COM-440, Introduction to Quantum Cryptography, Fall 2025

Homework # 1 Solutions

Below are indicative solutions to the homework problems. For the first two problems we explain the solution, but give slightly less justification than expected in those cases where essentially everyone did well. The last problem was computational and we include parts of the calculations.

1. **Perfect secrecy**

   (a) True.

   $\Rightarrow$: If an encryption scheme is perfectly secret, then the distribution of $\mathsf{Enc}_k(m_0)$ where $k \leftarrow \mathsf{Gen}$ is the same as the distribution of $\mathsf{Enc}_k(m_1)$ where $k \leftarrow \mathsf{Gen}$, and thus no function $\mathcal{A}$ can tell them apart.

   $\Leftarrow$: For a ciphertext c^* and messages m_0, m_1, construct an adversary $\mathcal{A}$ as follows: on input c, it outputs 0 if $c \neq c^*$; otherwise, it outputs 1. Then we have that

   $$\begin{aligned}&\Pr_{k\leftarrow\mathsf{Gen},\, b\leftarrow_U\{0,1\}}[\mathcal{A}(\mathsf{Enc}_k(m_b)) = b]\\ =&\frac{1}{2}(1 - \Pr_{k\leftarrow\mathsf{Gen}}[\mathsf{Enc}_k(m_0) = c^*]) + \frac{1}{2}\Pr_{k\leftarrow\mathsf{Gen}}[\mathsf{Enc}_k(m_1) = c^*]\ .\end{aligned}$$

   By assumption, this equals to $\frac{1}{2}$. Therefore,

   $$\Pr_{k\leftarrow\mathsf{Gen}}[\mathsf{Enc}_k(m_0) = c^*]) = \Pr_{k\leftarrow\mathsf{Gen}}[\mathsf{Enc}_k(m_1) = c^*]\ .$$

   As this holds for arbitrary c^*, m_0, m_1, the scheme is perfectly secret.

   (b) True. Consider the scheme $\mathsf{Enc}_k(m) = (k_1 \oplus m) \parallel k_2$ where $k = k_1 \parallel k_2$, $k_1 \in \{0,1\}$, $k_2 \in \{0,1\}^{99}$ and $m \in \{0,1\}$. This scheme is perfectly secret while the ciphertext always reveals 99% of the bits of the key k to the adversary.

   (c) True. The scheme $\mathsf{Enc}_k(m) = m$ is not perfectly secret, but the adversary cannot guess the key with probability greater than $1/|\mathcal{K}|$.

   (d) False. The perfect secrecy only means that for every c, m_0, m_1, $\mathbf{Pr}_{k\leftarrow\mathsf{Gen}}(\mathsf{Enc}_k(m_0) = c) = \mathbf{Pr}_{k\leftarrow\mathsf{Gen}}(\mathsf{Enc}_k(m_1) = c)$. It does not mean that the ciphertext is uniformly random. For example, $\mathsf{Enc}_k(m) = (m \oplus k) \parallel (m \oplus k)$ is perfectly secret where $k \in \{0,1\}, m \in \{0,1\}$, but the ciphertext is not uniform: for each m, $\mathbf{Pr}(\mathsf{Enc}_k(m) = 01) = 0$ while $\mathbf{Pr}(\mathsf{Enc}_k(m) = 00) = 1/2$.

   (e) True.

   $\Rightarrow$: If an encryption scheme is perfectly secret, by the law of total probability, it is not hard to see that for any $\bar{m} \in \mathcal{M}$ and $\bar{c} \in \mathcal{C}$, $\mathbf{Pr}_{m\leftarrow\mathcal{D},\, k\leftarrow\mathsf{Gen}}\left(\mathsf{Enc}_k(m) = \bar{c}\right) =$

