Effects of single-qubit quantum noise on entanglement purification

G. Benenti[1,2,a], S. Felloni[3], and G. Strini[4]

[1] Center for Nonlinear and Complex Systems, Università degli Studi dell'Insubria, Via Valleggio 11, 22100 Como, Italy
[2] Istituto Nazionale per la Fisica della Materia, Unità di Como and Istituto Nazionale di Fisica Nucleare, Sezione di Milano, 20133 Milano, Italy
[3] Dipartimento di Matematica, Università degli Studi di Milano, via Saldini 50, 20133 Milano, Italy
[4] Dipartimento di Fisica, Università degli Studi di Milano, via Celoria 16, 20133 Milano, Italy

Abstract. We study the stability under quantum noise effects of the quantum privacy amplification protocol for the purification of entanglement in quantum cryptography. We assume that the E91 protocol is used by two communicating parties (Alice and Bob) and that the eavesdropper Eve uses the isotropic Bužek-Hillery quantum copying machine to extract information. Entanglement purification is then operated by Alice and Bob by means of the quantum privacy amplification protocol and we present a systematic numerical study of the impact of all possible single-qubit noise channels on this protocol. We find that both the qualitative behavior of the fidelity of the purified state as a function of the number of purification steps and the maximum level of noise that can be tolerated by the protocol strongly depend on the specific noise channel. These results provide valuable information for experimental implementations of the quantum privacy amplification protocol.

PACS. 03.65.Yz Decoherence; open systems; quantum statistical methods – 03.67.Hk Quantum communication – 03.67.Dd Quantum cryptography

1 Introduction

A central problem of quantum communication is how to reliably transmit quantum information through a noisy quantum channel. The carriers of information (the qubits) unavoidably interact with the external world, leading to phenomena such as decoherence and absorption. In particular, if a member of a maximally entangled EPR (Einstein-Podolsky-Rosen) pair is transmitted from a sender (known as Alice) to a receiver (Bob) through a quantum channel, then noise in the channel can degrade the amount of entanglement of the pair. This problem is of primary importance for entanglement-based quantum cryptography. Indeed, in the idealized E91 protocol [1] Alice and Bob share a large number of maximally entangled states. Entanglement purification techniques exist [2,3]. In particular, they have been applied to quantum cryptography: in reference [4] a quantum privacy amplification (QPA) iterative protocol was proposed, that eliminates entanglement with an eavesdropper by creating a small number of nearly perfect (pure) EPR states out of a large number of partially entangled states. This protocol is based on the so-called LOCC, that is on local quantum

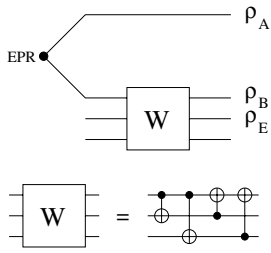[a] e-mail: giuliano.benenti@uninsubria.it

operations (quantum gates and measurements performed by Alice and Bob on their own qubits), supplemented by classical communication.

Under realistic conditions, the quantum operations themselves are unavoidably affected by errors and introduce a certain amount of noise. A first study of the impact of these errors on the QPA protocol was made in reference [5] and conditions for the security of QPA were found. However, the noise model considered in [5] was not the most general one. In particular, error channels like the amplitude damping or thermal excitations were not considered.

Studies of the impact of noise on the stability of quantum computation and communication are of primary importance for the practical implementation of quantum information protocols. In this paper, for the first time *all* single-qubit quantum noise channels are studied and compared and their different impact on the quantum privacy amplification protocol is elucidated. Errors acting on single qubits are described most conveniently using the Bloch sphere picture: quantum noise acting on a single qubit is described by 12 parameters, associated to rotations, deformations and displacements of the Bloch sphere. We study in detail the effects of these different errors and show that they impact *very differently* on the QPA algorithm.

Fig. 1. Top: quantum circuit representing the intrusion (by means of the Bužek-Hillery copying machine) of the eavesdropper Eve in the E91 protocol. The density matrices ρ_A, ρ_B and ρ_E represent the states of Alice's qubit, Bob's qubit and Eve's qubit after tracing over all other qubits. Bottom: decomposition of the unitary transformation W in four CNOT gates. By definition, $\mathrm{CNOT}|x\rangle|y\rangle = |x\rangle|y \oplus x\rangle$, with $x, y = 0, 1$ and $\oplus$ indicating addition modulo 2. The first (x) qubit in the CNOT gate acts as a control (full circle in the figure) and the second (y) as a target qubit ($\oplus$ symbol). Here and in the following circuits, any sequence of logic gates must be read from the left (input) to the right (output). From bottom to top, qubits run from the least significant to the most significant.

In particular, errors giving a displacement of the Bloch sphere are very dangerous. These results provide valuable information for experimentalists: indeed, knowing what are the most dangerous noise channels is useful to address experiments towards implementations for which these channels have negligible impact.

The paper is organized as follows. The eavesdropper's attack strategy is described in Section 2. Here we assume that the eavesdropper Eve attacks the qubits sent by Alice to Bob by means of the quantum copying machine of Bužek and Hillery [6]. As a result, Alice and Bob share partially entangled pairs. Each pair is now entangled with the environment (Eve's qubits) and described by a density operator. The QPA protocol, reviewed in Section 3, can be used to purify entanglement and, as a consequence, reduce the entanglement with any outside system to arbitrarily low values (a maximally entangled EPR pair is a pure state automatically deentangled from the outside world). We then consider the effects of noise acting on the purification protocol. The most general single-qubit noise channels are discussed in Section 4. We model each noise channel by means of equivalent quantum circuits, from which the usual Kraus representation and the transformation (rotation, deformation or displacement) of the Bloch sphere coordinates can be derived. The impact of these errors on the entanglement purification is discussed in Section 5. Finally, in Section 6 we present our conclusions.

