Trojan-horse attacks on quantum-key-distribution systems

N. Gisin,[1] S. Fasel,[1] B. Kraus,[1] H. Zbinden,[1] and G. Ribordy[2]
[1]*Group of Applied Physics, University of Geneva, 1211 Geneva 4, Switzerland*
[2]*id Quantique SA, 3 Ch. de la Marbrerie, 1227 Carouge/Geneva, Switzerland*
(Received 26 July 2005; published 13 February 2006)

General Trojan-horse attacks on quantum-key-distribution systems, i.e., attacks on Alice or Bob's system via the quantum channel, are analyzed. We illustrate the power of such attacks with today's technology and conclude that all systems must implement active counter measures. In particular, all systems must include an auxiliary detector that monitors any incoming light. We show that such counter measures can be efficient, provided that enough additional privacy amplification is applied to the data. We present a practical way to reduce the maximal information gain that an adversary can gain using Trojan-horse attacks. This does reduce the security analysis of the two-way *plug-and-play* implementation to those of the standard one-way systems.

DOI: 10.1103/PhysRevA.73.022320 PACS number(s): 03.67.Dd

I. INTRODUCTION

The prominent application of quantum information science is quantum key distribution (QKD), which, together with quantum random number generators, is the most advanced realization of quantum devices operating at the single quanta level [1]. QKD offers the potential to develop provenly secure communication channels between distant partners. The latter should be connected by a so-called quantum communication channel, i.e., a channel able to transmit individual quantum systems well enough isolated from the outside world such that the receiver gets them almost unperturbed. In practice these quantum communication channels can be realized, among others, with standard telecom optical fibers or with free space in line-of-sight optical channels. In both cases the transmitted individual systems are photons. Quantum physics, in particular, the no-cloning theorem (a form of the famous Heisenberg uncertainty relations, suitable for the analysis of QKD) guarantees the following.

(1) The presence of any eavesdropper on the quantum communication channel can be detected by the legitimate users.

(2) The legitimate users can upper bound the information that any eavesdropper could gain by eavesdropping the quantum communication channel. Consequently, the legitimate users can lower bound the amount of privacy amplification they need to apply to their data in order to reduce the eavesdropper's information to an exponentially small value.

Accordingly, quantum physics guarantees potential [24] security against any possible attack on the quantum communication channel [2–6].

Today a lot is known about the most powerful attacks Eve could ever perform against the quantum channel, assuming Eve has absolutely no technological limits, i.e., she can do everything that quantum physics does not explicitly forbid. But, clearly, Eve's attacks are not limited to the quantum communication channel. For instance, Eve could attack Alice or Bob's apparatuses, or she could exploit weaknesses in the actual implementation of abstract QKD.

Quantum physics does not help protecting Alice and Bob's apparatuses. Indeed, as soon as the information is encoded in a classical physics system, it is vulnerable to copying and broadcasting. Hence, Alice and Bob's electronics have to be protected by classical means. Interestingly, one may ask where the transition from quantum coding to classical coding happens. This is an old question, the famous quantum to classical foggy transition, but here in a modern setting: it determines what can be protected by quantum means and what has to be protected by classical means. But we shall not consider this question in this paper. It is anyway obvious that Alice and Bob's apparatuses need classical protections.

Actual implementations of abstract QKD uses today's technology (and economical constrains). Hence they necessarily move somewhat away from the ideal scheme. It is thus of vital importance for QKD to analyze properly the consequences of these compromises. Indeed, some compromises might render the entire system totally insecure, while some other compromises can be proven to maintain absolute security, provided their analyzes are properly taken into account. Let us stress this important point: some well implemented compromises do not at all reduce the security of QKD [7–10].

An example of a very common and convenient compromise is the use of weak laser pulses instead of the single-photon sources that are closer to abstract qubits. To the best of our knowledge this was first shown to open new eavesdropping strategies [11,12]. Next, it has been proven that secure QKD is nevertheless possible, provided the weak intensity of the pulses and the quantum communication channel loss are properly taken into account [7–10]. Finally, recently, variations of the basic QKD protocols have been proposed that significantly lighten the conditions for secure QKD using weak laser pulses [13–15].

