Limitations on Practical Quantum Cryptography

Gilles Brassard,[1] Norbert Lütkenhaus,[2] Tal Mor,[3,4] and Barry C. Sanders[5]
[1]*Département IRO, Université de Montréal, C.P. 6128, succursale centre-ville, Montréal, Québec Canada H3C 3J7*
[2]*Helsinki Institute of Physics, P.O. Box 9, 00014 Helsingin yliopisto, Finland*
[3]*Electrical Engineering, University of California at Los Angeles, Los Angeles, California 90095-1594*
[4]*Electrical Engineering, College of Judea and Samaria, Ariel, Israel*
[5]*Department of Physics, Macquarie University, Sydney, New South Wales 2109, Australia*

(Received 2 February 2000)

We provide limits to practical quantum key distribution, taking into account channel losses, a realistic detection process, and imperfections in the "qubits" sent from the sender to the receiver. As we show, even quantum key distribution with perfect qubits might not be achievable over long distances when the other imperfections are taken into account. Furthermore, existing experimental schemes (based on weak pulses) currently do not offer unconditional security for the reported distances and signal strength. Finally we show that parametric down-conversion offers enhanced performance compared to its weak coherent pulse counterpart.

PACS numbers: 03.67.Dd, 05.40.Ca, 42.50.Dv, 89.80.+h

Quantum information theory suggests the possibility of accomplishing tasks that are beyond the capability of classical computer science, such as information theoretically secure cryptographic key distribution [1,2]. Currently, we lack security proofs for standard (secret and public) key distribution schemes, and the most widely used classical schemes become insecure against potential attacks by quantum computers [3].

Whereas the security of idealized quantum key distribution (QKD) schemes has been reported against very sophisticated collective [4] and joint [5] attacks, we show here that already very simple attacks severely disturb the security of existing experimental schemes, for the chosen transmission length and signal strength. For a different parameter region a positive security proof against individual attacks has been given recently [6] making use of ideas presented here.

In the four-state scheme [1], usually referred to as Bennett-Brassard-84 (BB84), the sender (Alice) and the receiver (Bob) use two conjugate bases (say, the rectilinear basis, $+$, and the diagonal basis, $\times$) for the polarization of single photons. In basis $+$ they use the two orthogonal basis states $|0_+\rangle$ and $|1_+\rangle$ to represent "0" and "1," respectively. In basis $\times$ they use the two orthogonal basis states $|0_\times\rangle = (|0_+\rangle + |1_+\rangle)/\sqrt{2}$ and $|1_\times\rangle = (|0_+\rangle - |1_+\rangle)/\sqrt{2}$ to represent 0 and 1. The basis is revealed later on via an authenticated classical channel that offers no protection against eavesdropping. The signals where Bob used the same basis as Alice form the *sifted key* on which Bob can decode the bit value. The remaining signals are ignored in the protocol and in this security analysis. Finally, Alice and Bob use error correction and privacy amplification [7,8] to obtain a secure final key [5].

In order to be practical and secure, a QKD scheme must be based on existing—or nearly existing—technology, but its security must be guaranteed against an eavesdropper with unlimited computing power whose technology is limited only by the laws of quantum mechanics. The experiments are usually based on weak coherent pulses (WCP) as signal states with a low probability of containing more than one photon [7,9–11]. Initial security analysis of such weak-pulse schemes was done [7,12], and evidence of some potentially severe security problems (not existing for the idealized schemes) was shown [12,13].

Using a conservative definition of security, we provide several explicit limits on experimental QKD. First, we show that secure QKD to arbitrary distance can be totally impossible for given losses and detector dark counts, even with the assumption of a perfect source. Second, we show that QKD can be totally insecure even with perfect detection, due to losses and multiphoton states. Combining these results we compute a maximal distance beyond which (for any given source and detection units) secure QKD schemes cannot be implemented. Finally, we establish the advantage of a better source, which makes use of parametric down-conversion (PDC).

