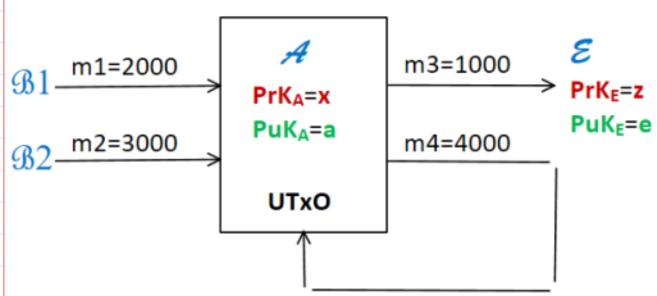
Actors: *B1* *B2* *Alice* *Emily* *Net* *Audit Authority - AA*

Public Parameters PP = (p, g); p=268435019; g=2;

Alice
PrK=*x*; **PuK**=*a*.
>> x=int64(randi(p-1))
x = 125777467
>> a=mod_exp(g,x,p)
a = 233074861

Emily
PrK=*z*; **PuK**=*e*.
>> z=int64(randi(p-1))
z = 139168670
>> e=mod_exp(g,z,p)
e = 256500680

AA
PrK=*u*; **PuK**=*v*.
>> u=int64(randi(p-1))
u = 107550077
>> v=mod_exp(g,u,p)
v = 19235345

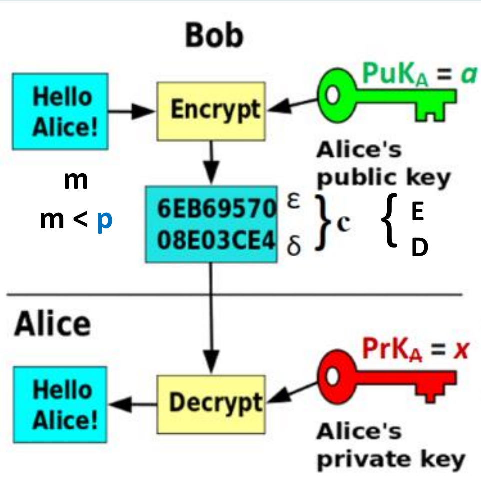


UTxO

A:
Enc(*e*,i3,m3) = cE ----------------------> Dec(*z*,cE) = m3

AA:
Enc(*v*,i3,m3) = cAA ---> Dec(*u*,cAA) = m3

Q1. How *AA* and *Net* should know that sums transferred from *A* to them are the same, i.e. equal to **m3** since **cE** can not be decypted neither by *AA* nor by *Net* since they do not know *E*'s **PrK$_A$** For decryption.



B:

$Enc(a, i, m) = c = (E, D)$

$i \leftarrow randi\,(p-1)$

$E = m * a^i \bmod p$

$D = g^i \bmod p$

```
>> m=5000;
>> i = int64(randi(p-1))
i = 62634864
>> a_i=mod_exp(a,i,p)
a_i = 216885678
>> E=mod(m*a_i,p)
E = 219348259
>> D=mod_exp(g,i,p)
D = 179010250
```

A:

$Dec(x, c) = m$

$D^{(-x) \bmod (p-1)} \bmod p = D'$

$E * D' \bmod p = m$

$(-x) \bmod (p-1) = (p - 1 - x)$

```
>> mx = mod(-x,p-1)
ans = 198691311
>> mod(x+mx,p-1)
ans = 0
>> D_mx=mod_exp(D,mx,p)
D_mx = 162923742   % D_mx=D'
mm = mod(E*D_mx,p)
>> mm = mod(E*D_mx,p)
mm = 5000
```

$i_3 \leftarrow randi$

D = 179010250

mm = 5000

$i_3 \leftarrow \text{randi}$

$$\underline{C_{AA}} = \underline{(E_{AA}, D_{AA})} = (\underline{m_3 * v^{i_3} \bmod p}, \underline{\cancel{g^{i_3} \bmod p}})$$

$$C_E = (E_E, D_E) = (m_3 * e^{i_3} \bmod p, \cancel{g^{i_3} \bmod p})$$

Property:

$$\frac{E_{AA}}{E_E} \equiv \frac{\cancel{m_3} * v^{i3} \bmod p}{\cancel{m_3} * e^{i3} \bmod p} \equiv \frac{v^{i3} \bmod p}{e^{i3} \bmod p} \bmod p \equiv \frac{v^{i3}}{e^{i3}} \bmod p \equiv (v/e)^{i3} \bmod p = d^{i3} \bmod p.$$

Public keys ratio is denoted by **d**=(**v**/**e**) **mod p** that is known to ***AA*** and all ***Net***.