2 Eavesdropping

We assume that Alice has at her disposal a source of EPR pairs and sends a member of each pair to Bob. The eavesdropper Eve wants, on one hand, to find out as much information as possible on the transmitted qubits and, on the other hand, make his intrusion as unknown as possible to Alice and Bob. Isotropic cloning by means of the Bužek-Hillery machine [6] is the most natural way to meet these two requirements. We also note that isotropy is necessary only in the case in which Alice and Bob use a six-state protocol, that is, the measurements are performed along the x-, y- and z-axis of the Bloch sphere. The isotropy condition may be relaxed when Alice and Bob use a four-state protocol: they measure only along x and z and Eve knows what are the measurement axes. In this case, it would be sufficient for Eve to send Bob qubits that reproduce as faithfully as possible the x and z-coordinates, but with no constraints about y. We have also studied this case (non
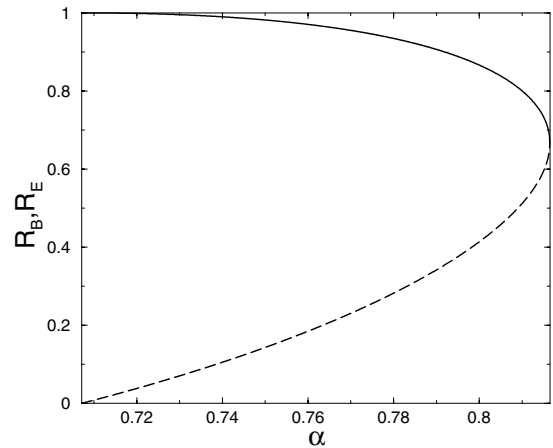
Fig. 2. Ratios R_B (solid line) and R_E (dashed line) for the isotropic Bužek-Hillery copying machine versus the parameter α.

isotropic cloning) but not reported it on the paper for the sake of simplicity.

In the following we assume that, as shown in Figure 1, Eve attacks the qubits sent by Alice using the Bužek-Hillery machine [6]. The two bottom qubits in Figure 1 are prepared by Eve in the state

$$|\Phi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle \qquad (1)$$

and we assume that $\alpha, \beta, \gamma, \delta$ are real parameters. Let us call ρ_B and ρ_E the density matrices describing the final states of Bob's qubit and Eve's qubit. As we have said, we assume isotropy, that is, if we call (x, y, z) the coordinates of the qubit sent from Alice to Bob before eavesdropping, then the Bloch sphere coordinates (x_B, y_B, z_B) and (x_E, y_E, z_E) associated to ρ_B and ρ_E are such that $x_B/x = y_B/y = z_B/z \equiv R_B$ and $x_E/x = y_E/y = z_E/z \equiv R_E$. As shown in Appendix 6, these conditions are fulfilled for

$$\beta = \frac{\alpha}{2} - \sqrt{\frac{1}{2} - \frac{3}{4}\alpha^2}, \quad \gamma = 0, \quad \delta = \frac{\alpha}{2} + \sqrt{\frac{1}{2} - \frac{3}{4}\alpha^2}. \quad (2)$$

It can be checked by direct computation (see again Appendix A) that in this case $(x_B, y_B, z_B) = 2\alpha\delta(x, y, z)$ and $(x_E, y_E, z_E) = 2\alpha\beta(x, y, z)$. Since the Bloch sphere coordinates must be real and nonnegative, we obtain $1/\sqrt{2} \leq \alpha \leq 2/\sqrt{6}$. The ratios R_B and R_E are shown in Figure 2. It can be seen that the two limiting cases $\alpha = 1/\sqrt{2}$ and $\alpha = 2/\sqrt{6}$ correspond to no intrusion ($x_B = x$, $y_B = y$, $z_B = z$) and maximum intrusion ($x_E = x_B$, $y_E = y_B$,
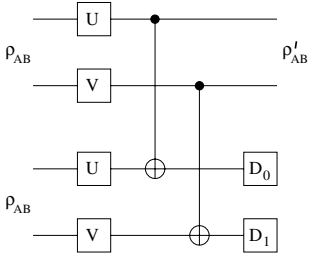
Fig. 3. Schematic drawing of the QPA entanglement purification scheme. Note that the density matrix ρ'_{AB} describes the two top qubits only when the detectors D_0 and D_1 give the same outcome.

$z_E = z_B$), respectively. In the first case, the qubit sent from Alice to Bob is not attacked. In the latter case Eve makes two imperfect identical copies of the original qubit (symmetric Bužek-Hillery machine), that is $\rho_E = \rho_B$: in this way Eve both optimizes the information obtained about the transmitted state and minimizes the modification of the qubit received by Bob. The degree of Eve's intrusion is therefore conveniently measured by the intrusion parameter

$$f_\alpha = \frac{\alpha - 1/\sqrt{2}}{2/\sqrt{6} - 1/\sqrt{2}}, \qquad (3)$$

with $0 \le f_\alpha \le 1$.