It is thus timely to study another unavoidable aspect of QKD: the quantum channel itself is a potentially open door for an eavesdropper into Alice and Bob's apparatuses. Indeed, even if this door is properly designed, Eve could use it precisely at the same time as the legitimate users: Eve could send into Alice and/or Bob's apparatuses light pulses during the (short) times the quantum channel is open [25], see Fig. 1. If Alice is not careful enough, Eve could find out exactly which quantum state she prepared and access thus the entire key. In general, Eve's goal is to acquire as much information as possible on the states sent by Alice. If Alice is careful enough, she can limit this information and eliminate it by

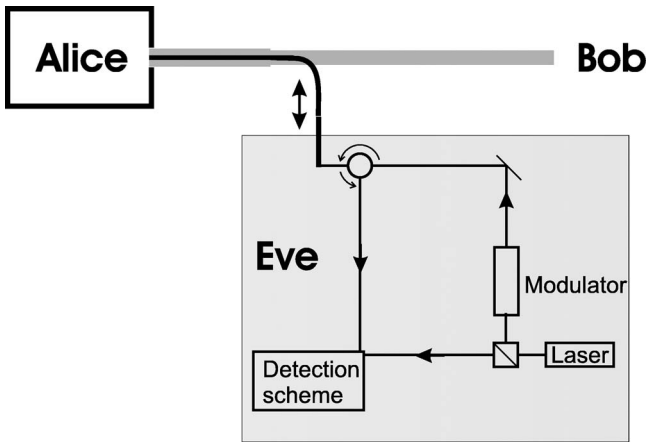

FIG. 1. Principle of a Trojan-horse attack. Eve occupied part of the quantum channel (i.e., the spatial, temporal, and frequency modes) to probe Alice's apparatus. Eve uses an auxiliary source, modulates it, and analyzes the backscattered signal with a detector. Note that her detection scheme can rely on specificities of her auxiliary source, for instance, on its phase. Eve may have to remove part of the legitimate signal, compensating the introduced loss by an improved quantum channel.

privacy amplification. But, in order to be able to apply privacy amplification, Alice and Bob must know a bound on Eve's information. Moreover, privacy amplification reduces the secret key rate. Hence, Alice and Bob's goal is to find ways to limit Eve's information to a bound as low as possible. Such attacks are known as Trojan-horse attacks.

In order to limit Trojan-horse attacks, the system should be designed in such a way that (1) only light at appropriate wavelength can enter (i.e. filters), (2) the "door" should be open only during short times, i.e., the encoding optical components should be active only during short times (i.e., activate phase modulators only when the qubits is there), and (3) the amount of reflected light that could be exploited by Eve is bounded by a known value.

The purpose of this paper is to analyze Trojan-horse attacks. In particular, we shall examine each of the above points in Sec. III. But, first, it is useful to get a better understanding of the techniques that such an adversary could use, see Sec. II. Next, in Sec. IV we derive the photon number statistics of any light used in Trojan-horse attacks and in Sec. V we compute the maximal information that Eve could gain using Trojan-horse attacks, i.e., compute how much additional privacy amplification is required in order to successfully combat such attacks. Finally, in Sec. VI we present a simple way to reduce this information, hence to increase the secret bit rate.

II. REFLECTOMETRY

Every optical element backscatters some amount of any incoming light. This might be small in optical fibers (about -70 dB/m) and angle-polished connectors (typically -40 dB), but medium for integrated optics components, such as phase modulators (≈ -20 dB) and large for mirrors ($\geqslant -1$ dB).

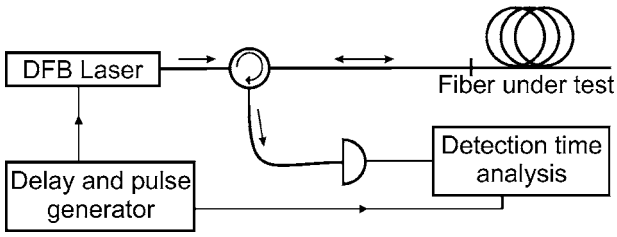

FIG. 2. Functional schematic of OTDR.

Consequently, every optical apparatus can be examined from the outside by shining into it a well controlled light and analyzing the backscattered light. This technique, named reflectometry, is a standard tool for optical engineers.

For security analysis of QKD one assumes an Eve without any technological limit. But it is useful to have an idea how the technique works in principle and to illustrate it with today's technology.

There are essentially two approaches to reflectometry.