$\mathbf{Pr}_{k\leftarrow\mathsf{Gen}}\big(\mathsf{Enc}_k(\bar{m})=\bar{c}\big)$. Therefore,

$$\begin{aligned}
&\mathop{\mathbf{Pr}}_{m\leftarrow\mathcal{D},\,k\leftarrow\mathsf{Gen}}\big(m=\bar{m}\wedge\mathsf{Enc}_k(m)=\bar{c}\big)\\
&=\mathop{\mathbf{Pr}}_{m\leftarrow\mathcal{D}}(m=\bar{m})\cdot\mathop{\mathbf{Pr}}_{m\leftarrow\mathcal{D},\,k\leftarrow\mathsf{Gen}}\big(\mathsf{Enc}_k(m)=\bar{c}|m=\bar{m}\big)\\
&=\mathop{\mathbf{Pr}}_{m\leftarrow\mathcal{D}}(m=\bar{m})\cdot\mathop{\mathbf{Pr}}_{k\leftarrow\mathsf{Gen}}\big(\mathsf{Enc}_k(\bar{m})=\bar{c}\big)\\
&=\mathop{\mathbf{Pr}}_{m\leftarrow\mathcal{D}}(m=\bar{m})\cdot\mathop{\mathbf{Pr}}_{m\leftarrow\mathcal{D},\,k\leftarrow\mathsf{Gen}}\big(\mathsf{Enc}_k(m)=\bar{c}\big)\ .
\end{aligned}$$

$\Leftarrow$: For $m_0\neq m_1$, we consider the uniform distribution over m_0 and m_1. Choose $\bar{m}=m_0$, we can get that

$$\mathop{\mathbf{Pr}}_{m\leftarrow\mathcal{D},\,k\leftarrow\mathsf{Gen}}\big(m=m_0\wedge\mathsf{Enc}_k(m)=\bar{c}\big)\ =\ \mathop{\mathbf{Pr}}_{m\leftarrow\mathcal{D}}(m=m_0)\cdot\mathop{\mathbf{Pr}}_{m\leftarrow\mathcal{D},\,k\leftarrow\mathsf{Gen}}\big(\mathsf{Enc}_k(m)=\bar{c}\big)\ .$$

The lefthand side equals to $\frac{1}{2}\,\mathbf{Pr}_{k\leftarrow\mathsf{Gen}}\big(\mathsf{Enc}_k(m_0)=\bar{c}\big)$. The righthand side equals to $\frac{1}{2}\left(\frac{1}{2}Pr_{k\leftarrow\mathsf{Gen}}\big(\mathsf{Enc}_k(m_0)=\bar{c}\big)+\frac{1}{2}Pr_{k\leftarrow\mathsf{Gen}}\big(\mathsf{Enc}_k(m_1)=\bar{c}\big)\right)$. Therefore, we get that

$$Pr_{k\leftarrow\mathsf{Gen}}\big(\mathsf{Enc}_k(m_0)=\bar{c}\big)=Pr_{k\leftarrow\mathsf{Gen}}\big(\mathsf{Enc}_k(m_1)=\bar{c}\big)\ .$$

As this holds for arbitrary $\bar{c},m_0,m_1$, the scheme is perfectly secret.

2. **Measurement attacks**

   (a) We evaluate the success probability of this attack for each of the 4 possible states. If the initial state is $|0\rangle$, the outcome $b=0$ is obtained with probability $|\alpha|^2$, and $b=1$ is obtained with probability $|\beta|^2$. Preparing the state $|u_b\rangle\langle u_b|\otimes|u_b\rangle\langle u_b|$ leads to success probabilities of $|\alpha|^4$ and $|\beta|^4$ respectively. For the state $|1\rangle$, the probabilties are exchanged. For the states $|+\rangle$ and $|-\rangle$, α and β are replaced with $(\alpha+\beta)/\sqrt{2}$ and $(\alpha-\beta)/\sqrt{2}$ respectively. Therefore, the overall success probability of this attack is

$$\frac{1}{4}\Big(2\big(|\alpha|^6+|\beta|^6\big)+2\Big(\Big|\frac{\alpha+\beta}{\sqrt{2}}\Big|^6+\Big|\frac{\alpha-\beta}{\sqrt{2}}\Big|^6\Big)\Big)\ .$$

   (b) The global phase does not affect the success probability, so without loss of generality, we can suppose $\alpha=\cos\theta$, $\beta=e^{i\varphi}\sin\theta$. We can rewrite the success probability in terms of θ and φ, and it is not hard to see that the optimum is achieved when $\varphi=0$. For example, when $\alpha=1,\beta=0$, the optimum is achieved.

