Problem 1

Consider the encryption defined using the secret key $k = a$ as follows. If the input state is $\rho_\psi = |\psi\rangle\langle\psi|$, then

$$\text{Enc}_a(\rho_\psi) = H^a \rho_\psi H^a$$
$$\text{Dec}_a(\rho_\psi) = H^a \rho_\psi H^a.$$

(a) Check the encryption scheme satisfies correctness.

\textbf{Solution.} For correctness we need to check that $\text{Dec}_k(\text{Enc}_k(\rho_\psi)) = \rho_\psi$ for any input state $\rho_\psi$. In our case we have that

$$\text{Dec}_a(\text{Enc}_a(\rho_\psi)) = H^a (H^a \rho_\psi H^a) H^a = (H^2)^a \rho_\psi (H^2)^a = I \rho_\psi I = \rho_\psi.$$

(b) Which are the possible encryptions for the following two quantum states.

i. $|\psi_1\rangle = |0\rangle$.

\textbf{Solution.} The input state is $\rho_{\psi_1} = |0\rangle\langle 0|$. If $a = 0$ then $\text{Enc}_a(\rho_{\psi_1}) = H^0 \rho_{\psi_1} H^0 = |0\rangle\langle 0|$. If $a = 1$ then $\text{Enc}_a(\rho_{\psi_1}) = H^1 \rho_{\psi_1} H^1 = H |0\rangle\langle 0| H = |+\rangle\langle +|.$

ii. $|\psi_2\rangle = \frac{1}{\sqrt{1+(\sqrt{2}-1)^2}} \left(|0\rangle + (\sqrt{2} - 1) |1\rangle\right)$.

\textbf{Solution.} The input state is

$$\rho_{\psi_2} = \frac{1}{1 + (\sqrt{2} - 1)^2} \left(|0\rangle + (\sqrt{2} - 1) |1\rangle\right) \left(|0\rangle + (\sqrt{2} - 1) |1\rangle\right)^\dagger.$$

If $a = 0$ then $\text{Enc}_a(\rho_{\psi_1}) = H^0 \rho_{\psi_2} H^0 = \rho_{\psi_2}$. For $a = 1$, first notice that $|\psi_2\rangle$ remains invariant when applying $H$. That is, $H |\psi_2\rangle = |\psi_2\rangle$. Thus, if $a = 1$ then $\text{Enc}_a(\rho_{\psi_1}) = H^1 \rho_{\psi_1} H^1 = H |\psi_2\rangle\langle \psi_2| H = |\psi_2\rangle\langle \psi_2| = \rho_{\psi_2}$.

(c) What are the average ciphertexts $\rho_E(\psi_1)$ and $\rho_E(\psi_2)$?

\textbf{Solution.} The average ciphertexts can be written using part (b) as

$$\rho_E(\psi_1) = \frac{1}{2} \sum_{a \in \{0,1\}} H^a \rho_{\psi_1} H^a = \frac{1}{2} (|0\rangle\langle 0| + |+\rangle\langle +|),$$

$$\rho_E(\psi_2) = \frac{1}{2} \sum_{a \in \{0,1\}} H^a \rho_{\psi_2} H^a = \frac{1}{2} (\rho_{\psi_2} + \rho_{\psi_2}) = \rho_{\psi_2} = |\psi_2\rangle\langle \psi_2|.$$

(d) Compute the fidelity of $\rho_E(\psi_1)$ and $\rho_E(\psi_2)$.

\textbf{Solution.} Because $\rho_E(\psi_2) = |\psi_2\rangle\langle \psi_2|$ is a pure state, we can use the simplified expression
Consider the Regev public-key cryptosystem with the parameters $q = 17$ and $n = 4$. The private key is defined as $s = (0, 13, 9, 11)$ and the public key is defined by $m = 4$ LWE samples

\[
(a_1 = (14, 15, 5, 2), b_1 = 8), \\
(a_2 = (13, 14, 14, 6), b_2 = 16), \\
(a_3 = (6, 10, 13, 1), b_3 = 3), \\
(a_4 = (9, 5, 9, 6), b_4 = 9).
\]

(a) What is the encryption $(a, c)$ for the message $\mu = 1$ if we pick the set $S = \{2, 4\}$?

**Solution.** To encrypt the message $\mu$, we first compute

\[
a = \sum_{i \in S} a_i = a_2 + a_4 = (13, 14, 14, 6) + (9, 5, 9, 6) = (22, 19, 23, 12), \\
b = \sum_{i \in S} b_i = b_2 + b_4 = 16 + 9 = 25.
\]
Now we take $a$ and $b$ modulo $q$ and we get $a = (5, 2, 6, 12)$ and $b = 8$. Finally,

$$c = b + \mu \cdot \left\lfloor \frac{q}{2} \right\rfloor = 8 + 1 \cdot 8 = 16.$$ 

Therefore, the ciphertext is $\text{Enc}(\mu) = (a, c) = ((5, 2, 6, 12), 16)$.

(b) Decrypt $(a, c)$ to verify the correctness of the cryptosystem.

Solution. To decrypt $\text{Enc}(\mu) = (a, c)$ using the secret key $s$ we first compute

$$\langle a, s \rangle = 5 \cdot 0 + 2 \cdot 13 + 6 \cdot 9 + 12 \cdot 11 = 212.$$ 

Next, we compute

$$\langle a, s \rangle - c \equiv 212 - 16 \pmod{q}$$

$$\equiv 196 \pmod{q}$$

$$\equiv 196 \pmod{17}$$

$$\equiv 9 \pmod{17}.$$ 

Finally, we observe that this quantity is closer to $\left\lfloor \frac{q}{2} \right\rfloor = 8$ than to 0, and so we conclude that $\mu = 1$. 