Yao Millionaire's Problem

Umang Jain - 17074016
Pankaj Jha - 17074010

OUTLINES

1. Problem Definition
2. Solution by Andrew C. Yao
3. Solution by Hsiao-Ying Lin and Wen-Guey Tzeng
4. Demo of both algorithm

Introduction to yao’s millionaire problem

Andrew Yao proposed the millionaire problem, which discussed how could two millionaires determine who is richer while keeping their actual wealth private.

Let say

Alice has 5 millions and Bob has 12 millions.

Then both need to know who is richer without revealing their actual wealth to other party.

secure multiparty computation

Secure multiparty computation(SMC), or secure computation, secure function evaluation(SFE) is an abstract of this kind of problems. SMC asks for protocols that enable several parties collaboratively compute a function without exposing their input.

In yao's Millionaire problem :- Their are two parties, Alice and Bob, and they need to compute

F(x,y) = argmax(x,y)

Solution by Andrew C. Yao himself

Solution

Let’s sat Alice has i millions and

Bob has j millions,

Also Ea be the Alice encryption funtion (RSA in implementation) with public key also known to Bob and private key only known to alice.

Let’s sat Alice has i millions and Bob has j millions, Also Ea be the Alice encryption funtion (RSA) with public key also known to Bob.

1. Bob picks a random N-bit integer, and computes privately the value of Ea(x); call the result k.

2. Bob sends Alice the number k − j ;

3. Alice computes privately the values of yu = Da(k− j + u) for u = 1, 2, . . . , 10.

4. Alice generates a random prime p of N/2 bits, and computes the values zu = yu (mod p) for all u; if all zu differ by at least 2 in the mod p sense, stop; otherwise generates another random prime and repeat the process until all zu differ by at least 2; let p, zu denote this final set of numbers;

5. Alice sends the prime p and the following 10 numbers to B: z1, z2, . . . , zi followed by zi + 1, zi+1 + 1, . . . , z10 + 1; the above numbers should be interpreted in the mod p sense.

6. Bob looks at the j-th number (not counting p) sent from Alice, and decides that i ≥ j if it is equal to x mod p, and i < j otherwise.

7. Bob tells Alice what the conclusion is.

Solution by Hsiao-Ying Lin and Wen-Guey Tzeng

Basic Idea

Basic idea is to find such encodings of x and y such that

intersection(Encoding[x], Encoding[y]) != NULL <===> (x>y)

Let s[n] s[n-1] s[n-2] …. S[0] be the binary representation of any number x

1 - encoding of s is S = {s[n] s[n-1] . . . s[i] |s[i] = 1}, all prefix of s ending in 1

0 - encoding of s is S = {s[n] s[n-1] . . . s[i+1] 1 |s[i] = 0}, all prefix of s ending in 0 with inversion of only the last bit.

Encoding[x] = 1 - encoding of x

Encoding[y] = 0 - encoding of y

Example

Let x = 12

Binary representation is 1100

0 encoding = { 111, 1101 }

1 encoding = {1, 11 }

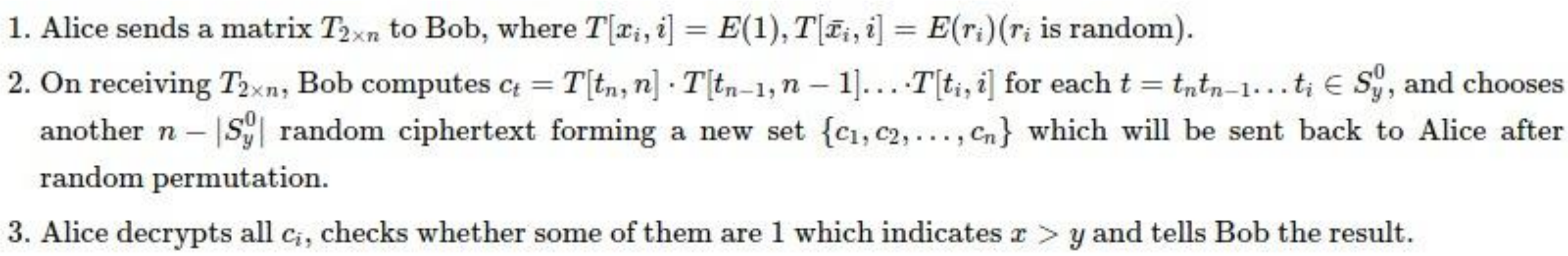
Let y = 6

Binary representation is 110

0 encoding = { 111 }

1 encoding = {1, 11 }

Protocol



1. Alice sends a matrix $T_{2\times n}$ to Bob, where $T[x_i, i] = E(1), T[\bar{x}_i, i] = E(r_i)(r_i$ is random).
2. On receiving $T_{2\times n}$, Bob computes $c_t = T[t_n, n] \cdot T[t_{n-1}, n-1] \ldots \cdot T[t_i, i]$ for each $t = t_n t_{n-1} \ldots t_i \in S_y^0$, and chooses another $n - |S_y^0|$ random ciphertext forming a new set $\{c_1, c_2, \ldots, c_n\}$ which will be sent back to Alice after random permutation.
3. Alice decrypts all c_i, checks whether some of them are 1 which indicates $x > y$ and tells Bob the result.

Encryption has to multiplicative homomorphic i.e E[x * y] = E[x] . E[y]

DEMO

References

1. A.C. Yao, Protocols for secure computations, in: Foundations of Computer Science, 1982, Sfcs'08. 23rd Annual Symposium on, IEEE, 1982: pp. 160–164.

2. H.-Y. Lin, W.-G. Tzeng, An efficient solution to the millionaires' problem based on homomorphic encryption, in: International Conference on Applied Cryptography and Network Security, Springer, 2005: pp. 456–466.

Thank you