Experimental Error Filtration for Quantum Communication Over Highly Noisy Channels

L.-P. Lamoureux,[1] E. Brainis,[2] N. J. Cerf,[1] Ph. Emplit,[2] M. Haelterman,[2] and S. Massar[3,1]

[1]*Quantum Information and Communication, Ecole Polytechnique, CP 165/59, Université Libre de Bruxelles, Avenue F. D. Roosevelt 50, 1050 Bruxelles, Belgium*

[2]*Optique et Acoustique, CP 194/5, Université Libre de Bruxelles, Avenue F. D. Roosevelt 50, 1050 Bruxelles, Belgium*

[3]*Laboratoire d'Information Quantique, CP 165/59, Université Libre de Bruxelles, Avenue F. D. Roosevelt 50, 1050 Bruxelles, Belgium*

(Received 7 May 2004; published 13 June 2005)

Error filtration is a method for encoding the quantum state of a single particle into a higher dimensional Hilbert space in such a way that it becomes less sensitive to noise. We have realized a fiber optics demonstration of this method and illustrated its potentialities by carrying out the optical part of a quantum key distribution scheme over a line whose phase noise is too high for a standard implementation of BB84 to be secure. By filtering out the noise, a bit error rate of $15.3\% \pm 0.1\%$, which is beyond the security limit, can be reduced to $10.6\% \pm 0.1\%$, thereby guaranteeing the cryptographic security.

DOI: 10.1103/PhysRevLett.94.230501 PACS numbers: 03.67.Dd, 03.67.Hk, 42.50.Dv, 42.81.−i

One of the central results in quantum information is that errors can, in principle, be corrected [1,2]. This discovery transformed quantum information from an intellectual game into a field which could revolutionize the way we process information. Practical realizations of quantum error correcting codes are, however, extremely difficult because they require multiparticle interactions. A first experimental demonstration of quantum error correction has recently been realized [3], but it is still very far from being usable in practical applications. An alternative method, called *error filtration*, allows errors to be filtered out during quantum communication, and can in contrast be easily implemented using present technology [4]. The main idea of error filtration is to encode one qubit in a single particle within a Hilbert space of dimension greater than two. It is then possible to detect, with high probability, whether an error has occurred, and if so, to discard the state. This quantum error detection scheme is less powerful than full error correction, but, for many applications such as quantum key distribution (QKD), discarding the state affected by noise is sufficient. The advantage of this method is that the encoding and decoding operations do not require multiparticle interactions, hence they are relatively easy to implement by interferometric techniques.

Here, we report on a proof-of-principle experimental demonstration of the capabilities of error filtration. For a detailed theoretical introduction to the method, we refer to [4] where it is also shown that error filtration can be extended to the purification of entanglement. Our experimental scheme is based on the fiber optics "plug-and-play" quantum cryptosystem [5,6] and its extension to more than two dimensions introduced in [7]. The interest of error filtration is illustrated by performing the optical part of a QKD scheme over a noisy quantum communication channel with so much noise that a secure BB84 protocol cannot be realized. (BB84, introduced in [8], is the standard protocol used in QKD. It is based on the use of two maximally conjugate bases in a two dimensional space.) It is known that if the bit error rate (BER) exceeds 14.6%, then a simple cloning attack makes the BB84 protocol insecure. On the other hand, if the BER is lower than 11.0%, then the BB84 protocol is provably secure; see [9] for a review. Between the two boundaries lies a gray zone where the security of BB84 is unknown [10]. In our experiment, we consider an error prone QKD scheme with a BER $= 15.3\% \pm 0.1\%$, which is therefore insecure. Using error filtration, the BER is brought down to $10.6\% \pm 0.1\%$ so that QKD is rendered secure. Nevertheless, the present work will probably not have immediate practical applications because phase noise is not the main limiting factor in present day QKD. However, better detectors and new techniques such as quantum repeaters (see [11] for a recent proposal) will be used in the future. Then, the contribution of phase noise could become the main limiting factor and error filtration could provide a solution. Finally, note that it was realized previously that the use of higher dimensional systems can increase the resistance of QKD to noise [12]. Error filtration presents advantages over these earlier suggestions as we discuss below.