   (c) The success probability is the same as obtained in class: 5/8.

3. **Improving Wiesner's quantum money.**

   (a) This boils down to a lengthy calculation. Namely, we will evaluate each of the six terms of the sum individually below and then add them together with the appropriate weighting. We begin:

i. $|\langle\psi_1|\langle\psi_1|U|\psi_1\rangle|0\rangle|^2 = |\langle 0|\langle 0||0\rangle|0\rangle|^2 = |\langle 0||0\rangle \otimes \langle 0||0\rangle|^2 = 1$

ii. $|\langle\psi_2|\langle\psi_2|U|\psi_2\rangle|0\rangle|^2 = |\langle 1|\langle 1||1\rangle|1\rangle|^2 = |\langle 1||1\rangle \otimes \langle 1||1\rangle|^2 = 1$

iii. $|\langle\psi_3|\langle\psi_3|U|\psi_3\rangle|0\rangle|^2 = |\langle +|\langle +|\frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)|^2 = \frac{1}{2}|\langle +|\langle +||0\rangle|0\rangle + \langle +|\langle +||1\rangle|1\rangle|^2 == \frac{1}{2}|1/2 + 1/2|^2 = \frac{1}{2}$

iv. $|\langle\psi_4|\langle\psi_4|U|\psi_4\rangle|0\rangle|^2 = |\langle -|\langle -|\frac{1}{\sqrt{2}}(|0\rangle|0\rangle - |1\rangle|1\rangle)|^2 = \frac{1}{2}|\langle -|\langle -||0\rangle|0\rangle - \langle -|\langle -||1\rangle|1\rangle|^2 = \frac{1}{2}|1/2 - 1/2|^2 = 0$

v. $|\langle\psi_5|\langle\psi_5|U|\psi_5\rangle|0\rangle|^2 = |\langle\psi_5|\langle\psi_5|\frac{1}{\sqrt{2}}(|0\rangle|0\rangle + i|1\rangle|1\rangle)|^2 = \frac{1}{2}|\langle\psi_5|\langle\psi_5||0\rangle|0\rangle + i\langle\psi_5|\langle\psi_5||1\rangle|1\rangle|^2 = \frac{1}{2}|1/2 + i^3/2|^2 = \frac{1}{2}(1/4 + 1/4) = \frac{1}{4}$

vi. $|\langle\psi_6|\langle\psi_6|U|\psi_6\rangle|0\rangle|^2 = |\langle\psi_6|\langle\psi_6|\frac{1}{\sqrt{2}}(|0\rangle|0\rangle - i|1\rangle|1\rangle)|^2 = \frac{1}{2}|\langle\psi_6|\langle\psi_6||0\rangle|0\rangle - i\langle\psi_6|\langle\psi_6||1\rangle|1\rangle|^2 = \frac{1}{2}|1/2 - i^3/2|^2 = \frac{1}{2}(1/4 + 1/4) = \frac{1}{4}$

We finally evaluate the full sum,

$$\mathbf{Pr}[\text{success}] = \frac{1}{6}\Big(1 + 1 + \frac{1}{2} + 0 + \frac{1}{4} + \frac{1}{4}\Big) = \frac{1}{2}$$

Now, suppose that U copies in the hadamard basis instead. This corresponds to the following definition; $U' : |+\rangle|+\rangle \to |+\rangle|+\rangle$, $U' : |-\rangle|+\rangle \to |-\rangle|-\rangle$. However, consider the following unitary operator,

$$B = H \otimes H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix} \otimes \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}.$$

