Report of cryptography

wangyi

29 December 2016

1.Problem Definition

The purport of secure two-party computation project is to compare the magnitude of two sides(Alice and Bob).But at the same time Alice/Bob learns no more information about y/x than what can be deduced from its own input of x/y and the output of f(x,y).In order to obtain the mentioned purpose foregoing ,I designed these protocols which based on oblivious transfer and garbled circuits to resolve this problems.

2.The overview of project

The project implements in some sections such as garbled circuit,oblivious transfer, private-key encryption,public-key encryption,ciphertext transfer.Firstly, the programing language implemented in this project is Python,concisely and conveniently for developers. Secondly,the private-key encryption applied in this project is DES(Data Encryption Standard),the public-key encryption utilized in this project is RSA.The oblivious transfer is based on RSA to deliver one of keys while the garbled circuit is a extraordinary part in this project. I won't implement complicated comparator circuit or adder circuit ,and I only use two independent garbled circuits to compare one bit for bit by bit,then it loops until one bit is bigger than another.First of the garbled circuit is based on XOR boolean calculation,the second of the garbled circuits is based on boolean calculation as $A \wedge \overline{B}$ true table.Firstly, run the first garbled circuit ,then if a bit of one side is same as the a bit of the other side, continue.If not match,run the $A \wedge \overline{B}$ garbled circuit,we can get one is bigger than the other one.The specific details will be introduced in the next paragraph.Lastly,the ciphertext transfer is tansfered via the sockets.

3.Principle Description

The special method distinguishing from other complex circuits in this project is using the double-comparison method to achieve comparing bit by bit,in this way,there is no need to remember the condition of last bit comparison.Let $x =$

$x_1x_2\ldots\ldots x_n, y = y_1y_2\ldots\ldots y_n \in \{0,1\}^n$first of all, we run $x_1 \oplus y_1$,if $x_1 = y_1$,then $x_1 \oplus y_1 = 1$,else $x_1 \oplus y_1 = 0$.if the XOR's result is 1,it shows this bit is equal,so we should compare the next.Then we continue to compute $x_2 \oplus y_2$,if XOR's result is 0,then use the single comparator circuit $X \wedge \overline{Y}$ to compare their size,if $x_1 > y_1$then $x_1 \wedge \overline{y}_1 = 1$,else $x_1 \wedge \overline{y}_1 = 0$,now we can get x/y is bigger,the comparison is end. Based on this principle,we can use it to construct our garbled circuit

4.The concrete steps

1.In the beginning,we should build the connection of sockets,Alice is the client,Bob is the server,they are bound in 127.0.0.1:50007,then they deliver data via sendall() and rect()
2.After the connection established,the first step is to transfer the input from decimal number to binary number,then Alice send data to Bob,if Alice/Bob is longger than the other,the shorter adds "0" in the head(beginning)so as to keep the lengths of two parts are equal.
3.Alice generates the keylist that includes 6 key:$k_0^u k_1^u k_v^0 k_v^1 k_w^0 k_w^1 k_0^u$means Alice's key while her input bit is "0",k_1^u means Alice's key while her input bit is "1",k_0^v means Bob's key while her input bit is "0",k_1^v means Bob's key while her input bit is "1",k_0^w means result is "0",k_1^w means result is "1".Then Alice use private-key encryption to encrypt k_w^0 and k_w^1 according to the xor true table,it creates encrypted Truth Table.Lastly Alice send these to Bob with the addition of k_a^u(Alice's key while her input bit is "a")
4.Bob get these keys.firstly,he use oblivious transfer(it will be introduced detailedly in section 5) to get k_v^b((Bob's key while her input bit is "b")).After he get k_a^u and k_v^b,he can try to use two keys to decryt the encrypted truth table, in fact one of the encrypted truth tables will work.Then Bob will send this one to Alice.
5. Alice uses this one to find its index in keylist.If its index is 4,it means the result of xor is 0,their bits are different,then we construct a new comparator circuit,it likes 3-5,we only need to change true table.If its index is 5,which means the result of xor is 0 ,then we loop this step then goto 3
6.In new comparator circuit, the only differentness is the true table,Alice also should use the result to find its index in new keylist,If its index is 4,it means Alice is bigger than Bob.If its index is 5,it means Bob is bigger than Alice.

5.Oblivious transfer

In this project, oblivious transfer is the most important part to transfer the Bob's bit and through choice from k.The key point is to use public-key encryption(RSA).
1.Firstly B generate two pairs of public-keys and private-keys then reserve the private-key of ones,and rename it as fake-private-key(the fake rule is if own in-

put bit is 0,then the second private-key is fake,and vice versa.)
2.Secondly Bob send two public-keys to Alice, Alice encrypt the two keys through the two public-keys and send them to Bob.
3.Thirdly, Bob use corresponding private-keys to decrypt them,but one of private-keys is fake,so only one key works,it is a input bit's key of Bob.
In this condition,Bob chooses a key he wants while he doesn't know the other key,besides Alice doesn't know Bob's choice.In this part,public-key encryption is based on RSA,Bob generates the two-pair keys,and send two public-keys to Alice,and Bob use the two public-keys to encrypt the key,After encryption Bob send it to Alice,ALice use private-key to decrypt it.

6.Private-key encryption

In this part,private-key encryption is base on DES. The private-key encryption is used in garbled circuit,firstly we generate the keylist($k_0^u k_1^u k_v^0 k_v^1 k_w^0 k_w^1$) and encrypted truth table.For example, according to XOR truth table we use k_v^0 to encrypt k_w^1,and then use k_u^1 to encrypt above result.Then Bob use two key from Alice and OT(the choice of Bob) to decrypt the ciphertext.

7.Garbled circuit

In this part,garbled circuit is constructed first by private-key encryption,Alice use DES encrypt the two key to encryted ture table from XOR true table ,and then add the k_u^a at the end.Bob get k_u^a from addition,learn k_v^b with OT_1^2 ,then Bob decrypt PETT with (k_u^a, k_v^b),and send the decryption result m to Alice,Alice find its index in keylist then decide the output and send to Bob.Now the two sides all know the result of exclusive-or operation. And the second garbled circuit is single comparator circuit $X \wedge \overline{Y}$,we use different true table in this garbled circuit,the others are the same.

The true table of $X \oplus Y$

X	Y	f(X,Y)
0	0	1
0	1	0
1	0	0
1	1	1

The true table of $X \wedge \overline{Y}$

X	Y	f(X,Y)
0	0	0
0	1	0
1	0	1
1	1	0

8.Test case

This project can be compatible with any n,First Alice input a Decimal number and press enter keythen Bob input a number and press enter key,the system entered into the phase of computing,compare the bits one by one,if Alice's input is bigger,the terminal will display "Alice is bigger" and vice versa.
There are some test cases as follow.
Input:Alice:1111,Bob:1111 Output:1 and "Alice is bigger"
Input:Alice:1234,Bob:4321 Output:0 and "Bob is bigger"
Input:Alice:121212,Bob:1212 Output:1 and "Alice is bigger"
Input:Alice:1001,Bob:1000 Output:1 and "Alice is bigger"
Input:Alice:9999,Bob:10000 Output:0 and "Bob is bigger"