J. Cryptol. (2012) 25: 1–13
DOI: 10.1007/s00145-010-9076-8

Journal of
CRYPTOLOGY

Resource Requirements of Private Quantum Channels and Consequences for Oblivious Remote State Preparation*

Rahul Jain
Centre for Quantum Technologies and Department of Computer Science, National University of Singapore, Kent Ridge, Singapore
rahul@comp.nus.edu.sg

Communicated by Stefan Wolf

Received 30 March 2006
Online publication 2 October 2010

Abstract. Shannon (Bell Syst. Tech. J. 27:623–656, 1948; Bell Syst. Tech. J. 28:656–715, 1949) in celebrated work had shown that n bits of shared key are necessary and sufficient to transmit n-bit classical information in an information-theoretically secure way, using one-way communication. Ambainis, Mosca, Tapp and de Wolf in (Proceedings of the 41st Annual IEEE Symposium on Foundation of Computer Science, pp. 547–553, 2000) considered a more general setting, referred to as *private quantum channels*, in which instead of classical information, quantum states are required to be transmitted and only one-way communication is allowed. They show that in this case $2n$ bits of shared key is necessary and sufficient to transmit an n-qubit state. We consider the most general setting in which we allow for all possible combinations, in one-way communication, i.e. we let the input to be transmitted, the message sent and the shared resources to be classical/quantum. We develop a general framework by which we are able to show simultaneously tight bounds on communication/shared resources in all of these cases and this includes the results of Shannon and Ambainis et al.

As a consequence of our arguments we also show that in a one-way *oblivious remote state preparation* protocol for transferring an n-qubit pure state, the entropy of the communication must be $2n$ and the *entanglement measure* of the shared resource must be n. This generalizes the result of Leung and Shor (Phys. Rev. Lett. 90, 2003) which shows the same bound on the length of communication in the special case when the shared resource is *maximally entangled*, e.g. EPR pairs, and hence settles an open question asked in their paper regarding protocols without maximally entangled shared resource.

Key words. Privacy, Quantum channels, Entropy, Strong sub-additivity, Remote state preparation, Substate theorem.

* This work was conducted at University of California at Berkeley, USA where it was supported by an Army Research Office (ARO), North California, grant number DAAD 19-03-1-00082.

1. Introduction

Suppose Alice is required to transmit an n-bit input string to Bob in an *information-theoretically secure* way, i.e. without leaking *any information* about her input to an eavesdropper Eve who has complete access to the channel between her and Bob. Shannon in [12,13] had shown that using n bits of shared key and by using *one-time pad* scheme Alice and Bob can accomplish this. He further showed that n bits of shared key are also required by any other scheme which accomplishes the same using one-way communication. Later Maurer [10] extended this result to show that n bits of key are required even if two-way communication is allowed between Alice and Bob. Ambainis, Mosca, Tapp and de Wolf [1] considered a generalization of this question in which instead of classical input, Alice has quantum input and only one-way of quantum communication between Alice to Bob is allowed. They referred to this setting as a private quantum channel (PQCs). They showed that in this case the requirement of shared key increases. Their main result was:

Theorem 1.1. *$2n$ bits of shared key are necessary and sufficient to transmit any n-qubit quantum state in an information-theoretically secure way.*

We further generalize the setting by letting the shared resource between Alice and Bob to be quantum. A natural generalization of classical shared keys in the context of quantum communication protocols is a *pure* quantum state $|\psi\rangle^{AB}$ shared between Alice and Bob. This is referred to as *shared entanglement* or simply entanglement. We consider private quantum channels that use entanglement between Alice and Bob to achieve security, and in order to distinguish them from PQCs which use classical shared keys, we call them PQCEs (the added E stands for entanglement). We formally define a PQCE as follows.

Definition 1.2. Let T be a subset of pure n-qubit states. Let $|\psi\rangle^{AB}$ be a bipartite pure state shared between Alice and Bob and let ρ be a quantum state.

1. *Alice's operations:* Alice gets an input pure state $|\phi\rangle \in T$. Alice's operation consists of attaching a few ancilla qubits in the state $|0\rangle$ to her input and her part of the bipartite state $|\psi\rangle^{AB}$. She then performs a unitary transformation on the combined quantum system of all her qubits and sends a subset of the resulting qubits to Bob. Let $\mathcal{A}$ represent Alice's operations. For the input $|\phi\rangle$, let $\mathcal{E}(|\phi\rangle)$ represent the (encoded) quantum state of the qubits sent to Bob. We have the following *security requirement* that $\forall |\phi\rangle \in T, \mathcal{E}(|\phi\rangle) = \rho$.
2. *Bob's operations:* Bob on receiving the quantum message from Alice attaches a few ancilla qubits in the state $|0\rangle$ to the combined system of the received message and his part of the bipartite state $|\psi\rangle^{AB}$. He then performs a unitary transformation on the combined system of all her qubits and outputs a subset of the resulting qubits. Let $\mathcal{B}$ represent Bob's operations. Let for input state $|\phi\rangle$ to Alice the final (decoded) output of Bob be represented by $\mathcal{D}(|\phi\rangle)$. We have the following *correctness requirement:* $\forall |\phi\rangle \in T, \mathcal{D}(|\phi\rangle) = |\phi\rangle\langle\phi|$.

