Cryptology

Read sections 7.1, 7.2, 7.3, 7.6 of chapter 7. We may get as far as to cover the first section of chapter 11.

Problems

To be discussed Wednesday, May 23, 2001.

1. Do problems 13.4.b, c, and d, 13.5, 13.6, and 7.4 in the textbook.

2. Consider MAJORITY gates with fan-in n, where $n = 2m+1$. The output should be one if at least $m+1$ of the inputs are one, and zero if at least $m+1$ of the inputs are zero. Suppose that user A has committed to n input bits, $b_1, b_2, ..., b_n$, and one output bit b_{n+1}, and produced blobs (bit commitments) $B_1, B_2, ..., B_n, B_{n+1}$, using the scheme based on the Goldwasser-Micali probabilistic encryption (pages 399-400 in the textbook). If user A wishes to prove to user B that $B_1, B_2, ..., B_n$, are commitments to the inputs to a MAJORITY gate and B_{n+1} is a commitment to the output of that same MAJORITY gate, user A only need show that there are $m+1$ inputs which are equal to the output. In order to hide which of the inputs are the same as the output, user A will produce n more blobs corresponding to the original input blobs for that gate. These additional n blobs will be encryptions of the same bits as the input blobs, but user A will send them to user B in random order, so user B will be unable to determine the correspondence. Now, user B will send user A a challenge $c \in \{0, 1\}$. If $c = 0$, user A will show user B the correspondence between the input blobs and the n additional blobs, telling user B which additional blob corresponds to which original input blob and proving it using the equality property (see problem 3 for May 2). If $c = 1$, user A will show that $m+1$ of the additional blobs are commitments to the same bit as B_{n+1} is, again using the equality property. Thus, the protocol is as follows ("random" means independently, from a uniform distribution):

Repeat the following $k(n+1)$ times, where k is the length of the blobs produced:

User A: Choose random $r_1, r_2, ..., r_n \in Z_N^*$.
Create $C_i = y^{b_i} r_i^2 \pmod N$, for $1 \le i \le n$.
Choose a random permutation σ of the numbers $1, 2, ..., n$.
Send user B the blobs $(D_1, D_2, ..., D_n) = (C_{\sigma(1)}, C_{\sigma(2)}, ..., C_{\sigma(n)})$.

User B: Choose random $e \in \{0, 1\}$.
Send e to user A.

User A: Case $e = 0$: Send σ to user A.
Use the equality property to show that $B_{\sigma(i)}$ and D_i are encryptions of the same bit, for $1 \le i \le n$.

Case $e = 1$: Choose a subset $\{D_{i_1}, D_{i_2}, ..., D_{i_{m+1}}\}$ of the D_is of size $m+1$, such that those D_i's are encryptions of the same bit as the output blob B_{n+1}. (If there are more than $m+1$ satisfying this, choose among them randomly.) Use the equality property to show that D_{i_j} and B_{n+1} are encryptions of the same bit, for $1 \le j \le m+1$.

User B accepts if user A has correctly answered all challenges and rejects otherwise.

a Show that the protocol described above is an interactive proof system proving that $B_1, B_2, ..., B_n$, are commitments to the inputs to a MAJORITY gate and B_{n+1} is a commitment to the output of that same MAJORITY gate.

b Show that the protocol described above is computational zero-knowledge, assuming the Quadratic Residuosity Assumption.

3. Use problem 2 to design a computational zero-knowledge interactive proof system proving that B_1 and B_2 are commitments to the inputs to an OR gate and B_3 is a commitment to the output to that same OR gate. (Hint: note that an OR gate has an even number of inputs, but the MAJORITY gate described above has an odd number of inputs. Try adding a special extra input to the OR gate.)