Midterm

Introduction to Quantum Information Science
Wednesday, October 23rd

Your Name and EID: _____

1.	/40
2.	/35
a)	/5
b)	/7
c)	/6
d)	/7
e)	/5
f)	/5
g) (Extra Credit)	/10
3.	/25
a)	/10
b)	/10
c)	/5
d) (Extra Credit)	/10
Total	/100

1. True or false? Write your answer on the provided line. **[40 Points, 2 Points per Part]**

_____ **a)** $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$ and $\frac{|1\rangle-|0\rangle}{\sqrt{2}}$ represent the same physical state.

Solution: True. Global phase does not matter.

_____ **b)** Any simulation of the CHSH correlations in a classical universe requires faster-than-light communication.

Solution: True. Otherwise, Bell's inequality is violated.

_____ **c)** A mixed state is defined as a coherent superposition of two or more pure states.

Solution: False.

_____ **d)** Wiesner's quantum money scheme has the key feature that anyone can independently verify a banknote as valid.

Solution: False. Only bank could verify.

_____ **e)** Generalizing the quantum teleportation protocol from 1 qubit to many, while preserving the qubits' entanglement, is a major open problem in quantum information.

Solution: False. Teleport qubits one by one with the same protocol would work.

_____ **f)** Loophole-free Bell experiments have ruled out all hidden-variable theories, including Bohmian mechanics.

Solution: False.

_____ **g)** Superdense coding would work equally well in a variant of quantum mechanics where all amplitudes were real.

Solution: True.

_____ **h)** In all finite dimensions D, the maximally mixed state $\frac{I}{D}$ is the unique state unaffected by all unitary transformations.

Solution: True.

_____ **i)** The Elitzur-Vaidman bomb problem can be solved just as well using a classical probabilistic bit, whose probability of being 1 gradually increases from 0 to 1.

Solution: False.

_____ **j)** The No-Cloning Theorem holds for classical probability distributions just as it does for quantum pure states.

Solution: True.

_____ **k)** The eigenvalues of a unitary matrix must all have magnitude 1.

Solution: True.

_____ **l)** The eigenvalues of a density matrix must all have magnitude 1.

Solution: False. E.g., the maximally mixed state.

_____ **m)** If a bipartite mixed state is unentangled, then Alice and Bob's local states are necessarily pure.

Solution: False. It could be the case that both Alice's and Bob's local states are mixed state, but they are not entangled.

_____ **n)** The state $\frac{|0\rangle+|1\rangle+|+\rangle}{\sqrt{3}}$ is properly normalized.

Solution: False. Note that $|+\rangle$ is not orthogonal with $|0\rangle$ and $|1\rangle$.

_____ **o)** If Alice and Bob win the CHSH game more than 75% of the time using copies of a state $|\psi\rangle$, they can conclude that $|\psi\rangle$ must be entangled, without even knowing which entangled state it is.

Solution: True.

_____ **p)** If Alice's quantum system is entangled with Bob's, and Bob's quantum system is entangled with Charlie's, then Alice's quantum system must be entangled with Charlie's.

Solution: False. Consider Alice and Bob share a EPR pair and Bob and Charlie share another EPR pair.

_____ **q)** The eigenvectors corresponding to different eigenvalues of a density matrix ρ are orthogonal.

Solution: True. Spectral theorem.

_____ **r)** An equal mixture of $\frac{|00\rangle+i|11\rangle}{\sqrt{2}}$ and $\frac{|00\rangle-i|11\rangle}{\sqrt{2}}$ is entangled.

Solution: False. The density matrix of this state is $diag(0.5, 0, 0, 0.5)$

_____ **s)** $\frac{|00\rangle+|11\rangle}{\sqrt{2}} = \frac{|++\rangle+|--\rangle}{\sqrt{2}}$

Solution: True.

_____ **t)** $\frac{|000\rangle+|111\rangle}{\sqrt{2}} = \frac{|+++\rangle+|---\rangle}{\sqrt{2}}$

Solution: False. Just by expanding the RHS.

