COM-440, Introduction to Quantum Cryptography, Fall 2025

Homework # 1 **due: 12:59PM, October 8th, 2019**

Ground rules:

Please format your solutions so that each problem begins on a new page, and so that your name appears at the top of each page.

You are encouraged to collaborate with your classmates on homework problems, but each person must write up the final solutions individually. You should note on your homework specifically which problems were a collaborative effort and with whom. You may not search online for solutions, but if you do use research papers or other sources in your solutions, you must cite them.

Late homework will not be accepted or graded. Extensions will not be granted, except on the recommendation of a dean. We will grade as many problems as possible, but sometimes one or two problems will not be graded. Your lowest homework grade of the semester will be dropped from your final grade.

Problems:

1. **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 optimum is achieved for $\alpha = \beta = \frac{1}{\sqrt{2}}$.

   (c) No... The success probability is the same: 5/8.

2. (12 points) **Improving Wiesner's quantum money.**

0.1

This boils down to an involved 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;

(a) $|\langle\psi_1|\langle\psi_1|U|\psi_1\rangle|0\rangle|^2 = |\langle 0|\langle 0||0\rangle|0\rangle|^2 = |\langle 0||0\rangle \otimes \langle 0||0\rangle|^2 = 1$

(b) $|\langle\psi_2|\langle\psi_2|U|\psi_2\rangle|0\rangle|^2 = |\langle 1|\langle 1||1\rangle|1\rangle|^2 = |\langle 1||1\rangle \otimes \langle 1||1\rangle|^2 = 1$

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

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

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

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

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;

$$B = H \otimes H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix} \otimes \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix},\ \det(H)^2\det(H)^2 = \Big(\frac{-1-1}{\sqrt{2}^2}\Big)^4 = 1$$

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

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

$$= \sum_{k=1}^{6}\frac{1}{6}\Big|\big(\langle\psi_k|H\otimes\langle\psi_k|H\big)U\big(H|\psi_k\rangle\otimes H|+\rangle\big)\Big|^2$$

In fact, H will permute 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

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

Since addition is commutative and thus permutation invariant.

0.2

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;

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

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

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

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

$$\langle 0|\langle 00|V^\dagger V|0\rangle|00\rangle = \Big(\frac{2}{\sqrt{6}}\langle 00|\langle 0| + \frac{1}{\sqrt{3}}\langle\phi^-|\langle 1|\Big)\Big(\frac{2}{\sqrt{6}}|00\rangle|0\rangle + \frac{1}{\sqrt{3}}|\phi^-\rangle|1\rangle\Big) = 4/6{+}1/3 = 1$$

Thus, V's conditions are all satisfied.

0.3

We first describe the three steps that will 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 now check that these operations reproduce our desired behavior of T on the density matrices $|0\rangle\langle 0|, |1\rangle\langle 1|, |+\rangle\langle +|$, and $|-\rangle\langle -|$.

(a) $T(|0\rangle\langle 0|)$:

$$\sum_x \mathbb{I}\otimes\langle u_x|\big(V|0\rangle|00\rangle\langle 0|\langle 00|V^\dagger\big)\mathbb{I}\otimes|u_x\rangle =$$

$$= \sum_x \mathbb{I}\otimes\langle u_x|\Big(\frac{2}{\sqrt{6}}|00\rangle|0\rangle + \frac{1}{\sqrt{3}}|\phi^-\rangle|1\rangle\Big)\Big(\frac{2}{\sqrt{6}}\langle 00|\langle 0| + \frac{1}{\sqrt{3}}\langle\phi^-|\langle 1|\Big)\mathbb{I}\otimes|u_x\rangle =$$

$$= \sum_x \Big(\frac{2}{\sqrt{6}}\mathbb{I}\otimes\langle u_x|00\rangle|0\rangle + \frac{1}{\sqrt{3}}\mathbb{I}\otimes\langle u_x|\phi^-\rangle|1\rangle\Big)\Big(\frac{2}{\sqrt{6}}\langle 00|\langle 0|\mathbb{I}\otimes|u_x\rangle + \frac{1}{\sqrt{3}}\langle\phi^-|\langle 1|\mathbb{I}\otimes|u_x\rangle\Big) =$$

