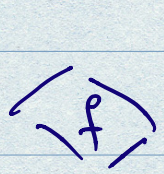
LECTURE - 19



Alice

Bob

a

b

$(pk, sk) \leftarrow \text{FHE.KeyGen}(1^\lambda; r_1)$

$ct_1 = \text{FHE.Enc}_{pk}(a; r_2)$

pk, ct_1 →

← ct_2

$ct_2 = \text{FHE.Eval}(f_b, ct_1; r_3)$

$\text{Dec}_{sk}(ct_2) = z$

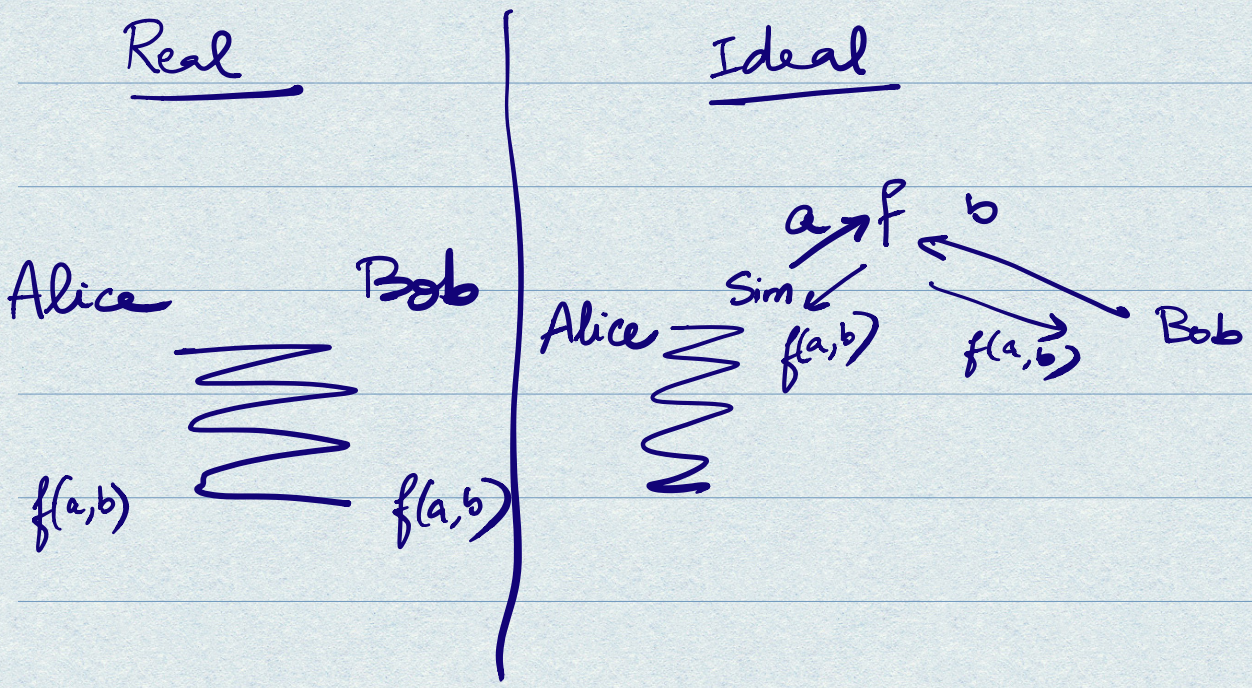
z →

$z = f(a, b)$

$z = f(a, b)$

Circuit-private FHE: $\text{FHE.Eval}_{pk}(f_b, ct_1; r_3), sk \approx \text{FHE.Enc}_{pk}(f(a,b); r), sk$

MALICIOUSLY SECURE COMPUTATION



Real view $\approx_c$ Ideal view

Example: Suppose given just a, $f(a,b)$ it is impossible to guess the first bit of b.

$\Rightarrow$ Alice cannot output the first bit of b w.p. $> \frac{1}{2}$ in ideal world

$\Rightarrow$ Alice cannot output n of bit w.p. $> \frac{1}{2} + \text{negl}$ in real world.

Alice

Bob.

$c_1 = com(r_1; r')$, $c_2 = com(s_1; s')$

r_2, s_2

PRIVATE COIN-FLIP

$pk, sk \leftarrow KeyGen(1^\lambda; r_1 \oplus r_2)$

$ct_1 = Enc_{pk}(a; s_1 \oplus s_2)$

pk, ct_1, ZKPoK π_1

π_1

proving that $x_1 \in L_1$, $x_1 = (c_1, c_2, ct_1, pk)$

$L = \{(c_1, c_2, ct_1, pk)$ s.t.