2. **[35 Points Total]** The following questions concern the state

$$|\psi\rangle = \frac{|00\rangle + |01\rangle + |10\rangle + i\,|11\rangle}{2},$$

with the left and right qubits held by Alice and Bob respectively.

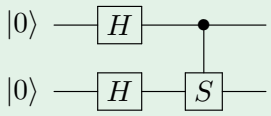
a) If Alice measures her qubit in the $\{|0\rangle, |1\rangle\}$ basis, with what probability does she see each result, and what is Bob's state conditioned on those results? **[6 points]**

Solution: By the partial measurement rule, the probability of measuring a 0 is $\left|\frac{1}{2}\right|^2 + \left|\frac{1}{2}\right|^2 = \frac{1}{2}$. Similarly, the probability of measuring a 1 is $\left|\frac{1}{2}\right|^2 + \left|\frac{i}{2}\right|^2 = \frac{1}{2}$.

If we measure a 0, Bob's state collapses to $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$, or $|+\rangle$, and if we measure a 1, Bob's state collapses to $\frac{|0\rangle+i|1\rangle}{\sqrt{2}}$, or $|i\rangle$.

b) Either draw or describe a quantum circuit to prepare $|\psi\rangle$, starting from $|00\rangle$. You can use any 1-qubit gates, as well as any controlled 1-qubit gates, as long as you specify what they are. **[7 points]**

Solution: Recall that $S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$. We can construct the state with the following circuit:



After the hadamards, the state evolves to

$$\frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2}$$

Then, with the controlled-S gate, the only affected terms are the $|10\rangle, |11\rangle$. Of these, the $|10\rangle$ is also unaffected, since $|0\rangle$ is unaffected by a phase gate. Finally, the $|11\rangle$ term has the phase applied to it, and becomes $i\,|11\rangle$, for a final state of

$$\frac{|00\rangle + |01\rangle + |10\rangle + i\,|11\rangle}{2}$$

as desired.

c) Calculate Alice's and Bob's reduced density matrices, ρ_A and ρ_B. **[6 points]**

Solution:

Alice: To calculate Alice's reduced density matrix ρ_A, we can rewrite the state as

$$|\psi\rangle = \frac{|0\rangle + |1\rangle}{2}|0\rangle + \frac{|0\rangle + i\,|1\rangle}{2}|1\rangle = \frac{1}{\sqrt{2}}|+\rangle\,|0\rangle + \frac{1}{\sqrt{2}}|i\rangle\,|1\rangle$$

We then have

$$\begin{aligned}\rho_A &= \frac{1}{2}|+\rangle\langle+| + \frac{1}{2}|i\rangle\langle i| \\ &= \begin{bmatrix}\frac{1}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{4}\end{bmatrix} + \begin{bmatrix}\frac{1}{4} & \frac{-i}{4} \\ \frac{i}{4} & \frac{1}{4}\end{bmatrix} \\ &= \begin{bmatrix}\frac{1}{2} & \frac{1-i}{4} \\ \frac{1+i}{4} & \frac{1}{2}\end{bmatrix}\end{aligned}$$

Bob: To calculate Bob's reduced density matrix ρ_A, we can rewrite the state as

$$|\psi\rangle = |0\rangle\frac{|0\rangle + |1\rangle}{2} + |1\rangle\frac{|0\rangle + i|1\rangle}{2} = \frac{1}{\sqrt{2}}|0\rangle|+\rangle + \frac{1}{\sqrt{2}}|1\rangle|i\rangle$$

We then have

$$\begin{aligned}\rho_B &= \frac{1}{2}|+\rangle\langle+| + \frac{1}{2}|i\rangle\langle i| \\ &= \begin{bmatrix}\frac{1}{2} & \frac{1-i}{4} \\ \frac{1+i}{4} & \frac{1}{2}\end{bmatrix}\end{aligned}$$

It makes sense that these two are the same, since the original state was symmetric with respect to qubit ordering.

