Invertible Quantum Operations and Perfect Encryption of Quantum States

Ashwin Nayak
U. Waterloo & Perimeter *

Pranab Sen
TIFR †

September 20, 2006

Abstract

In this note, we characterize the form of an invertible quantum operation, i.e., a completely positive trace preserving linear transformation (a CPTP map) whose inverse is also a CPTP map. The precise form of such maps becomes important in contexts such as self-testing and encryption. We show that these maps correspond to applying a unitary transformation to the state along with an ancilla initialized to a fixed state, which may be mixed.

The characterization of invertible quantum operations implies that one-way schemes for encrypting quantum states using a classical key may be slightly more general than the "private quantum channels" studied by Ambainis, Mosca, Tapp and de Wolf [1, Section 3]. Nonetheless, we show that their results, most notably a lower bound of $2n$ bits of key to encrypt n quantum bits, extend in a straightforward manner to the general case.

1 Introduction

The most general physically allowed operation on a quantum state consists of coupling it to another system (an ancilla) in a known state, via a unitary transformation, and then discarding part of the system. (In this article, a quantum state may be mixed and is modeled by a density matrix.) We say that a quantum operation E is *invertible*, if there is another *quantum operation* D such that $DE(\rho) = \rho$ for every state ρ in the domain of E. Mathematically, a quantum operation corresponds to a *completely positive trace preserving linear transformation*, a *CPTP map* [8, Section 8.2]. A CPTP map may be an invertible linear transformation, but may not correspond to an invertible quantum operation in the sense defined above. For example, the depolarizing channel is an invertible CPTP map, but its inverse is not even positive. However, if a CPTP map corresponds to an invertible quantum operation, it is necessarily also injective,

*Department of Combinatorics and Optimization, and Institute for Quantum Computing, University of Waterloo, 200 University Ave. W., Waterloo, ON N2L 3G1, Canada. E-mail: anayak@math.uwaterloo.ca. Research supported in part by NSERC, CIAR, MITACS, CFI, and OIT (Canada). A.N. is also Associate Member, Perimeter Institute for Theoretical Physics, Waterloo, Canada. Research at Perimeter Institute is supported in part by the Government of Canada through NSERC and by the Province of Ontario through MEDT.

†School of Technology and Computer Science, Tata Institute of Fundamental Research, Homi Bhabha Road, Colaba, Mumbai 400005, India. Email: pgdsen@tcs.tifr.res.in. This research was done while the author was at NEC Laboratories America, Inc., Princeton, NJ, U.S.A.

and therefore invertible on its image. This is because there is a basis for the domain consisting of density matrices alone.

In this note, we characterize the form of an invertible quantum operation. The precise form of such maps becomes important in contexts such as self-testing [11] and encryption [1]. A unitary operation is a natural example of a CPTP map that is also invertible. It seems intuitively obvious that *all* invertible quantum operations also be unitary. This is indeed the case for CPTP maps transforming a Hilbert space into itself [9, Chapter 3, Section 8, Exercise 3.2]. Here, we examine the more general case, where an invertible quantum operation may take d-dimensional states to states in a Hilbert space of possibly larger dimension. We show that these maps correspond to applying a unitary transformation to the state along with an ancilla initialized to a fixed state, which may be mixed (Theorem 2.1). We also extend this characterization to completely positive (CP) maps in Theorem 2.2. Its significance lies in the fact that when suitably scaled by a positive real number, CP maps correspond to the result of getting one of a subset of outcomes on a measurement.

Invertible quantum operations also occur in the context of error correction. There, the goal is to find a linear subspace of a Hilbert space such that the restriction of the noise operator to this space is invertible. The proof of our characterization theorem closely follows the proof of the error-correction criterion [8, page 436, Theorem 10.1].

A notion related to error-correction is that of a *reversible quantum operation*. Several authors [6, 7] consider operations that are completely positive maps defined by the process of making a measurement, and getting one of a subset of outcomes. They call such an operation E *reversible* on a subspace, if for all states ρ in the subspace, there is a quantum operation D such that $D(E(\rho))/\mathrm{Tr}(E(\rho)) = \rho$. Nielsen *et al.* [7] characterize such operations in information theoretic as well as algebraic terms (akin to the error-correction criterion).