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

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

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

$$= \Big(\frac{2}{\sqrt{6}}\,|00\rangle\Big)\Big(\frac{2}{\sqrt{6}}\,\langle 00|\Big)+\Big(\frac{1}{\sqrt{3}}\,|\phi^-\rangle\Big)\Big(\frac{1}{\sqrt{3}}\,\langle\phi^-|\Big) = \frac{2}{3}\,|00\rangle\langle 00|+\frac{1}{3}\,|\phi^-\rangle\langle\phi^-| = \rho_0$$

(b) $T(|1\rangle\langle 1|)$:

$$\sum_x \mathbb{I}\otimes\langle u_x|\,\big(V\,|1\rangle\,|00\rangle\langle 1|\,\langle 00|\,V^\dagger\big)\mathbb{I}\otimes|u_x\rangle =$$

$$= \sum_x \mathbb{I}\otimes\langle u_x|\,\Big(\frac{1}{\sqrt{3}}\,|\phi^-\rangle\,|0\rangle+\frac{2}{\sqrt{6}}\,|11\rangle\,|1\rangle\Big)\Big(\frac{1}{\sqrt{3}}\,\langle\phi^-|\,\langle 0|+\frac{2}{\sqrt{6}}\,\langle 11|\,\langle 1|\Big)\mathbb{I}\otimes|u_x\rangle =$$

$$= \sum_x \Big(\frac{1}{\sqrt{3}}\mathbb{I}\otimes\langle u_x|\,|\phi^-\rangle\,|0\rangle+\frac{2}{\sqrt{6}}\mathbb{I}\otimes\langle u_x|\,|11\rangle\,|1\rangle\Big)\Big(\frac{1}{\sqrt{3}}\,\langle\phi^-|\,\langle 0|\,\mathbb{I}\otimes|u_x\rangle+\frac{2}{\sqrt{6}}\,\langle 11|\,\langle 1|\,\mathbb{I}\otimes|u_x\rangle\Big) =$$

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

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

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

$$= \Big(\frac{1}{\sqrt{3}}\,|\phi^-\rangle\Big)\Big(\frac{1}{\sqrt{3}}\,\langle\phi^-|\Big)+\Big(\frac{2}{\sqrt{6}}\,|11\rangle\Big)\Big(\frac{2}{\sqrt{6}}\,\langle 11|\Big) = \frac{1}{3}\,|\phi^-\rangle\langle\phi^-|+\frac{2}{3}\,|11\rangle\langle 11| = \rho_1$$

(c) $T(|+\rangle\langle +|)$:

We first consider $V\,|+\rangle\,|00\rangle$ to simplify some of the following calculations. Denoting $M_1 = 2\,|00\rangle+\sqrt{2}\,|\phi^-\rangle$ and $M_2 = 2\,|11\rangle+\sqrt{2}\,|\phi^-\rangle$, observe that we can match the components that are tensored with the same C qubit,

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

$$= \frac{1}{\sqrt{12}}\Big(M_1\otimes|0\rangle+M_2\otimes|1\rangle\Big)$$

Yielding, just as above

$$\sum_x \mathbb{I}\otimes\langle u_x|\,\big(V\,|+\rangle\,|00\rangle\langle +|\,\langle 00|\,V^\dagger\big)\mathbb{I}\otimes|u_x\rangle =$$

$$= \frac{1}{12}\Big(M_1 \otimes \langle 0\rangle\, 0 M_1^\dagger \otimes \langle 0\rangle\, 0 + M_2 \otimes \langle 1\rangle\, 1 M_2^\dagger \otimes \langle 1\rangle\, 1\Big) = \frac{1}{12}\Big(M_1 M_1^\dagger + M_2 M_2^\dagger\Big) =$$

$$= \frac{1}{12}\Big((2\,|00\rangle + \sqrt{2}\,|\phi^-\rangle)(2\,\langle 00| + \sqrt{2}\,\langle\phi^-|) + (2\,|11\rangle + \sqrt{2}\,|\phi^-\rangle)(2\,\langle 11| + \sqrt{2}\,\langle\phi^-|)\Big) = \rho_+$$

