SuperSecureComputationalDevice Project - Description

Grayson Martis, Mohit Rathore, Chirayu Garg

El Gamal keys

- {Pk, Sk} El Gamal for MPC computation

- {CPk, CSk} El Gamal clients keys

What Players Have

P1 : OT $\{b_0^{p1}, b_1^{p1}, b_2^{p1}, b_3^{p1}\}$, b_c^{p2}, c^{p1}, and $Enc_{pk}(m_1)$

P2 : OT $\{b_0^{p2}, b_1^{p2}, b_2^{p2}, b_3^{p2}\}$, b_c^{p1}, c^{p2}, and $Enc_{pk}(m_2)$

P3 : $Enc_{pk}(m_3)$

MPC

P_1 P_2 P_3

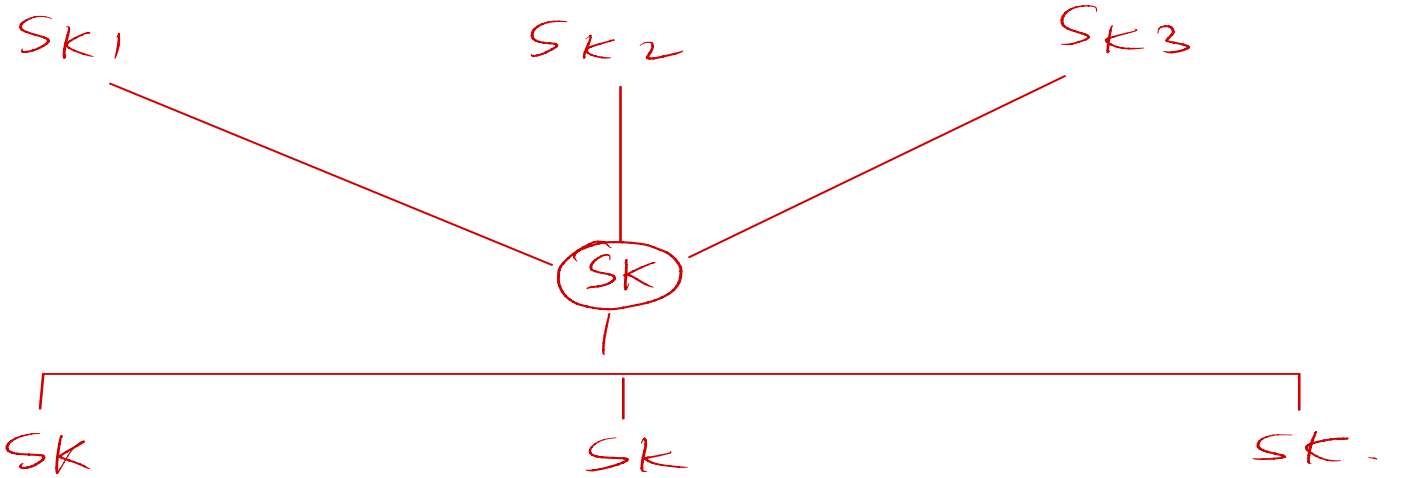
$\rightarrow$ $Enc_{PK}(m_1)$ $Enc_{PK}(m_2)$ $Enc_{PK}(m_3)$