Theorem 2.1 has implications for perfect encryption of quantum states using a classical private key (see, e.g., Ref. [1]). These protocols for encryption, also called "private quantum channels" by some authors, involve two parties, labeled Alice and Bob. The two parties share a secret, uniformly random bit-string k, called the private key. Alice wishes to send a quantum message, a d-dimensional quantum state ρ, to Bob. She would like to apply an invertible CPTP map E_k to the state, and send it to Bob so that when averaged over k, the result is a fixed density matrix (independent of the message). This would ensure that no eavesdropper be able to distinguish two different messages with any degree of success, and therefore guarantee information theoretic security. Bob, who also has the key k, can apply the inverse operation D_k to decrypt the message ρ perfectly. (We have implicitly assumed that the quantum channel is noiseless unless an eavesdropper tampers with it.)

The characterization of invertible quantum operations implies that in the most general one-way encryption scheme, Alice may apply a unitary operation to the state to be encrypted along with an ancilla *that depends upon the key*. This is slightly more general than the form studied by Ambainis, Mosca, Tapp and de Wolf [1, Section 3], where the ancilla is assumed to be independent of the key. Nonetheless, their results, most notably a lower bound of $2n$ bits of key to encrypt n quantum bits, extend in a straightforward manner to the general case. We summarize these observations in Section 3.

The lower bound of $2n$ classical key bits needed to encrypt quantum states was also shown by Boykin and Roychowdhury [2], *assuming that no ancilla is used*. Their proof was simplified by Ambainis *et al.* [1]. Since the addition of ancilla results in longer ciphertext, and hence is less efficient, this case is of special interest. We observe that this $2n$ lower bound follows directly from a "rank argument".

We point out that information theoretic proofs due to DiVincenzo, Hayden, and Terhal [3, Section IV] and Jain [4] follow a different route to the same lower bound on the length of key for general one-way

encryption schemes. We also note that the requirement of perfect information theoretic security imposes an additional constraint on the maps E_k, apart from invertibility. This constraint may simplify the mathematical structure of these schemes, and further simplify the proofs we give.

2 Invertible quantum operations

We refer the reader to the text [8] for basic concepts related to quantum states and operations, and present our characterization theorem directly.

Let $\mathrm{L}(\mathcal{H})$ denote the set of linear operators on the Hilbert space $\mathcal{H}$.

Theorem 2.1 *Let $E : \mathrm{L}(\mathbb{C}^p) \to \mathrm{L}(\mathbb{C}^q)$ be a completely positive, trace preserving linear transformation (a CPTP map). Suppose there is a CPTP map $D : \mathrm{L}(\mathbb{C}^q) \to \mathrm{L}(\mathbb{C}^p)$ such that $DE(\rho) = \rho$ for all density matrices $\rho \in \mathrm{L}(\mathbb{C}^p)$. I.e., E is an invertible quantum operation with inverse D.*

Then there is a density matrix $\omega \in \mathrm{L}(\mathbb{C}^{\lfloor q/p \rfloor})$, and a unitary operation on $\mathbb{C}^q$ such that $E(\rho) = U(\rho \otimes \omega)U^\dagger$. Furthermore, D corresponds to applying $U^\dagger$, and tracing out the $\lfloor q/p \rfloor$ dimensional ancilla.

Proof: As mentioned in Section 1, there is a close analogy between error-correction, and the invertibility of quantum operations. If we view $\mathbb{C}^p$ as a code subspace, and E as a noisy channel restricted to this subspace, then the decoding map D corrects any "errors" introduced by E. We may thus appeal to the error-correction criterion [8, page 436, Theorem 10.1] to give a short proof of the theorem. Instead, in the interest of completeness, we present the details below. Those familiar with the criterion may skip to Equation (2) and then to Equation (3) after picking up the notation in the next paragraph.