d) Calculate $|\psi\rangle$'s entanglement entropy. You do not need to numerically estimate the result. **[6 points]**

Solution: The eigenvalues of ρ_A are $\frac{1}{2} \pm \frac{\sqrt{2}}{4}$. The entanglement entropy is same as the von Neumann Entropy of ρ_A, which is

$$\left(\frac{1}{2} + \frac{\sqrt{2}}{4}\right)\log\left(\frac{1}{\frac{1}{2} + \frac{\sqrt{2}}{4}}\right) + \left(\frac{1}{2} - \frac{\sqrt{2}}{4}\right)\log\left(\frac{1}{\frac{1}{2} - \frac{\sqrt{2}}{4}}\right).$$

e) Calculate the result if Bob applies a Hadamard to his qubit of $|\psi\rangle$. **[5 points]**

Solution:

$$\begin{aligned}(I \otimes H)|\psi\rangle &= \frac{|0+\rangle + |0-\rangle + |1+\rangle + i|1-\rangle}{2} \\ &= \frac{(|00\rangle + |01\rangle) + (|00\rangle - |01\rangle) + (|10\rangle + |11\rangle) + i(|10\rangle - |11\rangle)}{2\sqrt{2}} \\ &= \frac{2|00\rangle + (1+i)|10\rangle + (1-i)|11\rangle}{2\sqrt{2}}\end{aligned}$$

f) Suppose $|\psi\rangle$ is measured in the Bell basis $\left\{\frac{|00\rangle+|11\rangle}{\sqrt{2}}, \frac{|00\rangle-|11\rangle}{\sqrt{2}}, \frac{|01\rangle+|10\rangle}{\sqrt{2}}, \frac{|01\rangle-|10\rangle}{\sqrt{2}}\right\}$. What are the probabilities of each of the possible outcomes? **[5 points]**

Solution:

$$\left|\left(\frac{\langle 00| + \langle 11|}{\sqrt{2}}\right)\left(\frac{|00\rangle + |01\rangle + |10\rangle + i\,|11\rangle}{2}\right)\right|^2 = \left|\frac{1}{2\sqrt{2}}(\langle 00|00\rangle + i\,\langle 11|11\rangle)\right|^2$$
$$= \left|\frac{1+i}{2\sqrt{2}}\right|^2 = \frac{1}{4}$$

$$\left|\left(\frac{\langle 00| - \langle 11|}{\sqrt{2}}\right)\left(\frac{|00\rangle + |01\rangle + |10\rangle + i\,|11\rangle}{2}\right)\right|^2 = \left|\frac{1}{2\sqrt{2}}(\langle 00|00\rangle - i\,\langle 11|11\rangle)\right|^2$$
$$= \left|\frac{1-i}{2\sqrt{2}}\right|^2 = \frac{1}{4}$$

$$\left|\left(\frac{\langle 01| + \langle 10|}{\sqrt{2}}\right)\left(\frac{|00\rangle + |01\rangle + |10\rangle + i\,|11\rangle}{2}\right)\right|^2 = \left|\frac{1}{2\sqrt{2}}(\langle 01|01\rangle + \langle 10|10\rangle)\right|^2$$
$$= \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}$$

$$\left|\left(\frac{\langle 01| - \langle 10|}{\sqrt{2}}\right)\left(\frac{|00\rangle + |01\rangle + |10\rangle + i\,|11\rangle}{2}\right)\right|^2 = \left|\frac{1}{2\sqrt{2}}(\langle 01|01\rangle - \langle 10|10\rangle)\right|^2$$
$$= 0$$

Alternatively, note that

$$\frac{|00\rangle + i\,|11\rangle}{2} = \left(\frac{1+i}{2\sqrt{2}}\right)\frac{|00\rangle + |11\rangle}{\sqrt{2}} + \left(\frac{1-i}{2\sqrt{2}}\right)\frac{|00\rangle - |11\rangle}{\sqrt{2}}$$

and so we have

$$|\psi\rangle = \left(\frac{1+i}{2\sqrt{2}}\right)\frac{|00\rangle + |11\rangle}{\sqrt{2}} + \left(\frac{1-i}{2\sqrt{2}}\right)\frac{|00\rangle - |11\rangle}{\sqrt{2}} + \frac{1}{\sqrt{2}}\frac{|01\rangle + |10\rangle}{\sqrt{2}} + 0\cdot\frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

from which we can directly compute the measurement probabilities, giving the same answers as above.

