Sending Sensitive Messages in Quantum Packages

Paul A. Lopata* and Thomas B. Bahder

U.S. Army Research Laboratory
2800 Powder Mill Road
Adelphi, Maryland 20783
(Dated: June 2, 2006)

A communication protocol is introduced that allows the receiver of a message to place an *a posteriori* bound on the amount of information that an eavesdropper could have obtained during transmission of that message. This quantum cryptographic protocol is distinct from quantum key distribution. The quantum states and measurements required by this protocol are simple enough that it can be implemented using existing technology.

A major concern when transmitting a secret message over a public communication channel is that an eavesdropper might intercept the message and learn its meaning. This is combatted by encrypting the message so that an eavesdropper cannot decipher the meaning of the intercepted message.[1, 2] In its most secure form, this relies upon the communicating parties sharing a single-use private key which is as long as the message.[1] Recently, great strides have been made at generating and distributing private keys using quantum mechanical systems sent through insecure channels.[3] Such quantum key generation (QKD) protocols have the distinct feature that an eavesdropper leaves evidence of her activity. However, due to their design, these QKD protocols do not convey messages.

In this Letter we introduce a quantum seal protocol, which is a method for two parties to communicate a message, not simply to generate a random key.[4, 5] Its utility comes from the fact that it allows the receiver to place an *a posteriori* bound on the amount of information an eavesdropper could have obtained over the course of the transmission. Each time a message is sent, there is a straightforward way in which an eavesdropper can attempt to intercept the message. Yet if this occurs, the receiver will be given an unambiguous indication that there was a disturbance in the system and an eavesdropper may have been tapping into the communication channel. If there is no eavesdropper and the quantum channel is relatively noise-free, then the receiver will have confidence that no other parties have read the message.

This protocol can be used to seal up and communicate an encrypted message, thereby providing an extra layer of assurance while sending sensitive material, on top of any sophisticated encryption technique that may currently be used.

The protocol involves a message sender, named Alice, trying to get a message bit b (whose values can be zero or one) to a receiver, called Bob. The entire process is initiated by Alice announcing that she has a message she wants to communicate to Bob. Then a routine is repeated many times. Each repetition is referred to as a single "shot", and proceeds as follows.

Bob starts the routine by preparing some physical sys-

TABLE I: Each shot, Alice makes one of the following eight announcements.

Bit-Announcements		Result-Announcements	
σ_1	$c = 0$	σ_1	$m = +1$
σ_1	$c = 1$	σ_1	$m = -1$
σ_3	$c = 0$	σ_3	$m = +1$
σ_3	$c = 1$	σ_3	$m = -1$

tem (which we refer to as a particle) in one of four quantum states, represented by density matrices $\rho^{(0)} \equiv |0\rangle\langle 0|$, $\rho^{(1)} \equiv |1\rangle\langle 1|$, $\rho^{(+)} \equiv |+\rangle\langle +|$, or $\rho^{(-)} \equiv |-\rangle\langle -|$. (Here we have used the standard notation for a qubit Hilbert space that is spanned by basis vectors $|0\rangle$ and $|1\rangle$ and $|\pm\rangle \equiv 2^{-\frac{1}{2}}[|0\rangle \pm |1\rangle]$.) Bob employs a randomized method of preparation so that he is equally likely to prepare the particle in any of these four states. Bob records which state he has prepared and sends the particle to Alice.

Upon receipt of the particle, Alice makes one of two measurements: with probability one-half she makes a measurement corresponding to $\sigma_1 \equiv |+\rangle\langle +| - |-\rangle\langle -|$, and with probability one-half she makes a measurement corresponding to $\sigma_3 \equiv |0\rangle\langle 0| - |1\rangle\langle 1|$. Alice records her measurement result as m (which will be $+1$ or -1) and announces whether her measurement corresponded to σ_1 or σ_3.