A CPTP map from $\mathrm{L}(\mathbb{C}^n)$ to $\mathrm{L}(\mathbb{C}^m)$ can be expressed in terms of linear transformations from $\mathbb{C}^n$ to $\mathbb{C}^m$ (*Kraus operators*), using an operator sum representation [8, Exercise 8.3]. Suppose we express both maps E and D in terms of some set of Kraus operators $\{A_i\}_{i\in\mathcal{I}}$ and $\{B_j\}_{j\in\mathcal{J}}$, respectively. Then, by the invertibility of E, we have, for every $\rho \in \mathrm{L}(\mathbb{C}^p)$

$$DE(\rho) \quad = \quad \sum_{i\in\mathcal{I}} \sum_{j\in\mathcal{J}} B_j A_i \; \rho \; A_i^\dagger B_j^\dagger \quad = \quad \rho.$$

Thus, the CPTP operation DE defined on $\mathrm{L}(\mathbb{C}^p)$ may equivalently be expressed in terms of the single Kraus operator $\mathbb{I}_p$, the identity operator on $\mathbb{C}^p$. By the unitary equivalence of Kraus representations [8, Page 372, Theorem 8.2], there are complex numbers α_{ij}, such that $\sum_{i\in\mathcal{I}} \sum_{j\in\mathcal{J}} |\alpha_{ji}|^2 = 1$, and for all $i \in \mathcal{I}$, $j \in \mathcal{J}$,

$$B_j A_i \quad = \quad \alpha_{ji} \, \mathbb{I}_p \, .$$

Therefore for all $i, i' \in \mathcal{I}$,

$$\sum_{j\in\mathcal{J}} A_{i'}^\dagger B_j^\dagger B_j A_i \quad = \quad \beta_{i'i} \, \mathbb{I}_p,$$

where

$$\beta_{i'i} \quad = \quad \sum_{j\in\mathcal{J}} \bar{\alpha}_{ji'} \alpha_{ji}. \tag{1}$$

Observe that $M = (\beta_{i'i})_{i',i\in\mathcal{I}}$ is a Hermitian matrix. Since, $\sum_{j\in\mathcal{J}} B_j^\dagger B_j = \mathbb{I}_q$, we have for all $i, i' \in \mathcal{I}$,

$$A_{i'}^\dagger A_i \quad = \quad \beta_{i'i}\mathbb{I}_p. \tag{2}$$

The conditions in Equation (2) imply that each Kraus operator A_i is a scaled isometric embedding of $\mathbb{C}^p$ into $\mathbb{C}^q$. However, the resulting images need not be mutually orthogonal. We therefore first derive an equivalent representation for E in which the Kraus operators embed into orthogonal subspaces.

Using equation (1) above, we have that for any vector $x \in \mathbb{C}^{\mathcal{I}}$,

$$\begin{aligned}
(x^\dagger M x) &= \sum_{i,i'\in\mathcal{I}} \bar{x}_{i'}\,\beta_{i'i}\,x_i \\
&= \sum_{i,i'\in\mathcal{I}}\sum_{j\in\mathcal{J}} \bar{x}_{i'}\,\bar{\alpha}_{ji'}\;\alpha_{ji}\,x_i \\
&= \sum_{j\in\mathcal{J}} \left(\sum_{i'\in\mathcal{I}} \bar{x}_{i'}\,\bar{\alpha}_{ji'}\right)\left(\sum_{i\in\mathcal{I}} x_i\,\alpha_{ji}\right) \\
&\geq 0.
\end{aligned}$$

So the matrix M is positive semi-definite. Moreover

$$\mathrm{Tr}(M) \quad = \quad \sum_{i\in\mathcal{I}}\beta_{ii} \quad = \quad \sum_{i\in\mathcal{I}}\sum_{j\in\mathcal{J}}|\alpha_{ji}|^2 \quad = \quad 1.$$

