CS 203.4860	Secure Multi-Party Computation	Fall 2021
	Homework 8: Report	
Lecturer: Dr. Adi Akavia		*Student(s): ()*

We will choose the following inputs to a, b, c, λ
$a = 1$
$b = 0$
$c = 1$
$\lambda = 4$

1 step 1

$sk \leftarrow Gen(1^\lambda)$

Gen first finds random odd number p in the range of $2^{3\cdot\lambda}$ to $2^{3\cdot\lambda+1}$, we randomly get $p = 6221$

2 step 2

At each encryption the algorithm create a mask r of size up to 2^λ (with random sign) and chose another random number q of size from $2^{3\cdot\lambda}$ to $2^{3\cdot\lambda+1}$.

$c_a \leftarrow Enc_{sk}(a)$

The random values we get are $r = -7$ and $q = 4901$ and then we calculate

$$c_a = q \cdot p + 2 * r + a = 6221 * 4901 + 2 * (-7) + 1 = 30,489,108$$

$c_b \leftarrow Enc_{sk}(b)$

The random values we get are $r = -7$ and $q = 4901$ and then we calculate

$$c_b = q \cdot p + 2 * r + b = 6221 * 4885 + 2 * (13) + 0 = 30,389,611$$

$c_c \leftarrow Enc_{sk}(c)$

The random values we get are $r = -7$ and $q = 4901$ and then we calculate

$$c_c = q \cdot p + 2 * r + c = 6221 * 5243 + 2 * (-7) + 1 = 32,616,690$$

3 step 3

In this step the values c_a, c_b, c_c are passed from Alice to Bob. Now Bob does the following calculations

$c_{XOR} \leftarrow XOR(c_a, c_b)$

The "encrypted version" of XOR is just addition and therefore Bob adds the two values $c_{XOR} = c_a + c_b = 30,489,108 + 30,389,611 = 60,878,719$

$c_{res} \leftarrow AND(c_{XOR}, c_c)$

The "encrypted version" of AND is just multiplication and therefore Bob multiplies the two values

$$c_{res} = c_{XOR} * c_c = 60,878,719 * 32,616,690 = 1,985,662,305,220,110$$

4 step 4

Now Alice gets back c_{res} from Bob.

$res \leftarrow DEC_{sk}(c_{res})$

the decoding process is done by taking the result modulo the secret key $sk = p = 6221$.

$$c_{res} (\text{mod } p) = 1,985,662,305,220,110 \,(\text{mod } 6221) = 6052$$

Alice now takes 6052 mod 2, as 6052 is bigger then 6221/2 we must flip the result, and therefore Alice gets:

$$res = (1 + (6052 \text{ mod } 2) \text{ mod } 2) = 1$$

5 step 5

At this point Alice compute AND(XOR(a,b),c) and compare it to the result. $AND(XOR(a,b),c) = AND(XOR(1,0),1) = AND(1,1) = 1$ this is same value as the result, therefore Alice output is $res = 1$.