   Then $[T, \mathcal{A}, \mathcal{B}, |\psi\rangle^{AB}, \rho]$ is called a private quantum channel with entanglement (PQCE).

Remarks.

1. From our description, the mapping $\mathcal{E} : |\phi\rangle \mapsto \mathcal{E}(|\phi\rangle)$ (and extended by linearity to mixed states) from Alice's input to her message forms a *quantum operation* (see Sect. 2 for definition) since it is a composition of quantum operations, like attaching a fixed ancilla, performing unitary transformation and tracing out a subsystem.
2. In the above definition of a PQCE, if we replace the bipartite shared pure state $|\psi\rangle^{AB}$ with shared random strings between Alice and Bob, we get a PQC. We represent a PQC by $[T, \mathcal{A}, \mathcal{B}, P, \rho]$, where P is the distribution of the shared random strings between Alice and Bob.
3. In [1] the authors made a comment that in the case of PQC's, without loss of generality, Alice's operations can be thought of as the following. On receiving the input she attaches a fixed mixed state ancilla ρ to it, applies a unitary U_i depending on the shared random string i on the combined system of the input and the ancilla and sends the resulting qubits to Bob. Please note that we do not make such an assumption here which in any case does not apply for PQCE's. Also it is clear from the above definition that for both PQC's and PQCE's, the operations of Alice and Bob are as general as possible.
4. It is easily seen that a PQCE/PQC for T is also PQCE/PQC respectively for $\tilde{T}$ which is the closure of T under convex combinations.
5. PQCEs were also considered by Leung [6] by the name of *Quantum Vernam Cipher* who considered issues like security of key recycling and reliability of message transfer. In this paper we are primarily concerned with bounds on communication and entanglement requirements of PQCEs.

We consider the following measures of our various resources.

Definition 1.3.

1. *Measure of communication:* For a PQC $[T, \mathcal{A}, \mathcal{B}, P, \rho]$ and a PQCE $[T, \mathcal{A}, \mathcal{B}, |\psi\rangle^{AB}, \rho]$, we let the measure of communication to be $S(\rho)$, the von Neumann entropy of ρ (please refer to the next section for definition). When we say that it requires 'n (qu)bits of communication' we mean $S(\rho) = n$.
2. *Measure of entanglement:* For a bipartite pure state $|\psi\rangle^{AB}$, consider its *Schmidt decomposition*, $|\psi\rangle^{AB} = \sum_{i=1}^{k} \sqrt{\lambda_i}|a_i\rangle \otimes |b_i\rangle$, where $\{|a_i\rangle\}$ is an orthonormal set and so is $\{|b_i\rangle\}$, $\lambda_i \geq 0$ and $\sum_i \lambda_i = 1$. The measure of entanglement of $|\psi\rangle^{AB}$ is defined to be $E(|\psi\rangle^{AB}) \stackrel{\text{def}}{=} -\sum_i \lambda_i \log \lambda_i$. For a PQCE $[T, \mathcal{A}, \mathcal{B}, |\psi\rangle^{AB}, \rho]$, we let the measure of entanglement to be $E(|\psi\rangle^{AB})$. When we say that it requires n ebits of entanglement we mean $E(|\psi\rangle^{AB}) = n$.
3. *Measure of shared randomness:* For a PQC $[T, \mathcal{A}, \mathcal{B}, P, \rho]$, we let the measure of shared randomness be $S(P)$. When we say that it requires n bits of shared randomness we mean $S(P) = n$.

We consider all possible cases i.e. when the input to Alice, the message sent by Alice and the shared resource between Alice and Bob is either classical or quantum. We develop a general argument by which we are able to show tight bounds simultaneously on

communication and shared resource usage in all the above cases. Following is a compilation of all the results we obtain due to our analysis. Below when we say the 'x, y, z' case (e.g. classical, quantum, classical case) we mean, Alice gets n-(qu)bits of x input, the communication is y and the shared resource is z.

Theorem 1.4.

1. *In the classical, classical, classical case, n bits of communication and n bits of shared key is required. The one-time pad scheme hence is simultaneously optimal in both communication and shared key usage. This is basically Shannon's result* [12,13].
2. *In the classical, quantum, classical case, n qubits of communication and n bits of shared key is required. Hence here again the one-time pad scheme is simultaneously optimal in both communication and shared key usage.*
3. *In the classical, classical, quantum case, n bits of communication and n ebits of entanglement is required. Hence here again the one-time pad scheme is simultaneously optimal in both communication and shared resource usage.*
4. *In the classical, quantum, quantum case, $n/2$ qubits of communication and $n/2$ ebits of entanglement is required. The simultaneously optimal upper bound here is achieved by the standard protocol for* super-dense coding [3,11] *which is a* PQCE. *In it, Alice transfers n bits of classical input in an information-theoretically secure manner to Bob using $n/2$ qubits of communication and $n/2$* EPR *pairs* [11] *shared between them. In this case the message of Alice is always in the maximally mixed state independent of her input.*
5. *The quantum, classical, classical case is impossible.*
6. *In the quantum, quantum, classical case, n qubits of communication and $2n$ bits of shared key is required. This is the main result of Ambainis et al.* [1]. *In the same paper they have exhibited a* PQC *which transfers an n-qubit state with n qubits of communication and $2n$ bits of shared randomness and is therefore simultaneously optimal in both communication and shared randomness.*
7. *In the quantum, classical, quantum case, $2n$ bits of communication and n ebits of entanglement are required. Here the simultaneously optimal scheme is the standard protocol for* teleportation [2,11] *which is a* PQCE. *In this protocol Alice can transfer n qubits to Bob in an information-theoretically secure way by using $2n$ bits of communication and using n* EPR *pairs between them. In this case the message of Alice always has uniform distribution independent of her input.*
8. *In the quantum, quantum, quantum case, n qubits of communication and n ebits of entanglement is required. In this case simultaneously optimal upper bound is achieved by a scheme using $(2, 3)$ quantum secret sharing scheme by Cleve, Gottesman and Lo* [4]. (*This scheme was pointed out to us by Gottesman.*)