Our experimental error filtration setup works with attenuated coherent states traveling in localized time bins in optical fibers (standard SMF-28); see Fig. 1. Bob uses a laser diode at 1.55 μm to produce a 3 ns light pulse. The pulse is attenuated by an optical attenuator (Agilent

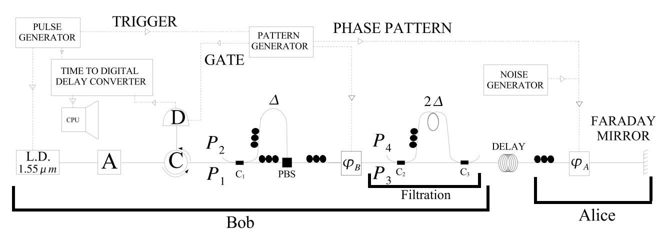

FIG. 1. Fiber optics QKD setup with error filtration. **A** represents the attenuator, **C** the circulator, and **D** the single photon detector.

8156A), and then split by a first 50/50 coupler (C_1) to produce two pulses. These pulses impinge on the input ports of a polarization beam splitter (PBS) with a time delay $\Delta = 60$ ns. Their polarizations are rotated, using polarization controllers, so that the two pulses exit by the same port of the PBS. Next, the two pulses are processed through an unbalanced Mach-Zehnder (MZ) interferometer C_2C_3 with a path length difference equivalent to 2Δ. This produces four emerging pulses traveling down a 900 ns delay line (representing the noisy communication channel). Then, at Alice's site, the pulses are reflected back by a Faraday mirror. The use of a Faraday mirror makes the setup insensitive to birefringence in the delay line. Alice may modify the phases of the four pulses using a phase modulator (ϕ_A) (Trilink) controlled by a pattern generator (Agilent 81110A). When they reach Bob's site, the pulses pass through the MZ interferometer and interfere at the C_2 coupler, which, as we shall show, realizes error filtration. The six emerging pulses then travel trough Bob's phase modulator (ϕ_B) (Trilink) and the PBS to the coupler C_1, where they interfere and are sent to a single-photon detector (id Quantique id200) via a circulator. The detector was gated by a pattern generator during a 5 ns window around the arrival time of the central pulse. Its output was registered using a time-to-digital delay converter (ACAM-GP1) connected to a computer. All electronic components were triggered by a pulse generator (Standford Research Inc. DG355). In order to maximize the interference visibilities, polarization controllers were introduced in the long arm of the MZ interferometer and in front of the polarization-sensitive phase modulators. Once optimized, the setup was stable for days.

Before discussing error filtration, let us first consider the case where the MZ interferometer C_2C_3 is absent. Then our setup is identical to the plug-and-play quantum cryptography setup [5]. The wave function describing the state after Alice has encoded her phase ϕ_A can be written as $\frac{1}{\sqrt{2}}(|t_0\rangle_H - e^{i\phi_A}|t_1\rangle_V)$, where the subscripts H and V represent the polarization states while the subscripts 0 and 1 represent the relative delay of time bin i, i.e., $t_i = i \cdot \Delta$. In the BB84 protocol, the phase ϕ_A must be chosen randomly in $\{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\}$. The (-1) phase in front of $|t_1\rangle_V$ takes into account the conventional relative phase of $\pi/2$ between the reflected and transmitted light at coupler C_1 and at the PBS. The state leaving Alice's site thus reads

$$|\psi\rangle = \frac{1}{\sqrt{2}}[|t_0\rangle_V - e^{i\phi_A}|t_1\rangle_H], \tag{1}$$

where the polarizations have been interchanged because of the Faraday mirror.

