Q1

(1)

The probability formula will be proved by induction. The base case is trivial: an empty set is always linearly independent, so the probability of drawing a linearly independent empty set is exactly 1.

For the induction, assume that $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_{t-1} \in \mathbb{F}_q^n$ are linearly independent, then consider the probability of drawing a t-th vector uniformly from $\mathbb{F}_q^n$ such that it is not in the linear span of the previous $t-1$ vectors: $\mathbf{a}_t \notin \text{Span}(\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_{t-1})$.

There are a total of q^n possible values for $\mathbf{a}_t$ to draw from. On the other hand, there are a total of q^{t-1} possible combinations of coefficients (including all zeros) for $t-1$ vectors. Singe $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_{t-1}$ are linearly independent, each unique combination of coefficients corresponds to a unique element in the linear span. Thus, there are a total of $q^n - q^{t-1}$ possible values that are outside the linear span of $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_{t-1}$, and the probability of uniformly drawing a $\mathbf{a}_t$ that's outside the linear span is $1 - \frac{q^{t-1}}{q^n}$.

In other words:

$$P(\mathbf{a}_t \notin \text{Span}(\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_{t-1}) \mid \{\mathbf{a}_i\}_{i=1}^{t-1} \text{ is linearly independent}) = 1 - q^{t-1-n}$$

From here, we can recursively compute the probability of drawing m linearly independent vectors:

$$\begin{aligned}
&P(\{\mathbf{a}_i\}_{i=1}^{m} \text{ is linearly independent}) \\
&= \prod_{j=0}^{m-1} P(\mathbf{a}_{j+1} \notin \text{Span}(\{\mathbf{a}_i\}_{i=1}^{j}) \mid \{\mathbf{a}_i\}_{i=1}^{j} \text{ is linearly independent}) \\
&= \prod_{j=0}^{m-1} (1 - q^{(j+1)-1-n}) \\
&= \prod_{j=0}^{m-1} (1 - q^{j-n})
\end{aligned}$$

(2)

We will bound the probability formula above from below by bounding each $1 - q^{j-n}$ term:

$$\forall 0 \le j < n,\ 1 - q^{j-n} \ge 1 - q^{-n}$$

And since $m = n \le 1024$, we have $1 - q^n \le 1 - q^{1024}$

Thus:

$$\begin{aligned}
&P(\{\mathbf{a}_i\}_{i=1}^{m} \text{ is linearly independent}) \\
&= \prod_{j=0}^{m-1} (1 - q^{j-n}) \\
&\ge \prod_{j=0}^{m-1} (1 - q^{-n}) \\
&\ge \prod_{j=0}^{1024-1} (1 - q^{-1}) \\
&= (1 - 3329^{-1})^{1024} \approx 0.7351 > \frac{2}{3}
\end{aligned}$$

(3)

For Kyber-512, the parameters are defined with $n = 256, q = 3329$. Plugging them into the formula:

```
from sympy import Rational

if __name__ == "__main__":
    q = 3329
    n = 256
    prod = 1
    for i in range(n):
        prod *= 1 - Rational(q) ** (i - n)
    print(f"Prob is {prod.evalf()}")
```

The result is 0.999699519257883

Q2

Where $m \leq n$, if $A \in \mathbb{F}_q^{m \times n}$ is full rank, then the columns of A span $\mathbb{F}_q^m$. Since $\mathbf{s} \leftarrow \mathbb{Z}_q^n$ is uniformly sampled, it naturally follows that $A\mathbf{s}$ is uniformly distributed across $\mathbb{F}_q^m$. As a result, $\mathbf{b} \leftarrow A\mathbf{s} + \mathbf{e}$ is uniformly distributed across $\mathbb{F}_q^m$ regardless of the choice of distribution of $\mathbf{e} \leftarrow \chi_e^m$, and the LWE samples are identically distributed as uniform random noise. Thus, when $m \leq n$, A is full rank, $\mathbf{s}$ is uniformly random, decisional-LWE is information-theoretically hard.