Then Alice makes a second announcement. With probability p_a she announces the classical bit c which is determined from the message bit b and the measurement result m using

$$c = \left(b + \frac{1-m}{2} \right) \bmod 2 , \qquad (1)$$

which we refer to as a *bit-announcement*. Or else, (with probability $[1 - p_a]$) she announces the value of m, which we refer to as a *result-announcement*. This completes the routine for a single shot.

Each time that Alice makes a bit-announcement Bob has a chance to determine the value of b, provided that he has prepared the particle in an eigenstate of the measurement operator corresponding to the measurement that

1. REPORT DATE **02 JUN 2006**	2. REPORT TYPE	3. DATES COVERED **00-00-2006 to 00-00-2006**
4. TITLE AND SUBTITLE **Sending Sensitive Messages in Quantum Packages**		5a. CONTRACT NUMBER
		5b. GRANT NUMBER
		5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)		5d. PROJECT NUMBER
		5e. TASK NUMBER
		5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Army Research Laboratory,2800 Powder Mill Road,Adelphi,MD,20783**		8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR'S ACRONYM(S)
		11. SPONSOR/MONITOR'S REPORT NUMBER(S)
12. DISTRIBUTION/AVAILABILITY STATEMENT **Approved for public release; distribution unlimited**		
13. SUPPLEMENTARY NOTES		
14. ABSTRACT		
15. SUBJECT TERMS		

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**4**	

Alice performs. In such a case, Bob uses his conjectured value of m (based on his knowledge of the state he prepared and his knowledge of the measurement made by Alice) along with the equation

$$b = \left(c + \frac{1-m}{2}\right) \bmod 2 \qquad (2)$$

to determine the value of b. Bob can only do this when the state in which he prepares the particle and the measurement that Alice performs have a "matching basis," which occurs with probability $p_a/2$. If a bit-announcement is made on a shot when Alice and Bob do not have a matching basis then Bob will not know which value of m to use in order to calculate the value of b. Similarly, since every outside observer lacks Bob's knowledge of the state in which he prepared the particle, both values of m are equally likely (for either measurement). An eavesdropper who is simply listening to the announcements made by Alice will not be able to determine the value of the message bit b. (The analysis below provides a rigorous method to support this last heuristic statement.)

In order to have a good chance that their bases will be matched up at least once on a bit-announcement, Bob and Alice will repeat this routine N times, where the value of N can be chosen in the following way. They set some target confidence level C_m, where $0 < C_m < 1$, and choose N so that the probability of matching bases during a bit-announcement will be at least C_m. This leads to the value of N which is the next integer greater than $\log(1-C_m)/\log(1-p_a/2)$. (This ignores the likelihood that some of the particles will not reach Alice due to imperfections in the quantum channel. This can be thought of as a "null" announcement by Alice and simply increases the number of shots that Bob needs to initiate in order to reach the target confidence level.)

Each time that Alice makes a result-announcement it gives Bob an opportunity to test the quantum channel for noise (which may be due to imperfections in the system or an eavesdropper). Since Bob knows the state in which he prepared the particle (for each shot), a statistical analysis of the measurement results allows him to determine if the state of the particle is being changed after it leaves him but before it is measured by Alice.

Bob expects to have $(1-p_a)N$, opportunities to check the measurement results; as p_a becomes very small, this grows as $-\log(1-C_m)[2/p_a - 5/2 + 11p_a/24 + O(p_a)^2]$. (Using the value of N determined earlier.) On the other hand, the number of bit-announcements (each of which provides an opportunity for an eavesdropper, called Eve, to gain knowledge of b) is expected to be $p_a N$; as p_a becomes very small, this only goes like $-\log(1-C_m)[2 - p_a/2 - O(p_a)^2]$. Of course, Alice and Bob are free to set p_a as close to zero as they wish. As they decrease p_a, N will increase, and the number of opportunities they get to characterize the channel will increase, but the number

of opportunities that Eve expects to get to obtain the message will not increase beyond $-2\log(1-C_m)$.

Now that we have given a description of this protocol, two parts remain to the analysis: First, to describe possible eavesdropping strategies and quantify the amount of information Eve expects to gain from her actions. Second, to show how Bob can place a bound on the Eve's expected information from his statistical error analysis.