Intrinsic noise in the plug-and-play QKD scheme is actually very low, see [6], so that in our experiment we had to simulate the noisy channel by making Alice's phase modulator imperfect. This was achieved by electronically combining the signal from the pattern generator with the output of a function generator (Agilent 33250A) producing Gaussian electronic noise with an adjustable amplitude and a 50 MHz 3 dB bandwidth. Since the time bins are separated by 60 ns, the phase noise in the successive time bins can be considered as independent. The state produced by Alice is thus

$$\frac{1}{\sqrt{2}}[e^{i\varphi_0}|t_0\rangle_V - e^{i(\phi_A+\varphi_1)}|t_1\rangle_H], \tag{2}$$

where the φ_i's are independent random phases drawn from a Gaussian probability distribution $P(\varphi_i) = \frac{1}{\sqrt{2\pi\sigma^2}} \times \exp[-\varphi_i^2/(2\sigma^2)]$ of tunable variance σ^2. The density matrix obtained by averaging over the random phases is $\rho = e^{-\sigma^2}|\psi\rangle\langle\psi| + (1 - e^{-\sigma^2})\mathbb{1}/2$, so that phase noise amounts to the admixture of isotropic noise. In terms of bit error rate, this noise level thus corresponds to $\mathrm{BER} = 1 - \langle\psi|\rho|\psi\rangle = (1 - e^{-\sigma^2})/2$.

The two pulses travel back to Bob, who performs a measurement in the $\frac{1}{\sqrt{2}}(|t_0\rangle_V \mp e^{-i\phi_B}|t_1\rangle_H)$ basis by applying the phase $\phi_B \in \{0, \frac{\pi}{2}\}$. Bob's detector is connected to either output port P_1 or P_2. The probability for Bob to detect a count (assuming a perfect detector) is $\frac{1}{2} \pm \frac{1}{2} \times \cos(\varphi_1 - \varphi_0 + \phi_A + \phi_B)$ where the sign depends on which output port is used. The predicted visibility of the

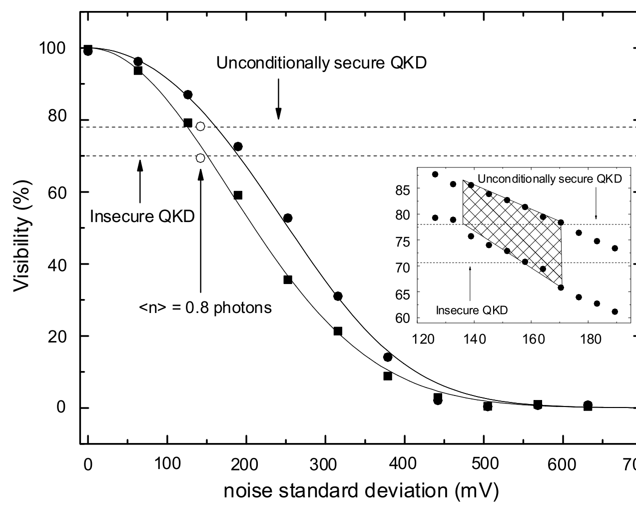

FIG. 2. Visibility (detector dark counts subtracted) as a function of the standard deviation of the noise signal produced by the function generator. The proportionality factor between the x axis and σ was determined by fitting the experimental data without filtration with Eq. (3). The squares (full circles) represent the measured visibilities without (with) filtration, while the curves are the theoretical predictions of Eqs. (3) and (7). The open circles show filtration in the quantum regime where the state sent by Alice contains on average 0.8 photons (which is in the regime where QKD is secure against photon-number splitting attacks [13]). The inset magnifies the data in the region where one passes from an insecure ($V \leq 70.7\%$) to a secure ($V > 78.0\%$) QKD protocol. The crisscrossed area shows that a visibility that is either insecure or of unknown security can be increased to a provably secure one. By averaging over 200 000 runs, the error bars were made smaller than the plotting points.

interference fringes measured by Bob is

$$V = \frac{I_{\max} - I_{\min}}{I_{\max} + I_{\min}} = e^{-\sigma^2}. \quad (3)$$

The measured values of V (after subtracting dark counts) agree well with this prediction; see the lower curve in Fig. 2. Note that the visibility is related to the bit error rate via BER $= (1 - V)/2$.