The effect of losses is that single-photon (SP) signals will arrive only with a probability F at Bob's site where they will lead to a detection in Bob's detectors with a probability η_B (detection efficiency). This leads to an expected probability of detected signals given by $p_{\rm exp}^{\rm signal} = F\eta_B$. For optical fibers, as used for most current experiments, the transmission efficiency F is connected to the absorption coefficient β and length ℓ of the fiber and a distance-independent constant loss in optical components c, via the relation

$$F = 10^{-(\beta\ell + c)/10} \tag{1}$$

which, for given β and c, gives a one-to-one relation between distance and transmission efficiency. Also, QKD can be achieved through free space [7,11], in which case

© 2000 The American Physical Society

the relevant efficiency-distance relation is dominated by beam broadening.

Each of Bob's detectors is also characterized by a dark count probability d_B per time slot in the absence of the real signal, so that for a typical detection apparatus with two detectors the total dark count probability is given by $p_{\mathrm{exp}}^{\mathrm{dark}} \approx 2d_B$. The dark counts are due to thermal fluctuations in the detector, stray counts, etc. Throughout the paper we assume conservatively that Eve has control on channel losses and on η_B, that all errors are controlled by Eve (including dark counts), and that Bob's detection apparatus cannot resolve the photon number of arriving signals. Without these assumptions, one gets a relaxed security condition, which, however, is difficult to analyze and to justify. For example, Eve might shift the wavelength of the signals into a region of higher detection efficiency. Although each specific manipulation can be counterattacked, it seems an impossible task to categorically exclude all manipulations to the same effect. The same holds for the dark counts.

The total expected probability of detection events is given by

$$\begin{aligned} p_{\mathrm{exp}} &= p_{\mathrm{exp}}^{\mathrm{signal}} + p_{\mathrm{exp}}^{\mathrm{dark}} - p_{\mathrm{exp}}^{\mathrm{signal}} p_{\mathrm{exp}}^{\mathrm{dark}} \\ &\leq p_{\mathrm{exp}}^{\mathrm{signal}} + p_{\mathrm{exp}}^{\mathrm{dark}}. \end{aligned} \tag{2}$$

There are two differently contributing error mechanisms. The signal contributes an error with some probability due to misalignment or polarization diffusion. On the other hand, a dark count contributes with probability approximately 1/2 to the error rate. Therefore, considering the relevant limit of increased losses where the coincidence probability between a signal photon and a dark count can be neglected, we have for the error rate e (per sent signal) the approximate lower bound

$$e \gtrsim \tfrac{1}{2} p_{\mathrm{exp}}^{\mathrm{dark}}, \tag{3}$$

where "$x \gtrsim y$" means that x is approximately greater than or equal to y, when second-order terms are neglected. The contribution to the error rate per sifted key bit is then given by $p_e = e/p_{\mathrm{exp}}$.

If the error rate per sifted key bit p_e exceeds 1/4, there is no way to create a secure key. With such an allowed error rate, a simple intercept/resend attack (in which Eve measures in one of the two bases and resends according to her identification of the state) causes Bob and Eve to share (approximately) half of Alice's bits and to know nothing about the other half; hence, Bob does not possess information that is unavailable to Eve, and no secret key can be distilled. Using $p_e = e/p_{\mathrm{exp}}$ and $p_e < \frac{1}{4}$, we obtain a necessary condition for secure QKD,

$$e < \tfrac{1}{4} p_{\mathrm{exp}}\,, \tag{4}$$

and, using Eqs. (2) and (3), we finally obtain $p_{\mathrm{exp}}^{\mathrm{signal}} \gtrsim p_{\mathrm{exp}}^{\mathrm{dark}}$.

For ideal SP states we therefore obtain (with $p_{\mathrm{exp}}^{\mathrm{signal}} = F\eta_B$ and $p_{\mathrm{exp}}^{\mathrm{dark}} \approx 2d_B$) the bound $F\eta_B \gtrsim 2d_B$. We see that even for ideal SP sources, the existence of a dark count rate leads to a minimum transmission efficiency,

$$F > F_{\mathrm{SP}} \approx 2d_B/\eta_B \tag{5}$$

below which QKD cannot be securely implemented. Even for perfect detection efficiency ($\eta_B = 1$) we get a bound $F > F_{\mathrm{SP}} \approx 2d_B$. These bounds correspond, according to Eq. (1), to a maximal covered distance for fibers, which mainly depends on β.

