Quantum mutual information and the one-time pad

Benjamin Schumacher[1] and Michael D. Westmoreland[2]

[1]*Department of Physics, Kenyon College, Gambier, Ohio 43022, USA*
[2]*Department of Mathematical Sciences, Denison University, Granville, Ohio 43023, USA*

Alice and Bob share a correlated composite quantum system *AB*. If *AB* is used as the key for a one-time pad cryptographic system, we show that the maximum amount of information that Alice can send securely to Bob is the quantum mutual information of *AB*.

PACS number(s): 03.67.Dd, 03.65.Ud

I. THE ONE-TIME PAD AND MUTUAL INFORMATION

A *one-time pad* [1] is a cryptographic protocol in which communicators Alice and Bob initially have correlated random variables, collectively called the "key," that are not correlated with any variables possessed by a potential eavesdropper Eve. (In most discussions, the key variables possessed by Alice and Bob are supposed to be perfectly correlated—e.g., they are identical copies of the same secret string of bits. We consider the more general case.) If the key variables are used only once, they allow Alice to send Bob a perfectly secret message over a public communication channel. The value of a key as a resource is the amount of information that can be sent secretly by its use.

In this paper we examine a quantum-mechanical analog of the one-time pad. Alice and Bob initially share a correlated composite quantum system *AB*. Alice encodes a classical message by performing one of several possible operations on her subsystem *A*, after which she transfers it to Bob. Bob reads the message via a measurement on the entire system *AB*. The eavesdropper Eve only has access to subsystem *A*; thus, to ensure the security of the secret message, Alice must ensure that the *A* by itself can provide no information to Eve.

Holevo [2] provided an upper bound for the accessible information in a measurement. Suppose a quantum system is prepared in a state ρ_α with probability p_α. The ensemble average state is $\rho=\Sigma_\alpha p_\alpha\rho_\alpha$. Holevo showed that, for any measurement, the mutual information *I* between the preparation and the measurement result is bounded above by

$$I \leq \chi = S(\rho) - \sum_\alpha p_\alpha S(\rho_\alpha), \tag{1}$$

where $S(\rho)=-\mathrm{Tr}\rho \log \rho$. Holevo [3] and Schumacher and Westmoreland [4] proved that, with appropriate choices of code and decoding observable, this upper bound can be approached asymptotically. Therefore, χ measures the classical information that can be conveyed using a particular ensemble of quantum states.

The quantity $\chi\geq 0$, with equality if and only if all of the possible states ρ_α are the same. We can say even more. The *only* situation in which zero information is provided by any measurement is the situation in which all of the possible states are the same. Since Alice wishes to exclude the eavesdropper, she must arrange that her various operations always lead to the same output state of *A*. That is, $\chi^A=0$.

However, Alice and Bob want to make sure that $\chi^{AB}>0$, since Bob needs to read the secret message by an *AB* measurement. Let ρ^{AB} be the initial "key" state of *AB*. Only the correlations within ρ^{AB} permit Alice and Bob to communicate at all. If the initial state ρ^{AB} is a product state, then it must remain a product state regardless of Alice's manipulation of it—and always the same product state, since ρ^B is unchanged and Alice's final state σ^A is fixed. Even with both *A* and *B* in his possession, Bob will not be able to infer anything about Alice's choice of operation, because he will always have the state $\sigma^A\otimes\rho^B$. Without correlations, the "key" state ρ^{AB} is useless.

We now put this intuitive observation on a more quantitative basis. Imagine that Alice performs the operation $\mathcal{E}^A_\alpha$ on *A* with probability p_α. We write

$$\sigma^{AB}_\alpha = (\mathcal{E}^A_\alpha \otimes \mathbf{I}^B)\rho^{AB}, \tag{2}$$

$$\sigma^{AB} = \sum_\alpha p_\alpha\sigma^{AB}_\alpha. \tag{3}$$

To exclude the eavesdropper, we require that $\sigma^A_\alpha=\sigma^A$ for every α. The information that Alice can send to Bob will be limited by

$$\chi^{AB} = S(\sigma^{AB}) - \sum_\alpha p_\alpha S(\sigma^{AB}_\alpha). \tag{4}$$