g) Put $|\psi\rangle$ into Schmidt form. [Note: By plotting ρ_A and ρ_B on the Bloch sphere, you may be able to do this geometrically, without needing to diagonalize any matrices explicitly.] **[Extra Credit, 10 points]**

Solution: We need to find $|\psi_{A,1}\rangle, |\psi_{A,2}\rangle, |\psi_{B,1}\rangle, |\psi_{B,2}\rangle$ such that the pairs $|\psi_{A,1}\rangle, |\psi_{A,2}\rangle$ and $|\psi_{B,1}\rangle$, $|\psi_{B,2}\rangle$ are orthogonal and

$$|\psi\rangle = \lambda_1\,|\psi_{A,1}\rangle\,|\psi_{B,1}\rangle + \lambda_2\,|\psi_{A,2}\rangle\,|\psi_{B,2}\rangle,$$

We can see that

$$\rho_A = \lambda_1^2\,|\psi_{A,1}\rangle\,\langle\psi_{A,1}| + \lambda_2^2\,|\psi_{A,2}\rangle\,\langle\psi_{A,2}|$$

and similarly

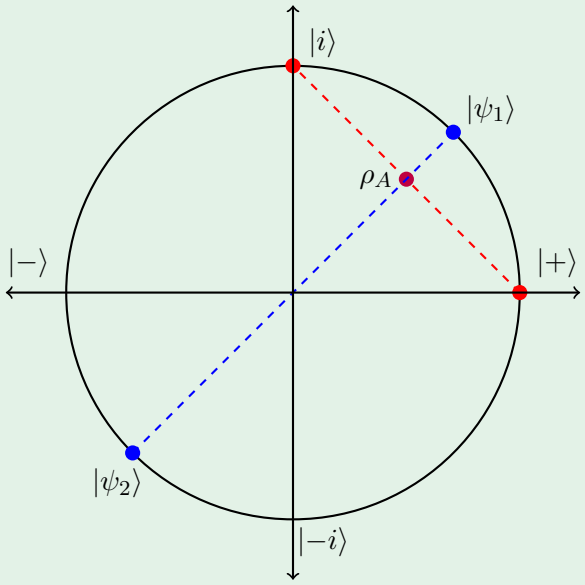
$$\rho_B = \lambda_1^2\,|\psi_{B,1}\rangle\,\langle\psi_{B,1}| + \lambda_2^2\,|\psi_{B,2}\rangle\,\langle\psi_{B,2}|$$

Since $\rho_A = \rho_B$, we can take $\psi_{A,1} = \psi_{B,1}$ and $\psi_{A,2} = \psi_{B,2}$. We will denote these as ψ_1, ψ_2 from now on.

Therefore, we are looking for a decomposition of the form

$$|\psi\rangle = \lambda_1 |\psi_1\rangle |\psi_1\rangle + \lambda_2 |\psi_2\rangle |\psi_2\rangle$$

where $|\psi_1\rangle, |\psi_2\rangle$ are orthogonal. To find these, we will turn to the Bloch sphere.



Based on our work in part (c), we can see that our mixed state ρ_A is halfway between the chord connecting $|i\rangle$ and $|+\rangle$. We want to represent ρ_A as a mixture between two states $|\psi_1\rangle, |\psi_2\rangle$ that are orthogonal. On a Bloch sphere, this corresponds to states that are antipodal. This means $|\psi_1\rangle, |\psi_2\rangle$ lie on midway along the arc connecting $|+\rangle, |-\rangle$ and $|-\rangle, |-i\rangle$, respectively.