(1) Send in short optical pulses and analyze the backscattered light intensity in a function of time. From the known speed of light, the time can be translated into distances. This technique is called optical time domain reflectometry (OTDR); it is a very standard tool of optical telecom engineers [16,17] (see Fig. 2).

(2) Send in coherent cw light while scanning its optical frequency and analyze the spectrum of the backscattered light. Different reflections correspond to different emission times, hence to different optical frequencies. They do thus produce a beat signal. Usually one produces on purpose one relatively large reflection (inside the instrument) which acts as a local oscillator. The frequency of the backscattered signal can be translated into distance by a Fourier transformation. This technique is called optical frequency domain reflectometry (OFDR). It is not yet as standard as OTDRs, but, thanks to its heterodyne detection scheme, it holds the potential of a much larger sensitivity and dynamical range [18] (See Fig. 3).

The main drawback of today's OFDRs compared to OTDRs is their limited distance range, due to the finite coherence length of the cw laser. But, as Eve has no technological limits, we shall mainly illustrate the potential of

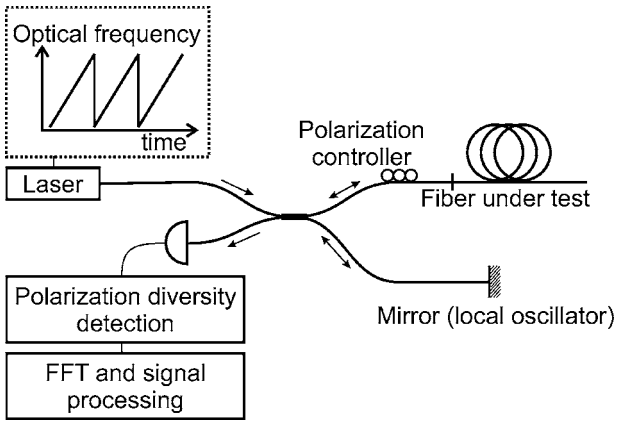

FIG. 3. Functional schematic of OFDR.

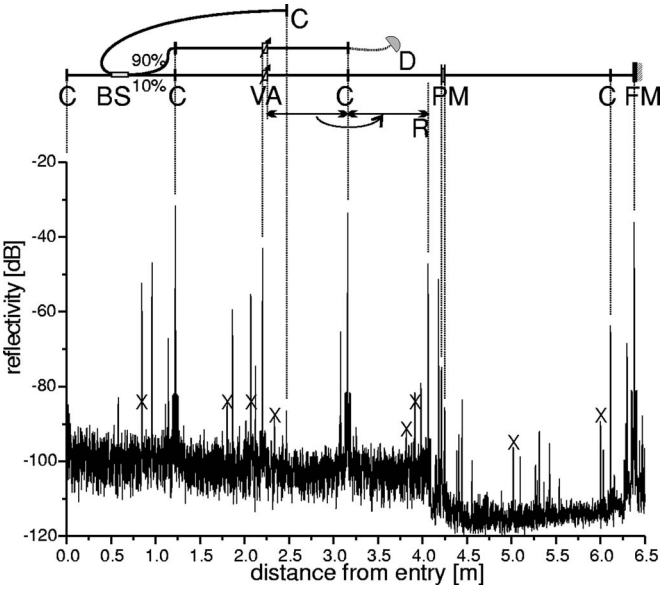

FIG. 4. An example of an OFDR trace of Alice's plug-and-play QKD system in which we removed the delay line and set the variable attenuator to its minimal value. A sketch of the optical circuit is displayed at the top with the corresponding reflections peaks below. The beam splitter (BS), connectors (C), variable attenuator (VA), detector (D), phase modulator (PM), and Faraday mirror (FM) are all clearly visible. The peak marked *R* corresponds to an example of multiple internal reflections. The peaks marked with a cross correspond to spurious reflections between the OFDR and Alice's components.