$\exists (r_1, r', s_1, s', a)$ s.t.

$c_1 = com(r_1; r')$, $c_2 = com(s_1; s')$,

$ct_1 = Enc_{pk}(a; s_1 \oplus s_2)$,

$pk \leftarrow KeyGen(1^\lambda; r \oplus r_2)\}$

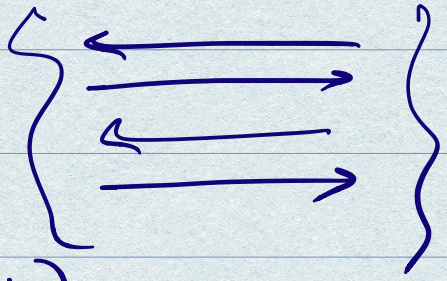
(contd.)

Alice Bob

$ct_2 = \text{FHE.Eval}(f_b, ct_1; r_3), \pi_2$ ← Bob → Alice

π_2 is ZKPoK : $x_2 \in L_2$ $x_2 = ct_2$

$L_2 = \{ ct_2 \text{ s.t. } \exists (b, r_3) \text{ s.t. } ct_2 = \text{FHE.Eval}(f_b, ct_1; r_3) \}$



$z = \text{Dec}_{sk}(ct_2)$

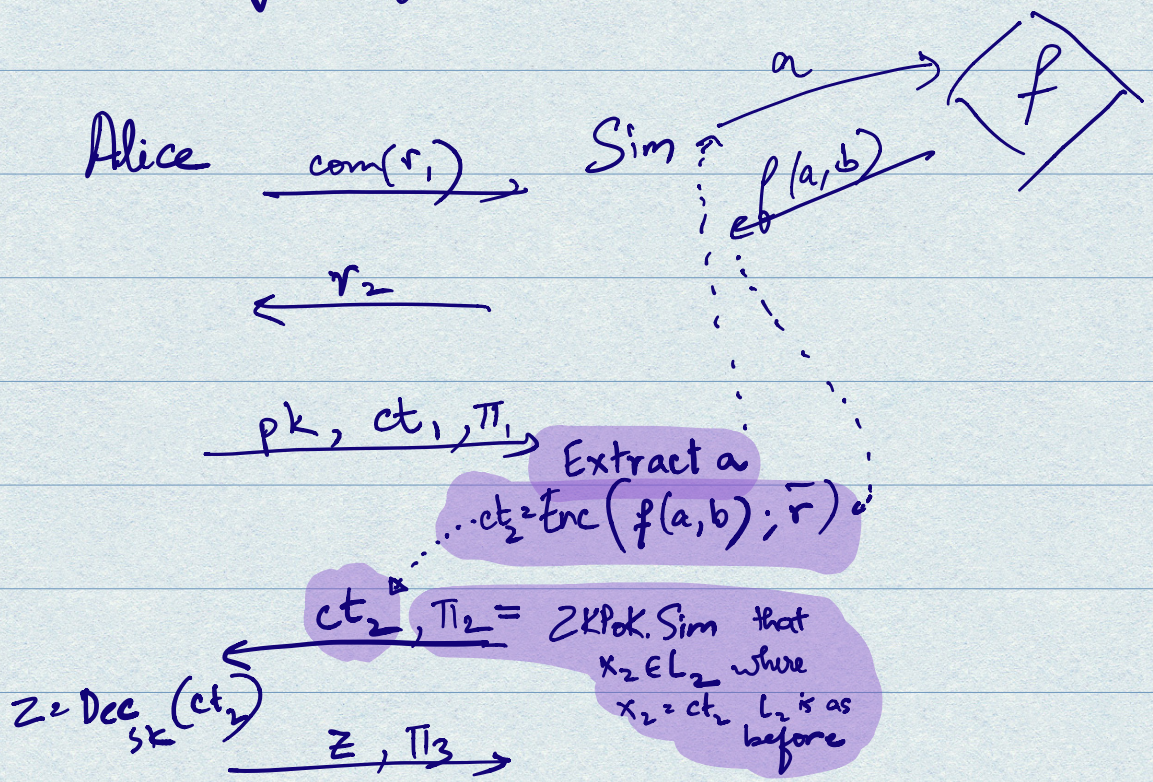
z, π_3 → Bob

π_3 is ZK : $x_3 \in L_3$ where 

$x_3 = (pk, z, c_1)$

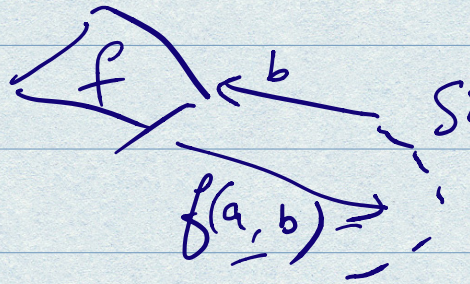
$L_3 = \{ (\tilde{pk}, \tilde{z}, \tilde{c_1}) \text{ s.t. } \exists (r_1, r') \text{ s.t. } \tilde{pk} \leftarrow \text{KeyGen}(1^\lambda; r_1 \oplus r_2) \text{ and } \tilde{c_1} = \text{com}(r_1; r') \text{ and } \tilde{z} = \text{Dec}_{sk}(ct_2) \}$

Security against corrupted Alice



NOTE (Semi-malicious): Secure against adv that follow protocol but use bad randomness

Security against corrupted Bob.



corrupted Bob

$\xrightarrow{\text{com}(r_1; c_{1,2}), \text{com}(s_1; c_{2,2})}$

$\xleftarrow{r_2 \; s_2}$

$(pk, sk) \leftarrow KG(1^\lambda; \hat{r})$

$ct_1 \leftarrow Enc_{pk}(0; \hat{s})$

$\xrightarrow{pk, ct_1, \pi_1 : ZKPoK \cdot Sim(x_1 \in L_1)}$

where $x_1 = (c_{1,1}, c_{2,2}, ct_1, pk)$

L_1 is same as before

$\xleftarrow{ct_2, \pi_2 : ZKPoK}$

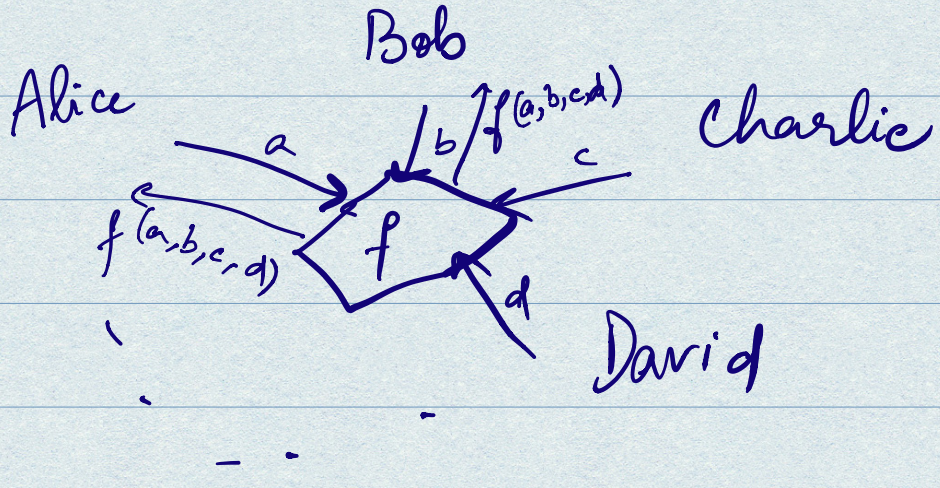
- Extract b from π_2.
- $f(a, b) \rightarrow z$

