Quantum Privacy and Quantum Coherence

Benjamin Schumacher
Department of Physics, Kenyon College, Gambier, Ohio 43022

Michael D. Westmoreland
Department of Mathematical Sciences, Denison University, Granville, Ohio 43023
(Received 8 October 1997)

We derive a simple relation between a quantum channel's capacity to convey coherent (quantum) information and its usefulness for quantum cryptography. [S0031-9007(98)06456-4]

PACS numbers: 89.70.+c, 03.65.Bz, 42.50.Dv

A quantum communication channel can be used to perform a variety of tasks, including the following:

(i) Conveying classical information from a sender to a receiver.

(ii) Conveying quantum information (including quantum entanglement) from a sender to a receiver.

(iii) Creating shared information between a sender and receiver, information that is reliably secret from any third party and can thus be used as a cryptographic key for later private communication. (The use of quantum channels to aid in cryptographic tasks such as key distribution is called quantum cryptography.)

Each of these tasks can be performed in the presence of noise. Indeed, in quantum cryptography the noise is of central importance in revealing the activity of an eavesdropper.

Deutsch *et al.* [1] examined the security of quantum cryptographic schemes over quantum channels that contain noise. They pointed out that any protocol which allowed "entanglement purification" between two parties automatically provided a means of communicating secret information that no third party could share. The privacy of quantum channels has also been investigated by Biham and Mor [2] as well as Bennett *et al.* [3]. Here we will continue this line of thought by showing that the privacy of the channel, measured by the amount of information available to the receiver that is not available to any eavesdropper, can be made at least as great as the channel's *coherent information* [4].

Suppose Alice prepares a quantum system Q in an initial state ρ^Q. Alice conveys the system Q through a noisy quantum channel to Bob. The noisy channel may be described by a superoperator $\mathcal{E}^Q$ so that the final state $\rho^{Q'} = \mathcal{E}^Q(\rho^Q)$.

The evolution of the channel given by the superoperator $\mathcal{E}^Q$ is in fact unitary evolution on a larger quantum system that includes the environment E of the system. This environment may be considered to be initially in a pure state $|0^E\rangle$. In this case, the superoperator is given by

$$\mathcal{E}^Q(\rho^Q) = \mathrm{Tr}_E U^{QE}(\rho^Q \otimes |0^E\rangle\langle 0^E|) U^{QE\dagger}. \qquad (1)$$

We can assume that the environment is initially in a pure state without any loss of generality, since we can always imagine that a "local" environment in a mixed state is just part of a larger system in a pure entangled state.

We imagine first that the initial mixed state ρ^Q of Q arises from Q's entanglement with some other "reference" system R in Alice's possession. Alice's goal in sending Q to Bob is to establish some quantum entanglement between her reference system R and Bob's output system Q'. That is, Alice is sending *quantum information* via the channel to Bob.

As discussed in [5], the entropy exchange S_e measures the amount of information that is exchanged between the system Q and the environment E during their interaction. If the environment is initially in a pure state, the entropy exchange is just the environment's entropy after the interaction, i.e., $S_e = S(\rho^{E'})$, where $\rho^{E'}$ is the final state of E. [The entropy here is just the ordinary von Neumann entropy of a density operator, $S(\rho) = -\mathrm{Tr}\, \rho \log \rho$.] The entropy exchange is determined entirely by the initial state ρ^Q of Q and the channel dynamics superoperator $\mathcal{E}^Q$; that is, the entropy exchange is a property "intrinsic" to Q and its dynamics.

The coherent information I_e, introduced in [4], is given by

$$I_e = S(\rho^{Q'}) - S_e. \qquad (2)$$

The coherent information has many properties that suggest it as the proper measure of the quantum information conveyed from Alice to Bob by the channel. For example, I_e can never be increased by quantum data processing performed by Bob on the channel output, and perfect quantum error correction of the channel output is possible for Bob if and only if no coherent information is lost in the channel [4]. The coherent information seems to be related to the capacity of a quantum channel to convey quantum states with high fidelity [6].