Remarks.

1. Many of the protocols mentioned above like teleportation, super-dense coding, $(2, 3)$ quantum secret sharing scheme etc. are known to be optimal with respect to different resources like communication, entanglement usage etc. However, these optimality proofs can not be lifted in our setting in a straightforward manner since privacy is often not a consideration in these settings.

2. We only consider perfect privacy in this work. It is known that if perfect privacy is not required then many of the resource requirements can be reduced in different settings. However considering imperfect privacy is beyond the scope of this work.

Consequence for Remote State Preparation We also present a consequence of our results for one-way, oblivious, remote state preparation (RSP) protocols. In an RSP protocol between Alice and Bob, Alice is required to transport a known quantum state $|\phi\rangle$ of n-qubits to Bob using classical communication and some shared entanglement. An RSP is called oblivious if at the end of the protocol, Bob gets a copy of Alice's input $|\phi\rangle$ and rest of his qubits are independent of $|\phi\rangle$. Leung and Shor [9] have shown that for one-way oblivious RSPs, if Alice and Bob start with a maximally entangled state then the worst case communication required by them is $2n$. We generalize on their result to provide bounds for all one-way oblivious RSP protocols independent of which shared pure state they start with.

Theorem 1.5. *For any one-way oblivious RSP protocol, the entropy of communication is at least $2n$ and the entanglement measure of the shared pure state is at least n. Therefore teleportation achieves both these bounds simultaneously.*

Two-Way Channels Finally we discuss two-way multiple round PQCs (MPQCs) and PQCEs (MPQCEs). We show that an MPQC which can transfer an n-qubit state must use n-bits of classical shared keys. Also an MPQCE which can transfer an n-qubit state must use $\Omega(n)$ ebits of entanglement. Hence there is not much saving even when multiple rounds are allowed.

Organization of the Paper In the next section we make a few definitions and state a few facts which we will be using later in our proofs. In Sect. 3 we present the proofs of all the parts of Theorem 1.4. In Sect. 3.1 we prove our result, Theorem 1.5, for one-way oblivious RSPs. In Sect. 4 we discuss two-way multiple round private quantum channels and conclude with some open questions.

2. Preliminaries

Let $\mathcal{H}_k$ represent the Hilbert space of dimension k. Let $\mathcal{C}_k$ represent the set of quantum states corresponding to the standard basis of $\mathcal{H}_k$, also referred to as the *classical states*. Let I_k represent the identity transformation in a k dimensional space. For an operator A let $A \geq 0$ represent that A is a positive semi-definite operator. By a quantum operation we mean a linear, completely positive, trace-preserving operation. Let $\mathcal{H}, \mathcal{K}$ be Hilbert spaces. For a state $\rho \in \mathcal{K}$, we call a pure state $|\phi\rangle \in \mathcal{H} \otimes \mathcal{K}$, a *purification* of ρ if $\mathrm{Tr}_{\mathcal{H}}|\phi\rangle\langle\phi| = \rho$. Vectors $|\phi\rangle, |\psi\rangle$ etc. represent pure states for us. Let us represent the four *Pauli operators* in the standard basis as $\sigma_0 \stackrel{\text{def}}{=} \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \sigma_1 \stackrel{\text{def}}{=} \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right), \sigma_2 \stackrel{\text{def}}{=} \left(\begin{smallmatrix} 0 & i \\ -i & 0 \end{smallmatrix}\right), \sigma_3 \stackrel{\text{def}}{=} \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. Let us identify a state in $\mathcal{C}_{2^{2n}}$ as a string $x (\stackrel{\text{def}}{=} x_1 x_2 \ldots x_n) \in \{0, 1, 2, 3\}^n$ in the natural way by pairing up the bits from left to right. Let $\sigma_x \stackrel{\text{def}}{=} \sigma_{x_1} \otimes \sigma_{x_2} \otimes \cdots \otimes \sigma_{x_n}$. Let an EPR pair mean the state $|\mathrm{EPR}\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. For $s \in \{0, 1, 2, 3\}$, the states

$(\sigma_s \otimes I)|\mathsf{EPR}\rangle$ are referred to as the four *Bell states*. Please note that all the four Bell states are orthogonal to each other.