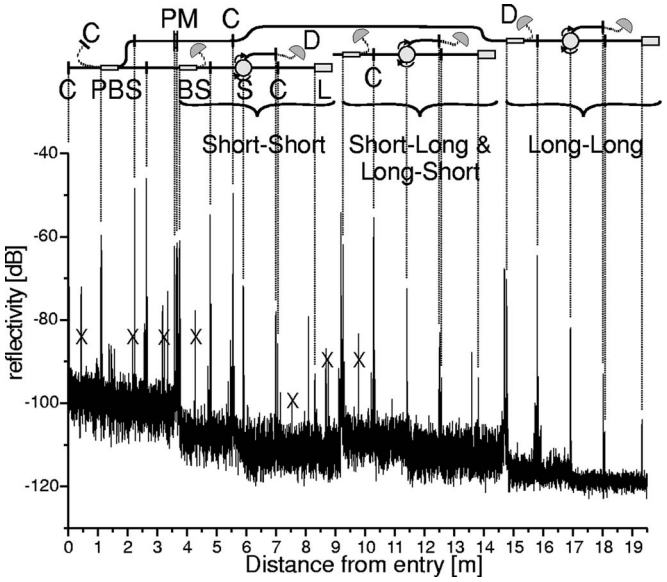

FIG. 5. Example of an OFDR trace of Bob's plug-and-play QKD system. Similar to Fig 4, but with the additional complication that each peak appears 3 times, because the incoming and reflected light both split in two, following the short and long path of the interferometer. For instance, one can notice that the long arm of the interferometer is about 11.5 meters longer than the short arm. Symbols are the same as in Fig. 4, plus circulators (S), polarization beam splitter (PBS), and laser (L).

Trojan-horse attacks using this technique. Let us emphasize that this section is only an illustration, clearly the counter measure by Alice and Bob should take into account reflectometry techniques beyond today's technique.

Figures 4 and 5 present the backscattered light from Alice and Bob's apparatuses, respectively, in the case of our plug-and-play quantum cryptography systems [19,20]. They illustrate that indeed quite a lot of information can be gained by probing the apparatuses from the outside. Let us emphasize that the same is true for all the other fiber-based apparatus, such as for instance, optical amplifiers [21] and any other quantum cryptography system. The details are given in the figure captions. Note that for the purpose of this demonstration, we removed about 10 km long delay line in Alice's apparatus, because our laser (contrary to that of Eve) has a coherence length limited to about 1 km.

Note that it is not yet clear how Eve could probe the setting of the phase modulator. However, Eve can indeed probe this setting by exploiting the change in birefringence in Titan-indiffused $LiNbO_3$ integrated waveguides, as illustrated in Fig. 6. For different kinds of phase modulators, or polarization modulators, it is highly likely that a similar technique applies. Figure 6 shows that it is easy to distinguish between two phase settings of Alice's phase modulator. To obtain Fig. 6 we had to keep the phase setting constant during about 1 sec, that is, a much longer time than in the usual use of the crypto system. We also had to adjust the polarization of the probe light and to use polarization-dependent OFDR settings to maximize the effect. Nevertheless, this result underlines that Trojan-horse attacks have to be analyzed seriously.

III. HARDWARE COUNTER MEASURES

The previous section demonstrated that Trojan-horse attacks on badly designed systems can be performed using today's techniques. Consequently, every proper implementation should take care that, (1) the door lets in only wave-

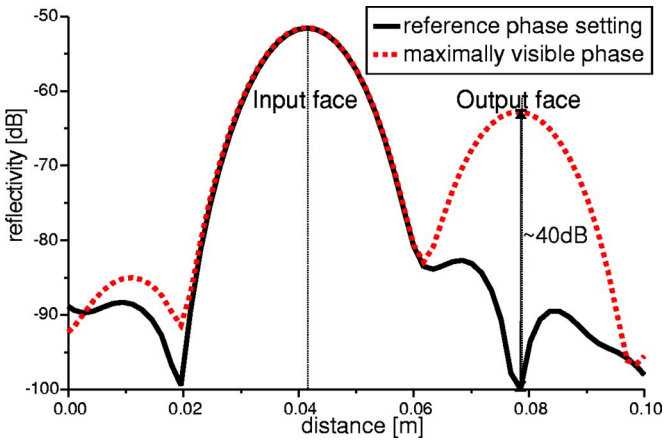

FIG. 6. (Color online) OFDR traces of an integrated optics phase modulator. Two different phase settings give rise to clearly distinguishable backscattering on the output face of the modulator. The two phase settings and the polarization of the probe light are chosen especially to exhibit a very clear effect. The measurement time is of about 1 s.

lengths close to the operating wavelength. Any other probe should be eliminated by properly designed filters, and (2) the door should be open only during a time as short as possible: the phase modulator, or polarization modulator, or whatever coding device is used, should be activated only during the short time when the legitimate signal is there.