Now, observe that $U' = BUB^\dagger$. So,

$$\begin{aligned}\sum_{k=1}^{6}\frac{1}{6}\Big|\big(\langle\psi_k| \otimes \langle\psi_k|\big)U'\big(|\psi_k\rangle \otimes |+\rangle\big)\Big|^2 &= \sum_{k=1}^{6}\frac{1}{6}\Big|\big(\langle\psi_k| \otimes \langle\psi_k|\big)BUB^\dagger\big(|\psi_k\rangle \otimes |+\rangle\big)\Big|^2\\ &= \sum_{k=1}^{6}\frac{1}{6}\Big|\big(\langle\psi_k|H \otimes \langle\psi_k|H\big)U\big(H|\psi_k\rangle \otimes H|+\rangle\big)\Big|^2.\end{aligned}$$

In fact, H permutes the indices of $|\psi_k\rangle$, where $\pi : (1,2,3,4,5,6) \to (3,4,1,2,5,6)$ and change signs for $|\psi_5\rangle$ and $|\psi_6\rangle$. However, a global sign flip is irrelevant due to the modulus, yielding

$$\begin{aligned}\sum_{k=1}^{6}\frac{1}{6}\Big|\big(\langle\psi_k|H \otimes \langle\psi_k|H\big)U\big(H|\psi_k\rangle \otimes |0\rangle\big)\Big|^2 &= \sum_{k=1}^{6}\frac{1}{6}\Big|\big(\langle\psi_{\pi(k)}| \otimes \langle\psi_{\pi(k)}|\big)U\big(|\psi_{\pi(k)}\rangle \otimes |0\rangle\big)\Big|^2\\ &= \frac{1}{2}.\end{aligned}$$

(b) Observe that V must maintain the orthogonality between $|0\rangle|00\rangle$ and $|1\rangle|00\rangle$, if it is to be unitary, and check their normality. However, since we do not have any other constraints on the nature of V we can pick some collection of mutually

orthonormal basis vectors that span the remainder of the space (using a method such as gram-schmidt), and have those vectors be the remainder of the columns of V. Observe that by construction, $V_i^\dagger V_j = \delta_{ij}$ for all i, j that are not the pair of columns associated with $|0\rangle|00\rangle$ and $|1\rangle|00\rangle$. For the pair associated with these two vectors, we directly check the orthogonality and the normality of both fixed vectors:

$$\langle 0|\langle 00|V^\dagger V|1\rangle|00\rangle = \Big(\frac{2}{\sqrt{6}}\langle 00|\langle 0| + \frac{1}{\sqrt{3}}\langle\phi^-|\langle 1|\Big)\Big(\frac{1}{\sqrt{3}}|\phi^-\rangle|0\rangle + \frac{2}{\sqrt{6}}|11\rangle|1\rangle\Big) =$$

$$= \frac{2}{\sqrt{6}\sqrt{3}}\Big(\langle 00|\phi^-\rangle\langle 0|0\rangle + \langle\phi^-|11\rangle\langle 1|1\rangle\Big) = 0$$

Since $\langle 00|\phi^-\rangle = \frac{1}{\sqrt{2}}\langle 00|\big(|01\rangle + |10\rangle\big) = 0 = \langle\phi^-|11\rangle$.

$$\begin{aligned}\langle 0|\langle 00|V^\dagger V|1\rangle|00\rangle &= \Big(\frac{1}{\sqrt{3}}\langle\phi^-|\langle 0| + \frac{2}{\sqrt{6}}\langle 11|\langle 1|\Big)\Big(\frac{1}{\sqrt{3}}|\phi^-\rangle|0\rangle + \frac{2}{\sqrt{6}}|11\rangle|1\rangle\Big)\\ &= 1/3 + 4/6 = 1\\ \langle 0|\langle 00|V^\dagger V|0\rangle|00\rangle &= \Big(\frac{2}{\sqrt{6}}\langle 00|\langle 0| + \frac{1}{\sqrt{3}}\langle\phi^-|\langle 1|\Big)\Big(\frac{2}{\sqrt{6}}|00\rangle|0\rangle + \frac{1}{\sqrt{3}}|\phi^-\rangle|1\rangle\Big)\\ &= 4/6 + 1/3 = 1\,.\end{aligned}$$