For a quantum state ρ with eigenvalues λ_i its *von Neumann entropy* is defined as $S(\rho) \stackrel{\text{def}}{=} -\sum_i \lambda_i \log \lambda_i$. Given a joint quantum system AB, the mutual information between them is defined as $I(A:B) \stackrel{\text{def}}{=} S(A) + S(B) - S(AB)$. Relative entropy between two states ρ and σ is defined as $S(\rho|\sigma) \stackrel{\text{def}}{=} \mathsf{Tr}\rho(\log \rho - \log \sigma)$. We require the following properties of von Neumann entropy, relative entropy and mutual information. Please refer to [11] for a good introduction to quantum information theory.

Fact 2.1.

1. $S(A) + S(B) - S(AB) \geq 0$. *This is called a sub-additivity property of von Neumann entropy. This implies* $I(A:B) \geq 0$.
2. $S(ABC) + S(A) \leq S(AB) + S(AC)$. *This is called the strong sub-additivity property. This implies* $I(\mathcal{E}(A):B) \leq I(A:B)$, *where* $\mathcal{E}$ *is a quantum operation.*
3. *We have the following chain rule of mutual information,* $I(A:BC) = I(A:B) + I(AB:C) - I(B:C)$, *which follows easily from definition.*
4. $S(AB) \geq |S(A) - S(B)|$. *This is called the* Araki–Lieb *inequality.*
5. *Given a bipartite system* ρ^{AB}, $I(A:B) = S(\rho^{AB}|\rho^A \otimes \rho^B)$, *where* ρ^A, ρ^B *are the states of the systems A and B respectively.*
6. *Given a joint system AB with A being a classical system,* $S(AB) \geq \max\{S(A), S(B)\}$.

We will need the following theorem.

Theorem 2.2 (Local Transition Theorem [6–8]). *Let* $\mathcal{K}, \mathcal{H}$ *be Hilbert spaces. Let* ρ *be a quantum state in* $\mathcal{K}$. *Let* $|\phi_1\rangle$ *and* $|\phi_2\rangle$ *be two purification of* ρ *in* $\mathcal{H} \otimes \mathcal{K}$. *Then there is a local unitary transformation U acting on* $\mathcal{H}$ *such that* $(U \otimes I)|\phi_1\rangle = |\phi_2\rangle$.

We will also need the following *substate theorem* from [5].

Fact 2.3. *Let* ρ, σ *be quantum state. If* $S(\rho|\sigma) \leq k$ *then,*

$$\sigma - \frac{\rho'}{2^{O(k)}} \geq 0$$

where $\mathsf{Tr}|\rho' - \rho| \leq 0.1$.

3. Resource Bounds

We first derive a few lemmas which will finally lead us to our results. In [1] it is shown that a PQC which can transmit n-qubit quantum states can be converted into a PQC which uses the same amount of shared classical randomness to transmit any $2n$ bit classical state. We show a similar thing for PQCE's. The following lemma states the same.

Lemma 3.1. *If there exists a* PQCE, $[\mathcal{H}_{2^n}, \mathcal{A}, \mathcal{B}, |\psi^{AB}\rangle, \rho]$ *then there exists a* PQCE, $[\mathcal{C}_{2^{2n}}, \mathcal{A}', \mathcal{B}', |\psi^{AB}\rangle, I_{2^n} \otimes \rho]$ *which uses the same bipartite state as the shared entanglement between Alice and Bob and uses an extra n qubits of communication.*

In order to prove this lemma we first prove here another lemma which is very similar to a lemma from [1].

Lemma 3.2. *Let $\mathcal{H}, \mathcal{K}$ be Hilbert spaces. Let $\mathcal{E}$ be a quantum operation acting on $\mathcal{H}$ such that $\forall|\phi\rangle \in \mathcal{H}, \mathcal{E}(|\phi\rangle\langle\phi|) = \rho$. Let $|\phi_1\rangle, |\phi_2\rangle \in \mathcal{H}$ be two orthogonal states, then $\mathcal{E}(|\phi_1\rangle\langle\phi_2|) = \mathcal{E}(|\phi_2\rangle\langle\phi_1|) = 0$.*

Proof. We note the following:

$$\rho = \mathcal{E}\big(|\phi_1\rangle\langle\phi_1|\big) = \mathcal{E}\big(|\phi_2\rangle\langle\phi_2|\big), \tag{1}$$

$$\rho = \mathcal{E}\left(\frac{1}{2}\big(|\phi_1\rangle + |\phi_2\rangle\big)\big(\langle\phi_1| + \langle\phi_2|\big)\right), \tag{2}$$

$$\rho = \mathcal{E}\left(\frac{1}{2}\big(|\phi_1\rangle + i|\phi_2\rangle\big)\big(\langle\phi_1| - i\langle\phi_2|\big)\right). \tag{3}$$

Now (1) and (2) imply $\mathcal{E}(|\phi_1\rangle\langle\phi_2|) + \mathcal{E}(|\phi_2\rangle\langle\phi_1|) = 0$ and (1) and (3) imply $\mathcal{E}(|\phi_1\rangle\langle\phi_2|) - \mathcal{E}(|\phi_2\rangle\langle\phi_1|) = 0$. Together the two imply $\mathcal{E}(|\phi_1\rangle\langle\phi_2|) = \mathcal{E}(|\phi_2\rangle\langle\phi_1|) = 0$. □

We get the following corollary of the above lemma:

Corollary 3.3. *Let $\mathcal{H}, \mathcal{K}$ be Hilbert spaces. Let $\mathcal{E}$ be a quantum operation acting on $\mathcal{H}$ such that $\forall|\phi\rangle \in \mathcal{H}, \mathcal{E}(|\phi\rangle\langle\phi|) = \rho$. Then $\forall|\psi\rangle \in \mathcal{K} \otimes \mathcal{H}$, $(I \otimes \mathcal{E})(|\psi\rangle\langle\psi|) = (\mathrm{Tr}_{\mathcal{H}}|\psi\rangle\langle\psi|) \otimes \rho$. This also means that for all mixed states $\sigma \in \mathcal{K} \otimes \mathcal{H}$, $(I \otimes \mathcal{E})(\sigma) = (\mathrm{Tr}_{\mathcal{H}}\sigma) \otimes \rho$.*

Proof. Let $|\psi\rangle = \sum_i \sqrt{\lambda_i}|a_i\rangle \otimes |b_i\rangle$, be as written in the Schmidt decomposition form. Then,

$$\begin{aligned}
(I \otimes \mathcal{E})\big(|\psi\rangle\langle\psi|\big) &= (I \otimes \mathcal{E})\left(\sum_i \sqrt{\lambda_i}|a_i\rangle \otimes |b_i\rangle\right)\left(\sum_j \sqrt{\lambda_j}\langle a_j| \otimes \langle b_j|\right) \\
&= \sum_{i,j} (I \otimes \mathcal{E})\sqrt{\lambda_i}\sqrt{\lambda_j}|a_i\rangle\langle a_j| \otimes |b_i\rangle\langle b_j| \\
&= \sum_{i,j} \sqrt{\lambda_i}\sqrt{\lambda_j}|a_i\rangle\langle a_j| \otimes \mathcal{E}\big(|b_i\rangle\langle b_j|\big) \\
&= \sum_i \lambda_i |a_i\rangle\langle a_i| \otimes \mathcal{E}\big(|b_i\rangle\langle b_i|\big) \quad \text{(from Lemma 3.2)} \\
&= \left(\sum_i \lambda_i |a_i\rangle\langle a_i|\right) \otimes \rho \\
&= \mathrm{Tr}_{\mathcal{H}}|\psi\rangle\langle\psi| \otimes \rho.
\end{aligned}$$

□

We are now ready to prove Lemma 3.1.

Proof of Lemma 3.1. In the PQCE, $[\mathcal{C}_{2^{2n}}, \mathcal{A}', \mathcal{B}', |\psi^{AB}\rangle, I_{2^n} \otimes \rho]$, let $x \in \{0,1,2,3\}^n$ correspond to the input state. Alice prepares n EPR pairs and applies the unitary σ_x on combined system of the first qubits of each pair. She then encrypts the combined system of the second qubits of each pair using $\mathcal{E}$, the encryption operation of the PQCE, $[\mathcal{H}_{2^n}, \mathcal{A}, \mathcal{B}, |\psi^{AB}\rangle, \rho]$. She now sends all the resulting qubits to Bob. From above corollary, we can see that the state of the message of this new PQCE will be $I_{2^n} \otimes \rho$ for all inputs in $\mathcal{C}_{2^{2n}}$. The decryption operation $\mathcal{B}'$ of Bob now corresponds to first decrypting the second half of the received qubits using $\mathcal{B}$ and then recovering the input classical state by making measurements on the n Bell states. □

Below we show a similar lemma which implies that a PQC/PQCE which transmits any n-qubit quantum state can be converted into a PQCE which uses the same communication and an extra n ebits of entanglement to transmit any $2n$ bit classical state. We show the proof for PQCEs and a similar proof holds for PQCs as well.

Lemma 3.4. *If there exists a* PQCE, $[\mathcal{H}_{2^n}, \mathcal{A}, \mathcal{B}, |\psi^{AB}\rangle, \rho]$ *then there exists a* PQCE, $[\mathcal{C}_{2^{2n}}, \mathcal{A}', \mathcal{B}', |\psi^{AB}\rangle \otimes (\frac{|00\rangle+|11\rangle}{\sqrt{2}})^{\otimes n}, \rho]$ *which uses the same communication and an extra n* EPR *pairs.*

Proof. In $[\mathcal{C}_{2^{2n}}, \mathcal{A}', \mathcal{B}', |\psi^{AB}\rangle \otimes (\frac{|00\rangle+|11\rangle}{\sqrt{2}})^{\otimes n}, \rho]$, let $x \in \{0,1,2,3\}^n$ correspond to the input state. Alice applies σ_x to her part of the extra n-EPR pairs, encodes them using the encoding procedure of the earlier PQCE $[\mathcal{H}_{2^n}, \mathcal{A}, \mathcal{B}, |\psi^{AB}\rangle, \rho]$, and sends the resulting qubits to Bob. The security property of $[\mathcal{H}_{2^n}, \mathcal{A}, \mathcal{B}, |\psi^{AB}\rangle, \rho]$ implies the security property of $[\mathcal{C}_{2^{2n}}, \mathcal{A}', \mathcal{B}', |\psi^{AB}\rangle \otimes (\frac{|00\rangle+|11\rangle}{\sqrt{2}})^{\otimes n}, \rho]$. On receiving Alice's message, Bob first applies the decoding procedure of $[\mathcal{H}_{2^n}, \mathcal{A}, \mathcal{B}, |\psi^{AB}\rangle, \rho]$, and recovers x by making measurements on the n Bell states. □

We will need the following lemma. Although parts of this lemma can be found in standard texts, we state and prove all parts here for completeness.