Q3

Recall that a centered binomial distribution is a binomial distribution left-shifted by its mean. Let $X \leftarrow \mathcal{B}(n,p)$ be some binomial distribution, then the centered binomial distribution is described by $Y = X - E[X]$:

$$P[Y=y] = P[X = y+\mu] = C(n, y+\mu)p^{y+\mu}(1-p)^{n-y-\mu}$$

(1)

The probability mass function (PMF) of a centered binomial distribution $X \leftarrow \mathcal{B}(n=6, p=0.5)$ is given by:

$$P(X=x) = \binom{n}{x+np} p^{x+np}(1-p)^{n-x-np} = \binom{6}{x+3} 2^{-6}$$

On the other hand, the PMF of a discrete Gaussian with $N(\mu = 3, \sigma^2 = \frac{3}{2})$ is given by:

$$P(X=x) = \frac{\rho(x)}{\sum_{j=0}^{q-1}\rho(y)}$$

I used some Python code to approximate the statistical distance:

```
import math

KYBER_Q = 3329

def centered_bin_pmf(val, n, p):
    if not (0 <= val + n * p <= n):
        return 0
    return (
        math.comb(n, int(val + n * p))
        * (p ** (val + n * p))
        * ((1-p) ** (n - val - n * p))
    )

def rho(val, mu, var):
    return math.exp(-(val - mu) ** 2 / (2 * var))

def dgaus(val, mu , var):
    return rho(val, mu, var) / sum(
        [rho(y, mu, var) for y in range(-KYBER_Q // 2, KYBER_Q // 2 + 1)]
    )

if __name__ == "__main__":
    n, p = 6, 0.5
    mu, var = 0, n * p * (1-p)
    dist = 0
    for val in range(
        math.ceil(mu - KYBER_Q / 2),
        math.ceil(mu + KYBER_Q / 2),
    ):
        lhs = centered_bin_pmf(val, n, p)
        rhs = dgaus(val, mu, var)
        dist += 0.5 * abs(lhs - rhs)
    print(dist)
```

The result is 0.017725703977230414.

(2)

I claim without proof that the most likely error $\mathbf{s} \leftarrow \chi_e^m$, is obtained by sampling the most likely value for each of the entry in. Assuming individual entries of $\mathbf{s}$ are independently sampled from identical distribution χ_e (a centered binomial distribution), the most likely value for a single entry is 0. Therefore, the most likely secret is $\mathbf{s} = \mathbf{0} \in \mathbb{F}_q^n$. The probability of drawing $\mathbf{0} \leftarrow \mathcal{B}(6, \frac{1}{2})$ is the product of drawing 512 0's:

$$P(\mathbf{s} = \mathbf{0}) = (\frac{5}{16})^{512}$$

(3)

Assume that $\mathbf{s} \leftarrow \mathbb{F}_q^n$ where $n = 512$. The probability of drawing a single 0 from a centered binomial distribution $\mathcal{B}(6, \frac{1}{2})$ is:

$$P(Y = 0) = P(X = 0 + 3) = C(6, 3)(\frac{1}{2})^3(\frac{1}{2})^3 = \frac{5}{16}$$

Since each entry of $\mathbf{s} \leftarrow \mathbb{F}_q^{512}$ is independently sampled from this centered binomial distribution, the count of 0's in $\mathbf{s}$ also follows a binomial distribution $\mathcal{B}(512, \frac{5}{16})$. The most likely number of 0 in the secret is thus $512 \cdot \frac{5}{16} = 160$.

In similar fashion, it can be computed that the probability of drawing 1 from the centered binomial distribution is $C(6, 4)(\frac{1}{2})^6 = \frac{15}{64}$, so the most likely number of ± 1 in the secret is $512 \cdot \frac{15}{64} = 120$, of ± 2 is 48, of ± 3 is 8.

(4)

(a)

A guess $\hat{\mathbf{s}} \leftarrow \mathbb{F}_q^n$ is correct if the corresponding error term $\hat{\mathbf{e}} \leftarrow \mathbf{b} - A\hat{\mathbf{s}}$ is bounded by the centered binomial distribution: $\hat{\mathbf{e}} \in \{-3, -2, \ldots, 2, 3\}^n$.

(b)

The total number of distinct keys with 160 entries being 0, 120 entries being -1, 48 entries being -2, 8 entries being -3, ... is as follows:

$$n = \frac{512!}{160!120!120!48!48!8!8!}$$

Assuming the uniqueness of the secret, there is exactly one correct value for for $\mathbf{s}$. The random process of drawing from n distinct keys without replacement, among which exactly 1 key is considered "success", is modeled by the negative hypergeometric distribution with $N = n, K = 1, r = (N - K) = n - 1$. The expectation of such a distribution is $\frac{n-1}{n}$

Q4

Using the Kyber described in the definition sheet, the LWE parameters are as follows: $n = m$, $q = 3329$, $\chi_s = \mathcal{B}(n = 6, p = 0.5)$, $\chi_e = \mathcal{B}(n = 4, p = 0.5)$, where $\mathcal{B}(n, p)$ denotes the centered binomial distributions.

