Name: LAU, Chi Hong

SID: 20852057

Email: chlaubc@connect.ust.hk

RNG protocol:

Goldwasser-Micali Cryptosystem

1. Key generation

- Casino picks two large prime numbers p and q

- set n = p*q

- Casino finds x in {0,1,..,n-1} such that x in not a QR mod p and not a QR mod q

- Publish (x,n) in the smart contract as the public key

- Keep (p,q) in secret as the private key

2. Encryption

- Let r = $A_0A_1…A_{15}$, where A is in {0,1}

- Each player helps generate a random number by sending 16 bits, r_i=$b_0b_2…b_{15}$ where b is in {0,1}

- For every b_i, the player has to pick y_i in {0,1,…,n-1} such that gcd(y_i,n)=1

- $c_i = y_i^2 * x^{bi}$

- $p_i = [c_0,c_1,…,c_{15}]$

- send p_i to the smart contract

3. Decryption

- The casino will receive the enc(r)= p = $p_0*p_1*…*p_n$ = $[B_0,B_1,…,B_n]$

- For each element in p, the casino checks whether B_i is a QR mod n using Fermat Little Theorem and Chinese Remainder Theorem

- B_i is a QR mod n if

$Bi^{(p-1)/2}$mod p = 1 (mod p) and $B_i^{(q-1)/2}$mod q = 1 (mod q)

- If B_i is a QR mod n, A_i=0, else A_i = 1

Homomorphic encryption

1. The casino will multiply each p_i

- enc(r)= p = $p_0*p_1*…*p_n$ = $[B_0,B_1,…,B_n]$

- enc(r_i) * enc(r_j) = enc(r_i^r_j) where i != j

It is the homomorphic property of GM

2. The casino will decrypt p

- A_i will equal to the XOR of all b_i

- r = $A_0A_1…A_{15}$

Casino player -> normal player -> authority player

The casino submits first, followed by normal players and authority players. This sequence must be held to make sure r is tamper-proof and unpredictable. It will be explained in the below.

Flow:

1. At the beginning of the day, before the start of the casino, anyone can join as a player to help generate the random number r. They have to submit an int array int[16]. For each element, it is encrypted using the public key given by the casino following the scheme of GM above.

2. After 1 hour, the players who are controlled by the authority have to submit the cipher text as well.

For example, the casino starts at 9 am, so non-authority players can contribute to the random number between 7-8 am by calling deposit_player(). Then authority players can contribute to the random number between 8-9 am by calling deposit_aplayer().

3. The random number r is generated in the encrypted form. When a player submits the cipher text. The smart contract will automatically take the XOR of each text.

Once all authority players have submitted the text, the casino can decrypt the cipher text off-chain following the scheme of GM. The casino will get r in 16bits.

4. For the next 8 hours, anyone can join as a bettor by calling deposit_bettor(). The casino will generate a random number by calling srand(r+k) and x=rand() off-chain. It then inputs the result (x%2) to the smart contract within a few blocks. The casino will call the give_result() to tell if they win.

5. After 8 hours, the casino has to reveal r and the secret key by calling reveal_r_sk(). If the casino does not reveal within 24 hours the casino starts, anyone can call compensate() to take 0.02 ethers.

6. Anyone can call verify_r() to check if r is really generated by the random function. If not, it will state the casino cheated. If the casino cheated, anyone can call compensate().

7. If the bettors wins, they can call withdraw_bettors() to get the reward. If not, they can call verify_x() to check if the random number is really generated by the random function to see if the casino cheated. If cheating is detected, anyone can call compensate().

8. After 24 hours, if no cheating is reported, the casino can collect its reward by calling withdraw_dealer().

Requirement Satisfaction:

(1) RNG protocol is provided. Detailed explanation is in the below(a-d)

(2) srand() and rand() are provided

(3) In order to construct the contract, the casino is required to deposit a huge amount of money.

(4) deposit_bettor() and give_result() are provided.

(5) reveal_r_sk(), verify_r() and verify_x() are provided to fulfil this requirement.

(6) compensate() is provided.

(7) withdraw_dealer() is provided.

(a) When a new player joins, the smart contract will accumulate the total number of players. It then takes t = (n/2)+1 (round up). t players will help generate the random number. Therefore, the authority must control at least half of the players.

(b) Every player submits an int[16] to the smart contract, which is the encrypted version of their choice of bit, using the public key given by the casino. Only the player and the casino know the bits. However, other players do not know others' choices since only the casino knows the private key. r is computed in the encrypted version using the homomorphic property of GM. Only the casino can decrypt it, so r is only visible to the casino.

(c) In the smart contract, once the player submitted the array, the contract will automatically multiply them with other p_i. r is computed automatically on chain and it is in an encrypted version. Once the casino starts, no one can submit r_i anymore so the encrypted version of r will remain the same on the chain. No one is able to call the function to change it afterward. The casino will have to reveal r and the private key at the end, so anyone can check if it is equal to the dec(p).

r is not under anyone's control, more details are explained in (d).

(d) For the casino, it cannot control the value of r. Although the casino can decrypt all the encrypted values and compute r, r is not under its control. Since the last player must be the one controlled by the authority, the authority will submit r_i and modify r and the casino does not know the choices of authority players before they submit it to the smart contract, the casino cannot control r beforehand.

For the authority, they do not know the value of r until it is revealed. Although the authority is the last one who contributes the value of r, they do not know the private key, so they cannot obtain any information about r before they submit it. In their sight, they are simply randomly changing the value of r.

There is a possible way to control r. If the casino collaborates with the authority, they both know the private key and are the last ones modifying r. r can be under their control. However, they hate each other, so I believe it will not happen.

(e) r is uniformly random in {0, 2^16-1}. r = $A_0A_1…A_{15}$, where A is in {0,1}. It is an integer represented in 16 bits in binary form, so its range is {0, 2^16-1}. A_i is determined the result of the XOR of all b_i and every player submits p_i which is int[16] that will possibly change the value of each A_i.

(f) Step 1 will never fail. Each player submits int[16] and the authority decrypt the XOR of them at the end. If the player does not follow the scheme, like submitting something that is not encrypted by the public key, r still can be computed. It is because the player must submit int[16] and it can still run in bitwise operation. It does not matter if a player gives some rubbishes to the smart contract. r is the result of XOR anyway.

(g) Although r can be computed if someone gives rubbish to it, we don't encourage this behavior. It is good to be an honest person, so an honest player can get a reward of (10% of the revenue of the casino/the number of total players). A player can prove his honesty by submitting his choice after the reveal, if it matches with the decrypted version, he can get the reward.

They are also encouraged to reveal the choice since it helps verify the public key and private key is generated at the same time. If they do not reveal, they will lose the deposit for participation.

(h) The casino must reveal the private key and r, otherwise the casino will be seen as cheated. Since the encrypted version of r is stored on-chain, anyone can use the private key to decrypt it and see if it matches with r. Every bettor can check if x is generated using the seed of k and r. The random functions are implemented on chain, so they can check the result of their choice of k and see if the casino cheated.

(i) The casino is required to deposit a huge amount of money when constructing the contract. I don't know how to solve the problem if all people around the world join the bet (7 billion bettors), but the smart contract will make sure the deposit is very large.

(j) I believe so.