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)

When the second error term e'' is omitted, in the IND-CPA RLWE encryption scheme, the second part of each ciphertext is:

$$c_2 = rb + m\lfloor\frac{q}{2}\rceil$$

Assuming that b is an invertible polynomial in $R_q = \mathbb{Z}_q/\langle p(x)\rangle$, an adversary who knows m can recover r:

$$r = (c_2 - m\lfloor\frac{q}{2}\rceil)b^{-1}$$

Where $m = 0$ is the zero polynomial, then $c_2 b^{-1} = r$ must have small coefficients. On the other hand, assuming that decisional RLWE holds, b is computationally indistinguishable from truly random, which implies that b^{-1} is also computationally indistinguishable from truly random. Therefore, it is safe to assume that it is easy to find some $m \in R_{\{0,1\}}$ such that $m\lfloor\frac{q}{2}\rceil b^{-1}$ has coefficients that are outside the bound of the secret distribution χ_s.

From here, the IND-CPA adversary proceeds as follows. Pick $m_0 = 0$, and m_1 such that $m_1\lfloor\frac{q}{2}\rceil b^{-1}$ has large coefficients. Upon receving the challenge ciphertext $c^* = (c_1^*, c_2^*)$, compute $c_2^* b^{-1}$. Where m_0 is chosen by the challenger, $c_2^* b^{-1}$ will have small coefficients. Where m_1 is chosen by the challenger, then $c_2^* b^{-1}$ will have large coefficients.