The entropy of the average state σ^{AB} is subadditive, so that $S(\sigma^{AB})\leq S(\sigma^A)+S(\sigma^B)$ (with equality if and only if $\sigma^{AB}=\sigma^A\otimes\sigma^B$). Thus,

$$\chi^{AB} \leq S(\sigma^B) + S(\sigma^A) - \sum_\alpha p_\alpha S(\sigma^{AB}_\alpha). \tag{5}$$

Note that $\sigma^B=\rho^B$ (since Alice only operates on *A*) and that, by assumption, the individual final *A* states satisfy $\sigma^A_\alpha=\sigma^A$ for all α:

$$\chi^{AB} \leq S(\rho^B) + \sum_\alpha p_\alpha[S(\sigma^A_\alpha) - S(\sigma^{AB}_\alpha)]. \tag{6}$$

No operation on *A* alone can lead to an increase in the coherent information [5] S^A-S^{AB}, so that for all α,

$$S(\sigma^A_\alpha) - S(\sigma^{AB}_\alpha) \leq S(\rho^A) - S(\rho^{AB}). \tag{7}$$

Therefore,

$$\chi^{AB} \leq S(\rho^A) + S(\rho^B) - S(\rho^{AB}). \qquad (8)$$

The quantity on the right is $I_\rho(A:B)$, the quantum mutual information between A and B, a measure of the degree of correlation in the original state ρ^{AB}. We have shown that the information that Alice can transmit secretly to Bob using ρ^{AB} as a one-time pad is bounded above by $I_\rho(A:B)$.

II. A SPECIAL CASE

Having shown that $\chi^{AB} \leq I_\rho(A:B)$, we will now show that Alice can choose an ensemble of operations so that $\chi^{AB} \to I_\rho(A:B)$ asymptotically. Since we know that we can achieve χ^{AB} as an asymptotic information rate, it follows that Alice can send up to $I_\rho(A:B)$ bits per key to Bob while keeping Eve completely excluded.

To do this, we will only need to consider unitary operations on A, given by unitary operators U_α^A. The new A states will be exactly the same as the original "key" state of A, so that

$$\sigma_\alpha^A = U_\alpha \rho^A U_\alpha^\dagger = \rho^A \qquad (9)$$

for all α. This amounts to saying that $[U_\alpha^A, \rho^A] = 0$.

We will first consider a special case in which we can make $\chi^{AB} = I_\rho(A:B)$ in a single composite system, without the need for an asymptotic argument. Suppose that the initial A state is maximally mixed on a subspace, so that $\rho^A = \frac{1}{d}\Pi$ (where Π is the projection onto a d-dimensional subspace). Then any unitary operator on A that commutes with Π will leave ρ^A invariant. Let us choose basis states $|k^A\rangle$ for the support of Π and write

$$\rho^{AB} = \sum_{kl} |k^A\rangle\langle l^A| \otimes w_{kl}^B. \qquad (10)$$

By considering $\rho^B = \mathrm{Tr}_A \rho^{AB}$, we can see that the B operators w_{kl}^B satisfy

$$\rho^B = \sum_k w_{kk}^B. \qquad (11)$$

What operators U_α^A does Alice include in her ensemble? We will say that her ensemble includes (1) all possible relative phase flips among the $|k^A\rangle$ basis states; (2) all permutations of the $|k^A\rangle$ basis states; and (3) all combinations of these. There are N such operators, and Alice uses each with probability $1/N$. Thus,

$$\sigma_\alpha^{AB} = \sum_{kl} (U_\alpha^A |k^A\rangle\langle l^A| U_\alpha^{A\dagger}) \otimes w_{kl}^B, \qquad (12)$$

$$\sigma^{AB} = \sum_{kl} \left(\frac{1}{N}\sum_\alpha U_\alpha^A |k^A\rangle\langle l^A| U_\alpha^{A\dagger} \right) \otimes w_{kl}^B. \qquad (13)$$

Consider the sum in the second expression. When $k \neq l$, the sum over α contains all relative phase flips among the A basis states with equal weights. In this case the sum must equal zero. The expression for σ^{AB} becomes

$$\sigma^{AB} = \sum_k \left(\frac{1}{N}\sum_\alpha U_\alpha^A |k^A\rangle\langle k^A| U_\alpha^{A\dagger} \right) \otimes w_{kk}^B. \qquad (14)$$