But even these two measures cannot completely prevent Trojan-horse attacks. Indeed, Eve can multiplex her probe signal with the legitimate signal either in polarization (if time-bin qubits are used by Alice and Bob) or in wavelengths (Eve could reduce the loss of the Q channel, filter out a part of the legitimate signal, and use this bandwidth for her Trojan-horse attack, see Fig. 1). Also, in practice, timing has a finite accuracy, hence Eve can add her probes immediately before or after the legitimate pulses.

Consequently, a first conclusion is that every sensitive apparatus (Alice for sure, Bob depending on the protocol) must have an active control on the intensity of the incoming light: they should use an auxiliary detector and monitor any incoming light. The software should be designed such as to stop QKD as soon as abnormal intensities are detected (actually, for each qubit, there should be a *test*).

An idea to circumvent the need for an auxiliary detector is the use of attenuators and/or isolators. However, since Eve is not limited by technology, she could merely send in more intense light [26].

A second idea could be the use of an "optical fuse," i.e., a device that cuts the quantum channel if a too intense beam passes through it. This is a delicate technological problem. Indeed, there is no such fuse operating for ultrashort pulses. Hence, this does not seem like a practical idea, though one should keep it in mind.

In practice there is a natural fluctuation in the legitimate light and real detectors and electronics also contribute to the fluctuation of the monitoring signal. Hence, being conservative, one has to evaluate how much light can go to Eve without being detected and how much information she could extract from it. Then, appropriate privacy amplification should be applied to Alice and Bob's data. The amount of necessary privacy amplification for any bounded probe by Eve is computed in the next section.

IV. STATISTICS OF EVE'S PROBE LIGHT

One may question which state of light Eve should use in order to maximize her information gain. However, it is a well-known fact that losses tend to turn any state into a state whose photon number statistics is Poissonian. This is illustrated on Fig. 7 for the cases of 10 and 20 dB losses (i.e., transmissions of 0.1 and 0.01, respectively) and the mean photon number, after attenuation, $\mu=0.5$. Since all quantum cryptography systems (should) have attenuators and/or isolators attenuating any light used in a Trojan-horse attack even more severely, it is sufficient to consider light with Poissonian statistics.

Note that this does also imply that Eve cannot significantly affect the statistics of the photon number emitted by Alice in the plug-and-play configuration, even if she replaced the intense coherent pulse send by Bob by a squeezed state. We elaborate on this is Sec. VII.

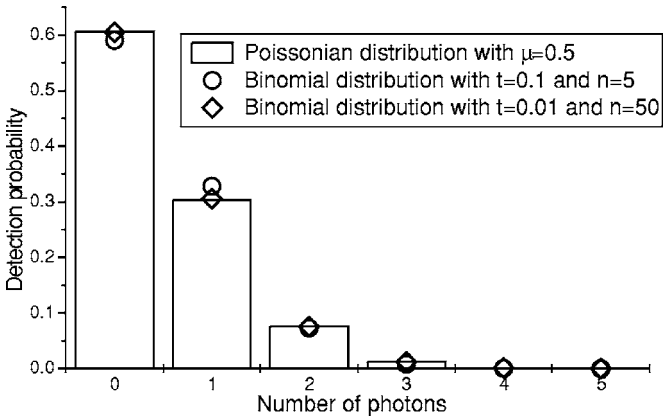

FIG. 7. Comparison of the photon-number distributions for Poissonian and binomial distributions of the same value. μ, average number of photons; t, transmission factor for Eve's probe light, corresponding, e.g., the the attenuation at Alice's input; n, number of photons in the Eve's Fock-state probe light.

V. EVE'S POTENTIAL INFORMATION GAIN

In this section we use well-known formulas to quantify the information that Eve can extract from a weak coherent state when she knows the "basis." Note, first that because of the huge attenuation that any Trojan-horse probe light undergoes, it will always return to Eve in a state extremely close to Poissonian, as described in Sec. IV. At best, from Eve's point of view, it bears some coherence, that is, it is a coherent state.

