1 Lecture 7

1.1 bit commitment

1.$OWP \ + \ HCP \ \rightarrow \ BC$
2.$OWF \ + \ HCP \ \rightarrow \ PRBG$
3.$PRBG \ \rightarrow \ BC$

We did 1. and 2. in the last lecture and now we are going to do 3.. Let $g : \{0,1\}^n \rightarrow \{0,1\}^{3n}$ be a Pseudo-Random bit generator.

- Bob picks a random $r \in_R \{0,1\}^{3n}$, and sends it to Alice,
- to commit to b=0, Alice sends $g(x)$ for random $x \in_R \{0,1\}^n$; to commit to b=1, Alice sends $g(x) \bigoplus r$ for random $x \in_R \{0,1\}^n$,
- to unveil Alice sends b, x.

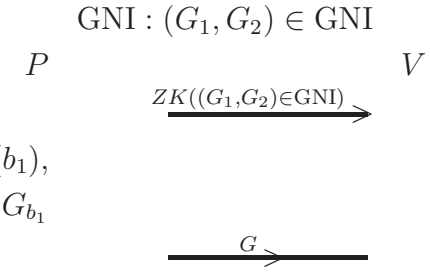
"**Concealing**": follows from Pseudo-Rrandomness of g.
"**Binding**": To cheat Alice needs $x_0, \ x_1$, s.t. $g(x_0) = w = g(x_1) \bigoplus r$. This means $g(x_0) \bigoplus g(x_1) = r$.

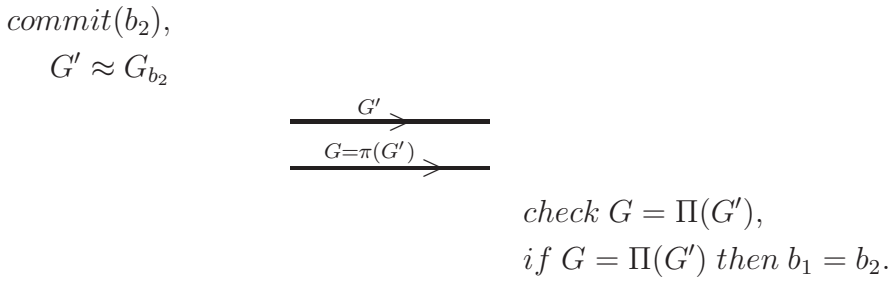
Since x $\in \{0,1\}^n$, then g(x) has at most 2^n possible values, hence $g(x_0) \oplus g(x_1)$ has at most 2^{2n} possible values. Therefore, Prob of cheating:

$$Prob \ (\exists \ x_0, \ x_1, \ s.t. \ g(x_0) \oplus g(x_1) = r) \ \leq 2^{2n}/2^{3n} = 1/2^n.$$

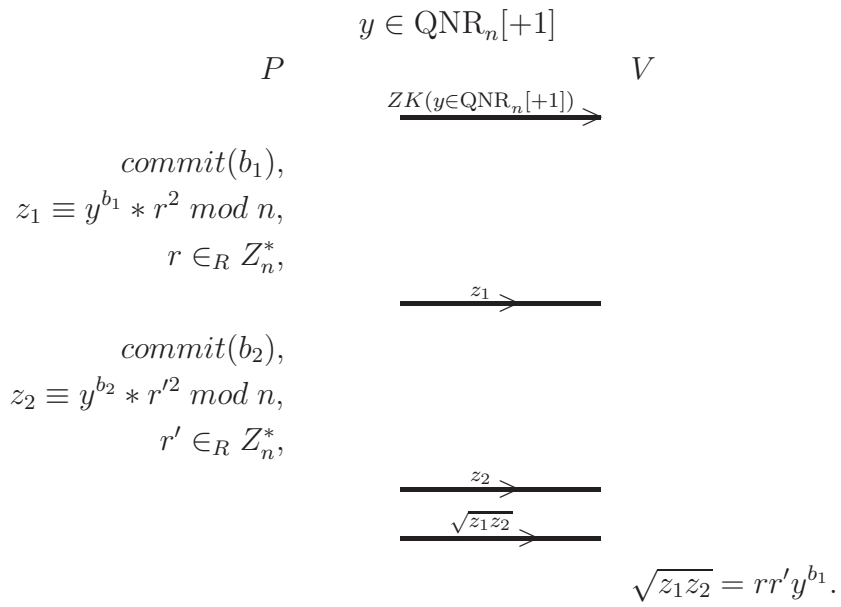
1.2 Comparing the equality of the two committed inputs