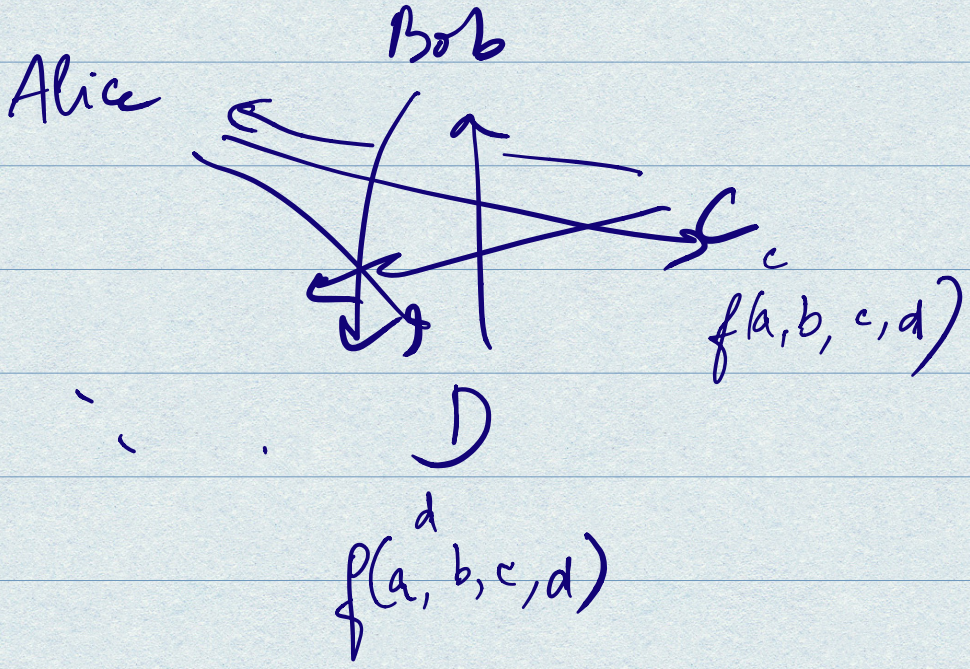
$\xrightarrow{z, \pi_3 : ZK \cdot Sim(x_3 \in L_3)}$