The idea of error filtration is that if the noise on the different time bins is independent, then one can reduce its effect by using more than two time bins. Indeed, if the receiver lets several time bins interfere then the noise will have a tendency to average out in the useful constructive port, while the anticorrelated part of the noise is rejected. This globally reduces the noise at the expense of intensity; see [4]. In order to implement this idea we use the additional MZ interferometer C_2C_3. Each pulse exiting from the PBS is split into two pulses by the MZ interferometer according to $|t_0\rangle_H \rightarrow (|t_0\rangle_H - |t_2\rangle_H)/2$, $|t_1\rangle_V \rightarrow (|t_1\rangle_V - |t_3\rangle_V)/2$. The factor 1/2 takes into account that half of the intensity is lost at coupler C_3. After Alice has encoded her phase ϕ_A and the pulses have been reflected by the Faraday mirror, the state becomes

$$\frac{1}{2\sqrt{2}}[|t_0\rangle_V - |t_2\rangle_V - e^{i\phi_A}(|t_1\rangle_H - |t_3\rangle_H)]. \quad (4)$$

This is formally identical to the BB84 protocol since Alice effectively uses the two-dimensional space S spanned by $(|t_0\rangle_V - |t_2\rangle_V)$ and $(|t_1\rangle_H - |t_3\rangle_H)$. The time bins t_2 and t_3 are just replicas of the time bins t_0 and t_1, respectively. Then, because of the noise, the four pulses get random phases φ_0, φ_1, φ_2, and φ_3, respectively. The state that Alice sends back to Bob is thus

$$\frac{1}{2\sqrt{2}}[e^{i\varphi_0}|t_0\rangle_V - e^{i\varphi_2}|t_2\rangle_V - e^{i\phi_A}(e^{i\varphi_1}|t_1\rangle_H - e^{i\varphi_3}|t_3\rangle_H)].$$

It now belongs to the full space spanned by $|t_0\rangle_V$, $|t_1\rangle_V$, $|t_2\rangle_H$, and $|t_3\rangle_H$, since the phase noise has taken it out of the space S. The idea of error filtration is for Bob to project the state back onto S in order to selectively enhance the visibility. This projection is realized by the MZ interferometer. At coupler C_3 each time bin has amplitude $1/\sqrt{2}$ of following the long path and amplitude $1/\sqrt{2}$ to follow the short path. The resulting state after C_2 is

$$\frac{1}{4\sqrt{2}}[e^{i\varphi_0}|t_0\rangle_V - e^{i(\phi_A+\varphi_1)}|t_1\rangle_H - (e^{i\varphi_0} + e^{i\varphi_2})|t_2\rangle_V + e^{i\phi_A}(e^{i\varphi_1} + e^{i\varphi_3})|t_3\rangle_H + e^{i\varphi_2}|t_4\rangle_V - e^{i(\phi_A+\varphi_3)}|t_5\rangle_H)]. \quad (5)$$

Time bins t_0, t_1, t_4, t_5 will not be used. As we discuss below, their appearance is due to the specific implementation we use and gives rise to a loss which is not intrinsic to the method.