Example 1.1 *Comparing the equality of two committed bits using bit commitment based on* GNI.





Example 1.2 *Comparing the equality of two committed bits using bit commitment based on* QNR.



To prove $b_1 \neq b_2$ P sends $\sqrt{yz_1z_2}$.

1.3 Computation on boolean circuits using committed inputs

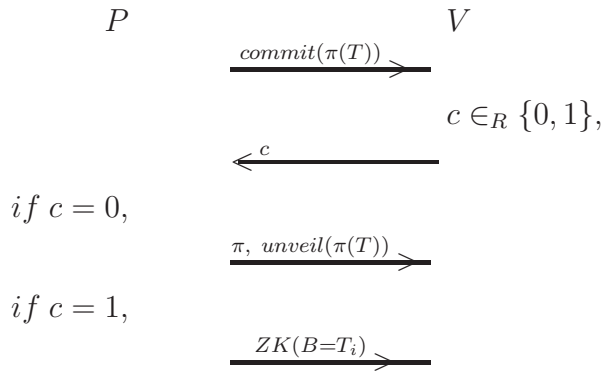
We shall use the previous two examples to do computations on boolean circuits. Prover commits to three bits: $b_1,\ b_2,\ b_3 \in \{0,1\}$, s.t. B: $b_1 \wedge b_2 = b_3$.

There are only four possible situations of B (see Table T), i.e. B (three bits) must belong to one of the following situation T_j (three bits).

Table T

$$T_1 : 0 \wedge 0 = 0$$
$$T_2 : 0 \wedge 1 = 0$$
$$T_3 : 1 \wedge 0 = 0$$
$$T_4 : 1 \wedge 1 = 1$$

We design the protocol by using the "Cut and Choose" technique in order to prove that $B \in T$. P permutes the Table T then commit to $(\pi(T))$ to V.



Note:

1. π is a permutation of Table T.

2. Using example 1.1, P can show to V that the three committed bits B: b_1, b_2 and b_3 are equal to the three committed bits of T_i respectly.

If $b_1 \wedge b_2 = b_3$, Pr[accept]=1,
If $b_1 \wedge b_2 \neq b_3$, Pr[accept]$\leq 1/2^k$, where k=# of rounds.
We can use this method for any logical gate: $\wedge, \vee, -, \oplus$.

1.4 Rudich's Trick

Now we are going to talk about a general way to obtain a bit commitment where we can prove equality based on any bit commitment. Here "Rudich's Trick" is the way to show two committed bits are equal.

Suppose $b = b'$, where $b, b' \in \{0, 1\}$, let u_i, x_i be random bits and v_i, y_i be defined according to $u_i \oplus v_i = b,\ x_i \oplus y_i = b',\ i = 1, \cdots 2n$. We shall use 4n committed bits to commit one bit.

	Alice	*Bob*
	$commit(b):$	$commit(b'):$
$\alpha_1:$	$C(u_1), C(v_1)$	$C(x_1), C(y_1) : \beta_1$
$\alpha_2:$	$C(u_2), C(v_2)$	$C(x_2), C(y_2) : \beta_2$
	$\vdots$	$\vdots$
$\alpha_n:$	$C(u_n), C(v_n)$	$C(x_n), C(y_n) : \beta_n$

where α_i and β_i are two committed bits and C denotes commit.

- Bob imposes two random permutations π_α, π_β to Alice who permutes α_i using π_α and β_i using π_β.