Let $V = (v_{i'i})_{i',i\in\mathcal{I}}$ be a unitary matrix that diagonalizes M. Let $\Gamma = V^\dagger M V$ be the resulting diagonal matrix, with $\gamma_i = \Gamma_{ii} \geq 0$ for all $i \in \mathcal{I}$, and $\sum_{i\in\mathcal{I}}\gamma_i = \sum_{i\in\mathcal{I}}\beta_{ii} = 1$. Then the Kraus operators $C_k = \sum_i v_{ik}\,A_i$, $k \in \mathcal{I}$ also represent the same map E, as may be checked by direct substitution (cf. [8, Page 372, Theorem 8.2]). Moreover, the range spaces of the various operators C_k are orthogonal. In fact for $k, k' \in \mathcal{I}$,

$$\begin{aligned}
C_{k'}^\dagger C_k &= \left(\sum_{i'\in\mathcal{I}} \bar{v}_{i'k'}\,A_{i'}^\dagger\right)\left(\sum_{i\in\mathcal{I}} v_{ik}\,A_i\right) \\
&= \sum_{i',i\in\mathcal{I}} \bar{v}_{i'k'}\,v_{ik}\left(A_{i'}^\dagger A_i\right) \\
&= \sum_{i',i\in\mathcal{I}} \bar{v}_{i'k'}\,v_{ik}\,(\beta_{i'i}\,\mathbb{I}_p) \\
&= \left(\sum_{i',i\in\mathcal{I}} \bar{v}_{i'k'}\,\beta_{i'i}\,v_{ik}\right)\cdot\mathbb{I}_p \\
&= \Gamma_{k'k}\,\mathbb{I}_p \\
&= \delta_{k'k}\,\gamma_k\,\mathbb{I}_p,
\end{aligned} \tag{3}$$

where δ is the Kronecker delta function.

Define $\mathcal{K} = \{k \in \mathcal{I} : \gamma_k \neq 0\}$. Looking at the singular value decomposition of C_k, $k \in \mathcal{K}$, we now conclude that all its singular values are equal to $\sqrt{\gamma_k}$, and that the various operators C_k are scaled unitary embeddings of $\mathbb{C}^p$ into orthogonal subspaces of $\mathbb{C}^q$: $C_k = \sqrt{\gamma_k}\;\sum_{l\in[p]}\;|y_{kl}\rangle\langle u_l^{(k)}|$, where $\{y_{kl}\}_{k\in\mathcal{K},l\in[p]}$ is an orthonormal

set of vectors in $\mathbb{C}^q$, and $\left\{u_l^{(k)}\right\}_{l\in[p]}$ is an orthonormal basis of $\mathbb{C}^p$ for each $k \in \mathcal{K}$. As a consequence, $q \geq p$, and $|\mathcal{K}| \leq \lfloor q/p \rfloor$.

We may now define $\omega = \sum_{k\in\mathcal{K}} \gamma_k \, |w_k\rangle\langle w_k|$, where $\{w_k\}_{k\in\mathcal{K}}$ is an orthonormal set in $\mathbb{C}^{\lfloor q/p \rfloor}$. Define U as any unitary extension to $\mathbb{C}^q$ of the map:

$$|u_l^{(k)}\rangle \otimes |w_k\rangle \quad \mapsto \quad |y_{kl}\rangle,$$

where $k \in \mathcal{K}$ and $l \in [p]$. A straightforward check confirms that E may be implemented by applying U to any state in $\mathbb{C}^p$ tensored with ancilla ω. Similarly, the inverse operation D may be implemented by applying $U^\dagger$ and tracing out the state ω. ■

The proof of the invertibility criterion tells us how to deal with the subtlety that the ancillary density matrix ω may be expressed as a multitude of mixtures, each of which gives rise to a different Kraus representation for the map E. For an arbitrary mixture $\sum_t \, r_t \, |\phi_t\rangle\langle\phi_t| = \omega$, the resulting Kraus operators $E_t = \sqrt{r_t}\, U(\mathbb{I}_p \otimes |\phi_t\rangle)$ are not necessarily in the form from which the operator U is evident. The diagonalization of the matrix M in the proof corresponds exactly to the diagonalization of ω and this allows us to "read out" the unitary matrix, and the ancilla state ω itself.

