Homework 03 Solutions

ECE 443/518, Fall 2024

Let's work on the garbled circuit between Alice and Bob who want to compute $f = NAND(a, b)$.

1. *(1 point)* Suppose 0 and 1 on each wire is encrypted into a 5-bit number (0 to 31). Alice chooses $A_0 = 7$, $A_1 = 17$, $B_0 = 19$, $B_1 = 3$, and $O_0 = 18$, $O_1 = 6$. What are S_A and S_B?

   Anwser:

   $$A_0 = 7 = (00111)_2, A_1 = 17 = (10001)_2$$

   $$B_0 = 19 = (10011)_2, B_1 = 3 = (00011)_2$$

   So $S_A = A_0(highest\ bit) = 0$ and $S_B = B_0(highest\ bit) = 1$.

2. *(1 point)* For the encryption function $e_{k_1||k_2}(x) = (k_1 + k_2 + x) \bmod 32$, show how Alice garbles the circuit. Suppose Alice chooses $a = 1$. What Alice should send to Bob as her input?

   Answer:

   $$e_{A_0,B_0}(O_1) = (7 + 19 + 6) \bmod 32 = 0$$

   $$e_{A_0,B_1}(O_1) = (7 + 3 + 6) \bmod 32 = 16$$

   $$e_{A_1,B_0}(O_1) = (17 + 19 + 6) \bmod 32 = 10$$

   $$e_{A_1,B_1}(O_0) = (17 + 3 + 18) \bmod 32 = 6$$

   Now we need to reorder them according to S_A and S_B, so Alice should send the reordered truth table $(S_A = 0, S_B = 0, 16)$, $(S_A = 0, S_B = 1, 0)$, $(S_A = 1, S_B = 0, 6)$, $(S_A = 1, S_B = 1, 10)$, or simply $(16, 0, 6, 10)$.

   For $a = 1$, Alice should send Bob 17.

3. *(1 point)* Suppose Bob chooses $b = 0$. Show how Bob encrypts his input with Alice's help using OT. Assume Alice's RSA public key to be $(n = 35, e = 5)$.

   Answer: First for RSA $k_{pub} = (n = 35, e = 5)$, Alice should compute $k_{pr} = (p = 5, q = 7, d = 5)$. Then OT goes as follows:

- Alice chooses two random numbers, say $x_0 = 1$ and $x_1 = 1$, and sends them to Bob.
- Bob picks $x_0 = 1$ since $b = 0$ and then chooses a random number, say $y = 3$. Bob computes v as follows and sends it to Alice.

$$v = (y^e + x_0) \bmod n = (3^5 + 1) \bmod 35 = 34$$

- Alice computes B_0' and B_1' accordingly and sends them to Bob.

$$B_0' = B_0 + ((v - x_0)^d \bmod n) = 19 + (33^5 \bmod 35) = 22$$

$$B_1' = B_1 + ((v - x_1)^d \bmod n) = 3 + (32^5 \bmod 35) = 5$$

- Bob uses B_0' to recover B_0

$$B_0 = B_0' - y = 22 - 3 = 19$$

4. *(1 point)* Show how Bob computes with the garbled circuit and the encrypted inputs, and then communicates with Alice to determine f.

   Answer: Now Bob knows $A = 17$ and $B = 19$, both with highest bit of 1, so he will use the last number among $(16, 0, 6, 10)$ to calculate O,

$$O = d_{17||19}(10) = 10 - 17 - 19 \bmod 32 = 6$$

   Bob sends $O = 6$ to Alice and then Alice reveals the output to be 1.

5. *(1 point)* Show that Bob cannot decide Alice's choice of a (assuming OT only reveals B_0 but no additional information). As a hint, is it possible for Alice to choose $A_0 = 17$, $A_1 = 7$ while sending Bob exactly the same garbled circuit and inputs?

   Answer: In such a case Alice will also have to choose $B_0 = 19$ as we want Alice to send Bob exactly same group of number except for those random numbers in OT. Therefore, now $S_A = S_B = 1$ and Alice could choose B_0, O_0, and O_1 differently by solving the equations below, assuming the same reordered truth table of $(16, 0, 6, 10)$

$$e_{A_0,B_0}(O_1) = (17 + 19 + O_1) \bmod 32 = 10$$

$$e_{A_0,B_1}(O_1) = (17 + B_1 + O_1) \bmod 32 = 6$$

$$e_{A_1,B_0}(O_1) = (7 + 19 + O_1) \bmod 32 = 0$$

$$e_{A_1,B_1}(O_0) = (7 + B_1 + O_0) \bmod 32 = 16$$

   We have a solution $O_1 = 6$, $B_1 = 15$, $O_0 = 26$.