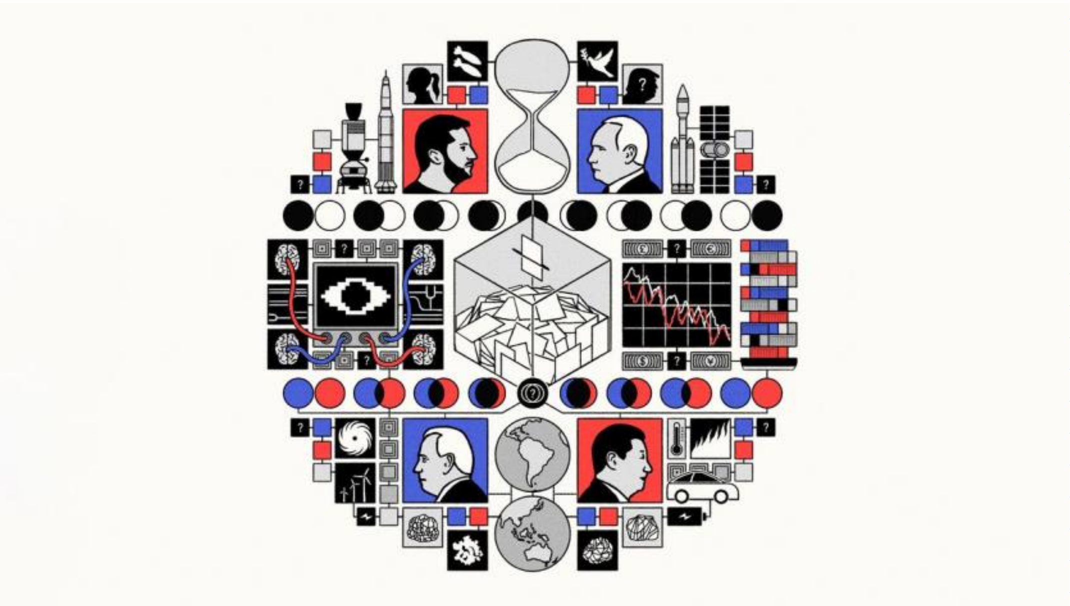


The World Achead 2024

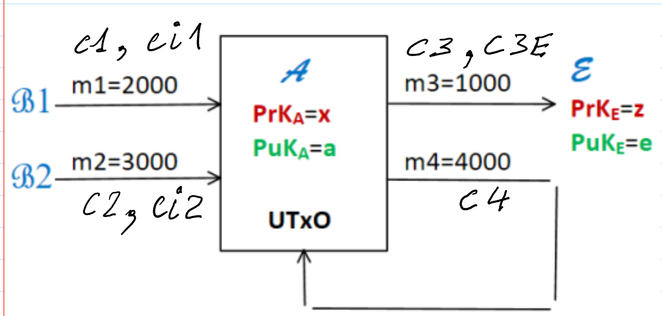
Confidential and Verifiable transactions

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

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

Actors: 𝔅1 𝔅2 *Alice* *Emily* ***Net***

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



Sums **m1** and **m2** are incomes-inputs.
Sums **m3** and **m4** are expenses-outputs.
UTxO - Unspent Transaction Output paradigm:
Balance between the input and output sums must hold
m1+m2 = m3+m4 = 5000. (1)

But how ***Net*** can verify that 𝒜 transaction is honest and balance equation **m1+m2** = **m3+m4** (1) holds?