(c) We describe the three steps that define our quantum map T: i) Add an ancillary state $|00\rangle_B C$ (can be seen as an isometry acting on the pure state); ii.) Apply the V discussed in part (4.b) above; iii.) Trace out the last qubit C and acquire the density matrix representation of AB. We can check that these operations reproduce the desired behavior of T on the density matrices $|0\rangle\langle 0|, |1\rangle\langle 1|, |+\rangle\langle +|,$

and $|-\rangle\langle -|$. Let's do this explicitly just for the case of $|0\rangle\langle 0|$:

$$
\begin{aligned}
&T(|0\rangle\langle 0|) \\
&= \sum_x \mathbb{I}\otimes\langle u_x|\left(V|0\rangle|00\rangle\langle 0|\langle 00|V^\dagger\right)\mathbb{I}\otimes|u_x\rangle \\
&= \sum_x \mathbb{I}\otimes\langle u_x|\Big(\frac{2}{\sqrt{6}}|00\rangle|0\rangle+\frac{1}{\sqrt{3}}|\phi^-\rangle|1\rangle\Big)\Big(\frac{2}{\sqrt{6}}\langle 00|\langle 0|+\frac{1}{\sqrt{3}}\langle\phi^-|\langle 1|\Big)\mathbb{I}\otimes|u_x\rangle \\
&= \sum_x \Big(\frac{2}{\sqrt{6}}\mathbb{I}\otimes\langle u_x|00\rangle|0\rangle+\frac{1}{\sqrt{3}}\mathbb{I}\otimes\langle u_x|\phi^-\rangle|1\rangle\Big)\Big(\frac{2}{\sqrt{6}}\langle 00|\langle 0|\mathbb{I}\otimes|u_x\rangle+\frac{1}{\sqrt{3}}\langle\phi^-|\langle 1|\mathbb{I}\otimes|u_x\rangle\Big) \\
&= \sum_x \Big(\frac{2}{\sqrt{6}}|00\rangle\otimes\langle u_x|0\rangle+\frac{1}{\sqrt{3}}|\phi^-\rangle\otimes\langle u_x|1\rangle\Big)\Big(\frac{2}{\sqrt{6}}\langle 00|\otimes\langle 0|u_x\rangle+\frac{1}{\sqrt{3}}\langle\phi^-|\otimes\langle 1|u_x\rangle\Big) \\
&= \Big(\frac{2}{\sqrt{6}}|00\rangle\otimes\langle 0|0\rangle+\frac{1}{\sqrt{3}}|\phi^-\rangle\otimes\langle 0|1\rangle\Big)\Big(\frac{2}{\sqrt{6}}\langle 00|\otimes\langle 0|0\rangle+\frac{1}{\sqrt{3}}\langle\phi^-|\otimes\langle 1|0\rangle\Big) \\
&+ \Big(\frac{2}{\sqrt{6}}|00\rangle\otimes\langle 1|0\rangle+\frac{1}{\sqrt{3}}|\phi^-\rangle\otimes\langle 1|1\rangle\Big)\Big(\frac{2}{\sqrt{6}}\langle 00|\otimes\langle 0|1\rangle+\frac{1}{\sqrt{3}}\langle\phi^-|\otimes\langle 1|1\rangle\Big) \\
&= \Big(\frac{2}{\sqrt{6}}|00\rangle\Big)\Big(\frac{2}{\sqrt{6}}\langle 00|\Big)+\Big(\frac{1}{\sqrt{3}}|\phi^-\rangle\Big)\Big(\frac{1}{\sqrt{3}}\langle\phi^-|\Big) \\
&= \frac{2}{3}|00\rangle\langle 00|+\frac{1}{3}|\phi^-\rangle\langle\phi^-| = \rho_0\ .
\end{aligned}
$$

