1 Lecture 11

1.1 One-Out-Of-Two (OT)

At the beginning of this lecture, we should introduce three basic concepts for OT:

- **R-OT,** or Rabin's OT, permits Alice to send a bit b to Bob. Bob receives b with 50-50 probability and knows whether he received the bit. Alice does not know whether Bob received the bit. This has been given in the last class.
- $\begin{pmatrix} 2 \\ 1 \end{pmatrix} - OT$, or "one-out-of-two" OT, permits Alice to send one of two bits, b_0 or b_1, to Bob. Bob chooses an index c and receives b_c. Alice does not learn c.

The following figure describes the second case:

$$A \qquad \begin{array}{c} b_0 \longrightarrow \\ b_1 \longrightarrow \end{array} \left[\begin{pmatrix} 2 \\ 1 \end{pmatrix} - OT \right] \begin{array}{c} \longleftarrow c \\ \longrightarrow b_c \end{array} \qquad B$$

Here the implementation assumes that Bob can not distinguish between $QR_n[+1]$ and $QNR_n[+1]$ given $(\frac{y}{n}) = 1$.

$$
\begin{array}{ccc}
 & n,\ y \in QNR_n[+1] & \\
A & & B \\
 & \xrightarrow{ZK\ (y \in QNR_n[+1])} &
\end{array}
$$

$$
\begin{aligned}
z_0 &= r_0^2\, y_0^{b_0} \\
z_1 &= r_1^2\, y_1^{b_1} \\
& (mod\ n)
\end{aligned}
$$

$$\xrightarrow{z_0,\ z_1}$$

$$
\begin{aligned}
& w \leftarrow z_c * r^2 * y^b, \\
& r \in_R Z_n^*, \\
& b \in_R \{0,\ 1\}
\end{aligned}
$$

$$\xleftarrow{w}$$

$$\xrightarrow{\left(\frac{w}{p}\right)}$$

$$\left(\frac{z_c}{p}\right) = (-1)^b \left(\frac{w}{p}\right)$$

Here, $\left(\frac{w}{p}\right)$ is the Legendre Symbol. If $w \in QR_n$, $\left(\frac{w}{p}\right) = 1$, otherwise $\left(\frac{w}{p}\right)$ = -1. (since $\left(\frac{w}{n}\right) = \left(\frac{w}{p}\right)\left(\frac{w}{q}\right)$). Bob knows the value of $\left(\frac{w}{p}\right)$, but he has no knowledge about p. Using $\left(\frac{z_c}{p}\right) = (-1)^b \left(\frac{w}{p}\right)$ Bob can compute the Legendre Symbol of z_c with p.

Let's modify the previous scheme in order to impose that w has the following forum: $w = z_c * r^2 * y^b$:
In the following figure, let ς be the security parameter such that the probability is $< \frac{1}{2^\varsigma}$ that *Bob* could succeed in convincing *Alice* that its questions are built properly on the two bit commitments of *Alice*.

