1 BC with equality

1.1 Comparing equality of two committed inputs

Example 1.1 *bit commitment based on* GNI.

$$\mathrm{GNI} : (G_1, G_2) \in \mathrm{GNI}$$

$$P \qquad\qquad\qquad\qquad V$$

$$\xrightarrow{ZK((G_1,G_2)\in \mathrm{GNI})}$$

$commit(b_1),$
$G \approx G_{b_1}$

$$\xrightarrow{G}$$

$commit(b_2),$
$G' \approx G_{b_2}$

$$\xrightarrow{G'}$$

$$\xrightarrow{G=\pi(G')}$$

$$if\ G = \pi(G')\ then\ accept\ b_1 = b_2.$$

Example 1.2 *bit commitment based on* QNR.

$$y \in \mathrm{QNR}_n[+1]$$

$$P \qquad\qquad\qquad\qquad V$$

$$\xrightarrow{ZK(y\in \mathrm{QNR}_n[+1])}$$

$commit(b_1),$
$z_1 \equiv y^{b_1} * r^2\ mod\ n,$
$r \in_R Z_n^*,$

$$\xrightarrow{z_1}$$

$commit(b_2),$
$z_2 \equiv y^{b_2} * r'^2\ mod\ n,$
$r' \in_R Z_n^*,$

$$\xrightarrow{z_2}$$

$$\xrightarrow{v:=rr'y^{b_1}}$$

$$if\ z_1 z_2 = v^2\ then\ accept\ b_1 = b_2.$$

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

1.2 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.

$$\begin{array}{lcl}
P & & V \\
 & \xrightarrow{commit(\pi(T))} & \\
 & & c \in_R \{0,1\}, \\
 & \xleftarrow{c} & \\
if\ c = 0, & & \\
 & \xrightarrow{\pi,\ unveil(\pi(T))} & \\
if\ c = 1, & & \\
 & \xrightarrow{ZK(B=T_i)} &
\end{array}$$

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: $\wedge, \vee, -, \oplus$.

1.3 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.

$$
\begin{array}{rl}
 & \textit{Alice} \qquad\qquad\qquad\qquad \textit{Bob} \\
\\
commit(b): & commit(b'): \\
\alpha_1 : C(u_1), C(v_1) & C(x_1), C(y_1) : \beta_1 \\
\alpha_2 : C(u_2), C(v_2) & C(x_2), C(y_2) : \beta_2 \\
\vdots & \vdots \\
\alpha_{2n} : C(u_{2n}), C(v_{2n}) & C(x_{2n}), C(y_{2n}) : \beta_{2n}
\end{array}
$$

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.

$$
\begin{array}{rl}
C(u_9), C(v_9) & C(x_2), C(y_2) \\
C(u_n), C(v_n) & C(x_7), C(y_7) \\
\vdots & \vdots \\
C(u_3), C(v_3) & C(x_6), C(y_6)
\end{array}
$$

- 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 "≠".

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

for example:

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

- 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:

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

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:

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