3 Quantum privacy amplification

We assume that Alice and Bob purify entanglement by means of the QPA protocol [4]. This is an iterative procedure, which we briefly review in what follows. At each iteration, the EPR pairs are combined in groups of two. The following steps are then taken for each group (see Fig. 3):

- Alice applies to her qubits a $\pi/2$ rotation about the x-axis of the Bloch sphere, described by the unitary matrix

$$U = R_x\left(\frac{\pi}{2}\right) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & -i \\ -i & 1 \end{bmatrix}; \qquad (4)$$

- Bob applies to his qubits the inverse operation

$$V = U^{-1} = R_x\left(-\frac{\pi}{2}\right) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix}. \qquad (5)$$

- both Alice and Bob perform a CNOT gate (defined in the caption of Fig. 1) using their members of the two EPR pairs;
- they measure the polarizations σ_z of the two target qubits;
- Alice and Bob compare the measurement outcomes by means of a public classical communication channel. If the outcomes coincide, the control pair is kept for the next iteration and the target pair discarded. Otherwise, both pairs are discarded.

In order to illustrate the working of the QPA procedure, let us consider the special case in which the initial mixed pairs are described by the density matrix ρ_{AB} obtained from the ideal EPR state $|\phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ after application of the Bužek-Hillery copying machine with

intrusion parameter f_α. After application of the unitary transformation W in Figure 1 the overall state of the four-qubit system becomes

$$(\alpha|0000\rangle + \beta|0101\rangle + \gamma|0110\rangle + \delta|0011\rangle$$
$$+ \alpha|1111\rangle + \beta|1010\rangle + \gamma|1001\rangle + \delta|1100\rangle)/\sqrt{2}. \quad (6)$$

After tracing over Eve's two qubits, we obtain

$$\rho_{AB} = \frac{1}{2} \begin{bmatrix} \alpha^2 + \delta^2 & 0 & 0 & 2\alpha\delta \\ 0 & \beta^2 + \gamma^2 & 2\beta\gamma & 0 \\ 0 & 2\beta\gamma & \beta^2 + \gamma^2 & 0 \\ 2\alpha\delta & 0 & 0 & \alpha^2 + \delta^2 \end{bmatrix}. \quad (7)$$

We note that this state is diagonal in the so-called Bell basis $\{|\phi^\pm\rangle = (|00\rangle \pm |11\rangle)/\sqrt{2}, |\psi^\pm\rangle = (|01\rangle \pm |10\rangle)/\sqrt{2}\}$. Indeed, we have

$$\rho_{AB} = A|\phi^+\rangle\langle\phi^+| + B|\phi^-\rangle\langle\phi^-|$$
$$+ C|\psi^+\rangle\langle\psi^+| + D|\psi^-\rangle\langle\psi^-|, \qquad (8)$$

where $A = (\alpha+\delta)^2/2$, $B = (\alpha-\delta)^2/2$, $C = (\beta+\gamma)^2/2$ and $D = (\beta - \gamma)^2/2$. The quantum circuit in Figure 3 maps the state ρ_{AB} of the control pair, in the case in which it is not discarded, onto another state ρ'_{AB} diagonal in the Bell basis. Namely, ρ'_{AB} can be expressed in the form (8), provided that new coefficients (A', B', C', D') are used instead of (A, B, C, D):

$$A' = \frac{A^2 + D^2}{N}, \quad B' = \frac{2AD}{N},$$
$$C' = \frac{B^2 + C^2}{N}, \quad D' = \frac{2BC}{N}, \qquad (9)$$

where $N = (A+D)^2 + (B+C)^2$ is the probability that Alice and Bob obtain coinciding outcomes in the measurement of the target qubits. Note that map (9) is nonlinear as a consequence of the strong nonlinearity of the measurement process. The fidelity after the purification procedure is given by

$$F = \langle\phi^+|\rho'_{AB}|\phi^+\rangle \qquad (10)$$

(note that $F = A'$). This quantity measures the probability that the control qubits would pass a test for being in the state $|\phi^+\rangle$. Map (9) can be iterated and we wish to drive the fidelity to one. It is possible to prove [7] that this map converges to the target point $A = 1, B = C = D = 0$ for all initial states (8) with $A > 1/2$. This means that, when this condition is satisfied and a sufficiently large number of initial pairs is available, Alice and Bob can distill asymptotically pure EPR pairs. Note that the quantum privacy amplification procedure is rather wasteful, since at least half of the pairs (the target pairs) are lost at every iteration. This means that to extract one pair close to the ideal EPR state after n steps we need at least 2^n mixed pairs at the beginning. However, this number can be significantly larger, since pairs must be discarded when Alice and Bob obtain different measurement outcomes. We
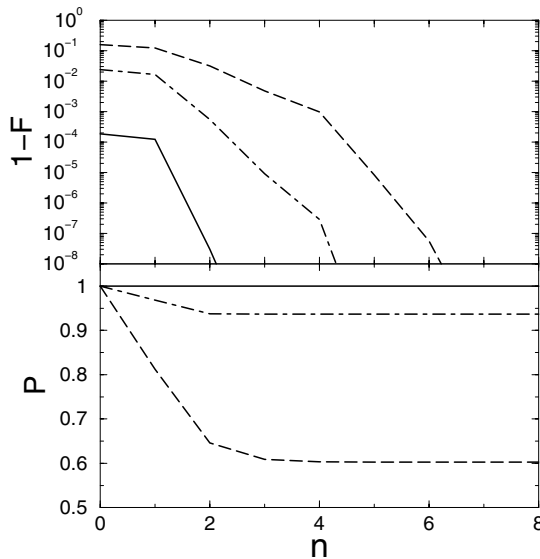
Fig. 4. Deviation $1 - F$ of the fidelity F from the ideal case $F = 1$ (top) and survival probability P (bottom) as a function of the number of iterations n of map (9). The different curves correspond to the intrusion parameter $f_\alpha = 0.95$ (dashed line), 0.5 (dot-dashed line) and 0.05 (solid line).