The converse of our theorem is manifestly true, so it provides a characterization of invertible quantum operations. An alternative characterization was pointed out to us by Jon Tyson [10]. Below, we state an extension of his characterization to completely positive (CP) but not necessarily trace preserving maps, and sketch its proof.

Theorem 2.2 *A completely positive (CP) linear transformation $E : \mathrm{L}(\mathbb{C}^p) \to \mathrm{L}(\mathbb{C}^q)$ has a CP inverse D iff there exists a positive semi-definite linear operator $Q \in \mathrm{L}(\mathbb{C}^q)$ and a real number $c > 0$ such that for all density matrices $\rho, \sigma \in \mathrm{L}(\mathbb{C}^p)$,*

$$\mathrm{Tr}(Q\,E(\rho)\,Q\,E(\sigma)) \quad = \quad c \cdot \mathrm{Tr}(\rho\sigma).$$

In addition, a CPTP map E has a CPTP inverse D iff Q may be taken to be the identity operator $\mathbb{I}_q$ in the above characterization.

Proof: We first sketch a proof of the forward direction of the theorem. Suppose we have a CP map E with a CP inverse D. Express E and D in terms of some set of Kraus operators $\{A_i\}_{i\in\mathcal{I}}$ and $\{B_j\}_{j\in\mathcal{J}}$, respectively. Arguing as in the proof of Equation (2) of Theorem 2.1, we have for all $i, i' \in \mathcal{I}$,

$$A_{i'}^\dagger Q A_i \quad = \quad \beta_{i'i}\, \mathbb{I}_p, \tag{4}$$

where $Q = \sum_{j\in\mathcal{J}} B_j^\dagger B_j$ and $\beta_{i'i}$ is as in Equation (1). Note that Q is positive semi-definite. From Equation (4), it follows that $\mathrm{Tr}(Q\,E(\rho)\,Q\,E(\sigma)) = c \cdot \mathrm{Tr}(\rho\sigma)$, where $c = \sum_{i,i'\in\mathcal{I}} |\beta_{i,i'}|^2$. Note that $c > 0$ since $\sum_{i\in\mathcal{I}} \beta_{ii} = 1$ as in the proof of Theorem 2.1.

We now sketch a proof of the reverse direction of the theorem. The condition $\mathrm{Tr}(Q\,E(\rho)\,Q\,E(\sigma)) = c \cdot \mathrm{Tr}(\rho\sigma)$, with Q positive semi-definite and $c > 0$ implies that

$$\begin{aligned} c\,\mathrm{Tr}(\rho\sigma) \quad &= \quad \mathrm{Tr}(Q\,E(\rho)\,Q\,E(\sigma)) \quad = \quad \mathrm{Tr}\left(\sum_{i,i'\in\mathcal{I}} Q A_i \rho A_i^\dagger Q A_{i'} \sigma A_{i'}^\dagger\right) \\ &= \quad \mathrm{Tr}\left(\rho \sum_{i,i'\in\mathcal{I}} A_i^\dagger Q A_{i'} \sigma A_{i'}^\dagger Q A_i\right), \end{aligned}$$