In a quantum optical implementation, single-photon states would be ideally suited for quantum key distribution. However, such states have not yet been practically implemented for QKD, although proposals exist and experiments have been performed to generate them for other purposes [14]. In the experiments, the signals contain n photons in the signal polarization mode with probability p_n. The multiphoton part of the signals, $p_{\mathrm{multi}} = \sum_{i\geq 2} p_i$, leads to a severe security gap, as has been anticipated earlier [7,12,13]. Let us present the *photon number splitting* (PNS) attack, which is a modification of an attack suggested in [12] (which was disputed in [13]): Eve deterministically splits one photon off each multiphoton signal. To do so, she projects the state onto subspaces characterized by the total photon number n using a quantum nondemolition (QND) measurement. This projection does not modify the polarization of the photons. Then she performs a polarization-preserving splitting operation, for example, by an interaction described by a Jaynes-Cummings Hamiltonian [15] (for details see [6]) or an active arrangement of beam splitters combined with further QND measurements. She keeps one photon and sends the other $n - 1$ photons to Bob. When receiving the data regarding the basis, Eve measures her photon and obtains full information. Each signal containing more than one photon in this way will yield its complete information to an eavesdropper without leading to errors in the sifted key.

The situation becomes worse in the presence of loss, in which case the eavesdropper can replace the lossy channel by a perfect quantum channel and forward to Bob only chosen signals. This suppression is controlled such that Bob will find precisely the number of nonempty signals as expected given the lossy channel. If there is a strong contribution by multiphoton signals, then Eve can suppress the SP signals completely, to obtain full information on the transmitted bits. For an error-free setup, this argument leads to the necessary condition for security,

$$p_{\mathrm{exp}} > p_{\mathrm{multi}}\,, \tag{6}$$

where now the signal contribution is given by $p_{\mathrm{exp}}^{\mathrm{signal}} = \sum_i p_i[1 - (1 - F)^i]$. If this condition is violated, Eve gets full information without inducing any errors or causing a change in the expected detection rate.

We make here also an important observation, which is useful for positive security proofs. For a general source (emitting into the four BB84 polarization modes) Alice can dephase the states to create a mixture of Fock states in the chosen polarization mode. Consequently, Eve can be assumed to perform the QND part of the PNS attack without loss of generality since it does not change the signal state. In that case it is much easier to check that it is sufficient to consider the PNS attack only for the proof of unconditional security. In realistic scenarios the dephasing happens automatically due to the lack of a reference phase to the signals. Following this observation, a complete positive security proof against all individual particle attacks has been given [6].

Let us return to the necessary condition for security. We can combine the idea of the two criteria equations (4) and (6) above to a single, stronger one, given by

$$e < \tfrac{1}{4}(p_{\mathrm{exp}} - p_{\mathrm{multi}}) . \tag{7}$$

This criterion stems from the scenario that Eve splits all multiphoton signals while she eavesdrops on some of the single-photon signals—precisely on a proportion $(p_{\mathrm{exp}} - p_{\mathrm{multi}})/p_1$ of them—via the intercept/resend attack presented before, and suppresses all other single-photon signals. We can think of the key as consisting of two parts: an error-free part stemming from multiphoton signals, and a part with errors coming from single-photon signals. The rescaled error rate within the second part has therefore to obey the same inequality as used in criterion (4).

We now explore the consequences of the necessary condition for security for two practical signal sources. These are the weak coherent pulses and the signals generated by parametric down-conversion.