therefore compute the survival probability $P(n)$, measuring the probability that a n-step QPA protocol is successful. More precisely, if p_i is the probability that Alice and Bob obtain coinciding outcomes at step i, we have

$$P(n) = \prod_{i=1}^{n} p_i. \qquad (11)$$

The efficiency $\xi(n)$ of the algorithm is given by the number of obtained pure EPR pairs divided by the number of initial impure EPR pairs. We have

$$\xi(n) = \frac{P(n)}{2^n}. \qquad (12)$$

Both the fidelity and the survival probability are shown in Figure 4. The different curves of this figure correspond to values of the intrusion parameter from $f_\alpha = 0.05$ (weak intrusion) to $f_\alpha = 0.95$ (strong intrusion). It can be seen that the convergence of the QPA protocol is fast: the fidelity deviates from the ideal case $F = 1$ by less than 10^{-7} in no more than $n = 6$ map iterations. Moreover, the survival probability is quite high: it saturates to $P_\infty \equiv \lim_{n \to \infty} P(n) = 0.60$ for $f_\alpha = 0.95$, $P_\infty = 0.94$ for $f_\alpha = 0.5$ and $P_\infty = 0.9995$ for $f_\alpha = 0.05$.

4 Single qubit errors

In any realistic implementation of the QPA protocol, errors acting on the purification operations are unavoidable. For the sake of simplicity we limit ourselves to consider errors affecting only a single qubit. Nevertheless, we would like to stress that a complete treatment of the effects of all
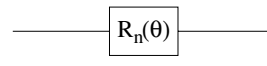
Fig. 5. Quantum circuit representing a rotation through an angle θ about the **n**-axis.
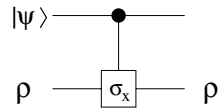
Fig. 6. Quantum circuit implementing the bit flip channel.

possible single-qubit noise channels on the QPA algorithm is provided in this paper.

We need 12 parameters to characterize a generic quantum noise operation acting on a single qubit [8]. Each parameter describes a particular noise channel (like bit flip, phase flip, amplitude damping, ...) and can be most conveniently visualized as associated to rotations, deformations and displacements of the Bloch sphere. In the following, we provide, for each noise channel,

(i)   the Kraus representation;
(ii)   the transformation of the Bloch sphere coordinates;
(iii)   an equivalent quantum circuit leading to a unitary representation in an extended Hilbert space. A great advantage of these equivalent quantum circuits is that the evolution of the reduced density matrix describing the single-qubit system is automatically guaranteed to be completely positive.

– *Rotations of the Bloch sphere* - Rotations through an angle θ about an arbitrary axis directed along the unit vector **n** are given by the operator [9]

$$R_n(\theta) = \left(\cos\frac{\theta}{2}\right) I - i\left(\sin\frac{\theta}{2}\right) \mathbf{n} \cdot \boldsymbol{\sigma}, \qquad (13)$$

where $\boldsymbol{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$, σ_x, σ_y and σ_z being the Pauli matrices. The quantum circuit representing rotations is shown in Figure 5. Any generic rotation can be obtained by composing rotations about the axes x, y and z. Let us write as an example the transformation of the Bloch sphere coordinates associated to a rotation through an angle θ about the z-axis:

$$\begin{cases} x' = (\cos\theta)x - (\sin\theta)y, \\ y' = (\sin\theta)x + (\cos\theta)y, \\ z' = z \end{cases} \qquad (14)$$

– *Deformations of the Bloch sphere* - The well-known bit flip, phase flip and bit-phase flip channels correspond to deformations of the Bloch sphere into an ellipsoid. An equivalent quantum circuit implementing the bit-flip channel is shown in Figure 6. Note that a single auxiliary qubit, initially prepared in the state $|\psi\rangle = \cos(\theta/2)|0\rangle + \sin(\theta/2)|1\rangle$ (with $0 \le \theta \le \pi$) is sufficient to obtain a unitary representation of this noise channel. The corresponding Kraus representation is defined by the Kraus operators

$$F_0 = \left(\cos\frac{\theta}{2}\right) I, \quad F_1 = \left(\sin\frac{\theta}{2}\right) \sigma_x. \qquad (15)$$
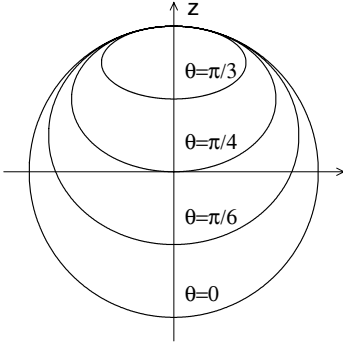
Fig. 7. Visualization of the minimum deformation required to displace the center of the Bloch sphere along the z-axis. The horizontal axis can be any axis in the (x, y)-plane.

The quantum operation

$$\rho' = \sum_k F_k \rho F_k^\dagger, \quad \left(\sum_k F_k^\dagger F_k = I \right), \qquad (16)$$

maps the Bloch sphere into an ellipsoid with x as symmetry axis:

$$\begin{cases} x' = x, \\ y' = (\cos \theta) y, \\ z' = (\cos \theta) z, \end{cases} \qquad (17)$$

The phase flip and bit-phase flip channels are obtained from quantum circuits analogous to Figure 6, after substitution of σ_x with σ_z and σ_y, respectively. In the phase flip channel the Bloch sphere is mapped into an ellipsoid with z as symmetry axis, while in the bit-phase flip channel the symmetry axis is y.