The sum over α also includes all permutations among the A basis states. This means that the result of this sum is independent of k. We conclude that the average state σ^{AB} is a product state, namely,

$$\sigma^{AB} = \rho^A \otimes \rho^B. \qquad (15)$$

For each α, σ_α^{AB} is just the original state ρ^{AB}, rotated by the unitary operator U_α^A. This rotated state will have the same entropy as the original. It follows that

$$\chi^{AB} = S(\sigma^{AB}) - \sum_\alpha p_\alpha S(\sigma_\alpha^{AB}) = S(\rho^A) + S(\rho^B) - S(\rho^{AB}) \qquad (16)$$

$$= I_\rho(A:B). \qquad (17)$$

In this special case, then, we can arrange for χ^{AB} to achieve its upper bound of $I_\rho(A:B)$ exactly.

Notice how this works. We have arranged Alice's ensemble of operations so that the correlations between A and B completely disappear on average—leaving σ^{AB} a product state. Let us think about this more generally. Once again, we suppose that we have a bunch of unitary operators U_α^A acting on A, which do not alter the subsystem state ρ^A. We have

$$\chi^{AB} = S(\sigma^{AB}) - S(\rho^{AB}) \qquad (18)$$

(since for each α the state σ_α^{AB} has the same entropy as ρ^{AB}). Noting that $\sigma^A = \rho^A$ and $\sigma^B = \rho^B$, we can rewrite this as

$$\chi^{AB} = I_\rho(A:B) - I_\sigma(A:B), \qquad (19)$$

where $I_\rho(A:B)$ and $I_\sigma(A:B)$ are the mutual information for ρ^{AB} and σ^{AB}, respectively. In other words, χ^{AB} is exactly the amount by which we have, on average, reduced the mutual information between the systems. In our special case, where the subsystem A is completely mixed, we can reduce this all the way to zero, and so $\chi^{AB} = I_\rho(A:B)$.

This points up a connection between our analysis and the work of Groisman *et al.* [6], who define the "total correlation" of two systems to be the amount of classical information that must be added to the system so that the correlations can be completely eliminated by local operations. They show that the total correlation is given by the quantum mutual information. The elimination of correlations is not our aim; rather, we wish to maximize χ^{AB} subject to the strict privacy condition that $\chi^A = 0$. Nevertheless, Eq. (19) tells us that these two tasks are closely related.

III. THE GENERAL CASE

Now let us consider a general state ρ^{AB}. The subsystem state ρ^A has D distinct eigenvalues λ_K. For a given K, the eigenspace of λ_K has dimension d_k. We can therefore choose a basis of ρ^A eigenstates and write

$$\rho^A = \sum_{K=1}^{D} \lambda_K \left(\sum_{m_K=1}^{d_K} |Km_K\rangle\langle Km_K| \right). \tag{20}$$

For a given K, we think of the basis states $|Km_K\rangle$ as comprising a "block" spanning the d_K-dimensional eigenspace of λ_K. This block has total "weight" $P_K = d_K\lambda_K$ in this mixture. We can write

$$\rho^A = \sum_K P_K \rho_K^A, \tag{21}$$

where each ρ_K^A is the density operator that is maximally mixed on the eigenspace of λ_K:

$$\rho_K^A = \sum_{m_K} \frac{1}{d_K} |Km_K\rangle\langle Km_K|. \tag{22}$$

The joint state ρ^{AB} can be written

$$\rho^{AB} = \sum_{KL} \left(\sum_{m_K n_L} |Km_K\rangle\langle Ln_L| \otimes w_{Km_K Ln_L}^B \right). \tag{23}$$

What can we say about the operators $w_{Km_K Ln_L}^B$? If we compare the partial trace of this expression with Eq. (20), we see that

$$\mathrm{Tr}\, w_{Km_K Ln_L}^B = \lambda_K \delta_{KL} \delta_{m_K n_L}. \tag{24}$$

Thus, given a value of K,

$$\sum_{m_K} w_{Km_K Km_K}^B = P_K \rho_K^B \tag{25}$$

for some density operator ρ_K^B. This will be useful below.

Notice that, for various values of K, the density operators ρ_K^A have orthogonal supports. In general, we can make no such claim about the supports of the density operators ρ_K^B.