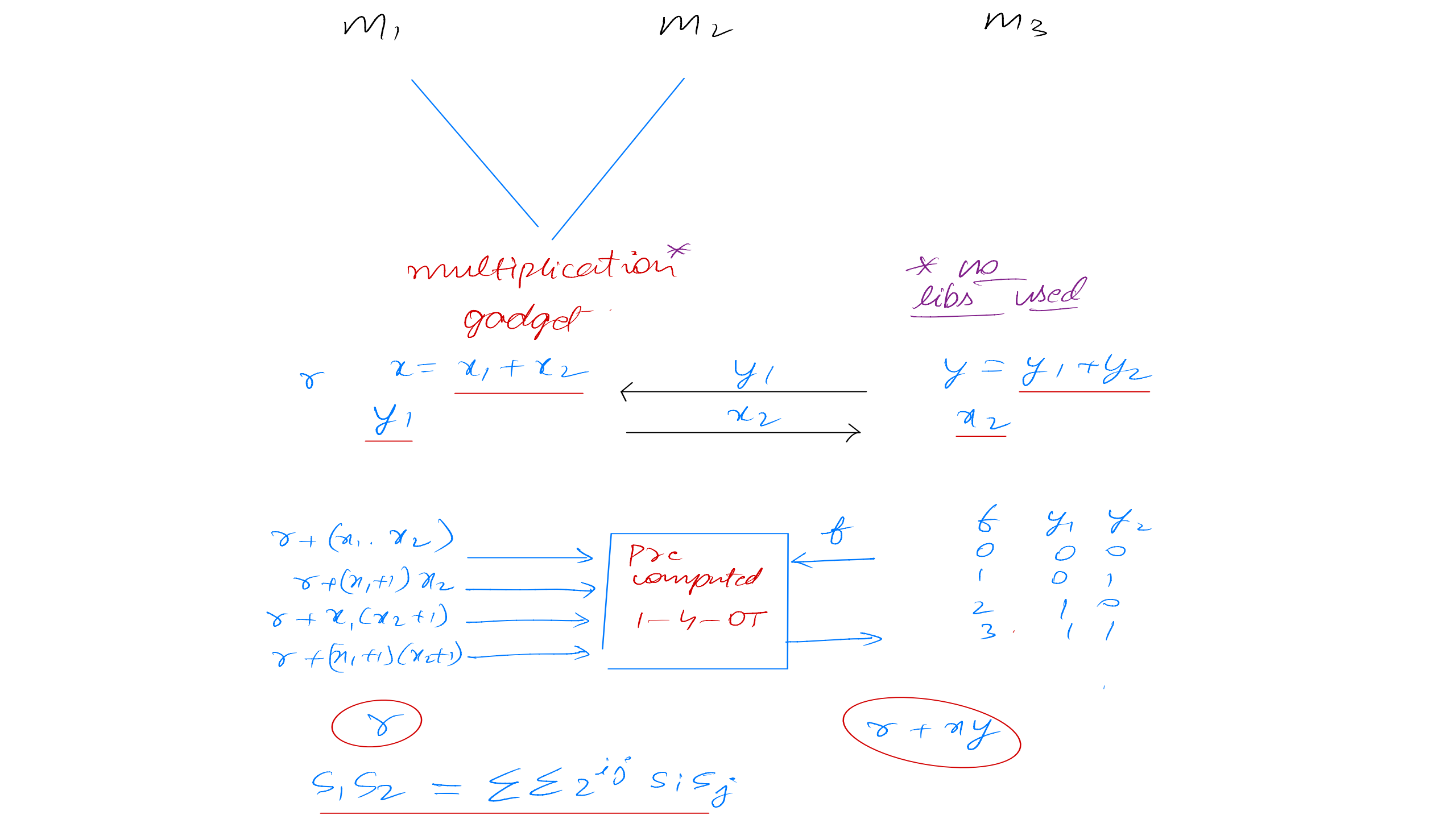
$P_i \rightarrow$ $m_i = \gamma_1 + \gamma_2 + (m_i - \gamma_1 - \gamma_2)$