Since $\mathbf{s} \leftarrow \chi_s^n$ is independently sampled from identical distributions, we can describe $\|\mathbf{s}\|^2$ as the sum of I.I.D. random variables:

$$\|\mathbf{s}\|^2 = \sum_{i=1}^{n} S_i^2$$

Therefore:

$$E[\|\mathbf{s}\|^2] = E\left[\sum_{i=1}^{n} S_i^2\right] = \sum_{i=1}^{n} E[S_i^2]$$

Because S_i follows the **centered** binomial distribution, $E[S_i] = 0$, so $E[S_i^2] = \mathrm{Var}[S_i]$. On the other hand, the variance of the centered binomial distribution is identical to that of the corresponding binomial distribution: $\mathrm{Var}[S_i] = 6 \cdot p(1-p) = \frac{3}{2}$. This is true because shifting a random variable by a constant does not change its variability.

Putting everything together:

$$E[\|\mathbf{s}\|^2] = \sum_{i=1}^{n} E[S_i^2] = \frac{3}{2}n$$

On the other hand, for calculating the variance of $\|\mathbf{s}\|^2$, we take advantage of the fact that the entries of $\mathbf{s}$ are independently drawn, and the variance of sum of independent random variables is the sum of variances:

$$\begin{aligned}
\mathrm{Var}[\|s\|^2] &= \mathrm{Var}[\sum_{i=1}^{n} S_i^2] \\
&= \sum_{i=1}^{n} \mathrm{Var}[S_i^2] \\
&= \sum_{i=1}^{n} (E[S_i^4] - E[S_i^2]^2) \\
&= \sum_{i=1}^{n} \left((\sum_{j=-3}^{3} (j^4 \cdot \binom{6}{j} \cdot 2^{-6}) - (\frac{3}{2})^2 \right) \\
&= \sum_{i=1}^{n} \left(6 - \frac{9}{4}\right) \\
&= \frac{15}{4}n
\end{aligned}$$

Replacing the secret distribution with the error distribution, we can compute the expectation and variance of the norm square of the error term in similar fashion. In conclusion:

$$\begin{aligned}
E[\|\mathbf{s}\|^2] &= \frac{3}{2}n \\
\mathrm{Var}[\|s\|^2] &= \frac{15}{4}n \\
E[\|\mathbf{e}\|^2] &= n \\
\mathrm{Var}[\|e\|^2] &= \frac{3}{2}n
\end{aligned}$$

Q5

(1)

Denote the columns of A by $A = [\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n]$. Without loss of generality, let $\mathbf{a}_n$ be a non-zero linear combination of the other $n-1$ columns: $\mathbf{a}_n = A'\mathbf{z}'$ for some $\mathbf{z} \in \mathbb{Z}^{n-1}$.

It is easy to see that because A' contains only a subset of columns of A, so $A'\mathbb{Z}^{n-1} \subseteq A\mathbb{Z}^n$. It naturally follows that

$$A'\mathbb{Z}^{n-1} + q\mathbb{Z}^m \subseteq A\mathbb{Z}^n + q\mathbb{Z}^m$$

On the other hand, let $\mathbf{v} \in A\mathbb{Z}^n + q\mathbb{Z}^m$, then there exist $\mathbf{x}_1 \in \mathbb{Z}^n, \mathbf{x}_2 \in \mathbb{Z}^m$ such that

$$\begin{aligned}
\mathbf{v} &= A\mathbf{x}_1 + q\mathbf{x}_2 \\
&= \sum_{i=1}^{n} (\mathbf{a}_i \mathbf{x}_{(1,i)}) + q\mathbf{x}_2 \\
&= (\sum_{i=1}^{n-1} \mathbf{a}_i x_{(1,i)}) + \mathbf{a}_n x_{(1,n)} + q\mathbf{x}_2 \\
&= A' \cdot (x_{(1,1)}, x_{(1,2)}, \ldots, x_{(1,n-1)}) + A'\mathbf{z}' x_{(1,n)} + q\mathbf{x}_2 \\
&= A'((x_{(1,1)}, x_{(1,2)}, \ldots, x_{(1,n-1)}) + \mathbf{z}' x_{(1,n)}) + q\mathbf{x}_2 \in A'\mathbb{Z}^{n-1} + q\mathbb{Z}^m
\end{aligned}$$

Therefore we have $A\mathbb{Z}^n + q\mathbb{Z}^m \subseteq A'\mathbb{Z}^{n-1} + q\mathbb{Z}^m$, and the two lattices are indeed equal.