Lemma 3.5. *Let ABX be a tripartite system. Then,*

1. $S(AX) + S(BX) - S(ABX) - S(X) \leq \min\{2S(A), 2S(B)\}$.
2. *If AX is a classical system then we have the stronger inequality* $S(AX) + S(BX) - S(ABX) - S(X) \leq \min\{S(A), S(B)\}$.
3. $I(A:B) \leq \min\{2S(A), 2S(B)\}$.

Proof.

1. $$\begin{aligned} S(AX) - S(ABX) + S(BX) - S(X) &\leq S(AX) - S(ABX) + S(B) \\ &\leq S(B) + S(B) = 2S(B). \end{aligned}$$

Above, the first inequality comes from part (1) and second inequality comes from part (4) of Fact 2.1. Similarly we get $S(AX) + S(BX) - S(ABX) - S(X) \leq 2S(A)$.

2. $S(AX) - S(ABX) + S(BX) - S(X) \leq S(BX) - S(X) \leq S(B)$.

Above, the first inequality arises from part (6), since AX is a classical system, and the second inequality comes from part (1) of Fact 2.1. Again, since A is a classical system, we get

$$S(AX) - S(X) + S(BX) - S(ABX) \leq S(AX) - S(X) \leq S(A).$$

Above, the first inequality comes from part (6) and the second inequality comes from part (1) of Fact 2.1.

3. $I(A:B) = S(A) + S(B) - S(AB) \leq S(A) + S(A) = 2S(A)$.

The inequality above follows from part (4) of Fact 2.1. Similarly $I(A:B) \leq 2S(B)$. □

We now have the following theorem.

Theorem 3.6. *If* $[\mathcal{C}_{2^n}, \mathcal{A}, \mathcal{B}, |\psi^{AB}\rangle, \rho]$ *is a* PQCE *then,*

1. $S(\sigma^B) \geq n/2$, *where* σ^B *is the quantum state corresponding to Bob's part of* $|\psi^{AB}\rangle$. *We note from definitions that* $S(\sigma^B) = E(|\psi\rangle^{AB})$.
2. $S(\rho) \geq n/2$.

Proof. Let X be a random variable which takes values in $\{1, 2, \ldots, 2^n\}$ uniformly. Suppose Alice is able to communicate X to Bob through the PQCE. We can assume that the operations of Alice are *safe* on X which means that at the beginning Alice makes a copy of X (since it is a classical state) and then her subsequent operations do not touch the original copy of X. Let M_1 be the quantum state corresponding to the message of Alice and let M_2 be the quantum state corresponding to Bob's part of $|\psi\rangle^{AB}$. Then from Fact 2.1,

$$\begin{aligned}
n = H(X) &= I\big(\mathcal{D}(X) : X\big) = I\big(\mathcal{B}\big(M_1M_2 \otimes |0\rangle\langle 0|_{\text{ancilla}}\big) : X\big) \\
&\leq I\big(M_1M_2 \otimes |0\rangle\langle 0|_{\text{ancilla}} : X\big) = I(M_1M_2 : X) \\
&= I(M_1 : X) + I(M_2 : M_1X) - I(M_1 : M_2) \\
&= I(M_1 : X) + I(M_2 : X) + I(M_2X : M_1) - I(M_1 : X) - I(M_1 : M_2) \\
&\leq 0 + 0 + I(M_2X : M_1) - I(M_1 : X) \\
&= S(M_2X) + S(M_1X) - S(M_1M_2X) - S(X) \\
&\leq \min\big\{2S(M_2), 2S(M_1)\big\}.
\end{aligned}$$

Above, the first inequality comes from part (2) of Fact 2.1. $I(M_1 : X) = 0$ because of the privacy property of the channel. $I(M_2 : X) = 0$ because they were independent to

begin with and Alice's operations are safe on X. The last inequality follows from part (1) of Lemma 3.5. □

We note in the proof of Theorem 3.6, due to part (2) of Lemma 3.5, that if either M_2 is a classical system (as in a PQC) or if M_1 is a classical system (when the message is classical), then we get $n \leq \min\{S(M_2), S(M_1)\}$. Therefore we have the following corollary:

Corollary 3.7.

1. *If* $[\mathcal{C}_{2^n}, \mathcal{A}, \mathcal{B}, P, \rho]$ *is a* PQC *then,* $S(P) \geq n$ *and* $S(\rho) \geq n$.
2. *If* $[\mathcal{C}_{2^n}, \mathcal{A}, \mathcal{B}, |\psi^{AB}\rangle, P]$ *is a* PQCE *with classical communication then,* $S(\sigma) \geq n$, *where* σ *is Bob's part of* $|\psi^{AB}\rangle$, *and* $S(P) \geq n$.

We are now set to show various parts of Theorem 1.4.

