Q10

Recall from textbook LWE the decryption routine:

$$\begin{aligned} D(\text{sk}, (\mathbf{c}_1, c_2)) &= c_2 - \mathbf{c}_1\mathbf{s} \\ &= (\mathbf{s}_1^\intercal \mathbf{b} + e' + m\lfloor\frac{q}{2}\rceil) - (\mathbf{s}_1^\intercal A\mathbf{s} + \mathbf{e}_1^\intercal \mathbf{s}) \\ &= (\mathbf{s}_1^\intercal (A\mathbf{s} + \mathbf{e}) + e' + m\lfloor\frac{q}{2}\rceil) - (\mathbf{s}_1^\intercal A\mathbf{s} + \mathbf{e}_1^\intercal \mathbf{s}) \\ &= \mathbf{s}_1^\intercal \mathbf{e} + e' + m\lfloor\frac{q}{2}\rceil - \mathbf{e}_1^\intercal \mathbf{s} \\ &= (\mathbf{s}_1^\intercal \mathbf{e} - \mathbf{e}_1^\intercal \mathbf{s}) + e' + m\lfloor\frac{q}{2}\rceil \end{aligned}$$

Also recall the definition of the rounding operator: $\lfloor a \rceil = a + \delta$ for some $-\frac{1}{2} \leq \delta < \frac{1}{2}$.

(1)

Where $\mathbf{e}_1$ is maliciously set to all zeros except for the i-th component, $\mathbf{e}_1^\intercal \mathbf{s}$ evaluates to $s_i \cdot \lfloor\frac{q}{2}\rceil$, where s_i is the i-th component of the LWE secret $\mathbf{s}$.

If $s_i = 2k$ is even, then

$$\begin{aligned} D(\text{sk}, (\mathbf{c}_1, c_2)) &= (\mathbf{s}_1^\intercal \mathbf{e} - \mathbf{e}_1^\intercal \mathbf{s}) + e' + m\lfloor\frac{q}{2}\rceil \\ &= \mathbf{s}_1^\intercal \mathbf{e} + e' - 2k(\frac{q}{2} + \delta) + m\lfloor\frac{q}{2}\rceil \\ &\equiv \mathbf{s}_1^\intercal \mathbf{e} + e' - 2k\delta + m\lfloor\frac{q}{2}\rceil \end{aligned}$$

Thus, where k is sufficiently small (corresponding to s_i being small), $\mathbf{s}_1^\intercal \mathbf{e} + e' + 2k\delta$ has a high probability of being less than $\frac{q}{4}$, so the ciphertext will be correctly decrypted.

If $s_i = 2k + 1$ is odd, then

$$\begin{aligned} D(\text{sk}, (\mathbf{c}_1, c_2)) &= (\mathbf{s}_1^\intercal \mathbf{e} - \mathbf{e}_1^\intercal \mathbf{s}) + e' + m\lfloor\frac{q}{2}\rceil \\ &= \mathbf{s}_1^\intercal \mathbf{e} + e' + (2k+1)\lfloor\frac{q}{2}\rceil + m\lfloor\frac{q}{2}\rceil \\ &\equiv \mathbf{s}_1^\intercal \mathbf{e} + e' + 2k\delta + \lfloor\frac{q}{2}\rceil + m\lfloor\frac{q}{2}\rceil \end{aligned}$$

Notice the additional $\lfloor\frac{q}{2}\rceil$ term in the R.H.S., which will cause decryption to be incorrect with high probability. Thus, with high probability, decryption will be correct if and only if s_i is even.

(2)

Eve can recover the parity of all entries of the secret $\mathbf{s} \in \chi_s^n$ by preparing n emails $\{(\mathbf{c}_{(i,1)}, c_{(i,2)})\}_{i=1}^n$ where $(\mathbf{c}_{(i,1)}, c_{(i,2)})$ is generated using the procedure described in part (1): $\mathbf{e}_{(i,1)}$ is all 0's except for the i-th entry, which is set to $\lfloor\frac{q}{2}\rceil$. For each of these n emails, Eve sends it to Alice's server and receives the auto-response. The quoted email in the auto-response is checked against the original email: if they are identical, then Alice's server correctly decrypted Eve's email, so the corresponding entry in $\mathbf{s}$ is even; otherwise, the corresponding entry in $\mathbf{s}$ is odd.

(3)

We will describe an algorithm for recovering the value of a single component of the secret key $\mathbf{s}$. From here, the algorithm can be repeated n times to recover the value of all components of the secret key. If the algorithm for recovering a single value is efficient, then repeating it n times is also efficient.

Consider the ciphertext $(\mathbf{c}_1, c_2)$ where all entries of $\mathbf{c}_1$ is set to 0 except for the i-th entry, which we denote by $\mathbf{c}_{(1,i)}$. Recall from the decryption procedure the fact that decryption outputs 0 if and only if $-\lfloor \frac{q}{4} \rceil \leq m' \leq \lfloor \frac{q}{4} \rceil$, which is equivalent to:

$$-\lfloor \frac{q}{4} \rceil + c_2 \leq c_{(1,i)} \cdot s_i \leq \lfloor \frac{q}{4} \rceil + c_2$$

Where s_i is the i-th entry of the secret $\mathbf{s}$.

In other words, we can check whether s_i falls within a certain range of values given some values of c_2 and $c_{(1,i)}$. In addition, changing the value of c_2 will translate the range, while changing the value of $c_{(1,i)}$ will scale the range. Thus, we can perform a binary search by adjusting the values of $c_2, c_{(1,i)}$ and pinpoint the value of s_i in $O(\log q)$ steps.

(4)

Converting textbook LWE to be resistant to chosen-ciphertext attack is non-trivial. In Kyber/Dilithium a tweaked version of Fujisaki-Okamoto transformation is applied to the textbook LWE to obtain a CCA2-secure cryptosystem. Due to time constraint, the details will not be covered in this write-up.