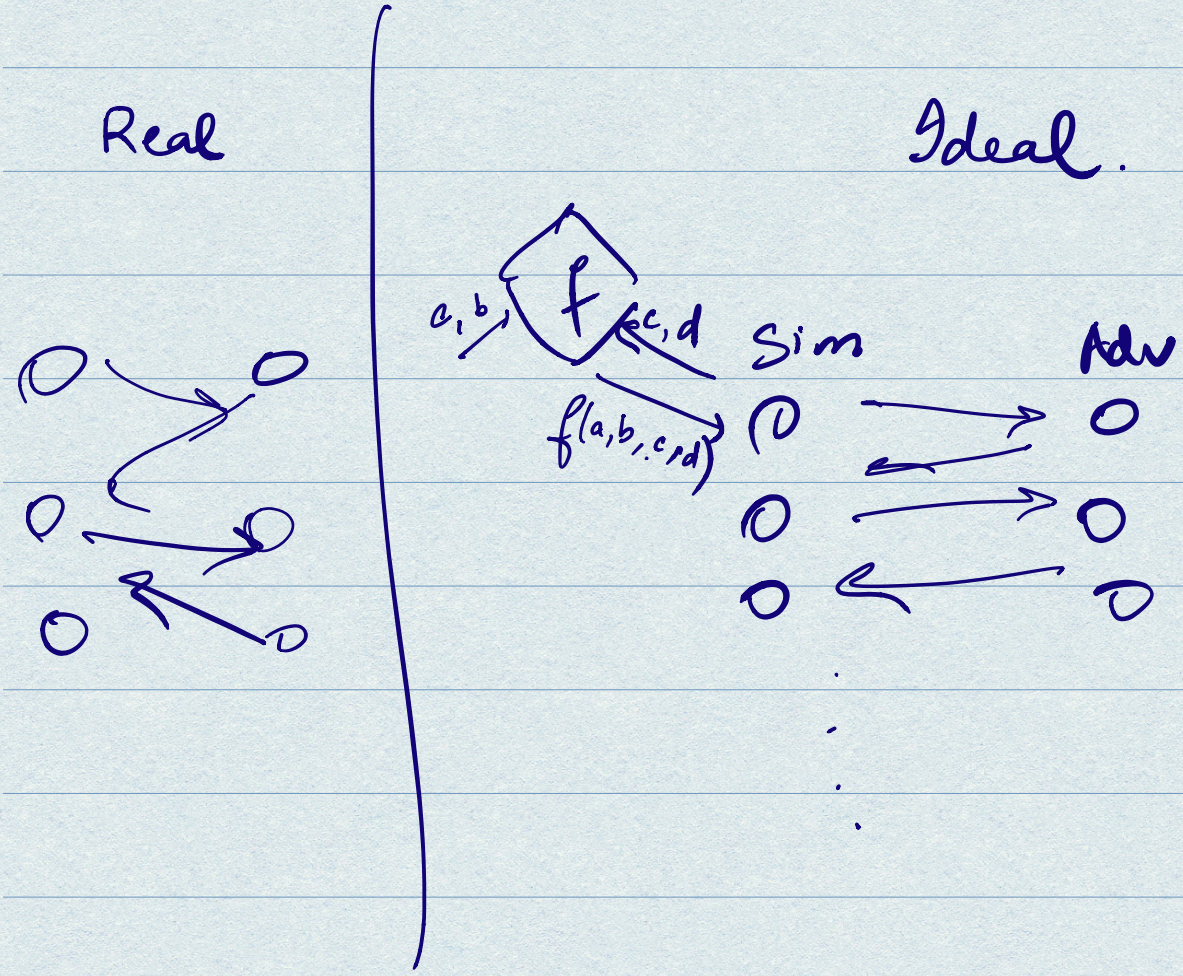
where $x_3 = z$,

L_3 is same as before.