– *Displacements of the Bloch sphere* - A displacement of the center of the Bloch sphere must go with a deformation of the sphere. This is necessary if we want that ρ' still represents a density matrix: the Bloch radius **r** associated to any density matrix must have length r such that $0 \le r \le 1$. This condition can be fulfilled as follows. Let us consider, for instance, a displacement of the center of the Bloch sphere along the $+z$-direction, so that the new center is $(0, 0, 1 - b)$, with $0 < b < 1$. We also assume that the Bloch sphere is deformed into an ellipsoid with z as symmetry axis:

$$\frac{x^2 + y^2}{a^2} + \frac{[z - (1 - b)]^2}{b^2} = 1. \qquad (18)$$

Imposing a higher order tangency of this ellipsoid to the Bloch sphere $x^2 + y^2 + z^2 = 1$ we obtain $b = a^2$. If we define $a = \cos \theta$ $(0 < \theta < \pi/2)$, then equation (18) becomes

$$\frac{x^2 + y^2}{\cos^2 \theta} + \frac{(z - \sin^2 \theta)^2}{\cos^4 \theta} = 1. \qquad (19)$$

Note that this equation corresponds to the minimum deformation required to the Bloch sphere in order to displace its center along the z-axis by $1 - b = \sin^2 \theta$. The graphic visualization of the mapping of the Bloch sphere onto an ellipsoid with displaced center is shown in Figure 7.

The mapping of the Bloch sphere onto the ellipsoid (19) can be obtained by means of the simple equivalent circuit drawn in Figure 8. This circuit leads to
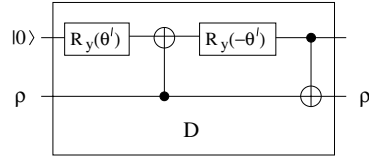
Fig. 8. Quantum circuit implementing a displacement of the Bloch sphere along the $+z$-direction. Note that $\theta' \equiv \pi/2 - \theta$.
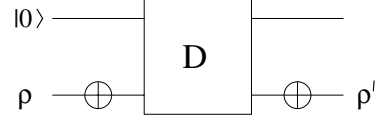
Fig. 9. Quantum circuit implementing a displacement of the Bloch sphere along the $-z$-direction. The unitary transformation D corresponds to the boxed part of the circuit in Figure 8. The $\oplus$ symbol stands for the NOT gate ($|0\rangle \rightarrow |1\rangle$, $|1\rangle \rightarrow |0\rangle$).
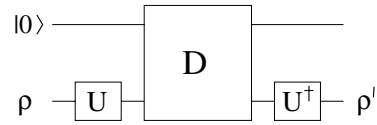
Fig. 10. Quantum circuit implementing a displacement of the Bloch sphere along the $\pm x$ or $\pm y$-directions. The unitary transformation D corresponds to the boxed part of the circuit in Figure 8.

a single-qubit quantum operation known as the amplitude damping channel. It is described by the Kraus operators

$$F_0 = \begin{bmatrix} 1 & 0 \\ 0 & \cos \theta \end{bmatrix}, \quad F_1 = \begin{bmatrix} 0 & \sin \theta \\ 0 & 0 \end{bmatrix}. \qquad (20)$$

The corresponding transformation of the Bloch sphere coordinates is

$$\begin{cases} x' = (\cos \theta) x, \\ y' = (\cos \theta) y, \\ z' = \sin^2 \theta + (\cos^2 \theta) z. \end{cases} \qquad (21)$$

While displacements of the center of the Bloch sphere along the positive direction of the z-axis can be seen as representative of zero temperature dissipation, thermal excitations are instead associated to displacements along the $-z$-direction. The equivalent quantum circuit describing thermal excitations is shown in Figure 9. It leads to the Kraus operators

$$F_0 = \begin{bmatrix} \cos \theta & 0 \\ 0 & 1 \end{bmatrix}, \quad F_1 = \begin{bmatrix} 0 & 0 \\ \sin \theta & 0 \end{bmatrix} \qquad (22)$$

and to the Bloch sphere coordinate transformation

$$\begin{cases} x' = (\cos \theta) x, \\ y' = (\cos \theta) y, \\ z' = -\sin^2 \theta + (\cos^2 \theta) z. \end{cases} \qquad (23)$$

We also consider displacements of the Bloch sphere along the directions $\pm x$ and $\pm y$. The equivalent quantum circuit is drawn in Figure 10. A displacement

along $\pm x$ takes place when the unitary transformation U in Figure 10 is described by the matrix

$$U = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & \pm 1 \\ \mp 1 & 1 \end{bmatrix}. \tag{24}$$

The corresponding Kraus operators and the transformation of the Bloch sphere coordinates are

$$F_0 = \frac{1}{2} \begin{bmatrix} 1 + \cos\theta & \pm(1 - \cos\theta) \\ \pm(1 - \cos\theta) & 1 + \cos\theta \end{bmatrix},$$

$$F_1 = \frac{1}{2} \begin{bmatrix} \mp \sin\theta & \sin\theta \\ -\sin\theta & \pm\sin\theta \end{bmatrix}, \tag{25}$$

$$\begin{cases} x' = \pm \sin^2\theta + (\cos^2\theta)x, \\ y' = (\cos\theta)y, \\ z' = (\cos\theta)z. \end{cases} \tag{26}$$

