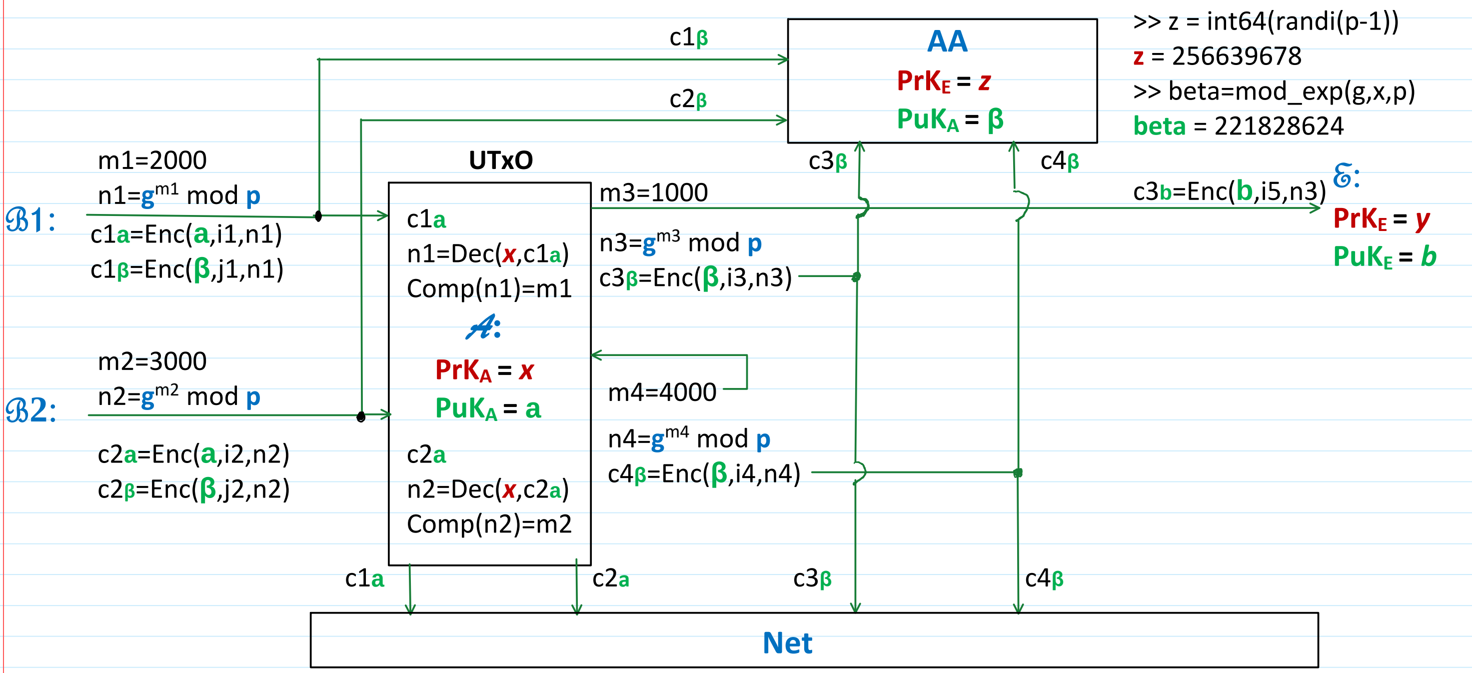
Confidential Verifiable Transactions **PP** = (*p*, *g*).



Net: Computes $c12a = c1a * c2a = (E1a, D1a) * (E2a, D2a) =$

$= (E1a * E2a \bmod p,\ D1a * D2a \bmod p) = (E12a, D12a)$

$c34\beta = c3\beta * c4\beta = (E3\beta, D3\beta) * (E4\beta, D4\beta) =$

$= (E3\beta * E4\beta \bmod p,\ D3\beta * D4\beta \bmod p) = (E34\beta, D34\beta)$

$$\left.\begin{array}{l} E3\beta = n_3 \cdot \beta^{i_3} \bmod p;\ D3\beta = g^{i_3} \bmod p; \\ E4\beta = n_4 \cdot \beta^{i_4} \bmod p;\ D4\beta = g^{i_4} \bmod p; \end{array}\right\} \begin{array}{l} E34\beta = n_3 \cdot n_4 \cdot \beta^{(i_3+i_4) \bmod (p-1)} \bmod p \\ D34\beta = g^{(i_3+i_4) \bmod (p-1)} \bmod p \end{array}$$

$$c_{34\beta} = (E34\beta = n_{34} \cdot \beta^{i} \bmod p,\ D34\beta = g^{i} \bmod p)$$

Taking in mind that:

1) If $m_{12} = m_1 + m_2 \bmod (p-1) = m_{34} = m_3 + m_4 \bmod (p-1)$

$n_{12} = n_1 \cdot n_2 \bmod p$ ═══ $n_{34} = n_3 \cdot n_4 \bmod p$

2) Then $Dec(PrK = x,\ c12a) = n_{12} = g^{(m_1+m_2) \bmod (p-1)} \bmod p$

$Dec(PrK = z,\ c34\beta) = n_{34} = g^{(m_3+m_4) \bmod (p-1)} \bmod p$

Then $c12a$ and $c34\beta$ encrypts the same number $n_{12} = n_{34} = n$.

But since $a \neq \beta$ ⟶ $c12a \neq c34\beta$ in any way!

Still since $a \neq \beta \Longrightarrow c12a \neq c34\beta$ in any way!

