Foundations of Privacy

Home Set 1
Date Due: April 15th

1. Our goal is to construct a 1-out-of-N OT protocol (secure against honest-but-curious adversaries) from any 1-out-2 OT protocol (secure in the same sense). Consider the following protocol:

   - The sender has input $X_0, X_1, \ldots, X_{N-1}$, where $N = 2^n$, and the chooser has input $0 \le I^* \le N-1$.
   - The sender prepares n pairs of random strings $(W_1^0, W_1^1), \ldots, (W_n^0, W_n^1)$, and for every $0 \le I \le N-1$ sets $Y_I = X_I \bigoplus_{j=1}^{n} W_j^{i_j}$ where $i_1 \cdots i_n$ is the binary representation of I. The strings $Y_1, \ldots, Y_N$ are sent to the chooser.
   - For every $1 \le j \le n$, the parties execute a 1-out-of-2 OT protocol on the strings (W_j^0, W_j^1) in which the chooser wishes to learn $W_j^{i_j^*}$, where $i_1^* \cdots i_n^*$ is the binary representation of I^*.
   - The chooser reconstructs $X_{I^*} = Y_{I^*} \bigoplus_{j=1}^{n} W_j^{i_j^*}$.

   (a) Show that this is NOT a good protocol for 1-out-of-N OT (no matter what 1-out-of-2 OT protocol is used).

   (b) Consider now a similar protocol, except that the masking of the X_I's is done differently. Let F_S be a pseudorandom function and treat the W_j^b's as keys to the function. Let $Y_I = X_I \bigoplus_{j=1}^{n} F_{W_j^{i_j}}(I)$. The rest of the protocol is as before, except that now the chooser reconstructs X_{I^*} by computing $Y_{I^*} \bigoplus_{j=1}^{n} F_{W_j^{i_j^*}}(I)$. Prove that this is a good 1-out-of-N protocol.

2. Recall the DDH based protocol for 1-out-of-2 Oblivious Transfer where the Chooser has a bit $\sigma \in \{0,1\}$ and wants learns m_σ. The chooser prepares $x = g^a$, $y = g^b$, $z_\sigma = g^{ab}$ and $z_1 - \sigma \ne z_\sigma$ and send (x, y, z_0, z_1). The sender chooses (r_0, s_0) and (r_1, s_1) and computes $w_0 = x^{s_0} \cdot g^{r_0}$ and $w_1 = x^{s_1} \cdot g^{r_1}$. The sender then encrypts m_0 using w_0 and m_1 using w_1.

   Suggest a generalization of this protocol to 1-out-of-N that does not increase the work by the chooser.

3. Recall that in a secret sharing scheme the goal is to split a secret s to between n participants $p_1, p_2 \ldots p_n$ so that

   - Any legitimate subset of participants should be able to reconstruct s.
   - No illegitimate subsets should learn anything about s.

The legitimate subsets are defined by a (monotone) access structure $\mathcal{A}$. Recall also that for any access structure there is a sharing scheme where the size of the shares is related to the total number of minimal subsets in $\mathcal{A}$.

Suppose that $\mathcal{A}$ is defined by a monotone formula of size L (i.e. the subsets satisfying it are those that correspond to truth assignments to the formula). Show that there is a sharing scheme where the size of the shares is related to L.