For a displacement along $\pm y$ we have

$$U = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & \pm i \\ \pm i & 1 \end{bmatrix}, \tag{27}$$

$$F_0 = \frac{1}{2} \begin{bmatrix} 1 + \cos\theta & \pm i(1 - \cos\theta) \\ \mp i(1 - \cos\theta) & 1 + \cos\theta \end{bmatrix},$$

$$F_1 = \frac{1}{2} \begin{bmatrix} \pm i\sin\theta & \sin\theta \\ \sin\theta & \mp i\sin\theta \end{bmatrix}, \tag{28}$$

$$\begin{cases} x' = (\cos\theta)x, \\ y' = \pm\sin^2\theta + (\cos^2\theta)y, \\ z' = (\cos\theta)z. \end{cases} \tag{29}$$

We have given a geometric interpretation of 9 out of the 12 parameters describing a generic single-qubit quantum operation (3 are associated to rotations about the axes x, y or z, 3 to displacements along the same axes, and 3 to deformations of the Bloch sphere into an ellipsoid, with x, y or z as symmetry axes). The remaining 3 parameters correspond to deformations of the Bloch sphere into an ellipsoid with symmetry axis along an arbitrary direction. Since these deformations can be obtained by combining the 9 previously studied quantum operations, then, for small errors, it will be sufficient to consider only 9 parameters.

5 Impact of noise on entanglement purification

We discuss the impact of the 9 noise channels described in the previous section on the QPA algorithm. We present numerical data for the case in which quantum noise acts on the top qubit in Figure 3 after the U-rotation. However, we point out that very similar results are obtained when noise acts on one of the other three qubits in the same figure. Data are obtained by iteration of a four-qubit noisy quantum map, with input state $\rho_{AB} \otimes \rho_{AB}$ and output state (for the first two qubits) ρ'_{AB} [10].

We measure the quality of the purified EPR pair by the fidelity F, defined in equation (10). Moreover, we compute
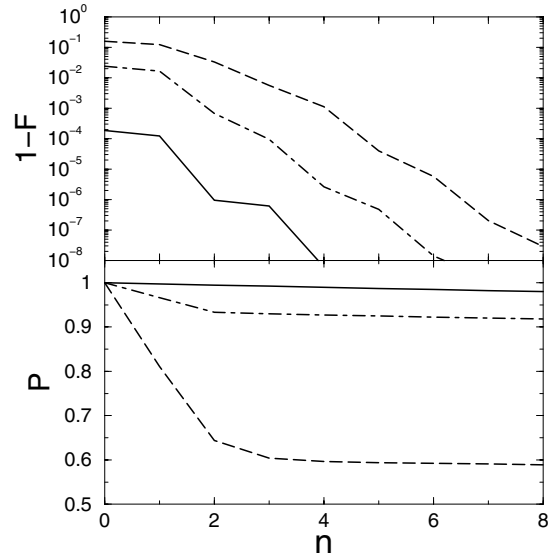
Fig. 11. Same as in Figure 4 but for the bit flip channel at $\theta = 10^{-1}$.

the survival probability $P(n)$, defined in equation (11), measuring the probability that a n-step QPA protocol is successful.

We note that the following symmetries in the effect of errors are observed for the QPA algorithm:

(i)   rotations through an angle $+\theta$ or $-\theta$ have the same impact;
(ii) displacements along the positive or the negative direction of a given axis have the same effect;
(iii) rotations about the x-axis and deformations with x as symmetry axis (bit flip channel) have the same effect; the same observation applies for the axes y and z as well.

The main result of our studies is the demonstration that the sensitivity of the quantum privacy protocol to errors strongly depends on the kind of noise. Two main distinct behaviors are observed:

(i) the fidelity is continuously improved by increasing the number of purification steps;
(ii) the fidelity saturates to a value $F < 1$ after a finite number of steps, so that any further iteration is useless [11].

As examples of behaviors of the kind (i) and (ii) we show the bit-flip channel in Figure 11 (for error strength $\theta = 10^{-1}$) and the displacement along x in Figure 12 ($\theta = 10^{-3}$). In both figures, the survival probability $P(n)$ can also be seen. Note that, for these sufficiently small error strengths, the values of $P(n)$ shown in Figures 11 and 12 are not very far from those of the ideal protocol (see Fig. 4).

It is important to point out that not only the behavior of $F(n)$ is qualitatively different depending on the noise channel but also the level of tolerable noise strength is channel-dependent. To give a concrete example, we show
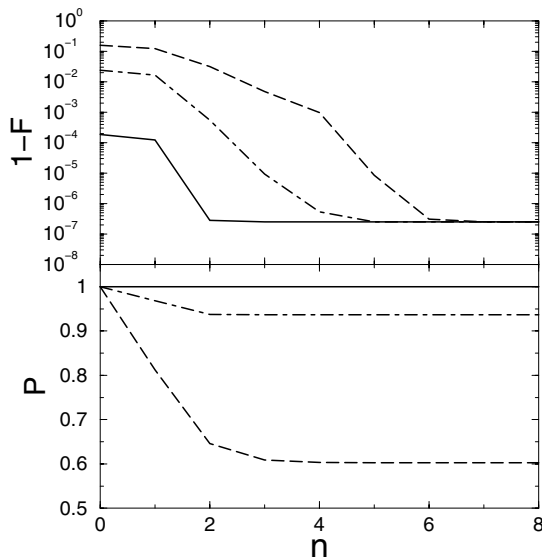
Fig. 12. Same as in Figure 4 but for the noise channel corresponding to a displacement along the x-axis of the Bloch sphere, at $\theta = 10^{-3}$.
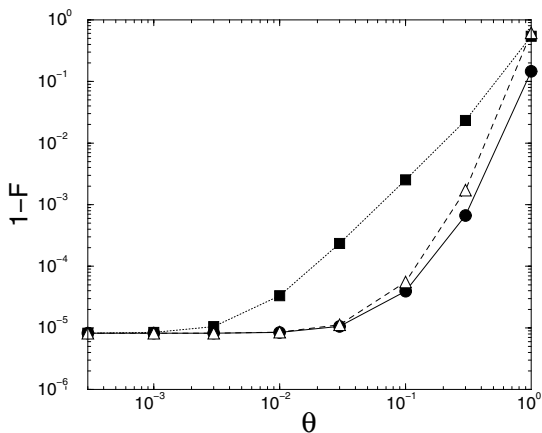
Fig. 13. Deviation $1 - F$ of the fidelity F from the ideal case $F = 1$ as a function of the noise strength θ, after $n = 5$ steps of the quantum privacy amplification protocol, for $f_\alpha = 0.95$, bit flip (circles), phase flip (squares) and amplitude damping (triangles) channels.