To provide confidentiality and verifiability transferred sums are placed in the following exponents:

$n1 = g^{m1} \bmod p$ $\quad$ $n3 = g^{m3} \bmod p$

$n2 = g^{m2} \bmod p$ $\quad$ $n4 = g^{m4} \bmod p$

If $\quad m1+m2 = m3+m4 \bmod (p-1).$

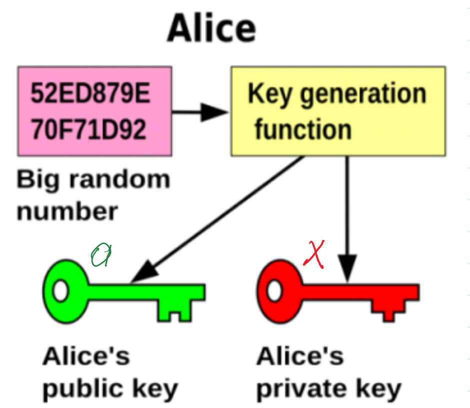
Then $\quad n1 * n2 = n3 * n4 \bmod (p).$

$a = g^{x} \bmod p$

$n_1 * n_2 \bmod p = g^{m_1} * g^{m_2} \bmod p = g^{(m_1+m_2) \bmod (p-1)} \bmod p$?

$$n_1 * n_2 \bmod p = g^{m_1} * g^{m_2} \bmod p = g^{(m_1+m_2) \bmod (p-1)} \bmod p$$
$$n_3 * n_4 \bmod p = g^{m_3} g^{m_4} \bmod p = g^{(m_3+m_4) \bmod (p-1)} \bmod p$$

To provide confidentiality , 𝔅1 and 𝔅2 encrypts their **m1**, **m2** sums using **PuK$_A$=*a***.
Then both **m1**, **m2** are confidential and only 𝒜 can decrypt **c1**, **c2** with her **PrK$_A$=*x***.

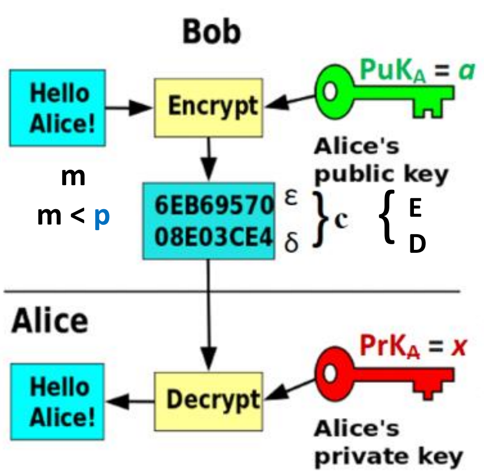


$$x \leftarrow int64(randi(p-1))$$
$$a = g^x \bmod p$$

```
>> x = int64(randi(p-1))
x = 69743707
>> a=mod_exp(g,x,p)
a = 95096100
```

Probabilistic encryption: encrypting 2 times the same plaintext m → the result is two different ciphertexts $c_1 \neq c_2$.

$$\left.\begin{aligned} Enc(a, i_1, m) &= c_1 \\ Enc(a, i_2, m) &= c_2 \end{aligned}\right\} \quad c_1 \neq c_2$$



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
```

Multiplicatively Homomorphic Encryption

$\mathcal{B}$:

n_1, n_2 - two messages to be encrypted: $1 < n_1, n_2 < p-1$. $\mathbb{Z}_p^*$

n_1: $i_1 \leftarrow randi(\mathbb{Z}_{p-1})$

$$\left.\begin{aligned} E_1 &= n_1 * a^{i_1} \bmod p \\ D_1 &= g^{i_1} \bmod p \end{aligned}\right\} \xrightarrow{c_1 = (E_1, D_1)}$$

$\mathcal{A}$: $Dec(\cancel{x}, c_1) = n_1$

n_2: $i_2 \leftarrow randi(\mathbb{Z}_{p-1})$

$$\left.\begin{aligned} E_2 &= n_2 * a^{i_2} \bmod p \\ D_2 &= g^{i_2} \bmod p \end{aligned}\right\} \xrightarrow{c_2 = (E_2, D_2)}$$

$Dec(\cancel{x}, c_2) = n_2$

$\mathcal{B}$: $n_{12} = n_1 * n_2 \bmod p$

$i_{12} = (i_1 + i_2) \bmod (p-1)$

n_{12}: $$\left.\begin{aligned} E_{12} &= n_{12} * a^{i_{12}} \bmod p \\ D &= g^{i_{12}} \bmod p \end{aligned}\right\} c = (E_{12}, D_{12})$$

Till this place