CS 203.4860	Secure Multi-Party Computation	Spring 2023
	Homework 8: Report	
Lecturer: Dr. Adi Akavia	*Student(s): Nir Segal, Hallel Weinberg, Michael Rodel*	

1 Introduction

In this assignment we will describe the details of a dry-run of a homomorphic evaluation. The cleartext computation is as follows:

Given three bits $a, b, c \in \{0, 1\}$, output $AND(XOR(a, b), c)$.

2 Choose Input Bits and Security Parameter

- Input bits: $a = 1$, $b = 0$, $c = 1$.
- Security parameter: $\lambda = 128$.

3 Step 1: Generate Keys

Generate keys $sk \leftarrow \text{Gen}(1^\lambda)$.

The input: $\lambda = 3$

The details of the computation: Generate sk, an odd number with a length of λ^2 bits.

The resulting outcome of the step: $sk = 471$.

4 Step 2: Encrypt the Inputs

Encrypt the input $c_a \leftarrow \text{Enc}_{sk}(a)$, $c_b \leftarrow \text{Enc}_{sk}(b)$, $c_c \leftarrow \text{Enc}_{sk}(c)$.

The input: $a = 1, b = 0, c = 1$ and $sk = 471$

The details of the computation: For each input bit b, generate q_b, a "large" number with a length of λ^5 bits and r_b, a "small" even number with a length of λ bits. compute $c_b = p \cdot q_b + 2 \cdot r_b + b$ where $p = sk$.
The parameters for each input bit:

1. $q_a = 13227508180736365427652432425341829447350829616451546311965174612433249107$
2. $r_a = 4$

3. $q_b = 120022159332133701837079461883746986133140175953498592850566443183034951 88$
4. $r_b = 4$
5. $q_c = 1370246967166904618483454817374944883387921756462745153421459373403165124 8$
6. $r_c = 6$

The resulting outcome of the step:

$c_a = 623015635312682811642429567233600166970224074934867831293559724245606032940 6$

$c_b = 565304370454349735652644265472448304687090228740978372326167947392094623355 6$

$c_c = 645386321535612075305707218983599040075711147293952967261507364872890773782 1$

5 Step 3: Homomorphically evaluate the Aforementioned Cleartext Computation

Homomorphically evaluate the aforementioned cleartext computation to obtain a result ciphertext c_{res}.

The input: Encrypted values

$c_a = 623015635312682811642429567233600166970224074934867831293559724245606032940 6$

$c_b = 565304370454349735652644265472448304687090228740978372326167947392094623355 6$

$c_c = 645386321535612075305707218983599040075711147293952967261507364872890773782 1$

The details of the computation: Homomorphically evaluate AND(XOR(c_a, c_b), c_c) to obtain a result ciphertext c_{res}.

$$c_{res} = (c_a + c_b) \cdot c_c$$

The resulting outcome of the step: $c_{res} = 153222266277439889145067278920780277329449860799982992619964353065717569136826807959957008066704941488410702989174619469650071949675185407104459733704906$

6 Step 4: Decrypt

Decrypt to obtain a cleartext result $res = \mathrm{Dec}_{sk}(c_{res})$.

The input: $c_{res} = 153222266277439889145067278920780277329449860799982992619964353065717569136826807959957008066704941488410702989174619469650071949675185407104459733704906$ and $sk = 471$

The details of the computation: Compute $res = LSB(c_{res} \bmod sk)$.

The resulting outcome of the step: $res = 1$.

7 Step 5: Verify the Result

Verify that the result is correct, i.e., check that $res = \text{AND}(\text{XOR}(a, b), c)$ if yes output res else output $Error$.

The input: $a = 1, b = 0, c = 1$ and $res = 1$

The details of the computation: $\text{AND}(\text{XOR}(a, b), c) = 1$ and therefore, $res = \text{AND}(\text{XOR}(a, b), c)$.

The resulting outcome of the step: $res = 1$.