	Alice		*Bob*
1	$r_0, r_1 \in_R \mathbb{Z}_n^*$ $z_0 \leftarrow {r_0}^2\, y_0^b \text{ mod } n$ $z_1 \leftarrow {r_1}^2\, y_1^b \text{ mod } n$	$\xrightarrow{(z_0, z_1)}$	
2		$\xleftarrow[(w_0, w_1)]{}$	$s_0, s_1 \in_R \mathbb{Z}_n^*$ $a_0, a_1 \in_R \{0, 1\}$ $w_0 \leftarrow z_0\, s_0^2\, y^{a_0} \text{ mod } n$ $w_1 \leftarrow z_1\, s_1^2\, y^{a_1} \text{ mod } n$
3		$\xleftarrow[\{(w_0^i, w_1^i)\}_{1 \le i \le \varsigma}]{}$	$s_{0_i}, s_{1_i} \in_R \mathbb{Z}_n^*$ $a_{0_i}, a_{1_i}, c_i \in_R \{0, 1\}$ ${w_{c_i}}^i \leftarrow z_0\, {s_{0_i}}^2\, y^{a_{0_i}} \text{ mod } n$ ${w_{\overline{c_i}}}^i \leftarrow z_1\, {s_{1_i}}^2\, y^{a_{1_i}} \text{ mod } n$ $1 \le i \le \varsigma$
4	$Define\ \mathcal{P}\ and\ \mathcal{O}\ such\ that:$ $\mathcal{P} \cup \mathcal{O} = \{1, 2, \ldots, \varsigma\}$ $\mathcal{P} \cap \mathcal{O} = \emptyset$	$\xrightarrow{\mathcal{P}, \mathcal{O}}$	
5		$\xleftarrow[\{(\theta_i, \delta_{0_i}, \delta_{1_i}, u_{0_i}, u_{1_i})\}_{i \in \mathcal{P}}]{}$ && $\{(c_i, a_{0_i}, a_{1_i}, s_{0_i}, s_{1_i})\}_{i \in \mathcal{O}}$	$\theta_i = c \oplus c_i$ $\delta_{c_i} = a_c \oplus a_{c_i}$ $\delta_{\overline{c_i}} = a_{\overline{c}} \oplus a_{\overline{c_i}}$ $u_c \leftarrow z_c\, s_c\, s_{c_i}\, y^{a_c \wedge a_{c_i}} \text{ mod } n$ $u_{\overline{c}} \leftarrow z_{\overline{c}}\, s_{\overline{c}}\, s_{\overline{c_i}}\, y^{a_{\overline{c}} \wedge a_{\overline{c_i}}} \text{ mod } n$ $i \in \mathcal{P}$
6	Verify : $w_{\theta_i}^i w_0 \equiv {u_0}^2\ y^{\delta_{0i}} \pmod{n}$ $w_{\overline{\theta_i}}^i w_1 \equiv {u_1}^2\ y^{\delta_{1i}} \pmod{n}$ $i \in \mathcal{P}$ $w_{c_i}^i \equiv z_0\, s_{0_i}^2\, y^{a_{0_i}} \text{ (mod } n)$ $w_{\overline{c_i}}^i \equiv z_1\, s_{1_i}^2\, y^{a_{1_i}} \text{ (mod } n)$ $i \in \mathcal{O}$		
7		$\xleftarrow[\tau]{}$	$\tau \leftarrow s \oplus c$
8	$\beta \leftarrow (w_\tau \in Q_n)$? 0 else 1 $\omega \in \mathbb{Z}_n \| w_\tau y^\beta \equiv w^2 \pmod{n}$	$\xrightarrow{\beta \text{ and } \omega}$	Verify $w_\tau y^\beta \equiv \omega^2 \pmod{n}$
9			$b_s \leftarrow \beta \oplus a_\tau$

Note: the second row is ZK proof.

1.2 Trapdoor Permutation

What is a trapdoor π?
π is trapdoor one-way function or permutation.
It implies:

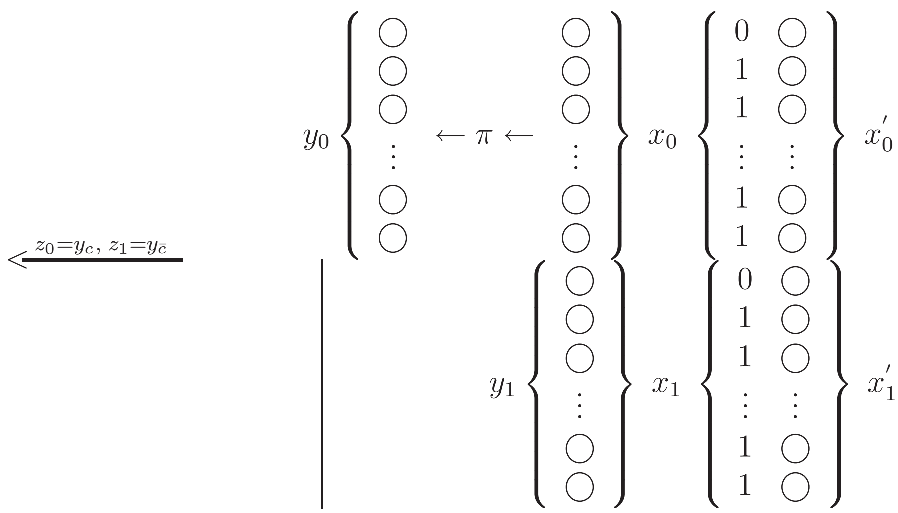
- π is a one-way function or permutation.
- π^{-1} can be computed efficiently given "a trapdoor".