Note furthermore that because of the vacuum component of the weak coherent state, the two states corresponding to the basis are not orthogonal [27]. Explicitly, Eve has to distinguish between the following two states $|\alpha\rangle\otimes|0\rangle$ and $|0\rangle\otimes|\alpha\rangle$. The measurement that maximizes her information gain is known [22] and provides her with,

$$I_{\mathrm{Eve}}^{\mathrm{Trojan}}(|\alpha|^2)=1-H(p), \tag{1}$$

where

$$p=\tfrac{1}{2}(1+\sqrt{1-|\langle\alpha,0|0,\alpha\rangle|^2}), \tag{2}$$

$$=\tfrac{1}{2}[1+\sqrt{1-\exp(-2|\alpha|^2)}], \tag{3}$$

$$\approx\frac{1+\sqrt{2}|\alpha|}{2}, \tag{4}$$

and H denotes the binary entropy. Hence

$$I_{\mathrm{Eve}}^{\mathrm{Trojan}}(|\alpha|^2)\approx\frac{1}{\ln(2)}|\alpha|^2+O(|\alpha|^4), \tag{5}$$

where $1/\ln(2)\approx 1.443$. This information gain is presented graphically in Fig 8.

Surprisingly, this is larger than the probability that the weak pulse is nonempty:

$$\mathrm{Prob(nonempty)}=1-\exp(-|\alpha|^2)\approx|\alpha|^2. \tag{6}$$

The reason for this difference is that Eq. (2) assumes that Eve does really hold a coherent state, i.e., that she holds a

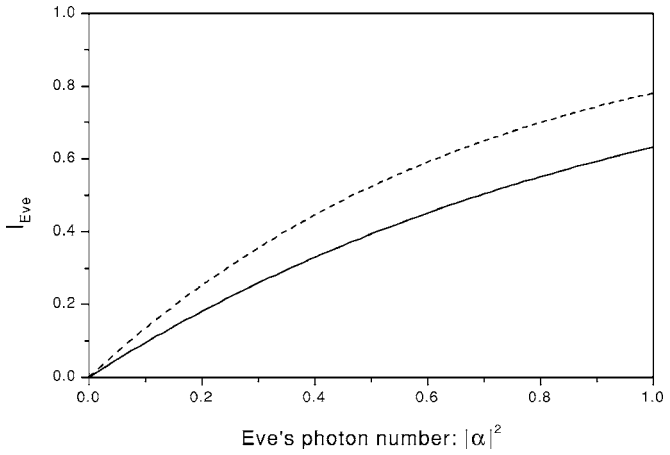

FIG. 8. Eve's optimal information gain per qubit in the function of the mean photon number $|\alpha|^2$ that she can collect without being detected by Alice and Bob. The upper curve corresponds to Eq. (1), the lower curve to the case that Alice and/or Bob applies phase randomization, Eq. (11). For example, if Alice's monitoring detector sets a limit to Eve's backscattered signal of 0.1 photon, then Eve may gain 0.135 and 0.095 bits if Alice does not apply or applies phase randomization, respectively.

phase reference relative to which α is defined. This observation leads to a possible way to reduce Eve's maximal information gain, as discussed in the next section.

VI. WAY TO REDUCE EVE'S INFORMATION

Figure 1 illustrates how Eve should probe Alice and/or Bob's apparatus in order to gain as much information as possible about their internal settings. Since Eve's gain can be significant, Alice and Bob have to sacrifice a significant fraction of their raw key before obtaining a secret key. It is thus of great interest to them to find ways to limit Eve's information. One possibility that we present in this section consists in Alice or Bob randomizing the phase of $|\alpha\rangle$ relative to Eve's reference. In this way, Eve does no longer hold $|\alpha,0\rangle$ or $|0,\alpha\rangle$, depending on the internal setting of the apparatus, but holds the mixed state ρ_0 or ρ_1, respectively, where

$$\rho_0 = \int_0^{2\pi} \frac{d\theta}{2\pi} |e^{i\theta}\alpha,0\rangle\langle e^{i\theta}\alpha,0|, \tag{7}$$

$$= \sum_{n\geqslant 0} P(n||\alpha|^2)|n,0\rangle\langle n,0|, \tag{8}$$

$$\rho_1 = \int_0^{2\pi} \frac{d\theta}{2\pi} |0,e^{i\theta}\alpha\rangle\langle 0,e^{i\theta}\alpha|, \tag{9}$$

$$= \sum_{n\geqslant 0} P(n||\alpha|^2)|0,n\rangle\langle 0,n|, \tag{10}$$

where $P(n||\alpha|^2)=(|\alpha|^{2n}/n!)e^{-|\alpha|^2}$ denotes the Poisson probability distribution. Eve optimal measurement distinguishing ρ_0 and ρ_1 is also known. Eve first measures the photon number. If she finds no photon, she clearly gains no information. However, whenever she finds one or more photon, then she gains full information. Hence her optimal information gain equals the probability that the weak coherent state $|\alpha\rangle$ is not empty:

$$I_{\text{Eve}}^{\text{reduced}}(|\alpha|^2) = 1 - P(0||\alpha|^2) = 1 - \exp(-|\alpha|^2) \approx |\alpha|^2. \tag{11}$$