The WCP signal states are described by coherent states in the chosen signal polarization mode and contain, on average, much less than one photon. Coherent states $|\alpha\rangle = e^{-\alpha^2/2}\sum_n \alpha^n/\sqrt{n!}\,|n\rangle$ with amplitude α (chosen to be real) give a photon number distribution $p_n(\alpha^2) = e^{-\alpha^2}(\alpha^2)^n/n!$. Since we analyze PNS attacks only, it does not matter if the realistic "coherent state" is a mixture of number states. Thus, $p_{\mathrm{exp}}^{\mathrm{signal}} = \sum_{n=1}^{\infty} p_n(F\eta_{\mathrm{B}}\alpha^2)$ and $p_{\mathrm{multi}} = \sum_{n=2}^{\infty} p_n(\alpha^2)$. With $p_{\mathrm{exp}} \le p_{\mathrm{exp}}^{\mathrm{signal}} + 2d_{\mathrm{B}}$ and the error rate $e \gtrsim d_{\mathrm{B}}$ in Eq. (7) we find for $\alpha^2 \ll 1$ (by expanding to 4th order in α and neglecting the term proportional to $F^2\eta_{\mathrm{B}}^2\alpha^4$) the result

$$F \gtrsim \frac{2d_{\mathrm{B}}}{\eta_{\mathrm{B}}\alpha^2} + \frac{\alpha^2}{2\eta_{\mathrm{B}}} . \tag{8}$$

The optimal choice $\alpha^2 = 2\sqrt{d_{\mathrm{B}}}$ leads to the bound

$$F > F_{\mathrm{WCP}} \approx 2\sqrt{d_{\mathrm{B}}}/\eta_{\mathrm{B}} . \tag{9}$$

To illustrate this example we insert numbers $\eta_{\mathrm{B}} = 0.11$ and $d_{\mathrm{B}} = 5 \times 10^{-6}$ taken from the experiment performed at 1.3 μm by Marand and Townsend [16]. Then the criterion gives $F \gtrsim 0.041$. With a constant loss of 5 dB and a fiber loss at 0.38 dB/km, this is equivalent, according to (1), to a maximum distance of approximately 24 km in optical fibers at an average (much lower than standard) photon number of 4.5×10^{-3}. With $\alpha^2 = 0.1$, as in the literature, secure transmission to any distance is impossible, according to our conditions. Frequently we find even higher average photon numbers in the literature, although Townsend has demonstrated the feasibility of QKD with intensities as low as $\alpha^2 = 3 \times 10^{-5}$ at a wavelength of 0.8 μm [10].

The WCP scheme seems to be prone to difficulties due to the high probability of vacuum signals. This can be overcome in part by the use of a PDC scheme. Parametric down-conversion has been used before for QKD [17,18]. We use a different formulation, which enables us to analyze the advantages and limits of the PDC method relative to the WCP approach.

To approximate a SP state, we use a PDC process where we create the state in an output mode described by photon creation operator $a^\dagger$ conditioned on the detection of a photon in another mode described by $b^\dagger$. If we neglect dispersion, then the output of the PDC process is described [19] on the two modes with creation operators $a^\dagger$ and $b^\dagger$ using the operator $T_{ab}(\chi) = \exp\{\mathrm{i}\chi(a^\dagger b^\dagger - ab)\}$, with $\chi \ll 1$, as $|\Psi_{ab}\rangle = T_{ab}(\chi)\,|0,0\rangle \approx (1 - \chi^2/2 + \frac{5}{24}\chi^4)\,|0,0\rangle + (\chi - \frac{5}{6}\chi^3)\,|1,1\rangle + (\chi^2 - \frac{7}{6}\chi^4)\,|2,2\rangle + \chi^3|3,3\rangle + \chi^4|4,4\rangle$. The states in this description are states of photon flux, and we assume the addition of choppers to cut pulses out of the flux. To these pulses we can assign again photon numbers.

