1 Lecture 9

1.1 General B.C. from any one-way permutation

Example 1.1

$$\pi\{0,1\}^n -> \{0,1\}^n$$

$$\begin{array}{rcl}
P & & V \\
 & & r \in_R \{0,1\}^n \\
 & \xleftarrow{\;r,\ \pi\;} & \\
x \in_R \{0,1\}^n & & \\
y_0 = \pi(x) & & \\
y_1 = y_0 \oplus r & & \\
 & \xrightarrow{\;y_b\ \ (y_{\bar{b}})\;} & \\
 & \xrightarrow{\;unveil\ \ x,\ b\;} &
\end{array}$$

This is not a good example, because if P is powerful enough P can find a $x' \in_R \{0,1\}^n$ s.t. $y_1 = \pi(x')$, then P can unveil both ways and cheat V easily.

Therefore we shall do it another way to improve it.

Example 1.2 *Let* $h : (H)_{n\times n-1}$.

$$\begin{array}{rcl}
P & & V \\
 & \xleftarrow{\;h,\ \pi\;} & \\
x \in_R \{0,1\}^n & & \\
y_0 = \pi(x) & & \\
y_1 \neq y_0 \ \ s.t. & & \\
h(y_0) = h(y_1) & & \\
 & \xrightarrow{\;y_b\ \ (y_{\bar{b}})\;} & \\
 & \xrightarrow{\;unveil\ \ x,\ b\;} &
\end{array}$$

Since the rank of H is n-1, there are two solutions for $(H)(w) = (0\,0 \cdots\ 0)^T, w = (0\ 0, \cdots, 0)$ or w=r s.t. $(H)(y_0 + r) = (H)(y_0)$. If P let $y_1 = y_0 + r$ $(y_1 \neq y_0$, but $h(y_0) = h(y_1)$), then P can cheat V. Therefore this model is "equivalent" to previous one, which is not good either.

Example 1.3 *Now we shall give the third model to deal with the problem.*

$$\begin{array}{rcl}
P & & V \\
 & \xleftarrow{H,\ \pi} & \\
x \in_R \{0,1\}^n & & \\
y_c = \pi(x) & & \\
y_c \neq y_{\bar{c}}\ s.t. & & \\
h(y_c) = h(y_{\bar{c}}) & & \\
 & \xrightarrow{h(y_0),\ y_0<y_1,\ b\oplus c} & \\
 & \xrightarrow{c,\ b} &
\end{array}$$

After P unveil b, V knows c (since V knows the result of $b \oplus c$*),*
if c=0, check $h(y_0) = \pi(x)$;
if c=1, check $h(\pi(x)) = h(y_0)$.

However this model has the same problem as the previous models: V gives the whole matrix H to P, therefore P can find the two solutions (y_0, y_1) of H then cheat V.

Now we shall give a model which can solve the problem. The different between this model and previous ones lies in that V gives H line by line in $\odot$, instead of giving the whole matrix at one time.

Example 1.4

$$\begin{array}{rcl}
P & & V \\
 & \xleftarrow{H_1,\ \pi} & \\
x \in_R \{0,1\}^n & & \\
y_c = \pi(x) & & \\
y_{\bar{c}} =? & & \\
 & \xrightarrow{H_1 \odot y_c} & \\
 & \xleftarrow{H_2} & \\
 & \xrightarrow{H_2 \odot y_c} &
\end{array}$$

$$\vdots$$

$$\vdots$$

$$\xleftarrow{H_{n-1}}$$

$$\xrightarrow{H_{n-1}\odot y_c}$$

$$\xrightarrow{c\oplus b, y_0<y_1}$$

Now we are going to show that the protocol is binding, i.e. we shall show that Prob (P cheats but caught by V) is quite big. Given $Z \in_R \{0,1\}^n$, *we want to find inverter* I *of* $\pi^{-1}(z)$, *s.t.*

$$Pr(I(z) = \pi^{-1}(z)) \geq 1/poly(n).$$

$$\pi, z \in_R \{0,1\}^n, H_i \in_R \{0,1\}^n, i = 1, \cdots, n, H_i \odot (H)^T = 0, \; for \; all \; i \neq j.$$

P'	$I(z)$
	$H_1 \in_R \{0,1\}^n$,
$\xleftarrow{H_1,\ \pi}$	
	$\uparrow$ *no : repeat and send another* H_1,
$\xrightarrow{b_1}$	$b_1 = H_1 \odot z$,
	$\downarrow$ *yes : continue and send* H_2,
$\xleftarrow{H_2}$	
	$\uparrow$ *no : repeat and send another* H_2,
$\xrightarrow{b_2}$	$b_2 = H_2 \odot z$,
	$\downarrow$ *yes : continue and send* H_3,
$\vdots$	
$\vdots$	
$\xleftarrow{H_{n-1}}$	
	$\uparrow$ *no : repeat and send another* H_{n-1},
$\xrightarrow{b_{n-1}}$	$b_{n-1} = H_{n-1} \odot z$,
$\xrightarrow{c\oplus b,\ y_0<y_1}$	

Note:

1. Inverter need to make sure that choosing H_i, independent with $H_1, \cdots H_{i-1}$.

2. Since I picks H_i at random, half probability b_i is 0, half probability b_i is 1.

3. Inverter verifies $z \in \{y_0,\ y_1\}$.

Pr(can unveil 0) + Pr(can unveil 1) > 1+1/poly(n)

$\pi(x) \in \{y_0, y_1\}$

unveil x, b $x = \pi^{-1}(z)$ with Prob>1/poly(n)