If we have one-way function, then we can have a digital signature scheme, but we need trapdoor one-way permutation to have a public key scheme. Trapdoor functions are harder to get than one-way permutation.

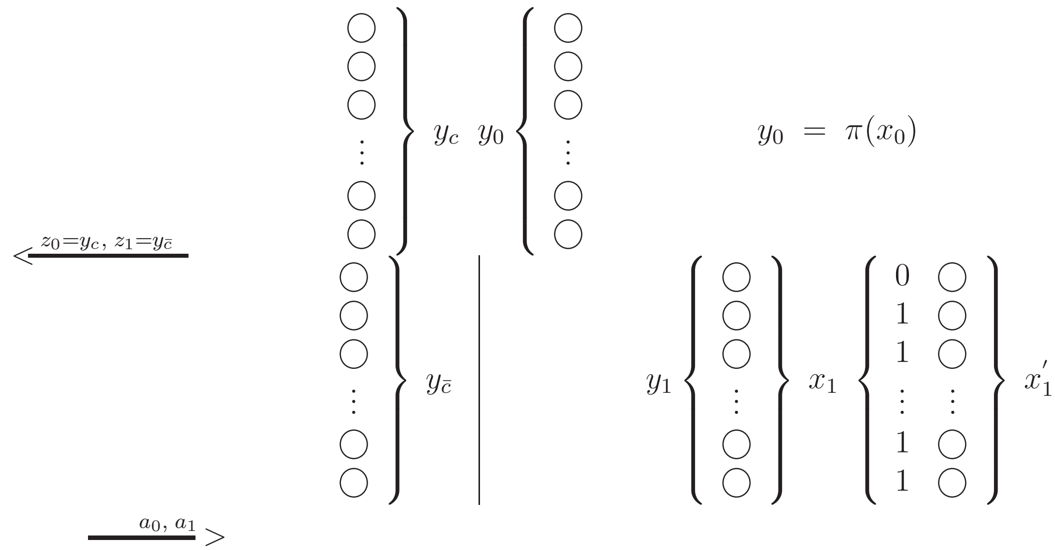
$$\pi\ (a\, T - D - O - W - P)$$
$$f:\ a\ hard\ core\ predicate\ of\ \pi$$
$$(given\ \pi(x),\ it\ is\ difficult\ to\ predicate\ f(x))$$

$$\begin{array}{ccc}
A & & B \\
 & & y_0 \leftarrow \pi \leftarrow x_0 \\
 & & y_1 \in_R \mathbb{Z}_n^* \\
 & \xleftarrow{z_0 = y_c,\ z_1 = y_{\bar{c}}} & \\
A\ naive\ way: & & \\
w_0 = \pi^{-1}(z_0), & & \\
w_1 = \pi^{-1}(z_1), & & \\
a_0 \leftarrow f(w_0) \bigoplus b_0, & & \\
a_1 \leftarrow f(w_1) \bigoplus b_1, & & \\
 & \xrightarrow{a_0,\ a_1} & \\
 & & b_c \longleftarrow a_c \bigoplus f(x_0),
\end{array}$$

In this scheme, Bob can cheat by choosing $y_1 = \pi(x_1)$, but this will be fixed later. Alice can not find out which is the bit that Bob is interested in by OT. So the scheme is modified as follows:



Bob commits x_0' and x_1' before Alice sends the two random numbers. So he cannot change his mind. Instead of ZK proving $y_0 = \pi(x_0)$ above, we can only prove $y_1 = x_1$. Thus the above scheme will change into:



In this scheme, firstly we will do the right-up section and then do the right-down section. Repeat y_{c_i} and $y_{\bar{c}_i}$ k times, we must show:

- $y^i_{c_i}$ and $y^i_{\bar{c}_i}$ are the same as y_0 and y_1.
- $y^i_{c_i}$ and $y^i_{\bar{c}_i}$ are the same as y_c and $y_{\bar{c}}$.
  .