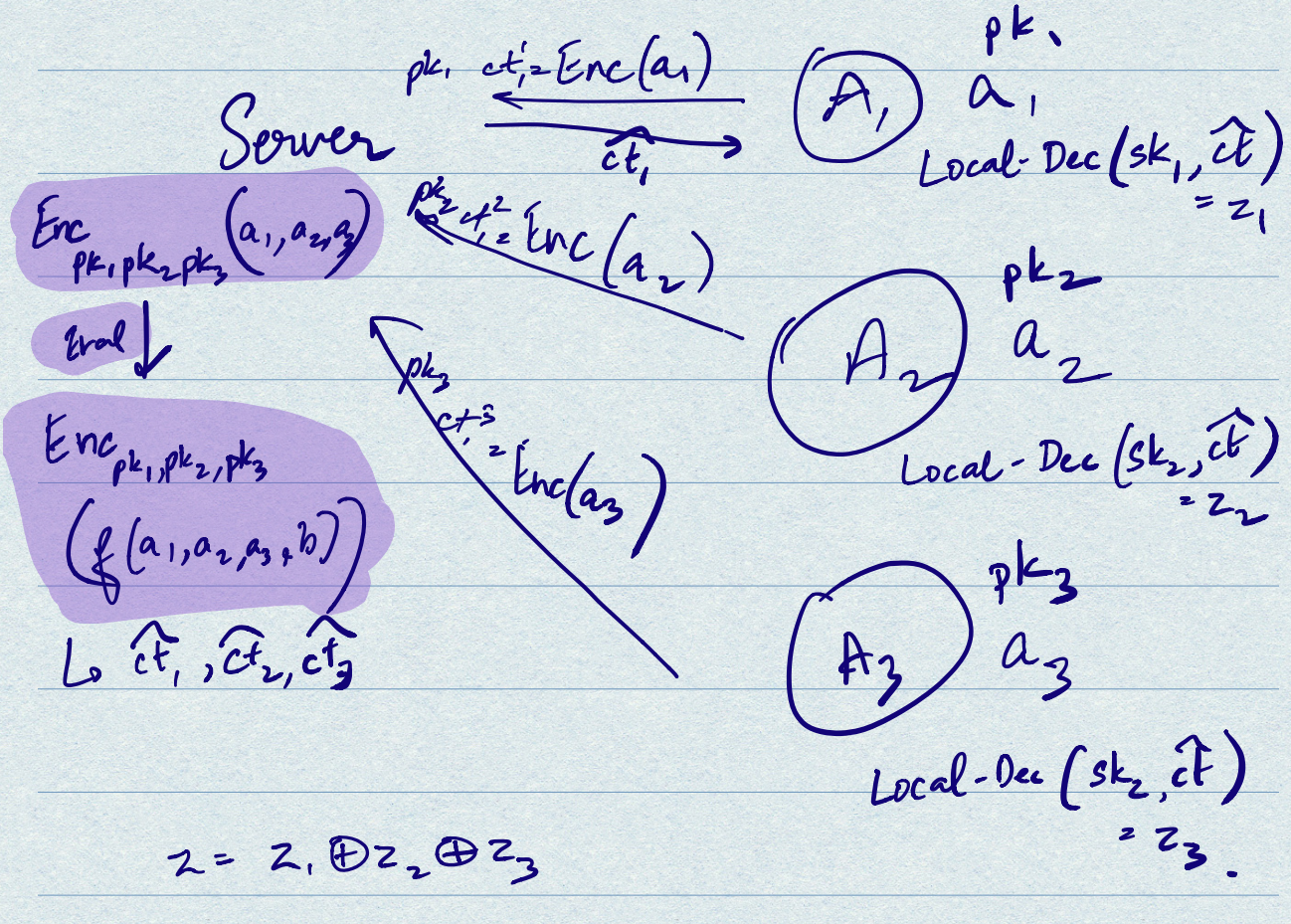
MULTI- PARTY COMPUTATION.