Due to the fact that Bob has a $1/4$ chance to produce any of the four possible initial states $\rho^{(0)}, \rho^{(1)}, \rho^{(+)}$, and $\rho^{(-)}$, Eve's best description of the initial state of the particle — on every shot — is $\rho = \frac{1}{2}I$, where I is the identity operator. An eavesdropper's goal is to choose her actions so that her description of the state of the particle is improved. This will lead to a better prediction of Alice's measurement results which will in turn allow her to deduce the message from Alice's announcements.

On each shot, an eavesdropper has only two options: either apply a quantum operation $\mathcal{E}$ to the particle or perform a measurement (POVM) $\mathcal{M}$ on the particle. Either option will generally change the state of the particle (according to Eve's description). A quantum operation is described by a set of operators $\{E_1, E_2, \ldots, E_r\}$ with the constraint $\sum_i E_i^\dagger E_i = I$. When applying a quantum operation to a particle described by the state ρ, the final state is described by $\rho' = \sum_i E_i \rho E_i^\dagger$. Similarly, a measurement with d possible outcomes is described by a set of operators $\{F_1, F_2, \ldots, F_d\}$ subject to the constraint $\sum_i F_i^\dagger F_i = I$. When the measurement is performed on the particle described by state ρ and the outcome i is found, the state after the measurement is then described by $\rho' = F_i \rho F_i^\dagger / \mathrm{Tr}(F_i \rho F_i^\dagger)$. Generally, we describe the mapping Π from the initial state of the particle ρ to its final state $\Pi(\rho) = \rho'$ as the *effective-evolution* of the state of the particle on that shot.

Over the course of the N shots, we describe the effective-evolution string of length N as $\mathcal{S} = (\Pi_1, \Pi_2, \ldots, \Pi_N)$ where Π_i is the effective-evolution which occurred on the ith shot. It can be shown that for the qubit case at hand, the set of all possible effective-evolution strings of length N is a compact set.

Generally, the particular effective-evolution that occurs on a given shot is decided randomly. (Especially in the case when an effective-evolution occurs as a result of measurement.) Therefore, the *a priori* description of an eavesdropper's effect on the state of the particle will be through a set of possible effective-evolution strings of length N, along with the probability $\Pr(\mathcal{S}_i)$ that the string $\mathcal{S}_i$ will be the one that occurs.

To describe how much of the message an eavesdropper expects to obtain by imposing a particular effective-evolution string on the particle, we use the mutual information between the random variable B describing all the possible messages and the random variable A describing all the possible announcement strings.

TABLE II: The probability for the eight possible announcements given a particular value for b and given that an eavesdropper causes the state to change from ρ to $\rho' = \Pi(\rho)$. For Eve, the initial state is always described by $\rho = \frac{1}{2}I$ whereas Bob's description of the initial state is based upon his knowledge of the particular pure state he prepared on that shot.

$\Pr(\sigma_1, c{=}0\|\Pi, \rho, b)$	$=$	$\frac{p_a}{4}[1 + (1 - 2b)\mathrm{Tr}(\sigma_1\rho')]$
$\Pr(\sigma_1, c{=}1\|\Pi, \rho, b)$	$=$	$\frac{p_a}{4}[1 - (1 - 2b)\mathrm{Tr}(\sigma_1\rho')]$
$\Pr(\sigma_3, c{=}0\|\Pi, \rho, b)$	$=$	$\frac{p_a}{4}[1 + (1 - 2b)\mathrm{Tr}(\sigma_3\rho')]$
$\Pr(\sigma_3, c{=}1\|\Pi, \rho, b)$	$=$	$\frac{p_a}{4}[1 - (1 - 2b)\mathrm{Tr}(\sigma_3\rho')]$
$\Pr(\sigma_1, m{=}{+}1\|\Pi, \rho, b)$	$=$	$\frac{1-p_a}{4}[1 + \mathrm{Tr}(\sigma_1\rho')]$
$\Pr(\sigma_1, m{=}{-}1\|\Pi, \rho, b)$	$=$	$\frac{1-p_a}{4}[1 - \mathrm{Tr}(\sigma_1\rho')]$
$\Pr(\sigma_3, m{=}{+}1\|\Pi, \rho, b)$	$=$	$\frac{1-p_a}{4}[1 + \mathrm{Tr}(\sigma_3\rho')]$
$\Pr(\sigma_3, m{=}{-}1\|\Pi, \rho, b)$	$=$	$\frac{1-p_a}{4}[1 - \mathrm{Tr}(\sigma_3\rho')]$