Bob now realizes his measurement by putting his phase ϕ_B on time bins 1, 3, and 5: $|t_{1,3,5}\rangle \rightarrow e^{i\phi_B}|t_{1,3,5}\rangle$. At the PBS the V-polarized photons take the long path whereas the H-polarized photons take the short path. The state at the output of C_1 is

$$\frac{-1}{4\sqrt{2}}[(e^{i\varphi_0} \pm e^{i(\phi_A+\phi_B+\varphi_1)})|t_1\rangle + (e^{i\varphi_2} \pm e^{i(\phi_A+\phi_B+\varphi_3)})|t_5\rangle - [(e^{i\varphi_0} + e^{i\varphi_2}) \pm e^{i(\phi_A+\phi_B)}(e^{i\varphi_1} + e^{i\varphi_3})]|t_3\rangle], \quad (6)$$

where the $\pm$ sign depends on which output port (P_1 or P_2) the state exits.

When the photon comes out in time bin t_3, the visibility of the interference fringes, assuming that the noise affecting the different time bins is independent, is

$$V = 2/(1 + e^{\sigma^2}). \quad (7)$$

Comparing with Eq. (3) we see that filtration affects an increase of visibility.

The generalization of Eq. (7) to the case where Alice uses $2N$ time bins to encode her qubit is immediate. One finds that the visibility becomes $V_{2N} = N/(N - 1 + e^{\sigma^2})$; see [4].

There are two sources of loss in the above implementation. The first is not intrinsic to the method and is due to the photons ending up in time bins t_1 and t_5 after Bob's measurement, see Eq. (6), which do not have improved visibility and are therefore discarded. In principle this could be remedied by replacing coupler C_3 by a switch that deterministically sends pulses t_0 and t_1 in the initial state Eq. (5) along the long path and pulses t_2 and t_4 along the short path. We did not implement this because high speed low loss switches do not exist commercially at present. The second source of loss is intrinsic to the method of error filtration: visibility is enhanced by separating the signal into two components: a noisy one which is discarded and a good one which is kept. This intrinsic loss occurs in our experiment at coupler C_2 in time bins t_2, t_3 where the light emerging from the unused output port (P_4) is completely noisy and is simply discarded. The probability of discarding the state in port P_4 is zero in the absence of noise and increases to 1/2 as the amount of noise increases. This should be contrasted with the fact that no intrinsic losses occur at coupler C_1: both output ports P_1 and P_2 contain useful information.

The measured average visibilities (after subtracting detector dark counts) are plotted in Fig. 2 as a function of the phase-noise standard deviation in the case where Alice applies $\phi_A = 0$ and Bob measures the output port P_1. In this case, without noise, the maximal visibilities exceeded 99%. With unfiltered noise (lower curve), the visibility decreases exponentially with the amount of noise in accordance with Eq. (3). The filtration achieved by our setup (upper curve) is also very close to the theoretical prediction of Eq. (7). Visibilities in the range from 65% to 78% are enhanced, by filtration, to the range from 78% to 85%; see inset of Fig. 2. Noting that the security threshold BER $<$ 11.0% translates into $V > 78.0\%$ while the insecurity threshold BER $\geq$ 14.6% corresponds to $V \leq 70.7\%$, we conclude that our setup transforms a BB84 protocol which is insecure (or of unknown security) into a provably secure one. Note that the visibilities were also tested for the other possible values of $\phi_A = \pi/2$, π, $3\pi/2$ used in the BB84 protocol and for both ports P_1 and P_2. The visibilities all exceeded 97.2% in the case where no noise is added. The lowest visibilities are associated with the cases where Alice and Bob choose the $\{\frac{\pi}{2}, \frac{3\pi}{2}\}$ basis since then both parties must apply a potential to their phase modulator which makes the setup noisier.