(d) We will consider the action of the aforementioned operator T on an arbitrary qubit, $|\psi\rangle = a|0\rangle + b|1\rangle$. Recalling that the operator T must be linear over density matrices as it is a valid quantum map (i.e. quantum channel), we evaluate,

$$T(|\psi\rangle\langle\psi|) = T\big((a|0\rangle+b|1\rangle)(\overline{a}\langle 0|+\overline{b}\langle 1|)\big) =$$

$$= a\overline{a}T(|0\rangle\langle 0|)+a\overline{b}T(|0\rangle\langle 1|)+\overline{a}bT(|1\rangle\langle 0|)+\overline{b}bT(|1\rangle\langle 1|)$$

$$T(|\psi\rangle\langle\psi|) = |a|^2T(|0\rangle\langle 0|)+a\overline{b}T(|0\rangle\langle 1|)+\overline{a}bT(|1\rangle\langle 0|)+|b|^2T(|1\rangle\langle 1|)$$

We now determine the action of T on $|1\rangle\langle 0|$ and its adjoint by executing each of the three steps discussed in part 4.c, which are denoted below as $T = T_3\circ T_2\circ T_1$.

$$T_1(|1\rangle\langle 0|) = |1\rangle_A|00\rangle_{BC}\langle 0|_A\langle 00|_{BC}$$

Similarly, T_2 applies V to both qubits

$$T_2(|1\rangle_A|00\rangle_{BC}\langle 0|_A\langle 00|_{BC}) = V|1\rangle_A|00\rangle_{BC}\langle 0|_A\langle 00|_{BC}V^\dagger =$$

$$= \Big(\frac{1}{\sqrt{3}}|\phi^-\rangle_{AB}|0\rangle_C+\frac{2}{\sqrt{6}}|11\rangle_{AB}|1\rangle_C\Big)\Big(\frac{2}{\sqrt{6}}|00\rangle_{AB}|0\rangle_C+\frac{1}{\sqrt{3}}|\phi^-\rangle_{AB}|1\rangle_C\Big)^\dagger$$

We now trace out C, which after some calculation yields

$$T(|1\rangle\langle 0|) = \frac{\sqrt{2}}{3}\Big(|\phi^-\rangle\langle 00|+|11\rangle\langle\phi^-|\Big)$$

Noting that $T(|0\rangle\langle 1|) = T(|1\rangle\langle 0|)^\dagger$

$$T(|0\rangle\langle 1|) = \frac{\sqrt{2}}{3}\Big(|00\rangle\langle\phi^-| + |\phi^-\rangle\langle 11| \Big)$$

Note the following, where $|\psi\psi\rangle = |\psi\rangle \otimes |\psi\rangle$,

$$\langle\phi^-|\psi\psi\rangle = \frac{1}{\sqrt{2}}\big(\langle 01|+\langle 10| \big)\big(aa\,|00\rangle+ab\,|01\rangle+ba\,|10\rangle+bb\,|11\rangle\big) = \frac{1}{\sqrt{2}}(ab+ba) = ab\sqrt{2}$$

Furthermore we have $\langle 00|\psi\psi\rangle = aa$ and $\langle 11|\psi\psi\rangle = bb$. Finally, for this arbitrary state we evaluate the probability of the bank accepting it and a copy by T, $\langle\psi\psi|\,T(|\psi\rangle\langle\psi|)\,|\psi\psi\rangle$. We evaluate every term of this sum, starting with the first;

$$|a|^2\,\langle\psi\psi|\,T(|0\rangle\langle 0|)\,|\psi\psi\rangle = \frac{2}{3}\langle\psi\psi|00\rangle\langle 00|\psi\psi\rangle+\frac{1}{3}\langle\psi\psi|\phi^-\rangle\langle\phi^-|\psi\psi\rangle = \frac{2|aa|^2|a|^2}{3}+\frac{2|ab|^2|a|^2}{3} =$$

$$= \frac{2|a|^4}{3}\Big(|a|^2+|b|^2\Big) = \frac{2|a|^4}{3}$$

The last equality follows from the normalization property of $|\psi\rangle$. We now compute the middle two terms,

$$a\bar{b}\,\langle\psi\psi|\,T(|0\rangle\langle 1|)\,|\psi\psi\rangle + \overline{a}b\,\langle\psi\psi|\,T(|1\rangle\langle 0|)\,|\psi\psi\rangle =$$