Interestingly, $I_{\text{Eve}}^{\text{reduced}}(|\alpha|^2) < I_{\text{Eve}}^{\text{Trojan}}(|\alpha|^2)$; it is thus of practical value for Alice and Bob to add random phases to any light that might get backscattered. Let us emphasize that, clearly, these random phases act as irrelevant global phases on the qubits, hence do not affect the proper operation of QKD, but these random phases are relative to any possible reference that Eve might hold, hence it does reduce by the significantly factor $1/\ln 2 \approx 1.44$ the maximal information that Eve could gain using this backscattered light [23].

VII. REDUCTION OF SECURITY ANALYSIS OF TWO-WAY SYSTEMS TO ONE-WAY SYSTEMS

In a two-way quantum cryptography system, such as the so-called plug-and-play configuration [19,20], Eve may hold the strong pulse that enters Alice's apparatus. Let's write $\psi = \Sigma_{n\leqslant 0} c_n|n\rangle$ its state, where $|n\rangle$ denotes a state of n photons in some appropriate mode. Note that we assume a pure state, i.e., that the phase reference, relative to which the complex amplitudes c_n are defined, is classical. It is straightforward to generalize the analysis to the case where Eve's reference is a quantum state, i.e., Eve sends into Alice's apparatus a state entangled with an auxiliary state held by Eve. We like to show that phase randomization, as presented in the previous section, together with the effect of strong attenuation on the photon number statistics, as presented in Sec. IV, allows one to reduce the security analysis of two-way quantum cryptography systems to that of one-way systems, such as those analyzed in [7–10]. Formally, the phase randomization separates Eve's state ψ into a mixture of Fock number states:

$$\rho_{\text{rand.ph.}} = \int \frac{d\Phi}{2\pi} \sum_{n,m\geqslant 0} e^{i\Phi(n-m)} c_n c_m^* |n\rangle\langle m| = \sum_{n\geqslant 0} |c_n|^2 |n\rangle\langle n|. \tag{12}$$

Next, denoting t the transmission coefficient of Alice's apparatus (go and return), one has

$$\rho_{\text{rand.ph.Att.}} = \sum_{m\geqslant 0} |q_m|^2 |m\rangle\langle m|, \tag{13}$$

where

$$|q_m|^2 = t^m \sum_{n\geqslant m} \binom{n}{m} |c_n|^2 (1-t)^{n-m}. \tag{14}$$

Accordingly, the probability of a multiphoton pulse is

$$\text{Prob}(m \geqslant 2) = \langle n(n-1)\rangle \frac{t^2}{2} + O(t)^3, \tag{15}$$

where $\langle\ldots\rangle$ denote the average. For a coherent input state ψ, one recovers $\text{Prob}(m\geqslant 2)=\langle n^2\rangle t^2/2=\mu^2/2$. For a Fock state

$\psi=|N\rangle$, one obtains, possibly surprisingly, a lower multiphoton probability: $\text{Prob}(m\geqslant 2)=(N^2-N)(t^2/2)<\mu^2/2$.

Note again that the phase randomization separates Alice from any possible reference system that Eve might have prepared. Consequently, provided Alice randomizes the global phase of each qubit, measures the incoming intensity of each pulse, and introduces sufficient attenuation, she can bound the probability of her sending a multiphoton pulse to Bob; hence Alice and Bob can apply the standard security proofs to their two-way system.

VIII. CONCLUSION

Trojan-horse attacks should be considered for every QKD systems. These include single-photon, weak laser pulses and continuous variable implementations, as all necessarily include a quantum channel that "enter" into the legitimate users apparatuses. Note that for single-photon sources, Alice does not use any attenuator, contrary to the weak pulse implementations. Hence, Trojan-horse attacks are especially dangerous for such single-photon systems. For the plug-and-play system, the amount of reflected light is larger than for most alternative systems. Hence, the pressure on Eve's attacking system is reduced.

