1-out-of-n Oblivious Transfer

Suppose A has a list $(x_1, \ldots, x_n)$, B has $i \in \{1, \ldots, n\}$.

We want a SFE protocol where $F_A = 0, F_B = x_i$, that is,

1. B learns x_i and nothing else
2. A learns nothing about i

Theorem: [Kilian'87] 1-out-of-2 OT is universal for 2-party SFE

In other words, given a 1-out-of-2 OT protocol, one can do any 2-party SFE. (Yao's construction requires a block cipher in addition to a 1-out-of-2 OT protocol.)

Note that oblivious transfer implies 2-party SFE, which implies key exchange, and hence 1-out-of-2 OT cannot be built from a blackbox one-way function. Instead, we build one using the DDH assumption [Bellare-Micali'92].

Bellare-Micali Construction

Let G be a group of prime order p, and let $g \in G$ be a generator, and $H : G \to \{0,1\}^n$ be a hash function.

Suppose A has $x_0, x_1 \in \{0,1\}^n$, and B has $b \in \{0,1\}$.

1. A publishes a random $c \leftarrow G$, B picks $k \leftarrow \mathbb{Z}_p$, sets $PK_b = g^K, PK_{1-b} = c/g^k$ and sends PK_0, PK_1 to A. A checks $PK_0 PK_1 = c$.
2. A encrypts x_0 with El Gamal using PK_0, i.e. sets $C_0 = [g^{r_0}, H(PK_0^{r_0}) \oplus x_0]$, encrypts x_1 using PK_1, and sends C_0, C_1 to B.
3. B decrypts C_b using K, i.e. if $C_b = [V_1, V_2]$, B computes $X_b = H(V_1^K) \oplus V_2$.

Security: A cannot learn anything about b (information theoretic result).

If B is honest-but-curious, then assuming DDH, B can only decrypt one of C_0 or C_1.

If B is malicious, then assuming DDH is not enough: conceivably B could generate PK_0, PK_1 in such a way that B knows partial information about their corresponding private keys, and perhaps B can then learn partial information about both x_0 and x_1. However, if H is a random oracle, then the protocol is secure under CDH.

Naor-Pinkas Construction

[Naor, Pinkas '00] Let G be a group of prime order q and let $g \in G$ be a generator. Suppose A has m_0, m_1 and B has $V \in \{0,1\}$.

1. B sends the tuple $(g, x = g^a, y = g^b, z_0 = g^{c_0}, z_1 = g^{c_1}$ to A, where $a, b \leftarrow \mathbb{Z}_q$, $c_v = ab$ and $c_{1-v} \leftarrow \mathbb{Z}_q$.

2. A verifies that $z_0 \neq z_1$ and applies a partial DDH random self-reduction: (g, x, y, z_0) becomes $T_0 = (g, x, y_0, z_0')$, and (g, x, y, z_1) becomes $T_1 = (g, x, y_1, z_1')$.

3. A encrypts m_0 using T_0 and m_1 using T_1, that is, A sends to B the ciphertexts $(CT_0 = (y_0, mz_0'), CT_1 = (y_1, mz_1'))$.

4. B decrypts CT_v.

This protocol is information theoretically secure against B, and DDH secure against A. The random self-reduction destroys any partial information in the message B sends to A. Note that this construction also generalizes to a 1-out-of-n protocol.

DDH Random Self-Reduction

Suppose we have a tuple g, g^x, g^y, g^z. Then to perform a random self-reduction, pick random $a, b \leftarrow \mathbb{Z}_p^*$, and output $g, g^{(x+b)a}, g^y, g^{(z+by)a}$.

Note that this transformation takes DH-tuples to DH-tuples, and non-DH-tuples to non-DH-tuples. Furthermore, the new exponents are independent of the originals. This is easy to see if we start with a DH tuple. On the other hand, if the tuple is not DH, then given any x', z', there exists a unique a, b such that $(x + b)a = x', (z + by)a = z'$ (we can solve to get $a = (z' - x'y)/(z - xy)$ and b can be easily determined from a). As expected, these solutions are

not well defined if $z = xy$, i.e. the original tuple is DH.

1-out-of-n From 1-out-of-2

We show how to construct a 1-out-of-n OT protocol from any 1-out-of-2 OT protocol.

Suppose A has $m_0, \ldots, m_N \in \{0,1\}^n$ and B has $t \in \{0, \ldots, N\}$. Assume $N = 2^l - 1$ for some l.

1. A prepares $2l$ keys $(K_1^0, K_1^1), \ldots, (K_l^0, K_l^1)$.
2. Let $F_k : \{0,1\}^l \to \{0,1\}^n$ be a PRF. A sends to B the tuple $(C_0, \ldots, C_N)$: view the message index as a bit string $I = I_1 \ldots I_l \in \{0,1\}^l$, and encrypt using

   $$C_I = m_I \oplus \oplus_{i=1}^{l} F_{K_i^{I_i}}(I)$$

   Note A sends $O(N)$ bits to B.
3. Let $t = t_1 \ldots t_l \in \{0,1\}^l$. Then l 1-out-of-2 OT's are performed where during the jth OT, A has (K_j^0, K_j^1) and B has $t_j \in \{0,1\}$.
4. B now has $K_1^{t_1}, \ldots, K_l^{t_l}$ and can decrypt C_t to get m_t.

Thus with $\log N$ 1-out-of-2 OT's, a single 1-out-of-N OT can be constructed, that has $O(N)$ communication complexity.

[My Homepage] *Email: blynn pleasedontspamme at cs dot stanford dot edu*