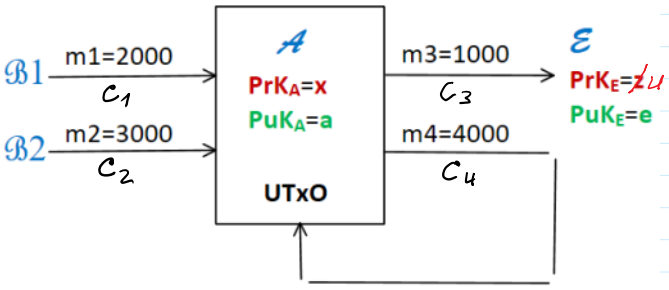
UTxO blockchain to provide confidentiality and verifiability of transferred money amounts.

Public Parameters PP = (p, g); p=268435019; g=2;
AA **- Audit Authority: PrK_{AA}=z, PuK_{AA}=AA.**

Zero Knowledge Proof (ZKP) of equivalence of 2 ciphertexts *c*3, *c*3*e* corresponding to the same plaintext *m* obtained by encryption with different Puks



How to provide anonymity of transaction amounts and to verify the **balance**: **m1+m2 = m3+m4** ?
n1= g^{m1} mod **p** **n3**= g^{m3} mod **p**
n2= g^{m2} mod **p** **n4**= g^{m4} mod **p**

1-to-1 function

If **(m1+m2) mod (p -1) = (m3+m4) mod (p-1)**,
Then **(n1*n2) mod p = (n3*n4) mod p**.

$n_1 \cdot n_2 \bmod p = g^{m_1+m_2} \bmod p$ $\quad$ $n_3 \cdot n_4 = g^{m_3+m_4} \bmod p$

If $n_1 \cdot n_2 \bmod p = n_3 \cdot n_4 \bmod p$

$c_1 \cdot c_2 = c_3 \cdot c_4$

$c_1 = Enc(a, i_1, n_1) = (E_1, D_1)$ $\quad$ $c_3 = Enc(a, i_3, n_3) = (E_3, D_3)$

$c_2 = Enc(a, i_2, n_2) = (E_2, D_2)$ $\quad$ $c_4 = Enc(a, i_4, n_4) = (E_4, D_4)$

$(i_1 + i_2) \bmod (p-1) = (i_3 + i_4) \bmod (p-1)$

$c_1 \cdot c_2 \bmod p = c_3 \cdot c_4 \bmod p$

$E_1 \cdot E_2 \bmod p = E_3 \cdot E_4 \bmod p$

$D_1 \cdot D_2 \bmod p = D_3 \cdot D_4 \bmod p$

$c_1 = (E_1, D_1) = (n_1 \cdot a^{i_1}, g^{i_1})$
$c_2 = (E_2, D_2) = (n_2 \cdot a^{i_2}, g^{i_2})$
$\bmod p \Rightarrow c_1 \cdot c_2 = (E_1 \cdot E_2, D_1 \cdot D_2) = (E_{12}, D_{12})$

$E_{12} = n_1 \cdot a^{i_1} \cdot n_2 \cdot a^{i_2} \bmod p = n_1 \cdot n_2 \cdot a^{(i_1+i_2) \bmod (p-1)} \bmod p$

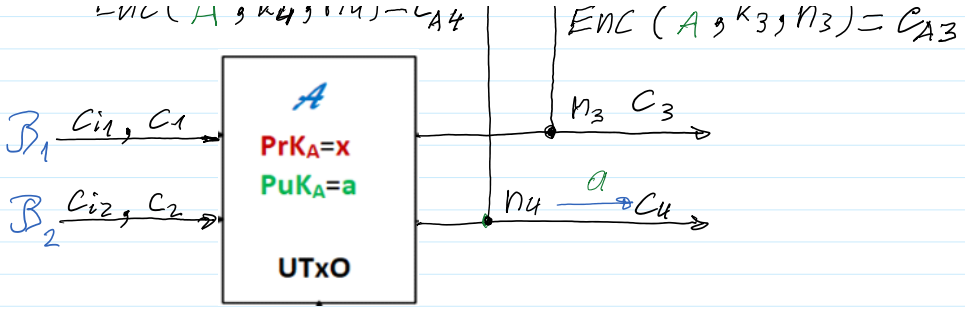
$E_{34} = n_3 \cdot a^{i_3} \cdot n_4 \cdot a^{i_4} \bmod p = n_3 \cdot n_4 \cdot a^{(i_3+i_4) \bmod (p-1)} \bmod p$