The possible messages are $b = 0$ and $b = 1$, both with *a priori* probability one-half.

There are 8^N possible announcement strings, which comes from the eight possible announcements (shown in Table I) for each of the N shots. The probability $\Pr(\mathbf{a}|b, \mathcal{S})$ that Alice makes the announcement-string $\mathbf{a} = (a_1, \ldots, a_N)$ given a particular value of b and given that Eve's actions result in the effective-evolution string $\mathcal{S} = (\Pi_1, \ldots, \Pi_N)$ is

$$\Pr(\mathbf{a}|b, \mathcal{S}) = \prod_{i=1}^{N} \Pr(a_i|b, \Pi_i) \ . \tag{3}$$

The probabilities for the eight different announcements on each shot are shown in Table II.

The mutual information $I_\mathcal{S}(A : B)$ between random variables A and B describes the amount of knowledge (on average) Eve expects to gain about the message from Alice's announcements when she imposes the effective-evolution string $\mathcal{S}$. It is calculated by

$$I_\mathcal{S}(A : B) = \sum_{b=0}^{1} \Pr(b) \sum_{\mathbf{a}^{(N)}} \Pr(\mathbf{a}|b, \mathcal{S}) \log \Pr(\mathbf{a}|b, \mathcal{S})$$
$$- \sum_{\mathbf{a}^{(N)}} \Pr(\mathbf{a}|\mathcal{S}) \log \Pr(\mathbf{a}|\mathcal{S}) \tag{4}$$

where the sum over $\mathbf{a}^{(N)}$ indicates that the sum is taken over possible announcement strings of length N, and where $\Pr(\mathbf{a}|\mathcal{S}) = \frac{1}{2}[\Pr(\mathbf{a}|b{=}0, \mathcal{S}) + \Pr(\mathbf{a}|b{=}1, \mathcal{S})]$.

Each possible announcement string $\mathbf{a}$ can be "split-up" into $\mathbf{x}$, the string of the bit-announcements in $\mathbf{a}$, and $\mathbf{y}$, the string of the result-announcements in $\mathbf{a}$. The probability $\Pr(\mathbf{a}|b, \mathcal{S})$ can be written as

$$\Pr(\mathbf{a}|b, \mathcal{S}) = \Pr(\mathbf{x}|b, \mathcal{T}) \Pr(\mathbf{y}|b, \mathcal{U}) \ , \tag{5}$$

where $\mathcal{T}$ is the effective-evolution string for the shots when bit-announcements are made and where $\mathcal{U}$ is the effective-evolution string for the shots when result-announcements are made.

Because of the probabilistic nature of the protocol, the number of bit-announcements is not fixed. The probability $\Pr(k)$ that Alice makes k bit-announcements can be calculated using the binomial distribution:

$$\Pr(k) = \frac{N!}{k!(N - k)!} p_a^k (1 - p_a)^{(N-k)} \ ,$$

where $k = 0, 1, \ldots, N$. In other words, this is the probability that the string $\mathbf{x}$ will have length k. The k bit-announcements can be distributed among the N shots in $\binom{N}{k} = \frac{N!}{k!(N-k)!}$ different ways. Since Eve does not know before-hand which shots will correspond to bit-announcements, when calculating the mutual information she must take into account that $\mathcal{T}$ can be chosen in $\binom{N}{k}$ ways from the effective-evolutions in $\mathcal{S}$.