for all density matrices ρ, σ. This means that $\sum_{i,i' \in \mathcal{I}} A_i^\dagger Q A_{i'} \sigma A_{i'}^\dagger Q A_i = c\,\sigma$ for all density matrices σ, since density matrices ρ form a basis for $\mathrm{L}(\mathbb{C}^p)$. This implies that the CPTP map defined by $\left\{c^{-1/2} A_i^\dagger Q A_{i'}\right\}_{i,i' \in \mathcal{I}}$ is the identity map on $\mathrm{L}(\mathbb{C}^p)$. By the unitary equivalence of Kraus operators, we see that there are complex numbers $\left\{\beta_{i,i'}\right\}_{i,i' \in \mathcal{I}}$, $\sum_{i,i'} |\beta_{i,i'}|^2 = c$ such that $A_i^\dagger Q A_{i'} = \beta_{i,i'} \mathbb{I}_p$, for all $i, i' \in \mathcal{I}$. Taking trace, we have $\beta_{i,i'} = p^{-1} \mathrm{Tr} A_i^\dagger Q A_{i'}$. The matrix $M = (\beta_{i,i'})_{i,i' \in \mathcal{I}}$ is Hermitian, and by arguing as in the proof of Theorem 2.1 we see that M is positive semi-definite. Let E' denote the CP map given by the Kraus operators $\left\{Q^{1/2} A_i\right\}_{i \in \mathcal{I}}$. Now we follow the proof of Theorem 2.1 from the argument for Equation (3) onwards to conclude that there exists a positive semi-definite matrix $\omega \in \mathrm{L}(\mathbb{C}^{\lfloor q/p \rfloor})$, and a unitary operation U on $\mathbb{C}^q$ such that $E'(\rho) = U(\rho \otimes \omega)U^\dagger$ for all density matrices ρ in $\mathrm{L}(\mathbb{C}^p)$. This shows that E has a CP inverse D which corresponds to conjugating by $U^\dagger Q^{1/2}$, and tracing out the $\lfloor q/p \rfloor$-dimensional ancilla ω.

Suppose now that CPTP map E has a CPTP inverse D. In the above argument, we get $Q = \sum_{j \in \mathcal{J}} B_j^\dagger B_j = \mathbb{I}_q$. Conversely, suppose that CPTP map E satisfies $\mathrm{Tr}(E(\rho)E(\sigma)) = c \cdot \mathrm{Tr}(\rho\sigma)$, $c > 0$ for all density matrices $\rho, \sigma \in \mathrm{L}(\mathbb{C}^p)$. The trace preserving property of E implies that the matrix M in the above argument has unit trace. This implies that the positive semi-definite matrix ω has unit trace, that is, ω is a density matrix. This shows that E has a CPTP inverse D which corresponds to applying $U^\dagger$, and tracing out the $\lfloor q/p \rfloor$-dimensional ancilla ω. ■

3 Perfect encryption of quantum states

A one-way protocol for perfect encryption of quantum states in $\mathrm{L}(\mathbb{C}^d)$ consists of a probability distribution $\{p_k, E_k\}$ over invertible quantum operations $E_k : \mathrm{L}(\mathbb{C}^d) \to \mathrm{L}(\mathbb{C}^D)$ such that the image of every state $\rho \in \mathrm{L}(\mathbb{C}^d)$ under the map

$$R(\rho) \quad = \quad \sum_k p_k \, E_k(\rho)$$

is a fixed state $\sigma \in \mathrm{L}(\mathbb{C}^D)$. This is also known as a *randomization scheme*, or a *private quantum channel*.

As mentioned in Section 1, the probability distribution $\{p_k\}$ corresponds to a random secret key that two parties Alice and Bob share. The map E_k is an encryption map that Alice applies to her quantum message ρ, and its inverse is the decryption map that Bob applies to retrieve the message. To an eavesdropper with no information about the secret key, the density matrix of the ciphertext is exactly $\sigma = R(\rho)$. Since this is completely independent of the message, the protocol achieves information theoretic security.

Our characterization theorem from the previous section implies that the most general one-way quantum encryption scheme R (with no decoding error in the absence of eavesdropping) is of the following form: for each value of key k, there is an ancilla ω_k, possibly mixed, and a unitary U_k such that $E(\rho) = \sum_k p_k \, U_k(\rho \otimes \omega_k)U_k^\dagger$. This is slightly more general than the form assumed by Ambainis, Mosca, Tapp, and de Wolf [1, Section 3], in that the ancilla may depend on the value of the key. However, their results, especially a proof that $2n$ bits of key are required to encrypt n quantum bits, extend to this form of encryption in a straightforward manner. Below we give a sketch of this extension.

We begin with the following the lemma.