$E_{12} = E_{34}$

AA **- Audit Authority: PrK_{AA}=z, PuK_{AA}=A.**

$Enc(A, k_4, n_4) = C_{A4}$ $\quad$ $Enc(A, k_3, n_3) = C_{A3}$

```
>> z=int64(randi(p-1))
z = 168034742
>> A=mod_exp(g,z,p)
A = 258784798
```



>> A=mod_exp(g,z,p)
A = 258784798

Google drive link:
https://docs.google.com/spreadsheets/d/15AqiZvP9TEg8qaJ9OocOTS9aqyOkg3G4/edit?usp=sharing&ouid=111502255533491874828&rtpof=true&sd=true
This link will be replaced by preserving computations for continuing further computations.

>> x=int64(randi(p-1))
x = 156653413
>> a=mod_exp(g,x,p)
a = 50249661
>> p=268435019

>> n1=mod_exp(g,m1,p)
n1 = 28125784
>> n2=mod_exp(g,m2,p)
n2 = 222979214

>> i1=int64(randi(p-1))
i1 = 148308050
>> i2=int64(randi(p-1))
i2 = 72210493

>> a_i1=mod_exp(a,i1,p)
a_i1 = 16650980
>> Ean1=mod(n1*a_i1,p)
Ean1 = 200625217
>> Dan1=mod_exp(g,i1,p)
Dan1 = 52535541

>> a_i2=mod_exp(a,i2,p)
a_i2 = 140298124
>> Ean2=mod(n2*a_i2,p)
Ean2 = 124804048
>> Dan2=mod_exp(g,i2,p)
Dan2 = 201744006

>> j1=int64(randi(p-1))
j1 = 268092642
>> a_j1=mod_exp(a,j1,p)
a_j1 = 56356998
>> Eai1=mod(i1*a_j1,p)
Eai1 = 251905498
>> Dai1=mod_exp(g,j1,p)
Dai1 = 40270879

>> j2=int64(randi(p-1))
j2 = 215965316
>> a_j2=mod_exp(a,j2,p)
a_j2 = 71707010
>> Eai2=mod(i2*a_j2,p)
Eai2 = 38288929
>> Dai2=mod_exp(g,j2,p)
Dai2 = 44403423

>> Ean12=mod(Ean1*Ean2,p)
Ean12 = 175453592
>> Dan12=mod(Dan1*Dan2,p)
Dan12 = 48312418

$n = g^m \bmod p$; $Enc(a, i, n) = c = (E, D)$.

A: $PrK_A = (x)$; $Dec(x, c) = m$;

1. $D^{(-x) \bmod (p-1)} \bmod p = (g^r)^{-x} \bmod p =$
$= g^{-rx} \bmod p$

2. $m = E * D^{-x} = m * a^r * g^{-rx} =$
$= m * (g^x)^r * g^{-rx} \bmod p =$

>> mx = mod(-x,p-1)

>> mx=mod(-x,p-1)
mx = 111781605
>> mod(x+mx,p-1)
ans = 0

$= m * (g^{x})^{r} * g^{-r \cdot x} \mod p =$

$= m * g^{xr} * g^{-xr} \mod p =$

$= m * g^{0} \mod p = m \mod p = m$

since $1 < m < p$

Till this place

A: Enc(**e**, n3) =
c3e=(E3e,D3e)
E3e= n3*e^{i3} mod **p**
D3e= g^{i3} mod **p**
Enc(**e**, i3) = ci3e
j3e <-- randi(**p**-1)
Ei3e= i3*e^{j3} mod **p**
Di3e= g^{j3} mod **p**

c_{3e} c_{i3e}

c3e=(E3e,D3e)
ci3e=(Ei3e,Di3e) → **E**: PrK=z; PuK=e.