Utilizing these results, we rewrite Equation (4) as

$$I_\mathcal{S}(A : B) = \sum_{b=0}^{1} \frac{1}{2} \sum_{k} \Pr(k) \sum_{\mathcal{T}^{(k)}} \frac{1}{\binom{N}{k}} \sum_{\mathbf{x}^{(k)}} \sum_{\mathbf{y}^{(N-k)}} \Pr(\mathbf{x}|b, \mathcal{T}) \Pr(\mathbf{y}|b, \mathcal{U}) \log \left[\Pr(\mathbf{x}|b, \mathcal{T}) \Pr(\mathbf{y}|b, \mathcal{U})\right]$$
$$- \sum_{k} \Pr(k) \sum_{\mathcal{T}^{(k)}} \frac{1}{\binom{N}{k}} \sum_{\mathbf{x}^{(k)}} \sum_{\mathbf{y}^{(N-k)}} \Pr(\mathbf{x}|\mathcal{T}) \Pr(\mathbf{y}|\mathcal{U}) \log \left[\Pr(\mathbf{x}|\mathcal{T}) \Pr(\mathbf{y}|\mathcal{U})\right] \tag{6}$$

where the sum over $\mathbf{x}^{(k)}$ $(\mathbf{y}^{(N-k)})$ indicates that the sum is taken over possible bit-announcement (result-announcement) strings of length k (respectively, $[N - k]$) and where the sum over $\mathcal{T}^{(k)}$ indicates that this sum is taken over all possible ways in which the effective-evolution string of length k (corresponding to bit-announcements) can be chosen from the effective-evolution string $\mathcal{S}$. The effective-evolution string $\mathcal{U}$ is the resulting effective-evolution string of length $N - k$ when the string $\mathcal{T}$ is "plucked-out" of the string $\mathcal{S}$. Because the result-announcements have no dependence on the message, neither do the result-announcement strings. That

is,

$$\Pr(\mathbf{y}|b=0,\mathcal{U}) = \Pr(\mathbf{y}|b=1,\mathcal{U}) = \Pr(\mathbf{y}|\mathcal{U}) \ ,$$

for every $\mathcal{U}$. It is straightforward to show that this results in a great simplification of Equation (6) to

$$
\begin{aligned}
I_{\mathcal{S}}(A:B) \ = \ & \\
\sum_k \frac{\Pr(k)}{\binom{N}{k}} \sum_{\mathcal{T}^{(k)}} \Bigg[& \frac{1}{2} \sum_{b=0}^{1} \sum_{\mathbf{x}^{(k)}} \Pr(\mathbf{x}|b,\mathcal{T}) \log \Pr(\mathbf{x}|b,\mathcal{T}) \\
& - \sum_{\mathbf{x}^{(k)}} \Pr(\mathbf{x}|\mathcal{T}) \log \Pr(\mathbf{x}|\mathcal{T}) \Bigg] \ .
\end{aligned} \tag{7}
$$

This leads to the natural introduction of $N+1$ new random variables, $X^{(k)}$ for $k = 0, 1, \ldots, N$, where $X^{(k)}$ describes the possible bit-announcement strings of length k. We can now rewrite Equation (7) as

$$I_{\mathcal{S}}(A:B) = \sum_{k=0}^{N} p_a^k (1-p_a)^{(N-k)} \sum_{\mathcal{T}^{(k)}} I_{\mathcal{T}}(X^{(k)}:B) \ . \tag{8}$$

This completes the analysis of the amount of information that an eavesdropper expects to gain about the message when her eavesdropping activity induces the effective-evolution string $\mathcal{S}$.

It is worthwhile mentioning here that using Eqs. (8) and (3) we can now provide quantitative support for our earlier comment about the ignorance of an eavesdropper who is listening to Alice's announcements but not interacting with the particle in any way. In this case, the effective-evolution mapping Π is the identity mapping on every shot. Therefore, it is straightforward to show that $I_{\mathcal{S}}(A:B) = 0$ because the probabilities for the bit-announcements (shown in Table II) do not depend on b.