As before, Alice will perform unitary operations on A that do not change the subsystem state ρ^A. The operators U_α^A include (1) all relative phase flips between distinct blocks; (2) all relative phase flips between basis states within each block; (3) all permutations of the basis states within each block; and (4) all combinations of these. Again, we say that there are N such operators, and Alice uses each with probability $1/N$.

The resulting average state σ^{AB} is

$$\sigma^{AB} = \sum_{KL} \sum_{m_K n_L} \left(\frac{1}{N} \sum_\alpha U_\alpha^A |Km_K\rangle\langle Ln_L| U_\alpha^{A\dagger} \right) \otimes w_{Km_K Ln_L}^B. \tag{26}$$

Since the average over α includes all phase flips between distinct values of K and L, the average in parentheses is zero unless $K=L$, so

$$\sigma^{AB} = \sum_K \sum_{m_K n_K} \left(\frac{1}{N} \sum_\alpha U_\alpha^A |Km_K\rangle\langle Kn_K| U_\alpha^{A\dagger} \right) \otimes w_{Km_K Kn_K}^B. \tag{27}$$

Also, we include all phase flips between distinct values of m_K and n_K, so the sum becomes

$$\sigma^{AB} = \sum_{Km_K} \left(\frac{1}{N} \sum_\alpha U_\alpha^A |Km_K\rangle\langle Km_K| U_\alpha^{A\dagger} \right) \otimes w_{Km_K Km_K}^B. \tag{28}$$

Finally, since the U_α^A operators include all permutations of basis states within a given block, the average in parentheses depends only on K and not on m_K. Indeed, this average is the uniform density operator on the λ_K eigenspace for ρ^A, which is just ρ_K^A. This means we can write

$$\sigma^{AB} = \sum_K P_K \rho_K^A \otimes \rho_K^B. \tag{29}$$

From this, noting that the ρ_K^A operators have orthogonal supports, we can calculate the quantum mutual information $I_\sigma(A:B)$ to be

$$I_\sigma(A:B) = S(\rho^B) - \sum_K P_K S(\rho_K^B). \tag{30}$$

The right-hand side of this equation is bounded above by $\log D$, the logarithm of the number of distinct eigenvalues of ρ^A (and thus the number of values of the eigenvalue index K). Therefore,

$$I_\sigma(A:B) \leq \log D. \tag{31}$$

Alice can therefore achieve a Holevo bound for the composite system satisfying

$$\chi^{AB} \geq I_\rho(A:B) - \log D. \tag{32}$$

Now consider the asymptotic problem. Alice and Bob share a large number n of copies of the pair AB, so that their initial joint state is $(\rho^{AB})^{\otimes n}$. The quantum mutual information of this state is just $nI_\rho(A:B)$. Alice performs operations on all of her copies together such that the final state of these copies is always the same. Alice's systems are delivered to Bob, who will try to distinguish which operation Alice performed. Regardless of Alice's operations,

$$\frac{1}{n}\chi^{(AB)^{\otimes n}} \leq I_\rho(A:B). \tag{33}$$

We will now show that, for a suitable ensemble of operations, Alice can approach equality, and therefore $I_\rho(A:B)$ is an asymptotically achievable information rate from Alice to Bob as $n \to \infty$.

First, we note that $(\rho^A)^{\otimes n}$ is a highly degenerate state for large n. If the Hilbert space $\mathcal{H}^A$ has dimension d, then $(\mathcal{H}^A)^{\otimes n}$ has dimension d^n (exponential in n), but the state $(\rho^A)^{\otimes n}$ has no more than $(n+1)^d$ (polynomial in n) distinct eigenvalues. These distinct eigenvalues correspond to the *type classes* [7] of sequences of n independent identically distributed random variables, each having d values. Therefore, if we use our previous method to choose an ensemble of unitary operators for Alice's systems that each leave $(\rho^A)^{\otimes n}$ unchanged, we can create an ensemble of $(AB)^{\otimes n}$ states such that

$$\chi^{(AB)^{\otimes n}} \geq nI_\rho(A:B) - \log(n+1)^d. \tag{34}$$

Therefore,

$$\frac{1}{n}\chi^{(AB)^{\otimes n}} \geqslant I_\rho(A{:}B) - \frac{d}{n}\log(n+1). \qquad (35)$$

Since the second term goes to zero as $n \to \infty$, we have found a sequence of procedures such that

$$\lim_{n \to \infty} \frac{1}{n}\chi^{(AB)^{\otimes n}} = I_\rho(A{:}B). \qquad (36)$$

The mutual information $I_\rho(A{:}B)$ is therefore the information capacity from Alice to Bob if Alice can perform only local operations on the A systems that always lead to the same A state (and will thus completely exclude any eavesdropper with access only to A).