Now, $|i\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\pi/2}|1\rangle\right)$ and $|+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{0i}|1\rangle\right)$. Rotating from $|+\rangle$ to $|i\rangle$ on the Bloch sphere linearly increases the phase angle from 0 to $\pi/2$. Based on this, we can see that the halfway state $|\psi_1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\pi/4}|1\rangle\right)$, and similarly that $|\psi_2\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - e^{i\pi/4}|1\rangle\right)$. This gives us the decomposition

$$\rho = c_1 |\psi_1\rangle \langle\psi_1| + c_2 |\psi_2\rangle \langle\psi_2|$$

We can expand these outer products into matrices:

$$|\psi_1\rangle \langle\psi_1| = \begin{bmatrix} \frac{1}{2} & \frac{e^{\pi i/4}}{2} \\ \frac{e^{-\pi i/4}}{2} & \frac{1}{2} \end{bmatrix}, \qquad |\psi_2\rangle \langle\psi_2| = \begin{bmatrix} \frac{1}{2} & -\frac{e^{\pi i/4}}{2} \\ -\frac{e^{-\pi i/4}}{2} & \frac{1}{2} \end{bmatrix}$$

We know $\rho = \begin{bmatrix} \frac{1}{2} & \frac{1-i}{4} \\ \frac{1+i}{4} & \frac{1}{2} \end{bmatrix}$, so we can combine the above three equations to get

$$\begin{bmatrix} \frac{1}{2} & \frac{1-i}{4} \\ \frac{1+i}{4} & \frac{1}{2} \end{bmatrix} = \begin{bmatrix} \frac{c_1+c_2}{2} & \frac{c_1-c_2}{2} e^{-\pi i/4} \\ \frac{c_1-c_2}{2} e^{\pi i/4} & \frac{c_1+c_2}{2} \end{bmatrix}$$

This means $c_1 + c_2 = 1$. Further, taking the square-root of the product of the two off-diagonal terms gives $c_1 - c_2 = \frac{\sqrt{2}}{2}$. Solving these equations gives $c_1 = \frac{2+\sqrt{2}}{4}, c_2 = \frac{2-\sqrt{2}}{4}$. You might recognize these quantities to be $\cos^2 \pi/8$ and $\sin^2 \pi/8$. Therefore, we get the final decomposition

$$\rho = \cos^2 \frac{\pi}{8} |\psi_1\rangle \langle\psi_1| + \sin^2 \frac{\pi}{8} |\psi_2\rangle \langle\psi_2|$$

with $|\psi_1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\pi/4}|1\rangle\right)$ and $|\psi_2\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - e^{i\pi/4}|1\rangle\right)$. This shows the Schmidt decomposition of

$$|\psi\rangle = \cos\frac{\pi}{8}|\psi_1\rangle|\psi_1\rangle + \sin\frac{\pi}{8}|\psi_2\rangle|\psi_2\rangle$$

also for the above defined $|\psi_1\rangle, |\psi_2\rangle$.

3. **[25 points total]** As we saw in class, the one-time pad lets Alice send a message m to Bob with complete secrecy, so long as Alice and Bob agreed in advance on a secret key k. Let m and k be 1 bit each for simplicity. Recall that it works by Alice sending the ciphertext $c = m \oplus k$, which Bob then decodes using the equation $m = c \oplus k$.

Now, suppose instead that Alice has a 1-qubit *quantum* state $|\psi\rangle$, which she wants to send Bob over a quantum channel.

a) Show that the classical one-time pad no longer works. In other words, suppose Alice and Bob share a random bit k, and Alice and Bob both apply NOT gates to $|\psi\rangle$ if and only if $k = 1$. Give an example of two orthogonal states $|v\rangle$ and $|w\rangle$ such that, if Eve intercepts Alice's message, she can still determine whether $|\psi\rangle = |v\rangle$ or $|\psi\rangle = |w\rangle$ even if Alice uses this code. **[10 points]**

Solution: Recall that the NOT operation does not affect the hadamard states $|+\rangle, |-\rangle$. Inspired by this, say Alice wants to send either $|+\rangle$ or $|-\rangle$. Alice will encode this state with the key. If $k = 1$, she will apply the not operation, making these states $|+\rangle, -|-\rangle$. Otherwise, she will not modify them.