in Figure 13 the deviation $1 - F$ of the fidelity from the ideal value $F = 1$ as a function of the noise strength θ. Data are obtained after $n = 5$ iterations of the QPA protocol, in the case of strong Eve's intrusion ($f_\alpha = 0.95$) and we consider the bit flip, the phase flip and the amplitude damping (displacement along z) channels. In the noiseless case we start from $1 - F = 1.57 \times 10^{-1}$ and improve the fidelity to $1 - F = 8.20 \times 10^{-6}$ after $n = 5$ iterations of the quantum privacy amplification protocol. Even though all noise channels degrade the performance of the protocol, the level of noise that can be safely tolerated strongly depends on the specific channel. For instance, it is clear from Figure 13 that the QPA protocol is much more resilient to

Table 1. Value of the noise strength θ such that $1 - F = 10^{-4}$ after $n = 5$ iterations of the purification protocol, at $f_\alpha = 0.95$.

Noise channel	θ
Rotation about x	1.55×10^{-1}
Rotation about y	2.69×10^{-1}
Rotation about z	1.92×10^{-2}
Bit flip	1.55×10^{-1}
Bit-phase flip	2.69×10^{-1}
Phase flip	1.92×10^{-2}
Displacement along x	1.91×10^{-2}
Displacement along y	1.91×10^{-2}
Displacement along z	1.27×10^{-1}

bit flip and amplitude damping errors than to phase flip errors.

A further confirmation of the very different impact of the various noise channels is shown in Table 1, showing, at $f_\alpha = 0.95$, the value of θ such as $1 - F = 10^{-4}$ after $n = 5$ map iterations. This gives an estimate of the maximum level of error tolerable for each noise channel. It is interesting to remark that displacements of the Bloch sphere along x and y are much more dangerous than displacements along z. We note that the value $1 - F = 10^{-4}$ has been chosen just for convenience but the same conclusions are obtained also for other values of $1 - F$. We also point out that, as shown in Table 1, it is possible to achieve very good fidelities in a small number of purification steps also for quite high errors $\theta \sim 10^{-1} \gg 1 - F$ affecting the QPA protocol.

6 Conclusions

We have performed a systematic study of the effects of the different single-qubit noise channels on the quantum privacy amplification protocol. Our results show the very different impact of the various noise channels on the QPA algorithm. In particular, we have distinguished between cases where it is possible to drive the fidelity arbitrarily close to one and others in which the fidelity saturates to a value different from one. Another important feature that emerges from our investigations is the strong dependence of the maximum noise strength tolerable for the QPA protocol on the noise channel. This is a valuable piece of information for experimental implementations. For instance, the fact that the QPA protocol is much less sensitive to displacements along z than along x or y suggests that the z-axis is chosen along "the direction of noise". We can then choose the axes x and y to minimize other noise effects. Finally, we remark that studies like the present one, taking into account all possible single-qubit quantum noise channels, promise to give useful insights also in the field of quantum computation.

Appendix A: Isotropic cloning

Let us first consider the case in which the initial state of Bob's qubit is pure, $|\psi\rangle = \mu|0\rangle + \nu|1\rangle$, where μ, ν are complex numbers, with $|\mu|^2 + |\nu|^2 = 1$. The unitary transformation W in Figure 1 maps the state $|\psi\rangle|\Phi\rangle$ (where $|\Phi\rangle$ is given by equation (1)) onto the state

$$|\Psi\rangle = \mu(\alpha|000\rangle + \beta|101\rangle + \gamma|110\rangle + \delta|011\rangle) + \nu(\alpha|111\rangle + \beta|010\rangle + \gamma|001\rangle + \delta|100\rangle). \quad (30)$$

We then obtain the density matrix ρ_B after tracing the density matrix $|\Psi\rangle\langle\Psi|$ over Eve's qubit and the ancillary qubit. We have

$$\rho_B = \begin{bmatrix} |\mu|^2(\alpha^2 + \delta^2) & 2\mu\nu^\star\alpha\delta \\ +|\nu|^2(\beta^2 + \gamma^2) & +2\mu^\star\nu\beta\gamma \\ \\ 2\mu^\star\nu\alpha\delta & |\mu|^2(\beta^2 + \gamma^2) \\ +2\mu\nu^\star\beta\gamma & +|\nu|^2(\alpha^2 + \delta^2) \end{bmatrix}. \quad (31)$$