Alice might, on the other hand, be using the channel to send classical information to Bob. Alice prepares Q in one of a set of possible "signal states" ρ_k^Q, which are used by Alice with *a priori* probabilities p_k. The average state ρ^Q is given by

$$\rho^Q = \sum_k p_k \rho_k^Q. \qquad (3)$$

Bob receives the kth signal as $\rho_k^{Q'} = \mathcal{E}^Q(\rho_k^Q)$. Because the superoperator is linear, the average received state is

$$\rho^{Q'} = \sum_k p_k \mathcal{E}^Q(\rho_k^Q) = \mathcal{E}^Q(\rho^Q). \tag{4}$$

Bob attempts to decode Alice's message (that is, to identify which signal state was chosen by Alice) by measuring some *decoding observable* on his received system Q'.

The amount of classical information conveyed from Alice to Bob, which we will denote H_{Bob}, is governed by the quantity $\chi^{Q'}$ defined by

$$\chi^{Q'} = S(\rho^{Q'}) - \sum_k p_k S(\rho_k^{Q'}). \tag{5}$$

This quantity is significant in two ways:

(*i*) $H_{\text{Bob}} \leq \chi^{Q'}$, regardless of the decoding observable chosen [7,8].

(*ii*) H_{Bob} can be made as close as desired to $\chi^{Q'}$ by a suitable choice of a code and decoding observable. To make H_{Bob} near $\chi^{Q'}$, Alice must in general use the channel many times and employ code words composed of many signals; Bob must perform his decoding measurement on entire code words. The net result is that the channel is used N times to send up to $N\chi^{Q'}$ bits of classical information reliably [9].

In short, $\chi^{Q'}$ represents an upper bound on the classical information conveyed from Alice to Bob, an upper bound that may be approached arbitrarily closely if Alice and Bob use the channel efficiently.

If this general picture is used to describe a quantum cryptographic channel, then the eavesdropper ("Eve") must have access to some or all of the environment system E with which Q interacts. In other words, the environment includes any apparatus used by Eve to gather information about Alice and Bob's communication. The evolution superoperator $\mathcal{E}^Q$ thus describes all of the effects of the eavesdropper on the channel; or, to put it another way, all of the eavesdropper's efforts at "tapping" the link between Alice and Bob are contained in the interaction operator U^{QE}. The information H_{Eve} available to the eavesdropper will be limited by

$$\chi^{E'} = S(\rho^{E'}) - \sum_k p_k S(\rho_k^{E'}). \tag{6}$$

The limitation $H_{\text{Eve}} \leq \chi^{E'}$ holds whether or not Eve has access to the entire environment. If Eve can only see a subsystem D of the full environment, then we can make the stronger statement $H_{\text{Eve}} \leq \chi^{D'}$, where $\chi^{D'} \leq \chi^{E'}$ [8].

We define the "privacy" P of a channel to be

$$P = H_{\text{Bob}} - H_{\text{Eve}}. \tag{7}$$

This definition makes sense because, in a classical context, any positive difference $H_{\text{Bob}} - H_{\text{Eve}}$ can be exploited by Alice and Bob, using public discussion, to create a reliably secret string of key bits of length about P [10]. (Matters are somewhat more subtle in the quantum case, since Eve may delay her choice of "eavesdropping observable" until after the public discussion by Alice and Bob. If she is forced to choose her observable before this discussion, the classical result holds.)

Alice and Bob wish to make P as large as possible. However, they cannot control the actions of the eavesdropper. Thus, they must assume that the eavesdropper is acquiring her greatest possible information from the channel. The "guaranteed privacy" $P_G = \inf P$, where the infimum is taken over all of Eve's possible strategies that are consistent with the superoperator $\mathcal{E}^Q$ describing the channel. Since $H_{\text{Eve}} \leq \chi^{E'}$, we have

$$P_G \geq H_{\text{Bob}} - \chi^{E'}. \tag{8}$$

Alice and Bob will want to use the channel to make the guaranteed privacy P_G as great as possible. Let $\mathcal{P} = \sup P_G$ be the optimal guaranteed privacy, where the supremum is taken over all strategies that Alice and Bob may employ to use the channel. How big is $\mathcal{P}$? As discussed above, by suitable choice of the code and decoding observable, H_{Bob} can be made arbitrarily close to $\chi^{Q'}$. Thus,

$$\mathcal{P} \geq \chi^{Q'} - \chi^{E'}. \tag{9}$$

If Alice and Bob were simply trying to optimize H_{Bob} over a given noisy channel, it is known [9] that they can do no better than to choose pure states of Q as the input signal states of the channel. Here, they are instead trying to maximize the guaranteed privacy P_G, so that pure state inputs may not be optimal. However, we can certainly find a lower bound for $\mathcal{P}$ by considering $\chi^{Q'} - \chi^{E'}$ for pure state inputs.