Eve, intercepting these qubits, can then simply measure in the Hadamard basis. If the message was $|+\rangle$, she will measure a $|+\rangle$ no matter what k was, and if the message was a $|-\rangle$, she will measure a $|-\rangle$ no matter what k was. So, she does not need to know what k was in order to decode the qubits, and this is no longer safe.

b) Now suppose that Alice and Bob share *two* secret random bits k and l. If $k = 1$, then Alice and Bob both apply NOT gates to $|\psi\rangle$, and otherwise not. If $l = 0$, they both apply the phase gate $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ to $|\psi\rangle$, and otherwise not. Show that this gives perfect security — in the sense that if Eve intercepts the qubit but knows neither k nor l, then her measurement statistics have no dependence on $|\psi\rangle$. **[10 points]**

Solution:

Solution #1, explicit computations: Suppose Eve measures in the basis defined by $|v\rangle, |w\rangle$, where $|v\rangle = \alpha|0\rangle + \beta|1\rangle$, for some α, β such that $|\alpha|^2 + |\beta|^2 = 1$. If Alice sends qubit $\gamma|0\rangle + \delta|1\rangle$, then the encoded qubit will have the following form, depending on the values of k and l.

k	l	encoded $\|\psi\rangle$
0	0	$\gamma\|0\rangle - \delta\|1\rangle$
0	1	$\gamma\|0\rangle + \delta\|1\rangle$
1	0	$\delta\|0\rangle - \gamma\|1\rangle$
1	1	$\delta\|0\rangle + \gamma\|1\rangle$

Now lets compute the probabilities of Eve's measurements. If $k = l = 0$, Eve gets a $|v\rangle$ with probability

$$\begin{aligned}|(\alpha^*\langle 0| + \beta^*\langle 1|)(\gamma|0\rangle - \delta|1\rangle)|^2 &= |\alpha^*\gamma - \beta^*\delta|^2 \\ &= |\alpha^*\gamma|^2 - 2|\alpha^*\gamma\beta^*\delta| + |\beta^*\delta|^2\end{aligned}$$

If $k = 0, l = 1$,

$$\begin{aligned}|(\alpha^* \langle 0| + \beta^* \langle 1|)(\gamma |0\rangle + \delta |1\rangle)|^2 &= |\alpha^*\gamma + \beta^*\delta|^2 \\ &= |\alpha^*\gamma|^2 + 2|\alpha^*\gamma\beta^*\delta| + |\beta^*\delta|^2\end{aligned}$$

If $k = 1, l = 0$,

$$\begin{aligned}|(\alpha^* \langle 0| + \beta^* \langle 1|)(\delta |0\rangle - \gamma |1\rangle)|^2 &= |\alpha^*\delta + \beta^*\gamma|^2 \\ &= |\alpha^*\delta|^2 - 2|\alpha^*\delta\beta^*\gamma| + |\beta^*\gamma|^2\end{aligned}$$

If $k = 1, l = 1$,

$$\begin{aligned}|(\alpha^* \langle 0| + \beta^* \langle 1|)(\delta |0\rangle + \gamma |1\rangle)|^2 &= |\alpha^*\delta + \beta^*\gamma|^2 \\ &= |\alpha^*\delta|^2 + 2|\alpha^*\delta\beta^*\gamma| + |\beta^*\gamma|^2\end{aligned}$$

Since k, l are uniform random bits, the resultant probability of measuring $|v\rangle$ is the average of these, which is (after some cancellations),

$$\begin{aligned}\frac{|\alpha^*\gamma|^2 + |\beta^*\delta|^2 + |\alpha^*\delta|^2 + |\beta^*\gamma|^2}{2} &= \frac{|\alpha^*|^2|\gamma|^2 + |\beta^*|^2|\delta|^2 + |\alpha^*|^2|\delta|^2 + |\beta^*|^2|\gamma|^2}{2} \\ &= \frac{(|\alpha^*|^2 + |\beta^*|^2)(|\gamma|^2 + |\delta|^2)}{2} = \frac{1}{2}\end{aligned}$$

(Here we have used the fact that $|v\rangle, |\psi\rangle$ are normalized, and that $|\alpha^*| = |\alpha|$, for any complex α.)

