Value discovery in complete graphs
Group 43
Shivneshwar Velayutham and Madhumitha Venkatesan

The protocol for a processor P_i to find it’s secret s_i is as below.

First step

All processors have read access to the secret value of all other processors. So, they can start by taking the first secret they can read and do an XOR operation on it with the next secret that they can read. The output of the previous operation should be XORed with the next secret and so on and so forth until all processor’s secrets (except the original processor’s secret of course) have been XORed upon. Write the final result of the operations to r_i.

Therefore, every r_i contains the following:

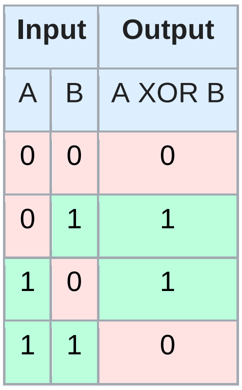
$r_i = s_1 \text{ xor } s_2 \dots \text{xor } s_{i-1} \text{ xor } s_{i+1} \text{ xor } s_{i+2} \dots \text{xor } s_n$

Second step

Once all processors are done with the first step, P_i can now look at another processor P_j and read the secret in s_j and the output of previous step in r_j. So now P_i will be able to compute the following:

$r_j \text{ xor } s_j = s_1 \text{ xor } s_2 \text{ xor } s_3 \dots \text{xor } s_n$

The important property of XOR is the fact that XOR is commutative (ie. the order in which XOR is applied does not matter and the result is always the same). Below is the truth table of XOR and it’s quite easy to see if A and B are switched, we would get the same output.



Input		Output
A	B	A XOR B
0	0	0
0	1	1
1	0	1
1	1	0

Third step

The other important property of XOR is that it's possible to undo XOR. For example, the way to undo addition would be to use subtraction therefore making subtraction the inverse of addition. Similarly, the inverse of XOR is actually XOR. Below is the proof of the same and uses the fact which we proved earlier that XOR is commutative.

x = a xor b

x xor a = a xor b xor a
x xor a = a xor a xor b (Using commutative property)

Using the truth table above we can see that XORing same bits we get the result as 0. So,
a xor a = 0
x xor a = 0 xor b

Using the truth table above we can see that 0 xor 0 = 0 and 1 xor 0 = 1. So 0 is XOR's identity value that doesn't change the value of the other operand similar to how 0 is the additive identity and 1 is the multiplicative identity.

Therefore,

x xor a = b proving that xor is the inverse of xor.

Since we have the result of the XORs of all the secret from the previous step and P_i has the XORs of all the secrets except its own secret from the first step. It's possible to calculate its secret by doing the following operation.

$s_i = r_j$ xor s_j xor r_i

Done