If we had an ideal detector resolving photon numbers (that is, a perfect counter), then we could create a perfect single-photon state by using the state in mode a conditioned on the detection of precisely one photon in the pulse in mode b. However, realistic detectors useful for this task have a single-photon detection efficiency far from unity and can resolve the photon number only at high cost, if at all. Therefore, we assume a detection model that is described by a finite detection efficiency η_{A} and gives only two possible outcomes: either it is not triggered or it is triggered, thereby showing that at least one photon was present. The detector may experience a dark count rate at d_{A} per time slot. The two elements of the positive operator valued measure describing this kind of detector can be approximated for our purpose by $E_0 = (1 - d_{\mathrm{A}})\,|0\rangle\langle 0| + \sum_{n=1}^{\infty}(1 - \eta_{\mathrm{A}})^n|n\rangle\langle n|$ and $E_{\mathrm{click}} = d_{\mathrm{A}}|0\rangle\langle 0| + \sum_{n=1}^{\infty}[1 - (1 - \eta_{\mathrm{A}})^n]\,|n\rangle\langle n|$. The reduced density matrix for the output signal in mode b conditioned on a click of the detector monitoring mode a is then given by

$$\rho = \frac{1}{N}\,\mathrm{Tr}_b[|\Psi_{ab}\rangle\langle\Psi_{ab}|E_{\mathrm{click}}] \approx \frac{1}{N}\left[d_{\mathrm{A}}\left(1 - \chi^2 + \frac{2}{3}\,\chi^4\right)|0\rangle\langle 0| + \eta_{\mathrm{A}}\chi^2\left(1 - \frac{5}{3}\,\chi^2\right)|1\rangle\langle 1| + \eta_{\mathrm{A}}(2 - \eta_{\mathrm{A}})\chi^4|2\rangle\langle 2|\right] \tag{10}$$

with the normalization constant N. To create the four signal states we rotate the polarization of the signal, for example using a beam splitter and a phase shifter.

After some calculation following the corresponding calculation in the WCP case, the necessary condition for security (7) takes for the signal state (10) the form

$$F \gtrsim \frac{2d_{\mathrm{A}}d_{\mathrm{B}}}{\eta_{\mathrm{A}}\eta_{\mathrm{B}}\chi^2} + \frac{2d_{\mathrm{B}}}{\eta_{\mathrm{B}}} + \frac{2-\eta_{\mathrm{A}}}{\eta_{\mathrm{B}}}\chi^2 \qquad (11)$$

since we assume $d_{\mathrm{B}} \ll 1$ and $\chi^2 \ll 1$ and neglect terms going as χ^4, $d_{\mathrm{B}}d_{\mathrm{A}}$, and $\chi^2 d_{\mathrm{B}}$. The first error term is due to coincidence of dark counts, the second error term is due to coincidence of a photon loss and a dark count at Bob's site, and the third term is the effect of multiphoton signal (signals that leak full information to the eavesdropper). As in the WCP case, the optimal choice of $\chi^2 = \sqrt{(2d_{\mathrm{A}}d_{\mathrm{B}})/[\eta_{\mathrm{A}}(2-\eta_{\mathrm{A}})]}$ leads to the necessary condition for security,

$$F > F_{\mathrm{PDC}} = 2\sqrt{\frac{2d_{\mathrm{A}}d_{\mathrm{B}}(2-\eta_{\mathrm{A}})}{\eta_{\mathrm{A}}\eta_{\mathrm{B}}^2}} + \frac{2d_{\mathrm{B}}}{\eta_{\mathrm{B}}}. \qquad (12)$$

If we now assume that Alice and Bob use the same detectors as in the WCP case with the numbers provided by [16], we obtain $F_{\mathrm{PDC}} \gtrsim 8.4 \times 10^{-4}$ corresponding via Eq. (1) to a distance of approximately 68 km in optical fibers.

Since we can use down-conversion setups that give photon pairs with different wavelength, we can use sources so that one photon has the right wavelength for transmission over long distances, e.g., 1.3 μm, while the other photon has a frequency that makes it easier to use efficient detectors [17]. In the limit of Alice using perfect detectors (but not perfect counters), $\eta_{\mathrm{A}} = 1$ and $d_{\mathrm{A}} = 0$, we obtain $F_{\mathrm{PDC}} \approx 2d_{\mathrm{B}}/\eta_{\mathrm{B}}$, as for single-photon sources, yielding a maximal distance of approximately 93 km.