(2)

Let $(A, \mathbf{b})$ be a sample from generic (aka potentially not full-rank) LWE(m, n, q, U_s, χ_e). Without loss of generality, assume that $A = [A_1 \mid A_2] \in \mathbb{Z}_q^{m \times (n_1 + n_2)}$ where A_1 is full-rank, and $A_2 = A_1 B$ for some non-zero $B \in \mathbb{Z}_q^{n_1 \times n_2}$. Denote the secret by $\mathbf{s} = [\mathbf{s}_1 \mid \mathbf{s}_2]$ where $\mathbf{s}_1 \leftarrow \chi_s^{n_1}, \mathbf{s}_2 \leftarrow \chi_s^{n_2}$, then:

$$\begin{aligned}
\mathbf{b} &= A\mathbf{s} + \mathbf{e} \\
&= (A_1\mathbf{s}_1 + A_2\mathbf{s}_2) + \mathbf{e} \\
&= A_1\mathbf{s}_1 + A_1 B\mathbf{s}_2 + \mathbf{e} \\
&= A_1(\mathbf{s}_1 + B\mathbf{s}_2) + \mathbf{e}
\end{aligned}$$

Because secrets are sampled from a uniform distribution, $\mathbf{s}_1 + B\mathbf{s}_2$ is uniformly random. Therefore $(A_1, \mathbf{b})$ is a valid sample from full-rank LWE(m, n, q, U_s, χ_e). We can thus feed $(A_1, \mathbf{b})$ to a full-rank LWE oracle, who will output some $\mathbf{s}'$. Assuming that the full-rank LWE problem has unique solution, we know $\mathbf{s}' = \mathbf{s}_1 + B\mathbf{s}_2$

Q6

(1)

Let $X \in \mathcal{B}(n,p)$ be a random variable that follows binomial distribution. Recall from the definition of a binomial distribution that $X = I_1 + I_2 + \ldots + I_n$ where each of I_i is an independent coin toss with PMF:

$$\begin{cases} P(I_i = 1) = p \\ P(I_i = 0) = 1 - p \end{cases}$$

Let $X_1 \in \mathcal{B}(n_1,p), X_2 \in \mathcal{B}(n_2,p)$ be two independent random variables following binomial distributions, then:

$$X_1 = \sum_{i=1}^{n_1} I_i$$
$$X_2 = \sum_{i=n_1+1}^{n_1+n_2} I_i$$

Therefore $X_1 + X_2 = \sum_{i=1}^{n_1+n_2} I_i$, which is a binomial distribution $\mathcal{B}(n_1+n_2,p)$.

Recall that centered binomial distribution is defined by subtracting the corresponding binomial distribution by a constant (the expectation of said binomial distribution): $C_i = X_i - E(X_i)$. Therefore, given centered binomial distributions $C_1 = X_1 - E[X_1], C_2 = X_2 - E[X_2]$:

$$\begin{aligned} C_1 + C_2 &= X_1 + X_2 - E[X_1] - E[X_2] \\ &= (X_1 + X_2) - E[X_1 + X_2] \end{aligned}$$

From the results above we know that because X_1, X_2 are independent binomial distributions, $X_1 + X_2$ follows binomial distribution $\mathcal{B}(n_1+n_2,p)$, thus C_1+C_2 follows centered binomial distribution $\mathcal{B}(n_1+n_2,p)$.

(2)

From part (a) we know that the sum of k i.i.d. random variables following binomial $\mathcal{B}(n,p)$ is a random variable following binomial $\mathcal{B}(kn,p)$.

Let $I^m = \{0,1\}^m$ denote the set of bit-masks with length m and $K \subseteq I$ denote the subset of vectors with exactly k entries being 1, then $|K| = \binom{m}{k}$. Thus we iterate through all possible values in $\mathbf{k} \in K$ and compute the inner product $\mathbf{e}^\intercal\mathbf{k}$. Since $\mathbf{k}$ has exactly k entries being 1 and $\mathbf{e}$ contains m independent samples from centered binomial (n,p), $\mathbf{e}^\intercal\mathbf{k}$ is the sum of k i.i.d. centered binomial with parameters (kn,p)

Q7

We can set one of the base vectors to be extremely short and all other base vectors extremely long. For ease of constructions we will build orthogonal basis.