In Fig. 2, the visibilities were measured in a regime where the overall number of photons in all time bins when they leave Alice's site is approximately 120 photons. In this way, the dark counts of the detector are negligible. To consider a realistic QKD implementation, we also ran the experiment in the regime where the quantum state sent by Alice back to Bob contains on average approximately 0.8 photons in total (which is in the regime where QKD is secure against photon-number splitting attacks [13]). The difficulty in this case is that dark counts become very important (they give a raw error rate of about 30%) because we use 3-ns pulses [14]. Nevertheless, we were able to show in this regime that a visibility of 69.4% $\pm$ 0.2% in the absence of filtration can be turned into 78.8% $\pm$ 0.2% by filtration (where the statistical error due to subtracting the dark counts was calculated for a 95% confidence level); see open circles in Fig. 2. These visibilities are averaged over all four choices of ϕ_A and for the two output ports P_1 and P_2, so they are the relevant quantities for characterizing a QKD scheme. This averaging explains why these points lie slightly off the curves in Fig. 2. Note that in QKD the errors due to the dark counts can in principle be removed using error correction codes without altering the security, although in practice this is probably impossible for the high level of dark counts we have here.

We conclude by comparing this method with other QKD schemes that use higher dimensional systems [12]. The noise model in both cases is the same: a d-dimensional state $|\psi\rangle$ entering the communication channel exits as $\rho = e^{-\sigma^2}|\psi\rangle\langle\psi| + (1 - e^{-\sigma^2})\mathbb{1}/d$. This makes the comparison meaningful. The QKD schemes based on sets of mutually unbiased bases considered in [12] can only tolerate a noise level up to $e^{-\sigma^2} < 1/2$. This is because when $e^{-\sigma^2} = 1/2$, there is a simple attack in which the eavesdropper (Eve) does not modify the state with probability $1/2$, while with probability $1/2$, she keeps the state and sends a random one instead. In contrast, error filtration can tolerate arbitrarily high levels of noise if d is sufficiently large since the visibility V_d tends to 1 for large d and fixed $e^{-\sigma^2}$. The reason why the above attack no longer works in the case of error filtration is that when Eve replaces the quantum state by a random one, the filtration preferentially removes the corresponding noisy term. In other words, the noise is replaced by a higher effective loss. On the other hand, this means that a QKD scheme using error filtration can be vulnerable to attacks which exploit loss when weak coherent states are used, such as photon splitting attacks. However, recent work [13] shows that this is a less serious issue than initially thought.

In summary, the present experiment demonstrates the optical part of a quantum key distribution scheme which can operate with a phase-noise level that is too high for a standard implementation of the BB84 to be secure. This demonstrates the power and simplicity of error filtration as a practical method for circumventing phase noise in quantum communication.

We are pleased to thank N. Gisin, S. Popescu, and N. Linden for helpful discussions. We acknowledge financial support from the Communauté Française de Belgique under ARC 00/05-251 and from the IUAP programme of Belgian government under Grant No. V-18.

[1] P. W. Shor, Phys. Rev. A **52**, R2493 (1995); A. M. Steane, Phys. Rev. Lett. **77**, 793 (1996).
[2] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).
[3] J.-W. Pan, S. Gasparoni, R. Ursin, G. Weihs, and A. Zeilinger, Nature (London) **423**, 417 (2003).
[4] N. Gisin, N. Linden, S. Massar, and S. Popescu, quant-ph/0407021 [Phys. Rev. A (to be published)].
[5] G. Ribordy *et al.*, Electron. Lett. **34**, 2116 (1998).
[6] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, New J. Phys. **4**, 41 (2002).
[7] E. Brainis, L.-P. Lamoureux, N. J. Cerf, Ph. Emplit, M. Haelterman, and S. Massar, Phys. Rev. Lett. **90**, 157902 (2003).
[8] C. H. Bennett and G. Brassard, *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179.
[9] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[10] These bounds refer to BB84 with one way classical postprocessing which is the case in all practical implementations. For two way postprocessing the bounds change. See H.-K. Lo and D. Gottesman, IEEE Trans. Inf. Theory **49**, 457 (2003).
[11] I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, and N. Gisin, Nature (London) **421**, 509 (2003).
[12] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002).
[13] H.-K. Lo, X. Ma, and K. Chen, quant-ph/0407021 [Phys. Rev. Lett. (to be published)].
[14] By using shorter laser pulses, we should be able to decrease the dark count rate by at least a factor of 10.