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 $\hat{\mathbf{e}} \leftarrow (\mathbf{b} - A\hat{\mathbf{s}}) \mod q$ 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 $\frac{n-1}{n}$