To counter such attacks, all QKD apparatuses should be properly designed, with filters and carefully designed timing. Additionally, auxiliary monitoring detectors must be implemented, if not the QKD system is insecure, irrespective of the quality of the source. Note that for the plug-and-play systems [19], Alice does already have such an auxiliary detector.

The accuracy of this monitoring detector determines how much privacy amplification has to be applied in order to defeat Trojan-horse attacks. In Sec. VI we presented a simple way to reduce this amount, hence to achieve larger secret keys.

ACKNOWLEDGMENTS

Discussions with Michele Mosca, Hoi-Kwong Lo, and Norbert Lütkenhaus stimulated this research. This work has been supported by EC under Project SECOQC (Contract No. IST-2003-506813).

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[2] D. Mayers, in *Advances in Cryptology—CRYPTO 1996, LNCS* (Springer, Berlin, 1996, Vol. 1109, pp. 343–357.
[3] E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury, in *Proceedings of the 32nd Annual ACM Symposium on the Theory of Computing* (ACM, Boston, 2000, pp. 715–724.
[4] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[5] H.-K. Lo, Quantum Inf. Comput. **1**, 2 (2001).
[6] R. Renner, N. Gisin, and B. Kraus, Phys. Rev. Lett. **95**, 080501 (2005); Phys. Rev. A **72**, 012332 (2005)
[7] H. Inamori, N. Lütkenhaus, and D. Mayers, e-print quant-ph/0107017.
[8] D. Gottesman, H-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **4**, 325 (2004).
[9] K. Tamaki and H. K. Lo, e-print quant-ph/0412035.
[10] M. Koashi, e-print quant-ph/0507154.
[11] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A **51**, 1863, (1995).
[12] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).
[13] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).
[14] V. Scarani, A. Acin, G. Ribordy, and N. Gisin, Phys. Rev. Lett. **92**, 057901 (2004).
[15] M. Koashi, Phys. Rev. Lett. **93**, 120501 (2004).
[16] E-G. Neumann, *Single-Mode Fibers, Fundamentals*, Springer Series in Optical Sciences, Vol. 57 (Springer, Berlin, 1988).
[17] M. Wegmuller, F. Scholder, and N. Gisin, J. Lightwave Technol. **22**, 390 (2004).
[18] G. Mussi, R. Passy, J-P. Von Der Weid, and N. Gisin, J. Lightwave Technol. **15**, 1 (1997).
[19] A. Muller, N. Gisin, T. Herzog, B. Huttner, W. Tittel, and H. Zbinden, Appl. Phys. Lett. **70**, 793 (1997).
[20] G. Ribordy, J. D. Gautier, N. Gisin, O. Guinnard, and H. Zbinden, Electron. Lett. **34**, 2116 (1998).
[21] J. P. Von Der Weid, R. Passy, and N. Gisin, IEEE Photonics Technol. Lett. **9**, 1253 (1997).
[22] A. Peres, *Quantum Theory: Concepts and Methods* (Kluwer Academic Publishers, Dordrecht, 1993).
[23] This is similar to H.-K. Lo and J. Preskill, e-print quant-ph/0504209, though there the authors did not consider Trojan-horse attacks.
[24] That is, assuming that the legitimate users do properly apply the rules of the game, in particular that they apply enough privacy amplification and interrupt the communication in case the detected noise (i.e., a potential eavesdropper) is too strong to be dealt with by privacy amplification.
[25] We consider the door as open only during the time when it potentially gives access to some useful information; the rest of the time the apparatus will merely backscatter a useless signal.
[26] Every physicist knows that there must be some limit, Eve cannot pulse a KJ in an ato-second pulse. At some point, a too large energy concentration should cause the devices to explode or melt. But this is hard to quantify. Admittedly, the larger the attenuator, the better.
[27] Most quantum cryptography protocols are presented with abstract qubits that can be prepared in different bases. However, most implementations use weak laser pulses, denoted $|\alpha\rangle$. The latter all share a common component on the vacuum, hence, strictly speaking, do not constitute bases. Typically, the logical qubit states $|0_L\rangle$ and $|1_L\rangle$ are coded in a weak pulse which can be in either of two modes: $|0_L\rangle=|\alpha\rangle\otimes|0\rangle$ and $|1_L\rangle=|0\rangle\otimes|\alpha\rangle$.