Question 2

(1)

Recall in the IND-CPA security proof, we defined three games:

1. Game 0 is the standard IND-CPA game for Module-LWE
2. Game 1 is identical to game 0, except in key generation, $\mathbf{b} = A\mathbf{s} + \mathbf{e}$ is replaced with a uniformly random sample $\mathbf{b} \leftarrow R_q^k$
3. Game 2 is identical to game 1, except the challenge ciphertexts are replaced with uniformly random samples $\mathbf{c}_1^* \leftarrow R_q^k, c_2^* \leftarrow R_q$

Further more, we defined two solvers for Module-decisional-LWE: solver 1 solves dLWE with $A \in R_q^{k\times k}$ and solver 2 solves dLWE with $A \in R_q^{(k+1)\times k}$.

Solver 2 decomposes $A, \mathbf{b}$ into the first k rows and the last row: $A = [A_1 \in R_q^{k\times k}, A_2 \in R_q^{1\times k}]$, $\mathbf{b} = [\mathbf{b}_1 \in R_q^k, b_2 \in R_q]$. A_1, A_2 is given to the IND-CPA adversary as the public key, and $\mathbf{c}_1^* = \mathbf{b}_1, c_2^* = b_2 + m\lfloor \frac{q}{2} \rceil$ as the challenge ciphertext. If Solver 2 receives LWE sample, then the IND-CPA adversary is playing game 1; if solver 2 receives truly random sample, then IND-CPA adversary is playing game 2. Therefore, the advantage of solver 2 is $\frac{1}{2}(\text{adv}_1 - \text{adv}_2)$

If in the encryption routine, the second error term e'' is removed, then $c_2^* = b_2 + m\lfloor \frac{q}{2} \rceil = A_2\mathbf{s} + e_2 + m\lfloor \frac{q}{2} \rceil$ is no longer a valid encryption of m. This means that when $A, \mathbf{b}$ is a LWE sample, the IND-CPA adversary is not playing game 1, but a new game that is identical to game 1 but with the second error term in the encryption routine. Denote the IND-CPA adversary's advantage in this game by adv_3.

Following the same procedure as in the IND-CPA security proof, we can show that:

$$\text{Adv in solving dLWE}(R_q^{k\times k}) + \text{Adv in solving dLWE}(R_q^{k+1\times k}) = \frac{1}{2}(\text{adv}_0 - \text{adv}_1) + \frac{1}{2}(\text{adv}_3 - \text{adv}_2)$$

Knowing that game 2 is unwinnable and that solving dLWE with higher dimension is harder, we can rearrange the equation above:

$$\text{adv}_0 \geq 4 \cdot \text{adv}_{\text{dLWE(k)}} + (\text{adv}_1 - \text{adv}_3)$$

It's possible that $\text{adv}_1 - \text{adv}_3$ is non-negligible, so adv_0 might be non-negligible, thus breaking IND-CPA security of the modified encryption routine.

(2)

Observe that when $m = \mathbf{0} \in R_{\{0,1\}}$, $c_2 = \mathbf{r}^\intercal \mathbf{b}$ is divisible by $\mathbf{b}$. On the other hand, if m is non-zero, then with very high probability, c_2 will not be divisible by $\mathbf{b}$.

Thus, an IND-CPA can challenge plaintexts as follows: $m_0 = \mathbf{0}$, m_1 is some arbitrary non-zero polynomial. Upon receiving the challenge ciphertext c^*, check if c_2 is divisible by $\mathbf{b}$ (which is part of the public key and hence accessible). If yes, then c^* is the encryption of m_0; otherwise c^* is the encryption of m_1.