Lemma 3.1 *Let $\{p_k, E_k\}$ define a perfect encryption map R for d-dimensional quantum states in $\mathrm{L}(\mathbb{C}^d)$. Then, for any two orthogonal states $|i\rangle, |j\rangle \in \mathrm{L}(\mathbb{C}^d)$, $R(|i\rangle\langle j|) = 0$.*

A simple proof of this lemma occurs in Theorem 5.2 of Ref. [5], and works verbatim for an encryption scheme as described above. We need only consider the action of R on the states $|i\rangle, |j\rangle, \frac{1}{\sqrt{2}}(|i\rangle + |j\rangle), \frac{1}{\sqrt{2}}(|i\rangle + \mathrm{i}|j\rangle)$, where $\mathrm{i} = \sqrt{-1}$, to arrive at the lemma. (A stronger version of this lemma occurs as Lemma 4.4 in Ref. [1] and also generalizes verbatim.)

An immediate corollary of Lemma 3.1 is that if one half of a bipartite Bell state is encrypted, the resulting bipartite state is independent of which Bell state was encrypted. In fact, if the encryption procedure is applied to the first half of the *any* input Bell state, the resulting state is proportional to $\sigma \otimes \mathbb{I}$ where σ the output state of the encryption procedure. Using this property, Ambainis *et al.* [5, 1] show that any protocol to encrypt n quantum bits may be transformed to a protocol that encrypts $2n$ classical bits.

Lemma 3.2 *Let $\{p_k, E_k\}$ define a perfect encryption map R for n qubit states. Then, there is a map R' given by a distribution $\{p_k, E'_k\}$ that perfectly encrypts $2n$ classical bits (i.e., a fixed basis of $\mathbb{C}^{2^{2n}}$).*

The idea behind this lemma is to encode the $2n$ bits into orthogonal Bell states over $2n$ qubits, then encrypt one half of the Bell state using R and finally send the bipartite state across as the encrypted message. The map R' is given by the composition of these steps.

Finally, we show how to extend Theorem 5.3 of Refs. [5, 1]. The proof relies on concepts from quantum information theory. We refer the reader to the two papers, and the text [8] for the required background.

Lemma 3.3 *Let $\{p_k, E_k\}$ define a perfect encryption map R for m classical bits. Then, the Shannon entropy $H(p)$ of the distribution p is at least m.*

Proof: Consider σ, the result of encrypting the basis state $|0\rangle\langle 0|$. Then, $R(|0\rangle\langle 0|) = \sigma = R(\mathbb{I}/2^m)$, since the completely mixed state may be viewed as a mixture of (classical) basis states. So

$$\begin{aligned}
\sigma &= \sum_k p_k \, E_k(|0\rangle\langle 0|) \\
&= \sum_k p_k \, U_k(|0\rangle\langle 0| \otimes \omega_k) U_k^\dagger \\
&= \sum_k p_k \, U_k \left(\frac{\mathbb{I}}{2^m} \otimes \omega_k \right) U_k^\dagger .
\end{aligned}$$

Invoking Theorem 11.10 on page 518 of Ref. [8], the von Neumann entropy of σ may be bounded above as

$$\begin{aligned}
S(\sigma) &= S\left(\sum_k p_k \, E_k(|0\rangle\langle 0|) \right) \\
&\leq H(p) + \sum_k p_k \, S(E_k(|0\rangle\langle 0|)) \\
&= H(p) + \sum_k p_k \, S(U_k(|0\rangle\langle 0| \otimes \omega_k) U_k^\dagger) \\
&= H(p) + \sum_k p_k \, S(\omega_k).
\end{aligned}$$

By concavity of von Neumann entropy, $S(\sigma)$ may also be bounded from below as

$$\begin{aligned} S(\sigma) &= S\left(\sum_k p_k\, U_k(\frac{\mathbb{I}}{2^m}\otimes\omega_k)U_k^\dagger\right) \\ &\geq \sum_k p_k\; S\left(U_k(\frac{\mathbb{I}}{2^m}\otimes\omega_k)U_k^\dagger\right) \\ &= \sum_k p_k\; S\left(\frac{\mathbb{I}}{2^m}\otimes\omega_k\right) \\ &= \sum_k p_k\; (S(\mathbb{I}/2^m)+S(\omega_k)) \\ &= m+\sum_k p_k\; S(\omega_k). \end{aligned}$$

The two bounds together give $H(p)\geq m$. ■

Lemmas 3.2 and 3.3 imply:

Theorem 3.4 *Let $\{p_k, E_k\}$ define a perfect encryption map R for n qubits. Then, the Shannon entropy $H(p)$ of the distribution p is at least $2n$.*

A weaker version of this theorem, where the encryption operations E_k are chosen to be unitary, was shown by Boykin and Roychowdhury [2]. We sketch how in this case, a lower bound of $2n$ bits for the size of key follows from a simple rank argument.

