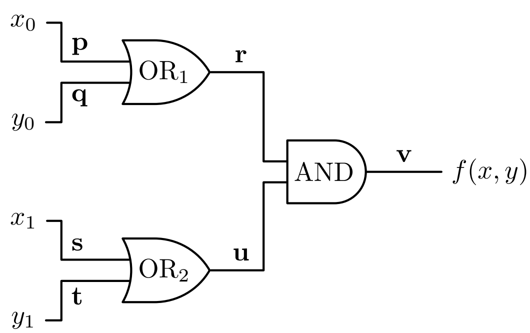
Privacy Protection Prof. Jean-Pierre Hubaux

Exercise: Garbled Circuits

October 7, 2016

The goal of this exercise is to gain some familiarity with Yao's garbled circuits. We will use Yao's scheme to allow two parties A and B with respective 2-bit inputs $x = x_0x_1$ and $y = y_0y_1$ to compute the function $f(x, y) = (x_0 \vee y_0) \wedge (x_1 \vee y_1)$. We use a simple encryption scheme based on the one-time pad over 4 bits. For a 4-bit key k and 4-bit plain text x, we have $E_k(x) = x \oplus k$.



The above figure represents the circuit of f. A's input bits (x_0 and x_1) are on the input wires **p** and **s**. B's input bits (y_0 and y_1) are on the input wires **q** and **t**.

a) You take the place of party A who is in charge of generating the garbled circuit. For the gate OR$_1$, you generate the following random keys:

Input wire **p** : $k^0_{\mathbf{p}} = 1010$ $k^1_{\mathbf{p}} = 1011$

Input wire **q**) : $k^0_{\mathbf{q}} = 0101$ $k^1_{\mathbf{q}} = 1111$

Output wire **r** : $k^0_{\mathbf{r}} = 1001$ $k^1_{\mathbf{r}} = 1100$

The keys $k^i_{\mathbf{p}}$ are *garbled values* for the two possible values of bit x_0. The keys $k^i_{\mathbf{q}}$ are garbled values for the two possible values of bit y_0. Finally, keys $k^i_{\mathbf{r}}$ are garbled values for the two possible output values of the gate.

Complete the garbled gate OR$_1$ below.

x_0	y_0	encryption	result
0	0	$k^0_{\mathbf{p}} \oplus k^0_{\mathbf{q}} \oplus k^0_{\mathbf{r}}$	0110
0	1		
1	0		
1	1		

b) You now take the place of party B to evaluate the circuit. From A, you receive all the garbled gates (OR$_1$, OR$_2$ and AND). You also receive A's garbled inputs $k_{\mathbf{p}} = 1011$ and $k_{\mathbf{s}} = 0001$. We assume that B's input is $y_0 = 0, y_1 = 0$. After running an oblivious transfer protocol with A, you obtain the garbled inputs $k_{\mathbf{q}} = 0101$ and $k_{\mathbf{t}} = 1101$.

At this point, B can't know the values of x_0 and x_1 because the garbled inputs $k_{\mathbf{p}}$ and $k_{\mathbf{s}}$ are random. The security of the oblivious transfer guarantees that A does not know y_0 and y_1.

The encrypted values for the garbled gate OR_2 are:

0111
1110
0010
1000

You know that exactly one of these values is the encryption of the garbled output $k_{\mathbf{u}}$ under keys $k_{\mathbf{s}}$ and $k_{\mathbf{t}}$. The problem is that you have no idea which one to decrypt! Yao's protocol actually requires the encryption scheme to be *checkable*, meaning that it should be easy for B to check whether a given cipher was indeed encrypted with a given key. The one time pad does not have this property, so to make things easier for you, we indicate (in bold) which entry in the garbled gate you should decrypt.

The garbled gate AND (that takes as inputs $k_{\mathbf{r}}$ and $k_{\mathbf{u}}$ is:

1110
0010
0101
0110

- What is the value of the garbled output $k_{\mathbf{u}}$ of OR_2?
- The garbled output of the gate OR_1 is $k_{\mathbf{r}} = 1100$. What is the garbled output of the circuit?
- Party A now reveals that the garbled outputs of the circuit are $k_{\mathbf{v}}^0 = 1111$ and $k_{\mathbf{v}}^1 = 0000$. What is the value of $f(x, y)$? What can B infer about x from $f(x, y)$? Could B also have inferred this information if B's input was something else than $y_0 = y_1 = 0$?