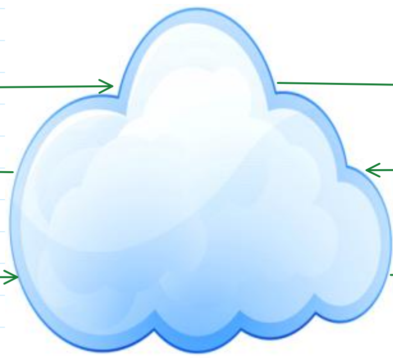
Schnorr Identification: Zero Knowledge Proof - ZKP

Schnorr Id Scenario: ***Alice*** wants to prove ***AA*** and ***Net*** that she knows her ***i3*** which is an exponent of Publicly known parameter **d**=(**v**/**e**) mod **p** and ratio of cihertexts E_{AA}/E_E **mod p**.

A*: ZKP of knowledge *i3:

having a data:
d=(***v***/***e***) **mod *p***
E_{AA}/E_E **mod *p***
1.Computes commitment ***t*** for ***i3***:
  l=randi(p-1)
  $t = g^l \bmod p$
3.Computes response ***res***:
$res = l + i3 * h \bmod p-1$

$\xrightarrow{t}$ $\xleftarrow{h}$ $\xrightarrow{res}$



$\xrightarrow{t}$ $\xleftarrow{h}$ $\xrightarrow{res}$

Net : ***d***=(***v***/***e***) **mod *p***
E_{AA}/E_E **mod *p***

2.Generates challenge ***h***:
h=**randi(*p*-1)**

Verifies:
$g^{res} = t d^h \bmod p$

t
h
res
Time

Correctness:

$d^{res} \bmod p = d^{l+i3*h} \bmod p = d^l d^{i3*h} \bmod p = t(d^{i3})^h \bmod p = t(E_{AA}/E_E)^h \bmod p.$

When ***a***, ***e*** and **Public Parameters PP = (p, g)** are given, ***Net*** having ***a***, ***e*** computes ***d***=(***a***/***e***) **mod *p***.
Then the verification is performed by ***Net*** verifying equation

$$d^{res} = t d^h \bmod p$$

Q2. How to prove the ciphertexts equivalency to the millions of ***Net*** nodes?
Schnorr digital signature helps.

A: $\text{Sign}(i_3, E_{AA}/E_E) = \sigma = (r, s)$ $\longrightarrow$ Net: verifies signature with known (public) param. (E_{AA}/E_A)

$l \leftarrow \text{randi}(p-1)$

$r = d^l \bmod p$

$h = H(r \| (E_{AA}/E_A))$

$s = l + i_3 * h \bmod p$

$\text{Ver}(\sigma, (E_{AA}/E_A)) = \{T, F\}$

$d^s \bmod p = r * (E_{AA}/E_A)^h \bmod p$

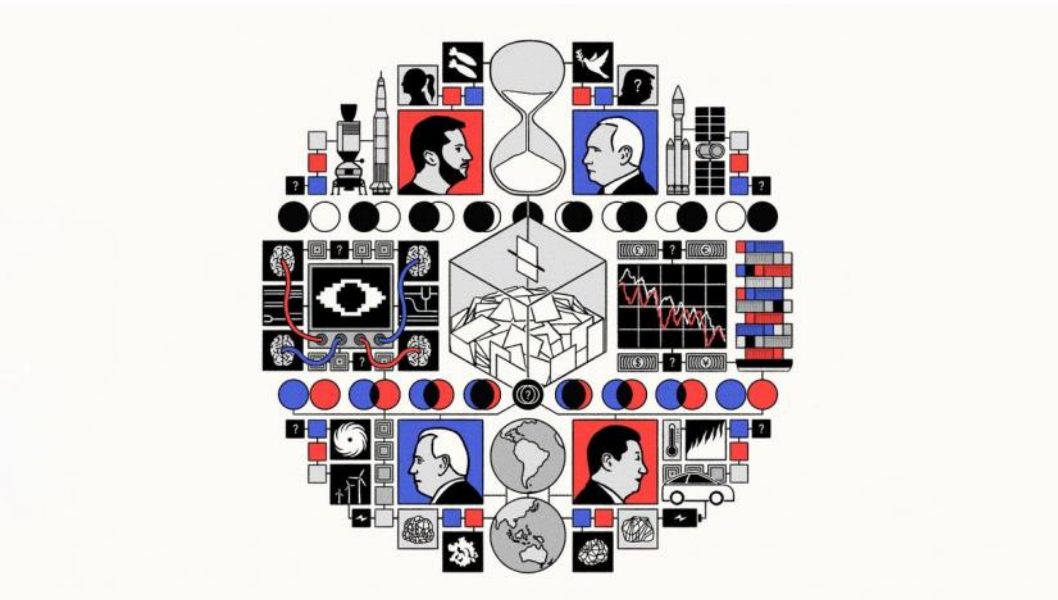
$s = l + i3 * h \bmod p$

$$\boxed{d^{s} \bmod p = r * (E_{AA}/E_{A})^{h} \bmod p}$$

correctness:

$$d^{s} \bmod p = d^{l + i3 * h} \bmod p = d^{l} * d^{i3 * h} \bmod p = r * (d^{i3})^{h} \bmod p =$$
$$= r * (E_{AA}/E_{A})^{h} \bmod p.$$

mini https



The Economist
The World Ahead 2024