After the N shots are performed, Alice will have made a specific string of announcements $\widehat{\mathbf{a}}$, which corresponds to specific strings of bit-announcements $\widehat{\mathbf{x}}$ (of length $\widehat{k}$) and result-announcements $\widehat{\mathbf{y}}$. For each of the announcements $\widehat{a}_i$, Bob knows the state ρ_i in which he prepared the particle. As discussed earlier, he uses this knowledge of the initial states, along with the $\widehat{k}$ bit-announcements $\widehat{x}_\alpha$ for $\alpha = 1, \ldots, \widehat{k}$ to determine the message. We will now describe how he uses Alice's $N - \widehat{k}$ result-announcements $\widehat{y}_\beta$ for $\beta = 1, \ldots, (N - \widehat{k})$ along with his knowledge of the corresponding initial states ρ_β for $\beta = 1, \ldots, (N - \widehat{k})$ to determine the likelihood that the message was exposed to an eavesdropper. We describe this string of initial states by $\boldsymbol{\rho} = (\rho_1, \rho_2, \ldots, \rho_{N-\widehat{k}})$, which corresponds to the shots where Alice makes result-announcements.

Given an effective-evolution string $\mathcal{S}$ that Eve induces by her actions, $\widehat{k}$ of these actions will have occurred on shots when Alice makes a bit-announcement and $N - \widehat{k}$ occurred on shots when Alice makes a

result-announcement. We can calculate $\Pr(\widehat{\mathbf{y}}|\mathcal{S},\boldsymbol{\rho})$ the probability (from Bob's point of view) of Alice making the result-announcements $\widehat{\mathbf{y}}$ given the effective-evolution string $\mathcal{S}$ induced by Eve's actions. To do this, we use the string $\mathcal{U} = \{\Pi_1, \ldots, \Pi_{N-\widehat{k}}\}$ of effective evolutions in $\mathcal{S}$ that occurred during shots when a result-announcement was made. This probability is determined using

$$\Pr(\widehat{\mathbf{y}}|\mathcal{S},\boldsymbol{\rho}) = \prod_{i=1}^{N-\widehat{k}} \Pr(a_i|\Pi_i, \rho_i) \ . \tag{9}$$

We now form a set of effective-evolution strings $\Sigma(\varepsilon)$ such that $\mathcal{S}$ is an element of $\Sigma(\varepsilon)$ if $\Pr(\widehat{\mathbf{y}}|\mathcal{S},\boldsymbol{\rho}) > \varepsilon$ for some number $0 < \varepsilon < 1$. That is, we include an effective-evolution string in the set $\Sigma(\varepsilon)$ if there is a substantial probability, based upon the result-announcement data, that that effective-evolution string was induced by an eavesdropper.

We define the exposure $I_E(\varepsilon)$ of the message to be

$$I_E(\varepsilon) = \max_{\mathcal{S} \in \Sigma(\varepsilon)} \frac{1}{\binom{N}{k}} \sum_{\mathcal{T}^{(\widehat{k})}} I_{\mathcal{T}}(X^{(\widehat{k})} : B). \tag{10}$$

This maximum is known to exist because $\Sigma(\varepsilon)$ is a compact set. This completes the analysis describing how the receiver sets a bound on the amount of a message exposed to any eavesdroppers.

While using this protocol to transmit messages, if some messages have been transmitted with no exposure to eavesdroppers, these messages could be used as crypto-keys for subsequent communication. Finally, we remark that the states and measurements described here are identical to those used in the BB84 protocol,[6] and any apparatus that is designed to implement BB84 can also implement this protocol with minor modifications.

---

* Electronic address: plopata@arl.army.mil

[1] C. E. Shannon, in *Claude Elwood Shannon Collected Papers* (IEEE Press, 1993), pp. 84–143.

[2] G. Brassard, *Modern Cryptology* (Springer-Verlag New York, Inc., 1988).

[3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[4] H. Bechmann-Pasquinucci, International Journal of Quantum Information **1**, 217 (2003).

[5] S. K. Singh and R. Srikanth, Physica Scripta **71**, 433 (2005).

[6] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (IEEE Press, 1984), pp. 175–179.