Proof of Theorem 1.4. 1. Follows from part (1) of Corollary 3.7.
2. Follows from part (1) of Corollary 3.7.
3. Follows from part (2) of Corollary 3.7.
4. Follows from Theorem 3.6.
5. Easy to see.
6. From PQC $[\mathcal{H}_{2^n}, \mathcal{A}, \mathcal{B}, P, \rho]$, using Lemma 3.1 we get a PQC $[\mathcal{C}_{2^{2n}}, \mathcal{A}', \mathcal{B}', P, I_{2^n} \otimes \rho]$. Part (1) of Corollary 3.7 now implies $S(P) \geq 2n$. The lower bound on communication follows from the fact that a PQC for $\mathcal{H}_{2^n}$ is also a PQC for $\mathcal{C}_{2^n}$ and Part (1) of Corollary 3.7.
7. The lower bound on communication follows from Lemma 3.4 and Part (2) of Corollary 3.7. The lower bound on entanglement follows from the fact that a PQCE for $\mathcal{H}_{2^n}$ is also a PQCE for $\mathcal{C}_{2^n}$ and Part (2) Corollary 3.7.
8. From $[\mathcal{H}_{2^n}, \mathcal{A}, \mathcal{B}, |\psi^{AB}\rangle, \rho]$ using Lemma 3.1 we get a PQCE $[\mathcal{C}_{2^{2n}}, \mathcal{A}', \mathcal{B}', |\psi^{AB}\rangle, I_{2^n} \otimes \rho]$. Theorem 3.6 now implies $E(|\psi^{AB}\rangle) \geq n$. Similarly the lower bound on communication follows from the Lemma 3.4 and Theorem 3.6. □

3.1. *Consequence for One-Way Oblivious Remote State Preparation Problem*

In a remote state preparation (RSP) protocol between Alice and Bob, Alice wants to transport a known n-qubit pure state $|\phi\rangle$ to Bob using classical communication and shared prior entanglement. Such a protocol is called oblivious if at the end of the protocol, Bob gets a single copy of Alice's input $|\phi\rangle$ and other than that all his qubits are independent of $|\phi\rangle$.

Proof of Theorem 1.5. Let us consider an oblivious RSP protocol. Let Alice want to transmit an n-qubit state $|\phi\rangle$ to Bob. Let ρ be Bob's part of the initial pure state shared between Alice and Bob. Let the state of the shared part of the entanglement on Bob's side after receiving message m to be $\rho_m^{|\phi\rangle}$. Since the protocol is oblivious, the probability with which a particular message m comes to Bob is independent of $|\phi\rangle$, which we denote by p_m. Therefore we note $\sum_m p_m \rho_m^{|\phi\rangle} = \rho$ for all $|\phi\rangle$, since the entanglement part of Bob's qubits has not changed due to Alice's operations.

Bob on receiving message m attaches ancilla $|0\rangle$ to his qubits and performs unitary U_m to them. Again since the protocol is oblivious, his state at the end of the unitary is $|\phi\rangle\langle\phi| \otimes \sigma_m$, where σ_m is independent of $|\phi\rangle$. Using these properties we now construct a PQC between Alice and Bob. Let Alice and Bob share classical randomness between them in which m is appears with probability p_m. Conditioned on the shared string being m, Alice attaches σ_m to $|\phi\rangle\langle\phi|$, applies $U_m^\dagger$ and sends the resulting state $\rho_m^{|\phi\rangle} \otimes |0\rangle\langle 0|$ to Bob. Now since $\sum_m p_m \rho_m^{|\phi\rangle} = \rho$ for all $|\phi\rangle$, Alice's message is independent of $|\phi\rangle$ and hence the privacy requirement is satisfied. Bob on receiving the quantum message applies U_m to it and discards σ_m. Therefore now from part 6 of Result 1.4 we get $S(\rho) \geq n$ and $S(P) \geq 2n$, where P is the distribution $\{p_m\}$. □

Remark. To the best of our knowledge, the reduction we present here from oblivious remote state preparation to private quantum channels is original and has not appeared in any previous works.

4. Multiple Round Private Quantum Channels

When we consider two-way multiple round PQCs, denoted MPQC, or multiple round PQCEs, denoted MPQCE, we note that keeping the privacy of *individual messages* cannot be the only criteria. For example let us consider a protocol in which in the first message Alice transfers EPR pairs followed by a junk message of Bob and then Alice transfers her quantum state privately using the earlier sent EPR pairs. In this protocol none of the individual messages give any information about the transferred state but it does not mean that Eve, who can access the channel in all rounds, cannot get any information about the transferred state. If all the messages are classical, the entire message transcript can be considered together for security requirement. However if some of the messages are quantum, then all of the messages cannot even be considered together. Therefore, we consider following security criterion for MPQC/MPQCE with n-bit (uniformly distributed) classical input: the probability with which an interfering Eve should be able to guess the input of Alice is at most 2^{-n}.

Below we discuss the resource requirements of MPQCs and MPQCEs with classical inputs.

Lemma 4.1. *Let P be the distribution of the shared random strings between Alice and Bob in an* MPQC *for $\mathcal{C}_{2^n}$. Then $S(P) \geq n$.*

Proof. Let s be a string which has highest probability according to P, say p. Consider an attack of Eve where she starts acting like Bob (to Alice) and assumes the shared string to be s. In the event that the shared random string between Alice and Bob is s, which happens with probability p, Eve gets to know Alice's input at the end of the protocol. Hence from the security criterion p should be at most 2^{-n}, which implies $S(\sigma) \geq n$. □

We show a similar statement for MPQCEs.