IV. SLIGHTLY INSECURE TRANSMISSION

Note that we have required absolute perfection—that is, we have required that, by examining system A by itself, the eavesdropper Eve cannot get any information at all. No matter what operation Alice performs, the final A state is exactly the same. But what if we relax this requirement? Since Alice now has a wider range of operations at her disposal, she should be able to increase the Holevo bound χ^{AB}, and thus the information that she can deliver to Bob. If Eve has access only to a finite specified amount of information, how much additional capacity can Alice and Bob achieve? We will now show that the extra capacity from Alice to Bob is no larger than the Holevo bound χ^A, which in turn bounds the accessible information of the eavesdropper. Thus, if the protocol is only slightly insecure (χ^A is small), the information capacity is only slightly increased.

We begin with the key state ρ^{AB}, and Alice performs the operation $\mathcal{E}_\alpha^A$ on A with probability p_α. We do not require the operations to be unitary. As before, the final states are

$$\sigma_\alpha^A = \mathcal{E}_\alpha^A(\rho^A), \qquad (37)$$

$$\sigma_\alpha^{AB} = \mathcal{E}_\alpha^A \otimes \mathbf{I}^B(\rho^{AB}), \qquad (38)$$

$$\sigma^A = \sum_\alpha p_\alpha \sigma_\alpha^A, \qquad (39)$$

$$\sigma^{AB} = \sum_\alpha p_\alpha \sigma_\alpha^{AB}. \qquad (40)$$

Then

$$\chi^{AB} - \chi^A = S(\sigma^{AB}) - S(\sigma^A) + \sum_\alpha p_\alpha[S(\rho_\alpha^A) - S(\rho_\alpha^{AB})]. \qquad (41)$$

By Eq. (7), remembering that $S(\sigma^B) = S(\rho^B)$ for A operations, this becomes

$$\chi^{AB} - \chi^A \leqslant S(\sigma^{AB}) - S(\sigma^A) + S(\rho^A) - S(\rho^{AB}) \qquad (42)$$

$$= I_\rho(A{:}B) - I_\sigma(A{:}B) \qquad (43)$$

$$\leqslant I_\rho(A{:}B). \qquad (44)$$

Thus,

$$\chi^{AB} \leqslant I_\rho(A{:}B) + \chi^A. \qquad (45)$$

Allowing a small nonzero χ^A can only increase χ^{AB} by that same small amount.

V. REMARKS

In our analysis of the quantum problem, we have also proven the analogous classical result. That is, suppose Alice and Bob possess a pair of correlated random variables X_A and X_B. Alice encodes her message by performing one of several possible operations on her own variable X_A. To prevent Eve (who has access to X_A) from reading the message, she arranges for the marginal probability distribution of X_A to be independent of her message. Bob receives X_A and reads the message by examining the joint value (X_A, X_B). In such a situation, the maximum achievable secure communication rate from Alice to Bob is the classical mutual information $I(X_A{:}X_B)$. This follows from our quantum result in the case that the quantum state of the composite system AB is a mixture of products of states drawn from orthogonal sets for A and B.

In other words, our analysis tells us that the mutual information is the answer to the *same* communication problem in both the classical and quantum settings. This illuminates the connections between classical and quantum information ideas. In particular, it sheds light on the meaning of the mutual information functional as a measure of the degree of correlation between physical systems.

[1] J. A. Buchmann, *Introduction to Cryptography* (Springer, New York, 2001).

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

[3] A. S. Holevo, IEEE Trans. Inf. Theory **44**, 269 (1998).

[4] B. Schumacher and M. Westmoreland, Phys. Rev. A **51**, 2738 (1995).

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

[6] B. Groisman, S. Popescu, and A. Winter, Phys. Rev. A **72**, 032317 (2005).

[7] T. M. Cover and J. A. Thomas, *Elements of Information Theory* (Wiley, New York, 1991).