CS 6601 Secure Data Analysis - Fall 2017
Homework 1

Adam Bowers
Sammie Bush
Dalton Cole

September 21, 2017

Problem 1 Show how to construct the garbled circuit.

The normal circuit for constructing an "=" operator can be seen in Figure 1. A circuit labeled with wires can be seen in 2. To construct a garbled circuit, first each wire has to be assigned two random t bit strings. There are two strings to cover the 0 and 1 input cases. In an actual garbled circuit, t would be set to 80. For demonstrative purposes, t will be 8 in this case. Table 1 shows the random strings assigned to each wire where v_a^b such that a is the wire and b is the bit the string represents. Next, a permutation bit must be randomly chosen for each wire. This can be found in Table 2. The random permutation is appended to v_i^j to form w_i^j such that $w_k^0 = v_k^0 \| (0 \oplus p_k)$ and $w_k^1 = v_k^1 \| (1 \oplus p_k)$. Each w_i^j value can be seen in Table 3.

Following this, each truth table is replaced with it's corresponding Garbled-Truth-Table (GTT) by replacing each 0 or 1 with w_k^0 or w_k^1 respectively. The GTT is replaced by the Encrypted-Garbled-Truth-Table (EGTT) which is an encrypted version of the GTT. The encryption is performed by SHA1 hashing $v_i^x \| k \| x' \| y'$ with the plane text w_k^x where $x' = x \oplus p_i$ and $y' = y \oplus p_j$ and x, y are the entries in the original truth table. This encryption will be represented as $Enc(w_i^j)$.

To make the Permutted-Encrypted-Garbled-Truth-Table (PEGTT), the rows in the EGTT have to be swapped based on the following rule: if $p_i = 1$, the first two entries of the table are swapped with the last two entries; if $p_j = 1$, then the first and third are swapped and the second and fourth entries are swapped. The GTT, EGTT, and PEGTT for gate 0 can be found in Table 4.

