma}_{bb}(\overline{\eta};t,t_0;a)=\sum_{n=0}^{\infty}\overline{\eta}^n\sigma_{bb}^{(n)}(t,t_0;a) \tag{B1}$$

Using this definition, we have

$$\frac{\partial}{\partial t}\tilde{\sigma}_{bb}(\overline{\eta};t,t_0;a)=\frac{\partial}{\partial t}\sigma_{bb}^{(0)}(\overline{\eta};t,t_0;a)+\sum_{n=1}^{\infty}\overline{\eta}^n\frac{\partial}{\partial t}\sigma_{bb}^{(n)}(\overline{\eta};t,t_0;a). \tag{B2}$$

We have, for every $n>0$, and from Eq. (5)

$$\frac{\partial}{\partial t}\tilde{\sigma}_{bb}(\overline{\eta};t,t_0;a)\frac{\partial}{\partial t}\sigma_{bb}^{(0)}(\overline{\eta};t,t_0;a)+\sum_{n=1}^{\infty}\overline{\eta}^n\Big[\Gamma\sigma_{22}^{(n-1)}(t,t_0;a)\sigma_{bb}^{(0)}(t,t;1) \tag{B3}$$

$$+\int_{t_0}^{t}\Gamma\sigma_{22}^{(n-1)}(t',t_0;a)\frac{\partial}{\partial t}\sigma_{bb}^{(0)}(t,t';1)dt'\Big]. \tag{B4}$$

As we obviously have $\sigma_{bb}^{(0)}(t,t;1)=\delta_{b1}$, and using Eq. (6), we can rewrite Eq. (B3):

$$\frac{\partial}{\partial t}\tilde{\sigma}_{bb}(\overline{\eta};t,t_0;a)=\sum_{c}r_{cb}^{(0)}\sigma_{cc}^{(0)}(\overline{\eta};t,t_0;a)+\sum_{n=1}^{\infty}\overline{\eta}^n\Big[\delta_{b1}\Gamma\sigma_{22}^{(n-1)}(t,t_0;a) \tag{B5}$$

$$+\sum_{c}r_{cb}^{(0)}\int_{t_0}^{t}\Gamma\sigma_{22}^{(n-1)}(t',t_0;a)\sigma_{cc}^{(0)}(t,t';1)dt'\Big]. \tag{B6}$$

Again using Eqs. (5) and (22), Eq. (B5) becomes

$$\frac{\partial}{\partial t}\tilde{\sigma}_{bb}(\overline{\eta};t,t_0;a)=\delta_{b1}\overline{\eta}\Gamma\tilde{\sigma}_{22}(t,t_0;a)+\sum_{c}r_{cb}^{(0)}\tilde{\sigma}_{cc}(\overline{\eta};t,t_0;a), \tag{B7}$$

which is equivalent to Eq. (23). Equation (7) can then be easily obtained by setting $\overline{\eta}=1$, since $\tilde{\sigma}_{bb}(1;t,t_0;a)=\sigma_{bb}(t,t_0;a)$.

[1] For a review, see W. Tittel, G. Ribordy, and N. Gisin, Phys. World **11**, 41 (1998).

[2] N. Lütkenhaus, Phys. Rev. A **59**, 3301 (1999); G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).

[3] F. De Martini, G. Di Giuseppe, and M. Marrocco, Phys. Rev. Lett. **76**, 900 (1996).

[4] F. De Martini, O. Jedrkiewicz, and P. Mataloni, J. Mod. Opt. **44**, 2053 (1997).

[5] C. K. Law and H. J. Kimble, J. Mod. Opt. **44**, 2067 (1997).

[6] S. C. Kitson, P. Jonsson, J. G. Rarity, and P. R. Tapster, Phys. Rev. A **58**, 620 (1998).
[7] C. Brunel, B. Lounis, P. Tamarat, and M. Orrit, Phys. Rev. Lett. **83**, 2722 (1999).
[8] J. Kim, O. Benson, H. Kan, and Y. Yamamoto, Nature (London) **397**, 500 (1999).
[9] A. Kuhn, M. Hennrich, T. Bondo, and G. Rempe, Appl. Phys. B: Lasers Opt. **69**, 373 (1999).
[10] L. Fleury, J.-M. Segura, G. Zumofen, B. Hecht, and U. P. Wild, Phys. Rev. Lett. **84**, 1148 (2000).
[11] P. Michler, A. Imamoglu, M. D. Mason, P. J. Carson, G. F. Strouse, and S. K. Buratto, Nature (London) **406**, 968 (2000).
[12] R. Brouri, A. Beveratos, J.-Ph. Poizat, and Ph. Grangier, Opt. Lett. **25**, 1294 (2000).
[13] C. Kurtsiefer, S. Mayer, P. Zarda, and H. Weinfurter, Phys. Rev. Lett. **85**, 290 (2000).
[14] H. J. Kimble, M. Dagenais, and L. Mandel, Phys. Rev. Lett. **39**, 691 (1977).
[15] F. Diedrich and H. Walther, Phys. Rev. Lett. **58**, 203 (1987).
[16] Th. Basché, W. E. Moerner, M. Orrit, and H. Talon, Phys. Rev. Lett. **69**, 1516 (1992).
[17] A. Dräbenstedt, L. Fleury, C. Tietz, F. Jelezko, S. Kilin, A. Nizovtev, and J. Wrachtrup, Phys. Rev. B **60**, 11 503 (1999).
[18] J. Bernard, L. Fleury, H. Talon, and M. Orrit, J. Chem. Phys. **98**, 850 (1993).
[19] P. Grangier, G. Roger, and A. Aspect, Europhys. Lett. **1**, 173 (1986).
[20] Ph. Grangier, J.-A. Levenson, and J.-Ph. Poizat, Nature (London) **396**, 537 (1998).
[21] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A **51**, 1863 (1995).
[22] W. T. Buttler, R. J. Hughes, P. G. Kwiat, S. K. Lamoreaux, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson, and C. M. Simmons, Phys. Rev. Lett. **81**, 3283 (1998); Comment by T. Durt, *ibid.* **83**, 2476 (1999).