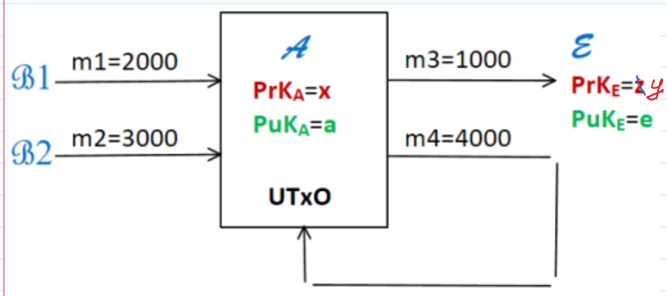
UTxO blockchain to provide confidentiality and verifiability of transferred money amounts.

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



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**

If **m1+m2 = m3+m4**,
Then **n1*n2 = n3*n4**.

$DEF(m) = g^m \bmod p = n$

$$\left.\begin{aligned} n_1 \cdot n_2 \bmod p &= g^{m_1} \cdot g^{m_2} \bmod p = g^{m_1+m_2} \bmod p \\ n_3 \cdot n_4 \bmod p &= g^{m_3} \cdot g^{m_4} \bmod p = g^{m_3+m_4} \bmod p \end{aligned}\right\}$$

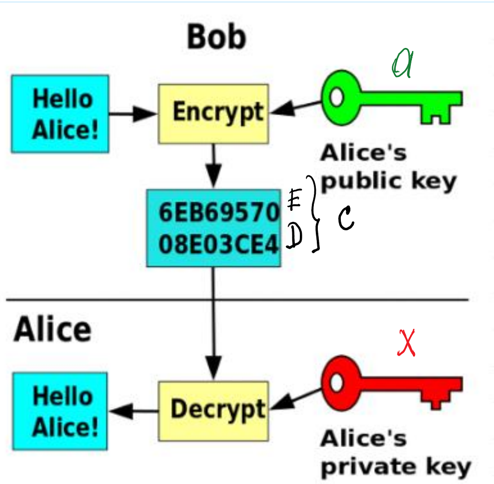
Since discrete exp. f. is 1-to-1 mapping then

$$g^{m_1+m_2} \bmod p = g^{m_3+m_4} \bmod p$$

ElGamal Encryption and ZKP based on **Schnorr Identification** are used.

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

ElPublic and Private keys generation
PrK_A = *x* = randi(*p*-1).
PuK_A = *a* = g^x mod *p*.



ElGamal Encryption - Decryption
c=Enc(PuK_A, m)=(E,D)
m=Dec(PrK_A, c)

B1: Enc(**a**, i1, **n1**) = c1
i1 = randi(**p**-1)
E1= n1*a^{i1} mod **p**
D1= g^{i1} mod **p** c1=(E1,D1)
Enc(**a**, j1, **i1**) = ci1
j1 = randi(**p**-1)
Ei1= i1*a^{j1} mod **p** ci1=(Ei1,Di1)
Di1= g^{j1} mod **p**

B2: Enc(**a**, i2, **n2**) = c2
i2 = randi(**p**-1)
E2= n2*a^{i2} mod **p**
D2= g^{i2} mod **p** c2=(E2,D2)
Enc(**a**, j2, **i2**) = ci2
j2 = randi(**p**-1)
Ei2= i2*a^{j2} mod **p** ci2=(Ei2,Di1)
Di2= g^{j2} mod **p**

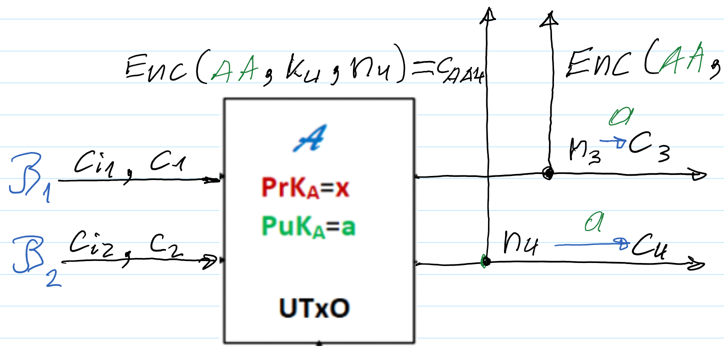
$\mathcal{B}1$: $\xrightarrow{c1=(E1,D1),\ ci1=(Ei1,Di1)}$ $\mathcal{A}$: Dec(**x**, c1) = **n1** & verifies if n1=g^{m1} mod **p**
Dec(**x**, ci1) = **i1**