(d) $T(|-\rangle\langle -|)$:

Surprisingly, we make a similar calculation to the above. Note well the carried sign difference; Denoting $M_1 = 2\,|00\rangle - \sqrt{2}\,|\phi^-\rangle$ and $M_2 = 2\,|11\rangle - \sqrt{2}\,|\phi^-\rangle$, observe that we can again match the components that are tensored with the same C qubit,

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

$$= \frac{1}{\sqrt{12}}\Big(M_1 \otimes |0\rangle + M_2 \otimes |1\rangle\Big)$$

Yielding, just as above

$$\sum_x \mathbb{I} \otimes \langle u_x|\left(V\,|-\rangle\,|00\rangle\,\langle -|\,\langle 00|\,V^\dagger\right)\mathbb{I} \otimes |u_x\rangle =$$

$$= \frac{1}{12}\Big(M_1 \otimes \langle 0\rangle\, 0 M_1^\dagger \otimes \langle 0\rangle\, 0 + M_2 \otimes \langle 1\rangle\, 1 M_2^\dagger \otimes \langle 1\rangle\, 1\Big) = \frac{1}{12}\Big(M_1 M_1^\dagger + M_2 M_2^\dagger\Big) =$$

$$= \frac{1}{12}\Big((2\,|00\rangle - \sqrt{2}\,|\phi^-\rangle)(2\,\langle 00| - \sqrt{2}\,\langle\phi^-|) + (2\,|11\rangle - \sqrt{2}\,|\phi^-\rangle)(2\,\langle 11| - \sqrt{2}\,\langle\phi^-|)\Big) = \rho_-$$

Thus, all of the requirements for T are satisfied.

0.4

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,

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

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

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

We now determine the action of T on $|1\rangle\langle 0|$ and it's 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

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

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

We now trace out C, which yields the following,

$$T(\left|1\right\rangle\left\langle 0\right|) = \mathrm{Tr}_C\bigg(\Big(\frac{1}{\sqrt{3}}\left|\phi^-\right\rangle_{AB}\left|0\right\rangle_C+\frac{2}{\sqrt{6}}\left|11\right\rangle_{AB}\left|1\right\rangle_C\Big)\Big(\frac{2}{\sqrt{6}}\left|00\right\rangle_{AB}\left|0\right\rangle_C+\frac{1}{\sqrt{3}}\left|\phi^-\right\rangle_{AB}\left|1\right\rangle_C\Big)^\dagger\bigg) =$$

$$= (\mathbb{I}_{AB}\otimes\left\langle 0\right|_C)\Big(\frac{1}{\sqrt{3}}\left|\phi^-\right\rangle_{AB}\left|0\right\rangle_C+\frac{2}{\sqrt{6}}\left|11\right\rangle_{AB}\left|1\right\rangle_C\Big)\Big(\frac{2}{\sqrt{6}}\left|00\right\rangle_{AB}\left|0\right\rangle_C+\frac{1}{\sqrt{3}}\left|\phi^-\right\rangle_{AB}\left|1\right\rangle_C\Big)^\dagger(\mathbb{I}_{AB}\otimes\left|0\right\rangle_C)$$

$$+(\mathbb{I}_{AB}\otimes\left\langle 1\right|_C)\Big(\frac{1}{\sqrt{3}}\left|\phi^-\right\rangle_{AB}\left|0\right\rangle_C+\frac{2}{\sqrt{6}}\left|11\right\rangle_{AB}\left|1\right\rangle_C\Big)\Big(\frac{2}{\sqrt{6}}\left|00\right\rangle_{AB}\left|0\right\rangle_C+\frac{1}{\sqrt{3}}\left|\phi^-\right\rangle_{AB}\left|1\right\rangle_C\Big)^\dagger(\mathbb{I}_{AB}\otimes\left|1\right\rangle_C)$$