Therefore, the measurement probabilities that Eve sees are independent of the initial state $|\psi\rangle$, and she therefore gets no information about the original state.

Solution #2, mixed states: We can compute the mixed state that $|\psi\rangle$ is in after the encoding. If we compute the outer product of each state with itself in the above table, we get the density matrices

$$\begin{bmatrix} |\gamma|^2 & -\delta\gamma^* \\ -\gamma\delta^* & |\delta|^2 \end{bmatrix}, \begin{bmatrix} |\gamma|^2 & \delta\gamma^* \\ \gamma\delta^* & |\delta|^2 \end{bmatrix}, \begin{bmatrix} |\delta|^2 & -\gamma\delta^* \\ \delta\gamma^* & |\gamma|^2 \end{bmatrix}, \begin{bmatrix} |\delta|^2 & \gamma\delta^* \\ \delta\gamma^* & |\gamma|^2 \end{bmatrix},$$

To find the total density matrix, we take the sum of these divided by four. This is just

$$\begin{bmatrix} \frac{2|\gamma|^2+2|\delta|^2}{4} & 0 \\ 0 & \frac{2|\gamma|^2+2|\delta|^2}{4} \end{bmatrix} = \begin{bmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{bmatrix} = \frac{I}{2}$$

which is the maximally mixed state, independent of ψ. So, any measurements of this state will also be independent of ψ, and Eve will get no information of ψ from measurements.

c) In part (b), a single qubit behaved as if it were "two classical bits," even though of course it's not literally. Give an example of a quantum information protocol where a similar doubling happens. Explain how part (b) relates to the consistency of that protocol with the No Superluminal Signalling principle. **[5 points]**

Solution: In quantum teleportation, 2 classical bits are used to transmit 1 qubit (aided by entanglement between Alice and Bob). Before Bob gets the classical bits, what he see is also the maximally mixed state, just like part(b). Therefore no information is transmitted as required by the No Communication theorem.

d) Generalizing part (a), prove that there's no scheme to perfectly encrypt 1 qubit using only 1 bit of

shared classical secret key. [**Extra Credit, 10 points**]

Solution: Assuming no ancilla bits are allowed.

Here, a perfect encryption protocol requires the following two properties:

1. **Prefect Correctness:** For any state $|\psi\rangle$ Alice start with, Bob will end with the exactly same state $|\psi\rangle$ with certainty;
2. **Prefect Security:** For any states $|\psi_1\rangle$, $|\psi_2\rangle$ Alice start with, and suppose Alice sends $|\phi_1\rangle$ and $|\phi_2\rangle$ respectively to Bob, Eve cannot distinguish between $|\phi_1\rangle$ and $|\phi_2\rangle$ given the randomness in their Alice and Bob's key.

For the perfect correctness, since no ancilla bits are allowed, the encryption protocol should never use any *measurement*. Also, without loss of generality, their protocol should be deterministic given their shared random key.

So a general protocol will be Alice apply U_0 when their common key is 0, and apply U_1 if their common key is 1. Bob then apply $U_0^\dagger$ and $U_1^\dagger$ respectively. Note that this protocol could be further simplified without loss of generality. Alice could do nothing if their key is 0, and apply U if their key is 1.

Now consider the two eigenstates of U, say they are $|v\rangle$ and $|w\rangle$. Alice essentially did nothing to $|v\rangle$ and $|w\rangle$ no matter what the key is. And Eve could perfectly distinguish between them if she measure in the $\{|v\rangle, |w\rangle\}$ basis.