$\mathcal{B}2$: $\xrightarrow{c2=(E2,D2),\ ci2=(Ei2,Di2)}$ $\mathcal{A}$: Dec(**x**, c2) = **n2** & verifies if n2=g^{m2} mod **p**
Dec(**x**, ci2) = **i2**

$\mathcal{A}$ makes her expenses $m_3 = 1000$, $m_4 = 4000$, **n3**= g^{m3} mod **p** ; **n4**= g^{m4} mod **p**

AA **- Audit Authority: PrK$_{AA}$=z, PuK$_{AA}$=AA.**

$\mathcal{A}$: Computes: i12=i1+i2 mod (**p**-1)
Generates: i3 = randi(**p**-1)
Computes: i4=i12-i3 mod (**p**-1)
Computes: i34=i3+i4 mod (**p**-1)
Verifies if: i12=i34=***i***



$$Enc(a, i_3, n_3) = c_3 = (E_3, D_3)$$
$$= (E_3 = n_3 \cdot a^{i_3} \bmod p,\ D_3 = g^{i_3} \bmod p)$$

$$Enc(a, i_4, n_4) = c_4 = (E_4, D_4)$$
$$= (E_4 = n_4 \cdot a^{i_4} \bmod p,\ D_4 = g^{i_4} \bmod p)$$

$$E_1 \cdot E_2 = n_1 \cdot a^{i_1} \cdot n_2 \cdot a^{i_2} \bmod p =$$
$$= n_1 \cdot n_2 \ a^{(i_1 + i_2) \bmod (p-1)} \bmod p =$$
$$= n_1 \cdot n_2 \cdot a^{i_{12}} \bmod p =$$
$$= n_1 \cdot n_2 \cdot a^{i} \bmod p.$$

$$E_3 \cdot E_4 = n_3 \cdot a^{i_3} \cdot n_4 \cdot a^{i_4} \bmod p =$$
$$= n_3 \cdot n_4 \cdot a^{(i_3 + i_4) \bmod (p-1)} \bmod p =$$
$$= n_3 \cdot n_4 \cdot a^{i_{34}} \bmod p =$$
$$= n_3 \cdot n_4 \cdot a^{i} \bmod p.$$

If $n_1 \cdot n_2 = n_3 \cdot n_4$ $\Leftarrow$ $m_1 + m_2 = m_3 + m_4$ balance

Then $E_1 \cdot E_2 = E_3 \cdot E_4$ $\Rightarrow$ $c_1 \cdot c_2 = c_3 \cdot c_4$

AA $Dec(z, c_{AA3}) = n_3 \Rightarrow n_3 = g^{m_3} \bmod p \Rightarrow m_3$
$Dec(z, c_{AA4}) = n_4 \Rightarrow n_4 = g^{m_4} \bmod p \Rightarrow m_4$
$\left.\begin{matrix} m_3 \\ m_4 \end{matrix}\right\}$ $m_3 + m_4 = m_{34}$

Decrypts also $\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_N$ declarations and verifies if
$$m_1 + m_2 = m_3 + m_4$$

Information adequate and available to Net is:
$c_1(a)$, $c_2(a)$ & $c_{AA3}(AA)$, $c_{AA4}(AA)$
$$c_1 \cdot c_2 \neq c_{AA3} \cdot c_{AA4}$$

The proof that balance equation is valid when $c_{12} = c_1 \cdot c_2$ and

$c_{AA34} = c_{AA3} \cdot c_{AA4}$ are ciphertexts of the same plaintext, i.e.

$$n_1 \cdot n_2 = n_3 \cdot n_4 = n$$

$Enc(a, i, n) = c_{12}$ $\longleftrightarrow$ $Enc(AA, i, n) = c_{AA34}$