$$= \Big(\frac{1}{\sqrt{3}}(\mathbb{I}_{AB}\otimes\left\langle 0\right|_C)\left|\phi^-\right\rangle_{AB}\left|0\right\rangle_C+\frac{2}{\sqrt{6}}(\mathbb{I}_{AB}\otimes\left\langle 0\right|_C)\left|11\right\rangle_{AB}\left|1\right\rangle_C\Big)\Big(\frac{2}{\sqrt{6}}\left\langle 00\right|_{AB}\left\langle 0\right|_C(\mathbb{I}_{AB}\otimes\left|0\right\rangle_C)+\frac{1}{\sqrt{3}}\left\langle\phi^-\right|_A$$

$$+\Big(\frac{1}{\sqrt{3}}(\mathbb{I}_{AB}\otimes\left\langle 1\right|_C)\left|\phi^-\right\rangle_{AB}\left|0\right\rangle_C+\frac{2}{\sqrt{6}}(\mathbb{I}_{AB}\otimes\left\langle 1\right|_C)\left|11\right\rangle_{AB}\left|1\right\rangle_C\Big)\Big(\frac{2}{\sqrt{6}}\left\langle 00\right|_{AB}\left\langle 0\right|_C(\mathbb{I}_{AB}\otimes\left|1\right\rangle_C)+\frac{1}{\sqrt{3}}\left\langle\phi^-\right|_{AB}$$

$$= \Big(\frac{1}{\sqrt{3}}\left|\phi^-\right\rangle_{AB}\Big)\Big(\frac{2}{\sqrt{6}}\left\langle 00\right|_{AB}\Big)+\Big(\frac{2}{\sqrt{6}}\left|11\right\rangle_{AB}\Big)\Big(\frac{1}{\sqrt{3}}\left\langle\phi^-\right|_{AB}\Big) = \frac{\sqrt{2}}{3}\Big(\left|\phi^-\right\rangle\left\langle 00\right|+\left|11\right\rangle\left\langle\phi^-\right|\Big)$$

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

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

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

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

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

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

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

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

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

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

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

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

Finally, we compute the last term,

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

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

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 be succeed in a cloned measurement with probability $\frac{2}{3}$. Quite surprising!

0.5

We begin by following the hint. In particular, we will consider states that are maximally separated on the Bloch sphere. In particular, 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 (which is perhaps why it gets the same optimal attack error probability and saves on qubits). Namely, to succeed with probability 1 every single qubit needs it's own measurement basis! Thus, this provides some intuitive support that the tetrahedral scheme should be somewhat more secure than Wiesner's, yet still no true hard evidence. So, the important features of the scheme seem to be that it's mixed states span a nondegenerate part of the bloch sphere and that each qubit must have it's own unique basis to be verified in. An further interesting effect is that at every vertex of the tetrahedron can be 'copied' with probability 2/3 (imagine averaging

all possible conjugations of the quantum map with the unitaries corresponding to the finite symmetries of the tetrahedron).

From here, we follow the intuition for the previous map T, as discussed in the lecture notes (chapter 2). Specifically, notice that the map T could be expressed as a projection of a mixed state onto the symmetric subspace of $\mathbb{C}^4$. The reason why this is significant is that all pairs $|\psi\rangle |\psi\rangle$ must necessarily lie in this symmetric subspace, so we wish to get our transformed qubits as close to it as possible. Thus, the following definition follows;

$$T(\rho) = \Pi_S(\rho \otimes \frac{1}{2}\mathbb{I})\Pi_S$$

where Π_S constitutes the projection onto the symmetric subspace. Note that we first generate a 'mixed pair,' in order to hopefully project out two correct copies (though of course there will be a probability that we project out incorrect copies). Notice though that such an attack must be optimal, as long as we limit the projection onto the symmetric subspace that also intersects the subspace of possible pairs. Since Wiesner's pair space was degenerate (corresponding to a flat slice through the bloch ball), we were able to restrict the space of the projection and do better. However, with the tetrahedron such an improvement is not possible due to it's non-degenerate intersection, and it will simply achieve the general optimal projection effect that the six state scheme did.