Figure 1: Normal Circuit

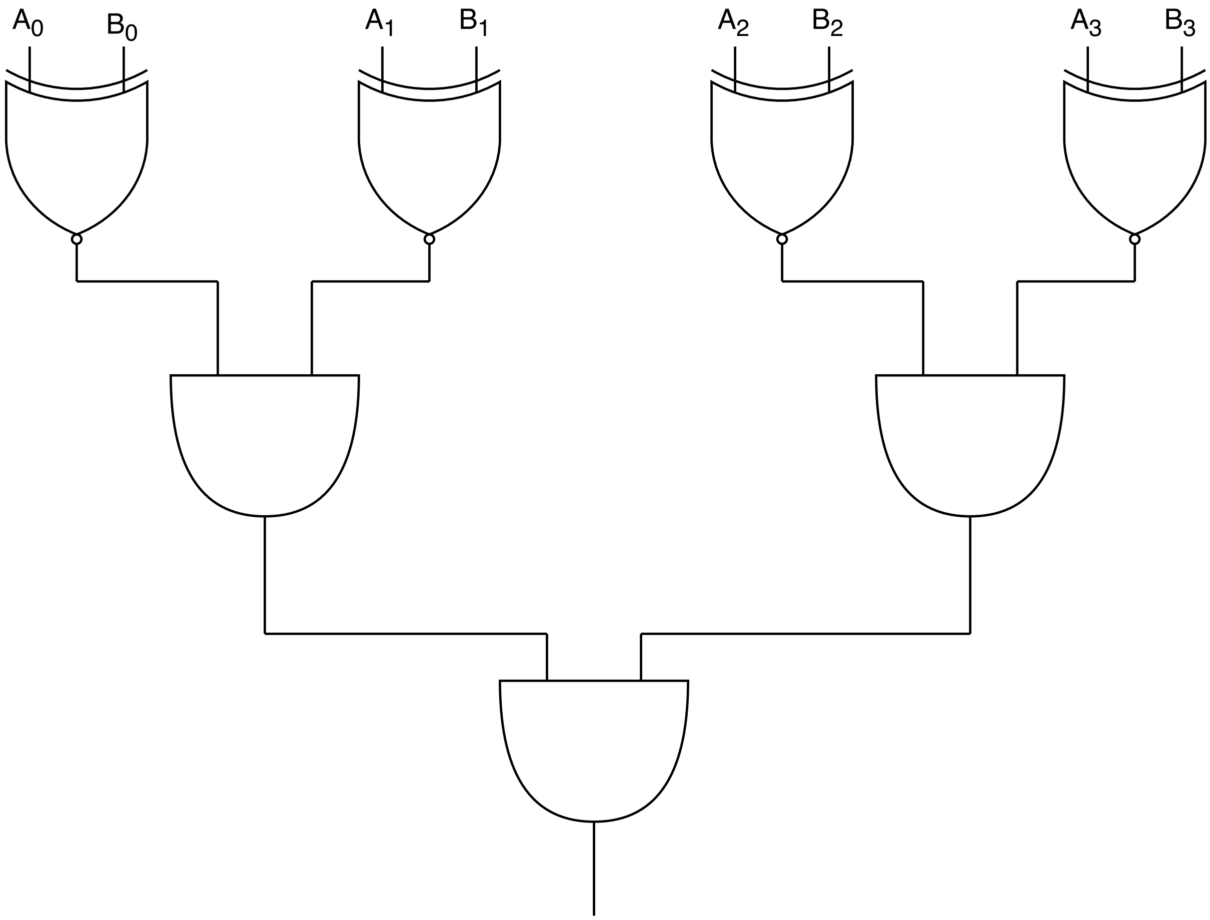

Table 1: Random t-bit Strings

$v_0^0 = 00000000$	$v_0^1 = 11111111$
$v_1^0 = 00000001$	$v_1^1 = 10000000$
$v_2^0 = 00000010$	$v_2^1 = 01000000$
$v_3^0 = 00000011$	$v_3^1 = 11000000$
$v_4^0 = 00000100$	$v_4^1 = 00100000$
$v_5^0 = 00000101$	$v_5^1 = 10100000$
$v_6^0 = 00000110$	$v_6^1 = 01100000$
$v_7^0 = 00000111$	$v_7^1 = 11100000$
$v_8^0 = 00001000$	$v_8^1 = 00010000$
$v_9^0 = 00001001$	$v_9^1 = 10010000$
$v_{10}^0 = 00001010$	$v_{10}^1 = 01010000$
$v_{11}^0 = 00001011$	$v_{11}^1 = 11010000$
$v_{12}^0 = 00001100$	$v_{12}^1 = 00110000$
$v_{13}^0 = 00001101$	$v_{13}^1 = 10110000$
$v_{14}^0 = 00001110$	$v_{14}^1 = 01110000$