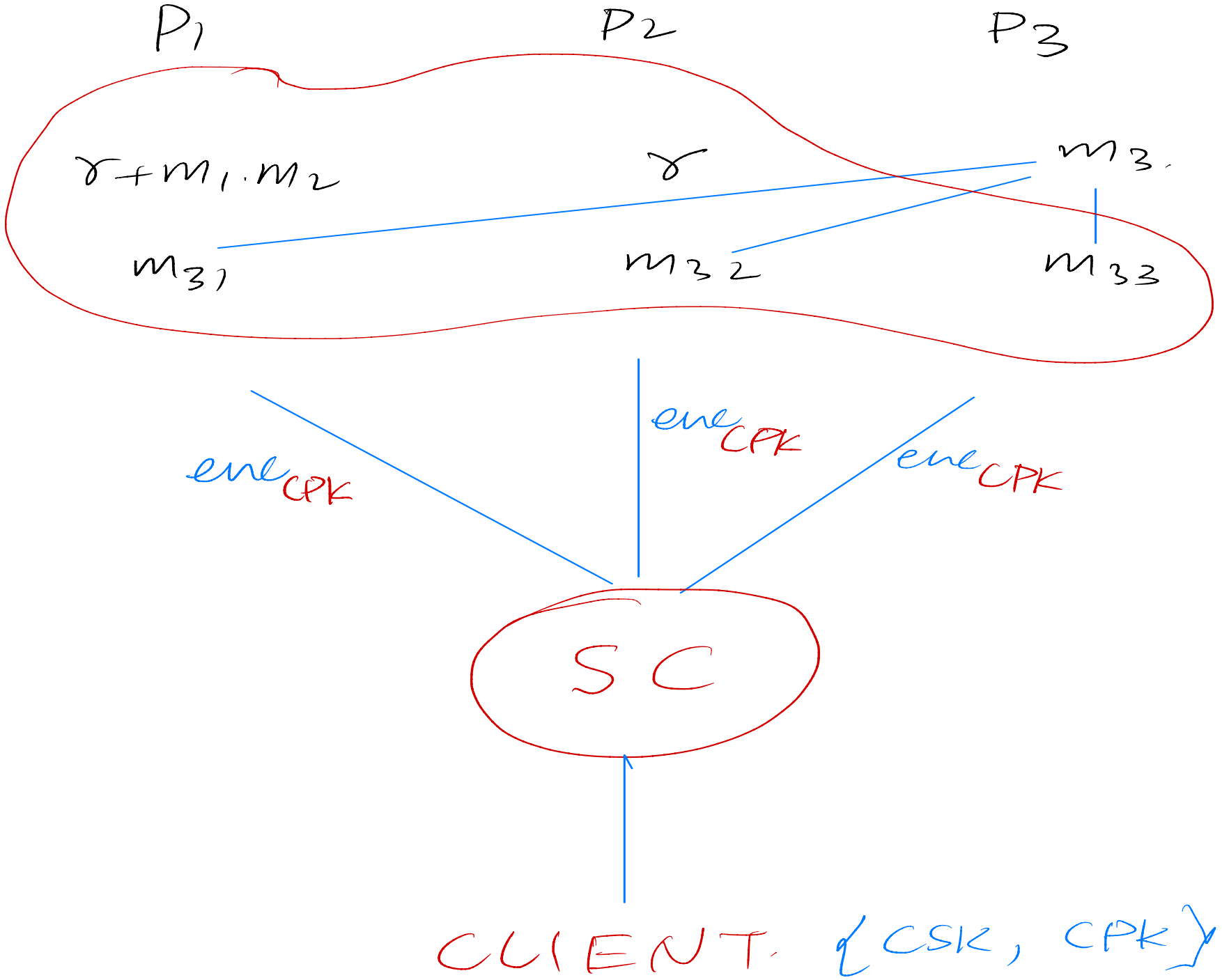
P_1 P_2 P_3

$\gamma_i \in R$.

Additive Sharing




m_1
m_2
m_3
multiplication* gadget
* no libs used
r
$x = x_1 + x_2$
y_1
y_1
x_2
$y = y_1 + y_2$
x_2
$r + (x_1 \cdot x_2)$
$r + (x_1+1)\, x_2$
$r + x_1 (x_2+1)$
$r + (x_1+1)(x_2+1)$
Prc computed 1-4-OT
b
b y_1 y_2
0 0 0
1 0 1
2 1 0
3 1 1
r
$r + xy$
$s_1 s_2 = \sum\sum 2^{ij} s_i s_j$


P1
P2
P3
r + m1 . m2
r
m3 .
m31
m32
m33
enc CPK
enc CPK
enc CPK
SC
CLIENT. {CSK, CPK}

Specifications

- Before the start of the main protocol, Client generates and reveals his public key.
- Each party at the end of our protocol sends (g^y , $m * h^y$) to the client/ posts it on the ledger.
- Once the Encrypted shares are posted on the ledger, we will consider our protocol done as only client will have the ability to decrypt those shares.
- Since, the ledger is public, Client will be able to access this ledger and then get the values.

Goals achieved -

- Only client can know the computed value, ONLY if he pays 10000 ALGOS and no one else can (even anyone amongst the players).
- Only encrypted values will be on the ledger.
- In case any party crashes, the client gets his 10000ALGOS back.
- M = {7,2,1}
- Ps computations (sent securely to client)- {2,13,0} = 15 = 7*2+1