We have shown a necessary condition for secure QKD which uses current experimental implementations. We find that secure QKD might be achieved with the present experiments using WCP if one would use appropriate parameters for the expected photon number, which are considerably lower than those used today. The distance that can be covered by QKD is mainly limited by the fiber loss, but, with $\alpha^2 > 0.1$, WCP schemes might be totally insecure even to zero distance due to imperfect detection. The distance can be increased by the use of parametric down-conversion as a signal source, but even in this case the fundamental limitation of the range persists.

The proposed "4 + 2" scheme [12], in which a strong reference pulse (as in [21]) from Alice is used in a modified detection process by Bob, might not suffer from the sensitivities discussed here, but the security analysis would have to follow different lines. The use of quantum repeaters (based on quantum error correction or entanglement purification) in the far future can yield secure transmission to any distance, and the security is not altered even if the repeaters are controlled by Eve [22].

We thank C.H. Bennett, J.H. Kimble, N. Gisin, E. Polzik, and H. Yuen for important comments. G.B. thanks Canada's NSERC, Québec's FCAR, and the Canada Council. N.L. is supported by Grant No. 43336 by the Academy of Finland. The work of T.M. was supported in part by Grant No. 961360 from the Jet Propulsion Lab, and Grant No. 530-1415-01 from the DARPA Ultra program.

[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, G. Brassard, and A. K. Ekert, Sci. Am. **267**, No. 4, 50 (1992).

[3] P.W. Shor, SIAM J. Comput. **26**, 1484 (1997).

[4] E. Biham and T. Mor, Phys. Rev. Lett. **79**, 4034 (1997); E. Biham, M. Boyer, G. Brassard, J. van de Graaf, and T. Mor, quant-ph/9801022.

[5] D. Mayers, in *Proceedings of Advances in Cryptology, CRYPTO '96* (Springer, Berlin, 1996), Vol. 1109, p. 343; D. Mayers, quant-ph/9802025; E. Biham, M. Boyer, P.O. Boykin, T. Mor, and V. Roychowdhury, in *Proceedings of the 32nd ACM Symposium on Theory of Computers* (ACM, New York, 2000), p. 715.

[6] N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000).

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

[8] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, IEEE Trans. Inf. Theory **41**, 1915 (1995).

[9] J. D. Franson and H. Ilves, J. Mod. Opt. **41**, 2391 (1994).

[10] P. D. Townsend, IEEE Photonics Technol. Lett. **10**, 1048 (1998).

[11] W. T. Buttler, R. J. Hughes, P. G. Kwiat, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson, and C. M. Simmons, Phys. Rev. A **57**, 2379 (1998).

[12] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A **51**, 1863 (1995).

[13] H. P. Yuen, Quantum. Semiclass. Opt. **8**, 939 (1996).

[14] J. Kim, O. Benson, H. Kan, and Y. Yamamoto, Nature (London) **397**, 500 (1999).

[15] Klaus Mølmer (private communication).

[16] C. Marand and P.D. Townsend, Opt. Lett. **20**, 1695 (1995).

[17] A. K. Ekert, J. G. Rarity, P.R. Tapster, and G.M. Palma, Phys. Rev. Lett. **69**, 1293 (1992).

[18] A. V. Sergienko, M. Atatüre, Z. Walton, G. Jaeger, B.E.A. Saleh, and M.C. Teich, Phys. Rev. A **60**, R2622 (1999).

[19] D.F. Walls and G.J. Milburn, *Quantum Optics* (Springer-Verlag, Heidelberg, 1994).

[20] K.J. Blow, R. Loudon, S.J.D. Phoenix, and T.J. Shepherd, Phys. Rev. A **42**, 4102 (1990).

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

[22] T. Mor, Ph.D. thesis, Technion, Haifa, 1997; quant-ph/9906073.