$\mathcal{A}$: Must prove that ciphertexts $c12a$ and $c34\beta$ encrypted the same number $n = n_{12} = n_{34} \Leftrightarrow$

$\Leftrightarrow$ balance $= (m_1 + m_2) \bmod (p-1) = (m_3 + m_4) \bmod (p-1) = 5000$.

This is named as ciphertexts equivalency problem.

Proof. $i = i_{34} = (i_3 + i_4) \bmod (p-1)$

```
>> i34=mod(i3+i4,p-1)
i34 = 115795473
```

1) $\mathcal{A}$ proves to the Net that she knows her $PrK_A = x$ by declaring her $PuK_A = a$ using NIZKP.

2) $\mathcal{A}$ proves to the Net that she knows her random parameter $i = i_{34}\,(i_3 + i_4) \bmod (p-1)$ for $n_{34} = n_3 * n_4 \bmod p$ encryption. Random parameters i_3 and i_4 must be secret otherwise encrypted values n_3 and n_4 can be decrypted without a knowledge of her $PrK = x$.

3) $\mathcal{A}$ referencing to these proofs provides a ciphertexts equivalency proof.

Non-Interactive Zero Knowledge Proof - NIZKP $\mathbf{PP} = (p, g)$.

$\mathcal{A}$: **NIZKP of knowledge** x:

$PrK_A = x =$ randi(p-1)

$PuK_A = a = g^x$ mod p

1. Computes r for random number u:

u=randi(p-1)

r=g^umod p

2. Generates h:

h=randi(p-1)

3. Computes:

s=u+xh mod (p-1)

$\xrightarrow[(r,\, s)]{PuK_A = a}$

$\mathcal{B}$: **$PuK_A = a$**

Verifies:

$g^s = ra^h$ mod p

$PrK_A = x$ is called witness for a statement $PuK_A = a$.

Let $\mathcal{A}$ wants to prove the knowledge of x and $i = i34$.

Then the statement $st = \{a = g^x \bmod p,\ D_{34\beta} = g^i \bmod p\}$

$u \leftarrow \text{randi}(\mathbb{Z}_p^*)$

$v \leftarrow \text{randi}(\mathbb{Z}_p^*)$

Commitments t_1 and t_2 are generated:

$$\left.\begin{array}{l} t_1 = g^u \bmod p \\ t_2 = g^v \bmod p \end{array}\right\} h = H(a \| D_{34\beta} \| t_1 \| t_2) \xrightarrow{Net} \begin{array}{l} \{a, D_{34\beta}, t_1, t_2\} \\ h = H(a \| D_{34\beta} \| t_1 \| t_2) \end{array}$$

$$\begin{array}{l} r = x \cdot h + u \bmod (p-1) \\ s = i \cdot h + v \bmod (p-1) \end{array} \longrightarrow \text{Net verifies} \quad \begin{array}{l} g^r = t_1 \cdot a^h \bmod p \\ g^s = t_2 \cdot (D_{34\beta})^h \bmod p \end{array}$$

Correctnes:

$$g^r = g^{(x \cdot h + u) \bmod (p-1)} \bmod p = g^{xh} \cdot g^u = (g^x)^h \cdot g^u = a^h \cdot t_1$$

$$g^s = g^{(i \cdot h + v) \bmod (p-1)} \bmod p = g^{ih} \cdot g^v = (g^i)^h \cdot g^v = (D_{34\beta})^h \cdot t_2$$

Till this place

However, the scheme presented above is insufficient to realize a proof of ciphertext equivalency. We propose the modification of the existing NIZKP to realize two ciphertext equivalency proofs, namely $C_{a,I}$ in (18), (19), and $C_{\beta,E}$ in (20), (21). Recall that $C_{a,I}$ is a ciphertext of plaintext I encryption with Alice's PuK=a and $C_{\beta,E}$ is a ciphertext of plaintext E encryption with the AA's PuK=β. The statement St of our proposed NIZKP consists of the following:

$$St = \{(\varepsilon_{a,I}, \delta_{a,I}), (\varepsilon_{\beta,E}, \delta_{\beta,E}), a, \beta\}. \quad (22)$$

The random integers $u \leftarrow randi(Z_q)$ and $v \leftarrow randi(Z_q)$ are generated by Alice, and the value $(-v) \bmod q$ is computed. The proof of ciphertext equivalence is computed using three computation steps:

1. The following commitments are computed:

$$t_1 = g^u \bmod p; \quad (23)$$
$$t_2 = g^v \bmod p; \quad (24)$$
$$t_3 = (\delta_{a,I})^u \cdot \beta^{-v} \bmod p. \quad (25)$$

2. The following h-value is computed using the cryptographically secure h-function H:

$$h = H(a \| \beta \| t_1 \| t_2 \| t_3 \|). \quad (26)$$

3. Alice, having her $PrK_A = x$ randomly generates the secret number l for E encryption and computes the following
two values:

$$r = x \cdot h + u \bmod q; \quad (27)$$
$$s = l \cdot h + v \bmod q. \quad (28)$$

Then Alice declares the following set of data to the Net:

$$\{a, \beta, t_1, t_2, t_3, r, s\} \rightarrow \text{Net}. \quad (29)$$

To verify the transaction's validity, the Net computes the h-value according to (26) and then verifies three identities:

$$g^r = a^h \cdot t_1; \quad (30)$$
$$g^s = (\delta_{\beta,E})^h \cdot t_2; \quad (31)$$
$$(\varepsilon_{\beta,E})^h \cdot (\varepsilon_{a,I})^{-h} \cdot (\delta_{a,I})^r \cdot \beta^{-s} = t_3. \quad (32)$$