Figure 2: Garbled Circuit Wires

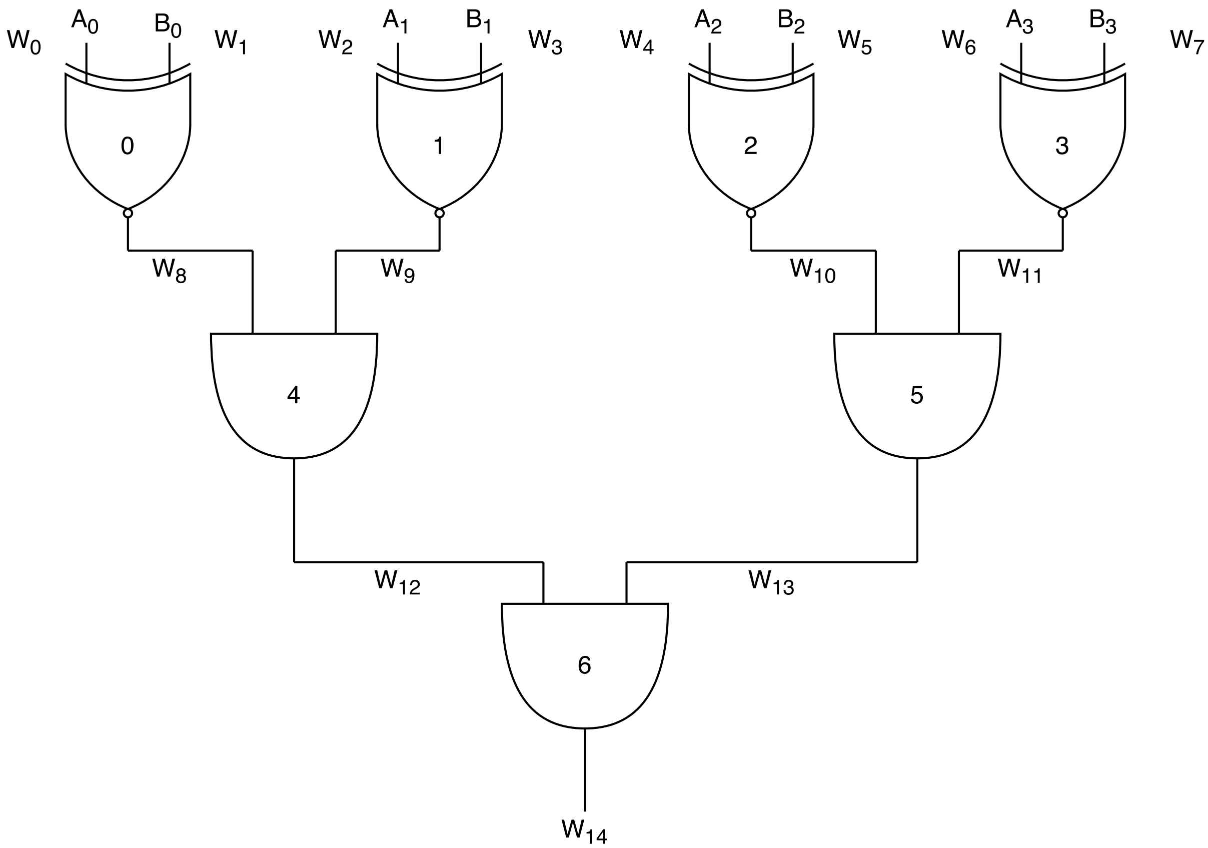

Table 2: Permutation Bit

$p_0 = 0$
$p_1 = 1$
$p_2 = 0$
$p_3 = 1$
$p_4 = 0$
$p_5 = 1$
$p_6 = 0$
$p_7 = 1$
$p_8 = 0$
$p_9 = 1$
$p_{10} = 0$
$p_{11} = 1$
$p_{12} = 0$
$p_{13} = 1$
$p_{14} = 0$

Table 3: Wire Strings

$w_0^0 = 000000000$	$w_0^1 = 111111111$
$w_1^0 = 000000011$	$w_1^1 = 100000000$
$w_2^0 = 000000100$	$w_2^1 = 010000001$
$w_3^0 = 000000111$	$w_3^1 = 110000000$
$w_4^0 = 000001000$	$w_4^1 = 001000001$
$w_5^0 = 000001011$	$w_5^1 = 101000000$
$w_6^0 = 000001100$	$w_6^1 = 011000001$
$w_7^0 = 000001111$	$w_7^1 = 111000000$
$w_8^0 = 000010000$	$w_8^1 = 000100001$
$w_9^0 = 000010011$	$w_9^1 = 100100000$
$w_{10}^0 = 000010100$	$w_{10}^1 = 010100001$
$w_{11}^0 = 000010111$	$w_{11}^1 = 110100000$
$w_{12}^0 = 000011000$	$w_{12}^1 = 001100001$
$w_{13}^0 = 000011011$	$w_{13}^1 = 101100000$
$w_{14}^0 = 000011100$	$w_{14}^1 = 011100001$

Table 4: GTT, EGTT, PEGTT for Gate 0

Truth Table			GTT			EGTT			PEGTT		
X	Y	Out	X	Y	Out	X	Y	Out	X	Y	Out
0	0	1	w_0^0	w_1^0	w_8^1	$Enc(w_0^0)$	$Enc(w_1^0)$	$Enc(w_8^1)$	$Enc(w_0^0)$	$Enc(w_1^0)$	$Enc(w_8^1)$