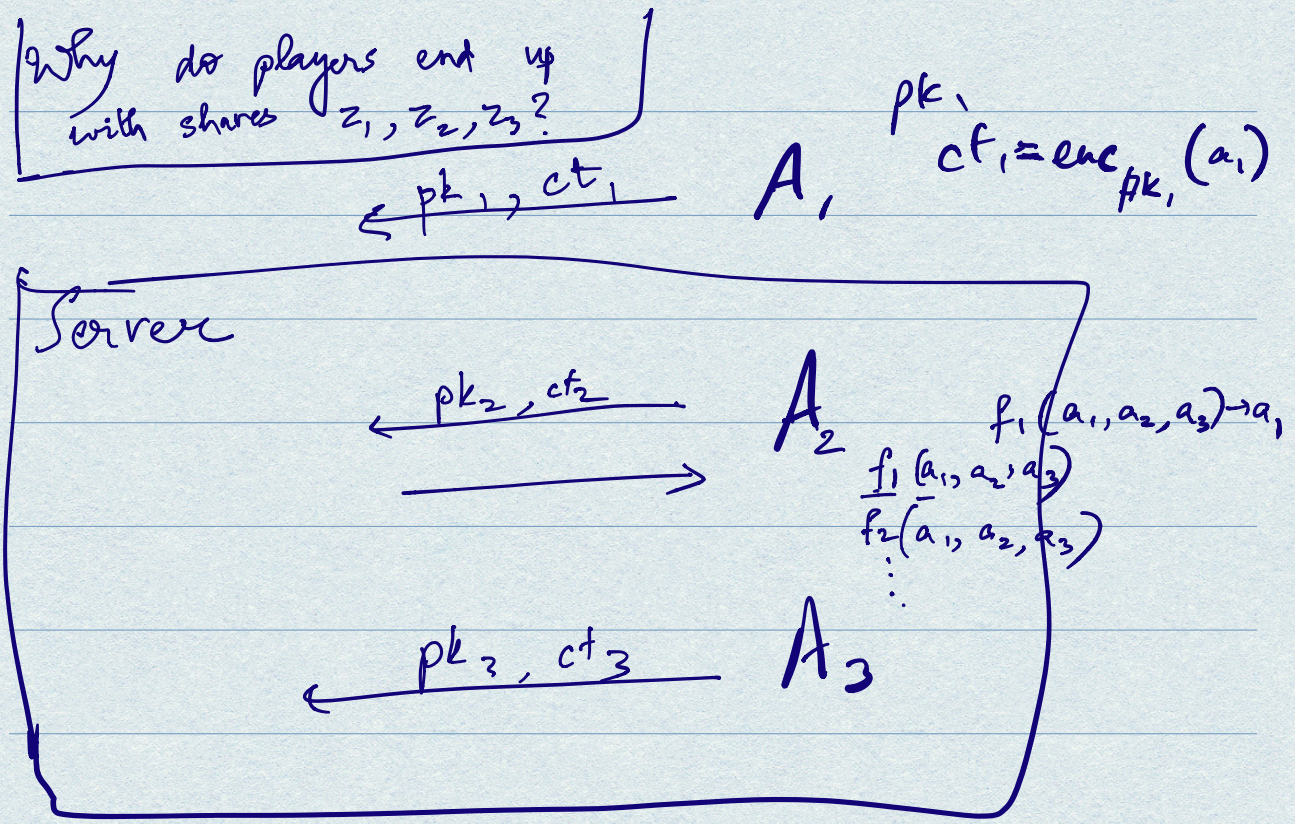
Real view ≈ Ideal view.



$z = z_1 \oplus z_2 \oplus z_3$

MULTI-KEY FHE.

(extend GSW FHE)



Extractable Commitments.

$C = com(m; r)$, ZKPoK : $\exists (m, r)$ s.t.

$C = com(m; r)$