In the same way we obtain the density matrix ρ_E after tracing over Bob's qubit and the ancillary qubit:

$$\rho_E = \begin{bmatrix} |\mu|^2(\alpha^2 + \beta^2) & 2\mu\nu^\star\alpha\beta \\ +|\nu|^2(\gamma^2 + \delta^2) & +2\mu^\star\nu\gamma\delta \\ \\ 2\mu^\star\nu\alpha\beta & |\mu|^2(\gamma^2 + \delta^2) \\ +2\mu\nu^\star\gamma\delta & +|\nu|^2(\alpha^2 + \beta^2) \end{bmatrix}. \quad (32)$$

Let us call (x, y, z), (x_B, y_B, z_B) and (x_E, y_E, z_E) the Bloch sphere coordinates corresponding to $|\psi\rangle\langle\psi|$, ρ_B and ρ_E. We have

$$\mu\nu^\star = \frac{1}{2}(x - iy), \quad |\mu|^2 = \frac{1}{2}(1 + z), \quad |\nu|^2 = \frac{1}{2}(1 - z). \quad (33)$$

After setting $\gamma = 0$, we obtain

$$\begin{cases} \frac{1}{2}(x_B - iy_B) = (\rho_B)_{01} = (x - iy)\alpha\delta, \\ \\ \frac{1}{2}(1 + z_B) = (\rho_B)_{00} = \frac{1}{2}(1 + z)(\alpha^2 + \delta^2) + \frac{1}{2}(1 - z)\beta^2, \end{cases} \quad (34)$$

which imply

$$\begin{cases} x_B = 2\alpha\delta x, \\ y_B = 2\alpha\delta y, \\ z_B = (\alpha^2 + \delta^2 - \beta^2)z. \end{cases} \quad (35)$$

The state ρ_B is an isotropic cloning of $|\psi\rangle\langle\psi|$ when $R_B = x_B/x = y_B/y = z_B/z$. Therefore we obtain

$$\begin{cases} 2\alpha\delta = \alpha^2 + \delta^2 - \beta^2, \\ \alpha^2 + \beta^2 + \delta^2 = 1, \end{cases} \quad (36)$$

so that

$$\delta = \frac{\alpha}{2} \pm \sqrt{\frac{1}{2} - \frac{3}{4}\alpha^2}. \quad (37)$$

In the same way we obtain

$$\begin{cases} x_E = 2\alpha\beta x, \\ y_E = 2\alpha\beta y, \\ z_E = (\alpha^2 + \beta^2 - \delta^2)z. \end{cases} \quad (38)$$

Isotropic cloning $(R_E = x_E/x = y_E/y = z_E/z)$ is obtained when

$$\begin{cases} 2\alpha\beta = \alpha^2 + \beta^2 - \delta^2, \\ \alpha^2 + \beta^2 + \delta^2 = 1, \end{cases} \quad (39)$$

so that

$$\beta = \frac{\alpha}{2} \pm \sqrt{\frac{1}{2} - \frac{3}{4}\alpha^2}. \quad (40)$$

Note that, if we choose the plus sign in (37), then the minus sign has to be taken in (40) in order that the normalization condition $\alpha^2 + \beta^2 + \delta^2$ is satisfied. This choice corresponds to equation (2).

Note that the cloning is isotropic also in the case in which the initial state ρ of Bob's qubits is mixed. In this case we can write $\rho = \sum_i p_i\rho_i$, with $\rho_i = |\psi_i\rangle\langle\psi_i|$ pure state. The Bloch vector $\mathbf{r}$ associated to ρ is the weighted sum of the Bloch vectors $\mathbf{r}_i$ associated to the density matrices ρ_i: $\mathbf{r} = \sum_i p_i\mathbf{r}_i$. Since we have seen that for pure initial states $(\mathbf{r}_i)_B = R_B\mathbf{r}_i$ and $(\mathbf{r}_i)_E = R_E\mathbf{r}_i$, then $\mathbf{r}_B = \sum_i p_i(\mathbf{r}_i)_B = R_B\mathbf{r}$ and $\mathbf{r}_E = \sum_i p_i(\mathbf{r}_i)_E = R_E\mathbf{r}$.

References

1. A.K. Ekert, Phys. Rev. Lett. **67**, 661 (1991)
2. C.H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J.A. Smolin, W.K. Wootters, Phys. Rev. Lett. **76**, 722 (1996)
3. C.H. Bennett, D.P. DiVincenzo, J.A. Smolin, W.K. Wootters, Phys. Rev. A **54**, 3824 (1996)
4. D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996)
5. H. Aschauer, H.J. Briegel, Phys. Rev. A **66**, 032302 (2002)
6. V. Bužek, M. Hillery, Phys. Rev. A **54**, 1844 (1996); e-print arXiv:quant-ph/9801009
7. C. Macchiavello, Phys. Lett. A **246**, 385 (1998)
8. See, e.g., M.A. Nielsen, I.L. Chuang, *Quantum computation and quantum information* (Cambridge University Press, Cambridge, 2000), Ch. 8
9. See, e.g., G. Benenti, G. Casati, G. Strini, *Principles of Quantum Computation and Information*, Vol. 1: Basic Concepts (World Scientific, Singapore, 2004), p. 110
10. We have also developed an alternative numerical technique, in which 2^n imperfect EPR pairs are considered at the beginning, to obtain, after n steps and when the QPA algorithm is successful (coinciding outcomes for Alice and Bob's measurements), a single purified EPR pair. This numerical approach gives the same results as the simpler four-qubit mapping when the action of quantum noise is identical for each pair of EPR states. However, it has the advantage that more general situations can be treated, for instance the noise strength can depend on the considered pair of EPR states
11. We note that in the case of strong noise it is also possible that the fidelity degrades when the QPA algorithm is iterated