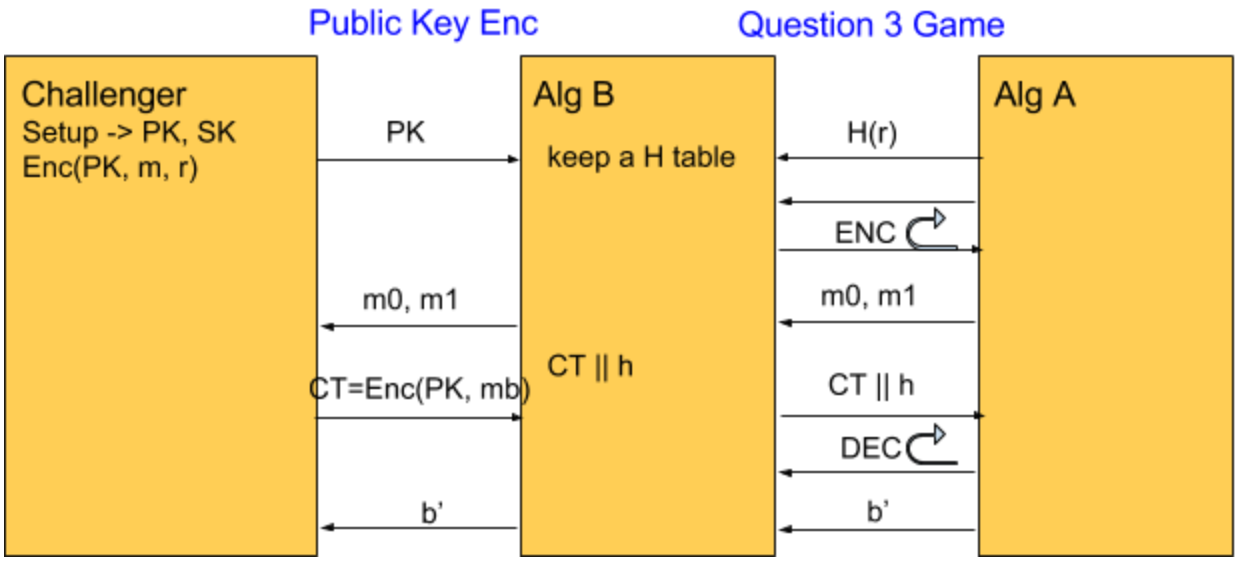
Public Key Enc
Question 3 Game
Challenger
Setup -> PK, SK
Enc(PK, m, r)
PK
Alg B
keep a H table
H(r)
Alg A
ENC
m0, m1
m0, m1
CT || h
CT=Enc(PK, mb)
CT || h
DEC
b'
b'

Figure 1

1. **Vector Distribution**

   An example for A that the attacker can achieve non-negligible advantage in distinguishing these two distributions is a $m*n$ zero matrix. The first vector $As+e$ turns to e, which contains random +1s and -1s. The second vector are consisted of random elements in Z_p^*. Apparently, the two distributions look different than one another.

   If the condition is changed to $m < n$, then we conjunct an identity matrix of m with a zero matrix of $m * (n - m)$.

$$\begin{bmatrix} 1 & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 1 & 0 & \dots & 0 & 0 \end{bmatrix}$$

   As is the first m rows of s, which are of random elements, and elements in e are also random between +1 and -1. The superposition of two seemingly random matrices should also appear random. Therefore, the first distribution $As+e$ appears random just as the second. The attacker will not gain non-negligible advantage in this case.

2. **Quantum Grouping**

   We will show that the Shor's Algorithm still applies if a group generator contains two element parameters g and h. In other word, given g, h, and $f(x) = g^x h^x$, the quantum computer is able to solve for x.

   Assuming the associativity that $g^x h^x = (gh)^x$, we define $F(k, b) = (gh)^{kx+b}$. Because group g and h are periodical,

$$(g^x h^x)^k = (gh)^{(k+c_1)x},$$

$$(gh)^b = (gh)^{b+c_2}.$$

   Multiplying both equations,

$$F(k, b) = (gh)^{kx+b} = (gh)^{(k+c_1)x+(b+c_2)} = F(k + c_1, b + c_2)$$

   which has a period of (c_1, c_2).

$$(g^x h^x)^a * (gh)^b = (g^x h^x)^{a+c_1} (gh)^{b+c_2},$$

   so

$$(g^x h^x)^{c_1} (gh)^{c_2} = 1,$$

$$c_1 x + c_2 = 0,$$

$$x = -\frac{c_2}{c_1}.$$

   According to the Shor's Algorithm, we can find such c_1 and c_2, and obtain x for given $f(x)$.

3. **IND-CCA2 Public Key**

We prove the scheme is secure using the reduction. Suppose there is an algorithm A that has advantage playing the game in IND-CCA2. Then we design an algorithm B between the Challenger and the Attacker, as shown in Figure 1. Algorithm B in the middle keeps a table to store m, r, $H(m||r)$, and CT for each different query. For the encryption oracle, B calls $Enc(PK, m, r)$ with random r for CT and returns $CT||H(m||r)$. For the decryption oracle, B searches through the table and find $H(m||r)$ with matched r and CT, and responds with m. If nothing is found in the table, then return $\perp$. Then, B sends random bit strings of length $\mid (m||r) \mid$. At last, B passes on b' from A back to the challenger. From the reduction, because we know that the public key encryption is secure, we are ensured that the game proposed in the question is also secure.

4. **Shamir with Liar**

My design is similar to Shamir secret sharing, except that the share owned by each person is two points on a plane. The encrypted message is the radius of the circle, r, that the four points from any pair of two people. It is a mathematical property that any three points that do not fall onto the same line can determine a unique circle. If any three of the six points from all three people are on the same line or do not form a circle, then one of them must be lying. If there is only on person lying at a time, the four points from other two people can form a circle, meaning that the third person is the liar.