Assume that the states of Q initially prepared by Alice are pure states $|\phi_k^Q\rangle$; also recall that the environment E can be presumed to begin in a pure state $|0^E\rangle$. After Q and E interact unitarily, the joint state $|\Psi_k^{QE'}\rangle = U^{QE}|\phi_k^Q\rangle \otimes |0^E\rangle$ will also be a pure state, generally an entangled one. The subsystem states, described by density operators,

$$\begin{aligned}\rho_k^{Q'} &= \text{Tr}_E|\Psi_k^{QE'}\rangle\langle\Psi_k^{QE'}|, \\ \rho_k^{E'} &= \text{Tr}_Q|\Psi_k^{QE'}\rangle\langle\Psi_k^{QE'}|,\end{aligned} \tag{10}$$

will have exactly the same nonzero eigenvalues, so that $S(\rho_k^{Q'}) = S(\rho_k^{E'})$. Therefore

$$\begin{aligned}I^Q &= S(\rho^{Q'}) - S_e \\ &= S(\rho^{Q'}) - S(\rho^{E'}) \\ &= S(\rho^{Q'}) - \sum_k p_k S(\rho_k^{Q'}) - S(\rho^{E'}) + \sum_k p_k S(\rho_k^{E'}) \\ I^Q &= \chi^{Q'} - \chi^{E'}.\end{aligned} \tag{11}$$

We conclude that

$$\mathcal{P} \geq I^Q. \tag{12}$$

In other words, the ability of the quantum channel to send *private* information is at least as great as its ability to send *coherent* information. This result may be viewed as a quantum information theoretic basis for quantum cryptography.

It is interesting to note that, although both $\chi^{Q'}$ and $\chi^{E'}$ depend on the choice of pure state inputs for the channel Q, the difference $\chi^{Q'} - \chi^{E'}$ depends only on the overall density operator ρ^Q for the inputs.

We have assumed that the properties of the channel, given by the superoperator $\mathcal{E}^Q$, are known to Alice and Bob. If $\mathcal{E}^Q$ is known, and if $I^Q > 0$ for some ρ^Q, then the channel may be used to send private information securely. However, this does not address the question of how Alice and Bob can establish the necessary properties of the channel without being deceived by Eve.

We would like to thank W. K. Wootters and M. A. Nielsen for helpful conversations and suggestions.

[1] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).

[2] E. Biahm and T. Mor, Report No. quant-ph/9605010; E. Biham and T. Mor, Report No. quant-ph/9605007.

[3] C. H. Bennett, T. Mor, and J. A. Smolin, Report No. quant-ph/9604040.

[4] B. Schumacher and M. A. Nielsen, Phys. Rev. A **54**, 2629 (1996).

[5] B. Schumacher, Phys. Rev. A **54**, 2614 (1996).

[6] S. Lloyd, Phys. Rev. A **55**, 1613 (1997); H. Barnum, M. A. Nielsen, and B. Schumacher, Report No. quant-ph/9702049.

[7] A. S. Kholevo, Probl. Pereda. Inf. **9**, 3 (1973) [Probl. Inf. Transm. **9**, 110 (1973)].

[8] B. Schumacher, M. D. Westmoreland, and W. K. Wootters, Phys. Rev. Lett. **76**, 3452 (1996).

[9] P. Hausladen, R. Jozsa, B. Schumacher, M. D. Westmoreland, and W. K. Wootters, Phys. Rev. A **54**, 1869 (1996); B. Schumacher and M. D. Westmoreland, Phys. Rev. A **56**, 131 (1997); A. S. Holevo, IEEE Trans. Inf. Theory (to be published).

[10] I. Csiszár and J. Körner, IEEE Trans. Inf. Theory **24**, 339 (1978); U. M. Maurer, IEEE Trans. Inf. Theory **39**, 733 (1993).