$$= \frac{\sqrt{2}}{3}\left(a\bar{b}\Big(\langle\psi\psi|00\rangle\langle\phi^-|\psi\psi\rangle+\langle\psi\psi|\phi^-\rangle\langle 11|\psi\psi\rangle\Big)+\overline{a}b\Big(\langle\psi\psi|\phi^-\rangle\langle 00|\psi\psi\rangle+\langle\psi\psi|11\rangle\langle\phi^-|\psi\psi\rangle\Big)\right)$$

$$= \frac{2\sqrt{2}}{3}\mathrm{Re}\left(\Big(a\bar{b}\Big(\overline{a}\overline{a}ab\sqrt{2}+\overline{a}\bar{b}\sqrt{2}bb\Big)\right) = \frac{4}{3}\mathrm{Re}\Big(a\bar{b}\overline{a}\overline{a}ab+a\bar{b}\overline{a}\bar{b}bb\Big) = \frac{4}{3}\mathrm{Re}\Big(a\overline{a}a\overline{a}b\bar{b}+a\overline{a}b\bar{b}b\bar{b}\Big) =$$

$$= \frac{4}{3}\Big(|a|^4|b|^2+|a|^2|b|^4\Big) = \frac{4}{3}|a|^2|b|^2\Big(|a|^2+|b|^2\Big) = \frac{4}{3}|a|^2|b|^2$$

Finally, we compute the last term,

$$|b|^2\,\langle\psi\psi|\,T(|1\rangle\langle 1|)\,|\psi\psi\rangle = \frac{2}{3}\langle\psi\psi|11\rangle\langle 11|\psi\psi\rangle+\frac{1}{3}\langle\psi\psi|\phi^-\rangle\langle\phi^-|\psi\psi\rangle = \frac{2|bb|^2|b|^2}{3}+\frac{2|ab|^2|b|^2}{3} =$$

$$= \frac{2|b|^4}{3}\Big(|b|^2+|a|^2\Big) = \frac{2|b|^4}{3}$$

Thus, we have,

$$\langle\psi\psi|\,T(|\psi\rangle\langle\psi|)\,|\psi\psi\rangle = \frac{2}{3}|a|^4+\frac{4}{3}|a|^2|b|^2+\frac{2}{3}|b|^4 = \frac{2}{3}\Big(|a|^4+2|a|^2|b|^2+|b|^4\Big) = \frac{2}{3}(|a|^2+|b|^2)^2 = \frac{2}{3}$$

As a consequence, we see that for any input vector the map T will generate a pair that will succeed in a cloned measurement with probability $\frac{2}{3}$.

(e) We follow the hint. In particular, we will consider states that are maximally separated on the Bloch sphere. Such a configuration leads us directly to the idea that our four alternative states should be the vertices of the largest (and in fact only) regular tetrahedron inscribed within the Bloch sphere. Furthermore, intuitively this seems to already have better geometric properties than Wiesner's original scheme: The mixed states spanned by these four states span a volume inside the Bloch ball similar to our six state scheme, while Wiesner's only spanned a two dimensional slice of the Bloch ball. Additionally, it is significant to note that the orthogonal states in Wiesner's scheme did not play a large role; the significance in hiding the information laid in mixing between the Hadamard basis and the computational one. However, no significance was given to whether the encoding was $|0\rangle$ or $|1\rangle$, in fact we could see this as a weakening of the security because it allowed us to get away with copying 'two types' of money encodings with only one basis measurement. Notice that the tetrahedral arrangement has no such orthogonal basis encodings; in this it even beats our 6 state encoding scheme from before. Namely, to succeed with probability 1 every single qubit needs its own measurement basis. This provides some intuitive support that the tetrahedral scheme should be somewhat more secure than Wiesner's, yet still no true hard evidence. To get hard evidence two proof approaches are possible. Firstly, we can use the semidefintie duality based method seen in class, and this will yield the right bound. Secondly, we can use symmetries of the money scheme to conclude that any adversary's cloning map must respect the same symmetries, and eventually deduce sufficiently many constraints that the map can be fully characterized and shown to equal (be equivalent to) the "optimal cloner" from the previous question.