E: Dec(**z**, c3e) = n3 & verifies if n3=g^{m3} mod **p**
Dec(**z**, ci3e) = i3

Net:

A: c3=(E3,D3)
E3= n3*a^{i3} mod **p**
D3= g^{i3} mod **p**
$c_3 = (E_3, D_3)$

A: c3e=(E3e,D3e)
E3e= n3*e^{i3} mod **p**
D3e= g^{i3} mod **p**
$c_{3e} = (E_{3e}, D_{3e})$

$c_3 \neq c_{3e}$

Let $\mathcal{E}$ knows i_3, then $\mathcal{E}$ can verify that c_3 and c_{3e} encrypts the same number $n_3 = g^{m_3} \mod p$, when $m_3 = 1000$.
$\mathcal{E}$ takes a ratio

$$\frac{E_3}{E_{3e}} = \frac{n_3 \cdot a^{i_3} \mod p}{n_3 \cdot e^{i_3} \mod p} = \left(\frac{a}{e}\right)^{i_3} \mod p$$

Schnorr Identification: Zero Knowledge Proof - ZKP

Schnorr Id scenario: **Alice** wants to prove **Bank** that she knows her Private Key - $PrK_A = x$ which corresponds to her Public Key - $PuK_A = a = g^x \mod p$ not revealing $PrK_A = x$.

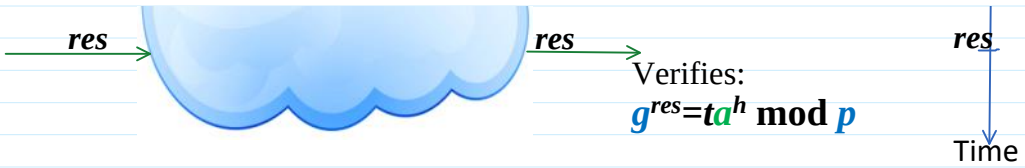
A: ZKP of knowledge x:
PrK_A = x = randi(p-1)
$PuK_A = a = g^x \mod p$
1.Computes commitment ***t*** for ***i***:
i=randi(***p***-1)
t=g^i mod ***p***
3.Computes response ***res***:
res=***i***+***x h*** mod (***p***-1)

B: $PuK_A = a = g^x \mod p$
2.Generates challenge ***h***:
h=randi(***p***-1)
Verifies:

$t=g^i \bmod p$

3.Computes response ***res***:

$res=i+xh \bmod (p-1)$



Correctness:

$g^{res} \bmod p = g^{i+xh} \bmod p = g^i g^{xh} \bmod p = t(g^x)^h \bmod p = ta^h \bmod p.$

$r \leftarrow randi(\mathcal{I}_p^*)$; $\mathcal{I}_p^* = \{1, 2, 3, \ldots, p-1\}$; $*$ mod p; $/$ mod p

$u = g^r \bmod p$; $v = \left(\frac{a}{e}\right)^r \bmod p$.

$h = H(u \| v)$

$w = (i_3 \cdot h + r) \bmod (p-1)$ $\xrightarrow[a,e]{u,v,w}$ Net : $h = H(u \| v)$

Ver1: $g^w = (D_3)^h \cdot u \bmod p =$

Ver2: $\left(\frac{a}{e}\right)^w = \left(\frac{E_3}{E_{3e}}\right)^h \cdot v \bmod p =$

Correctness:

Ver1: $g^w = g^{(i_3 \cdot h + r) \bmod (p-1)} \bmod p = (g^{i_3})^h \cdot g^r \bmod p = (D_3)^h \cdot u \bmod p.$

Ver2: $\left(\frac{a}{e}\right)^w \bmod p = \left(\frac{a}{e}\right)^{(i_3 \cdot h + r) \bmod (p-1)} \bmod (p-1) =$

$= \left(\frac{a}{e}\right)^{i_3 \cdot h} \cdot \left(\frac{a}{e}\right)^r \bmod p = \left(\frac{a^{i_3}}{e^{i_3}}\right)^h \cdot v \bmod p =$

$= \left(\frac{n_3 a^{i_3}}{n_3 e^{i_3}}\right)^h \cdot v \bmod p = \left(\frac{E_3}{E_{3e}}\right)^h \cdot v \bmod p.$

A: ⟶ ***Net***