Denote the columns of the identity matrix $I_n \in \mathbb{R}^{n \times n}$ by $I = [\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n]$.

Let $\mathcal{L}(\{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n\}) \subset \mathbb{R}^n$ be spanned by the basis $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$, where $\mathbf{b}_1 = \mathbf{e}_1$, and $\mathbf{b}_i = 3R\mathbf{e}_i$ for $i > 1$. Finally, set $\mathbf{v} = (0, 1.1R, 0, 0, \ldots, 0)$.

It is easy to see that $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$ form an orthogonal basis. The shortest vector in $\mathcal{L}$ is $\mathbf{b}_1$, so $\lambda_1(\mathcal{L}) = 1$. The closest lattice point to $\mathbf{v}$ is $\mathbf{0}$, so the distance between $\mathbf{v}$ and $\mathcal{L}$ is $\|\mathcal{L} - \mathbf{v}\| = 1.1R > R$

Q8

Recall that the decryption is computed with the following routine:

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

Where $\mathbf{s}, \mathbf{s}'$ are coordinate-wise drawn from the secret distribution and $\mathbf{e}, \mathbf{e}', e''$ are coordinate-wise drawn from the error distribution.

According to the decryption routine, a decryption error occurs if and only if the "noise" $(\mathbf{s}'^{\intercal}\mathbf{e} - \mathbf{e}'^{\intercal}\mathbf{s}) + e''$ exceeds $\lfloor\frac{q}{4}\rceil$. So to find a modulus that guarantees correct decryption all the time, we need to find the upper bound of noise.

With (baby) Kyber-512, $\chi_s = \mathcal{B}(n = 6, p = 0.5), \chi_e = \mathcal{B}(n = 4, p = 0.5)$. Noise is maximized when all entries of $\mathbf{s}, \mathbf{e}$ reach the extremes of the support of their respective distributions. For example, with $\mathbf{s} = \mathbf{s}' = (3, 3, \ldots, 3)$, $\mathbf{e} = (2, 2, \ldots, 2)$, $\mathbf{e}' = (-2, -2, \ldots, -2)$, $e'' = 2$, the noise term evaluates to $(6 \cdot 512 + 6 \cdot 512) + 2 = 6146$. The smallest prime q such that $\lfloor\frac{q}{4}\rceil \geq 6146$ is 24593.

Q9

Let $(A, \mathbf{b}) \leftarrow \text{LWE}(n, n, q, \chi_e, \chi_s)$. In other words, A is uniformly randomly sampled from all full-rank matrices $\mathbb{F}_q^{n \times n}$, $\mathbf{s} \leftarrow \chi_e^n$, $\mathbf{e} \leftarrow \chi_s^n$, and $\mathbf{b} \leftarrow A\mathbf{s} + \mathbf{e}$.

I claim that matrix inversion $A \mapsto A^{-1}$ on the set of full-rank matrices is a bijection. This is true because the inverse of two distinct matrices is necessarily distinct (injectivity), and every full-rank matrix is the inverse of its inverse (surjectivity).

Because matrix inversion is a bijection from the set of invertible matrices onto itself, if A is uniformly sampled from all full-rank matrices $\mathbb{F}_q^{n \times n}$, then A^{-1} is also a uniformly randomly sampled matrix from the set all full-rank matrices.

Notice that $A^{-1}\mathbf{b} = A^{-1}A\mathbf{s} + \mathbf{e} = A^{-1}\mathbf{e} + \mathbf{s}$. Since $\mathbf{e}$ is sampled from the secret distribution and $\mathbf{s}$ is sampled from the error distribution, A^{-1} is a uniformly random sample, $(A^{-1}, A^{-1}\mathbf{b}) = (A^{-1}, A^{-1}\mathbf{e} + \mathbf{s})$ is a sample from $\text{LWE}(n, n, q, \chi_s, \chi_e)$. If there exists an oracle for $\text{LWE}(n, n, q, \chi_s, \chi_e)$, then this oracle can recover $\mathbf{e}$, and from here we can recover $\mathbf{s}$ in $\text{LWE}(n, n, q, \chi_e, \chi_s)$.

The argument above did not assume anything specific to χ_s or χ_e, so they can be swapped, and we will arrive at the inverse conclusion that $\text{LWE}(n, n, q, \chi_s, \chi_e)$ reduces to $\text{LWE}(n, n, q, \chi_e, \chi_s)$, as well. Therefore, the two problems are equivalent.

Q10

Recall from textbook LWE the decryption routine:

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

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

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

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

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

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.