Let $\{p_k, U_k\}$ define a perfect encryption map R for n qubits for some unitary operators U_k. Note that R is a unital map; it maps the completely mixed state to itself. Therefore, the output state of R is the completely mixed state $\sigma=\frac{\mathbb{I}_{2^n}}{2^n}$. For any bipartite pure state ρ on $2n$ qubits, the rank of $(\mathbb{I}\otimes R)\rho$, where R acts on one half of ρ, is at most the number of non-zero p_k. However, from the corollary to Lemma 3.1 mentioned above, if we choose ρ to be any pure bipartite Bell state, one half of which is encrypted,

$$(\mathbb{I}\otimes R)\rho \quad = \quad \frac{\mathbb{I}_{2^n}}{2^n}\otimes\sigma \quad = \quad \frac{\mathbb{I}_{2^{2n}}}{2^{2n}},$$

which has rank 2^{2n}. Thus, the support of the probability distribution of the secret key has size at least 2^{2n}, which gives the claimed lower bound. Note that this does not imply the stronger claim of Theorem 3.4 that the entropy of the distribution is $2n$, or the stronger characterization of optimal perfect encryption schemes (without ancilla) due to Boykin and Roychowdhury [2, Section III].

References

[1] Andris Ambainis, Michele Mosca, Alain Tapp, and Ronald de Wolf. Private quantum channels. In *Proceedings of the 41st Annual Symposium on Foundations of Computer Science*, pages 547–553. IEEE Press, Los Alamitos, CA, USA, 2000.

[2] P. Oscar Boykin and Vwani Roychowdhury. Optimal encryption of quantum bits. *Physical Review A*, 67, 2003. Article no. 042317.

[3] David P. DiVincenzo, Patrick Hayden, and Barbara M. Terhal. Hiding quantum data. *Foundations of Physics*, 33(11):1629–1647, 2003. David Mermin Festschrift. Also Technical Report quant-ph/0207147, ArXiv.org Preprint Archive, `http://www.arxiv.org/abs/quant-ph/`, July 2002.

[4] Rahul Jain. Resource requirements of private quantum channels. Pre-print quant-ph/0507075, ArXiv.org e-print Archive, http://www.arxiv.org/abs/quant-ph, July 2005.

[5] Michele Mosca, Alain Tapp, and Ronald de Wolf. Private quantum channels and the cost of randomizing quantum information. Pre-print quant-ph/0003101, ArXiv.org e-Print Archive, http://www.arxiv.org/abs/quant-ph, March 2000.

[6] Michael A. Nielsen and Carlton M. Caves. Reversible quantum operations and their application to teleportation. *Physical Review A*, 55(3):2547–2556, 1997.

[7] Michael A. Nielsen, Carlton M. Caves, Benjamin Schumacher, and Howard Barnum. Information-theoretic approach to quantum error correction and reversible measurement. *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 454(1969):277–304, 1998.

[8] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, UK, 2000.

[9] John Preskill. Quantum computation. Lecture Notes, available at `http://www.theory.caltech.edu/people/preskill/ph229/`, California Institute of Technology, Pasadena, CA, 1998.

[10] Jon Tyson. Personal communication, May 2006.

[11] Wim van Dam, Frédéric Magniez, Michele Mosca, and Miklos Santha. Self-testing of universal and fault-tolerant sets of quantum gates. In *Proceedings of 32nd ACM Symposium on Theory of Computing*, pages 688–696. ACM Press, New York, NY, USA, 2000.