Lemma 4.2. *Let $|\psi\rangle^{AB}$ be the prior shared pure state between Alice and Bob in an* MPQCE*s for $\mathcal{C}_{2^n}$. Let $\sigma^{AB} = |\psi\rangle\langle\psi|$. Let σ^A and σ^B denote state of Alice's and Bob's parts respectively in σ^{AB}. Then $E(|\psi\rangle^{AB}) = S(\sigma^A) = S(\sigma^B) = \Omega(n)$.*

Proof. Let $S(\sigma^B) = k$. As in the proof of the previous lemma, let us consider a cheating strategy of Eve in which she imitates Bob. She starts with the state σ^B in the register which holds Bob's part of the entanglement and then behaves exactly like Bob. Let M_1 and M_2 represent Alice and Bob's parts in σ^{AB}. Then, from Lemma 3.5 we get

$$S\left(\sigma^{AB}|\sigma^A \otimes \sigma^B\right) = I(M_1 : M_2) \leq 2S(\sigma_B) = 2k.$$

From the substate theorem, there exists state σ'^{AB} such that

$$\sigma^A \otimes \sigma^B - \frac{\sigma'^{AB}}{2^{O(k)}} \geq 0$$

and $\mathsf{Tr}|\sigma'^{AB} - \sigma^{AB}| \leq 0.1$

This implies that, in case Alice and Bob start with σ'^{AB} as the prior entangled state, Eve's output equals the input of Alice with probability at least $2^{-O(k)}$. Since $\mathsf{Tr}|\sigma'^{AB} - \sigma^{AB}| \leq 0.1$, Eve's output will be equal to the input of Alice with probability at least $(0.8)2^{-O(k)}$. Because of the security criterion $(0.8)2^{-O(k)}$ should be at most 2^{-n} which implies $k = \Omega(n)$. □

Remark. Consider an implementation of a private quantum channel in which Alice and Bob first use *quantum key distribution* (QED) protocols like BB84 for key generation and then use these keys to transfer quantum states privately. However it is not strictly an MPQC according to our definition, because current implementations of QEDs require the existence of a classical broadcast channel which is unjammable by Eve. Also such a protocol would not be perfectly secure and there would still be a small amount of information that Eve can obtain even in case Alice does not abort the protocol.

4.1. *Conclusion*

We have considered private quantum channels with one-way communication of all possible kinds and in all the cases we have shown simultaneously optimal resource requirements. Even when we allow two-way communication but if Eve is allowed arbitrary access to the channel, we show that there is not much saving possible on prior entanglement/shared randomness.

It will be interesting to further investigate MPQC/MPQCEs and determine tight resource bounds in different cases as considered for PQC/PQCEs. In connection with RSPs it will be interesting to show similar bounds on resources when we do not have the oblivious condition or for two-way multiple round (non)-oblivious protocols.

Acknowledgements

We thank Daniel Gottesman, Hartmut Klauck, Gatis Midrijanis, Ashwin Nayak and Ronald de Wolf, for useful discussions. We thank Andris Ambainis for pointing out reference [6] and Jaikumar Radhakrishnan and Pranab Sen for useful comments on an earlier draft.

References

[1] A. Ambainis, M. Mosca, A. Tapp, R. de Wolf, Private quantum channels, in *Proceedings of the 41st Annual IEEE Symposium on Foundations of Computer Science* (2000), pp. 547–553

[2] C. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, W. Wootters, Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels. *Phys. Rev. Lett.* **70**, 1895–1899 (1993)

[3] C.H. Bennett, S.J. Wiesner, Communication via one and two particle operators on Einstein–Podolsky–Rosen states. *Phys. Rev. Lett.* **69**, 2881–2884 (1992)

[4] R. Cleve, D. Gottesman, H.K. Lo, How to share a quantum secret. *Phys. Rev. Lett.* **83**, 648–651 (1999)

[5] R. Jain, J. Radhakrishnan, P. Sen, A property of quantum relative entropy with an application to privacy in quantum communication. *J. ACM* **56**(6), 1–32 (2009)

[6] D.W. Leung, Quantum Vernam cipher. *Quantum Inf. Comput.* **2**, 14–34 (2002)

[7] H.-K. Lo, H.F. Chau, Is quantum bit commitment really possible? *Phys. Rev. Lett.* **78**, 3410–3413 (1997)

[8] H.-K. Lo, H.F. Chau, Why quantum bit commitment and ideal quantum coin tossing are impossible. *Physica D* **120**, 177–187 (1998)

[9] D.W. Leung, P.W. Shor, Oblivious remote state preparation. *Phys. Rev. Lett.* **90**, 127905 (2003)

[10] U.M. Maurer, Secret key agreement by public discussion from common information. *IEEE Trans. Inform. Theory* **39**, 733–742 (1993)

[11] M. Nielsen, I. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000)

[12] C.E. Shannon, A mathematical theory of communication. *Bell Syst. Tech. J.* **27**, 623–656 (1948)

[13] C.E. Shannon, Communication theory of secrecy systems. *Bell Syst. Tech. J.* **28**, 656–715 (1949)