$C(u_9), C(v_9)$	$C(x_2), C(y_2)$
$C(u_n), C(v_n)$	$C(x_7), C(y_7)$
$\vdots$	$\vdots$
$C(u_3), C(v_3)$	$C(x_6), C(y_6)$

- Regardless of b, u_i, x_i and v_i, y_i are either identical or opposite. Alice will claim for the first half of the lines whether they are "=" or "$\neq$".

$C(u_9), C(v_9)$	$=$	$C(x_2), C(y_2)$
$C(u_n), C(v_n)$	$\neq$	$C(x_7), C(y_7)$
$\vdots$		$\vdots$
$C(u_{41}), C(v_{41})$	$=$	$C(x_{63}), C(y_{63})$
$C(u_{99}), C(v_{99})$		$C(x_{n-9}), C(y_{n-9})$
$C(u_{2n}), C(v_{2n})$		$C(x_{55}), C(y_{55})$
$\vdots$		$\vdots$
$C(u_3), C(v_3)$		$C(x_6), C(y_6)$

for example:

$$
\begin{array}{ll}
\qquad\qquad b = b' = 0 & \qquad\qquad b = b' = 1 \\
0 \oplus 0 = 0 \oplus 0 \ : \ u_i = x_i, \ v_i = y_i, & 0 \oplus 1 = 0 \oplus 1 : \ u_i = x_i, \ v_i = y_i, \\
0 \oplus 0 = 1 \oplus 1 \ : \ u_i \neq x_i, \ v_i \neq y_i, & 1 \oplus 0 = 0 \oplus 1 : \ u_i \neq x_i, \ v_i \neq y_i.
\end{array}
$$

- For each line Bob randomly chooses to see the both left sides or both right sides, but not both sides, then Alice unveils them to Bob.

$$
\begin{array}{rcl}
C(u_9), U(v_9) & = & C(x_2), U(y_2) \\
U(u_n), C(v_n) & \neq & U(x_7), C(y_7) \\
\vdots & & \vdots \\
C(u_{41}), U(v_{41}) & = & C(x_{63}), U(y_{63}) \\
\hline
C(u_{99}), C(v_{99}) & & C(x_{n-9}), C(y_{n-9}) \\
C(u_{2n}), C(v_{2n}) & & C(x_{55}), C(y_{55}) \\
\vdots & & \vdots \\
C(u_3), C(v_3) & & C(x_6), C(y_6)
\end{array}
$$

where U denotes unveil.

If Alice wants to cheat, suppose b=1, b'=0 and Alice cliams that $\alpha_i = \beta_i$, for example:

$$
\begin{array}{rcl}
b = 1 & & b' = 0 \\
\alpha_i : \ 0 \oplus 1 & = & 1 \oplus 1 \ : \beta_i
\end{array}
$$

With 1/2 probability, Bob will request to see the left sides and Alice unveils to him that $(u_i = 0) \neq (x_i = 1)$, then Bob rejects.

With 1/2 probability, Bob will request to see the right sides and Alice unveils to him that $v_i = 1 = y_i$, then Bob accepts. So if $b \neq b'$, 1/2 probability Bob will be cheated.

Therefore,

If b=b', Pr[accept]=1,

If $b \neq b'$, Pr[accept]$\leq (1/2)^n$, at each line, if $b \neq b'$, regardless of Alice's answer, the probability Bob finds out that Alice is cheating is 1/2.

After a test is conclusive, Alice can construct a new valid commitment to represent both b and b' using the untouched commitments:

$$
\begin{aligned}
&commit(b, b') : \\
&C(u_{99}), C(v_{99}) \\
&C(u_{2n}), C(v_{2n}) \\
&\vdots \\
&C(u_3), C(v_3) \\
&C(x_{n-9}), C(y_{n-9}) \\
&C(x_{55}), C(y_{55}) \\
&\vdots \\
&C(x_6), C(y_6)
\end{aligned}
$$