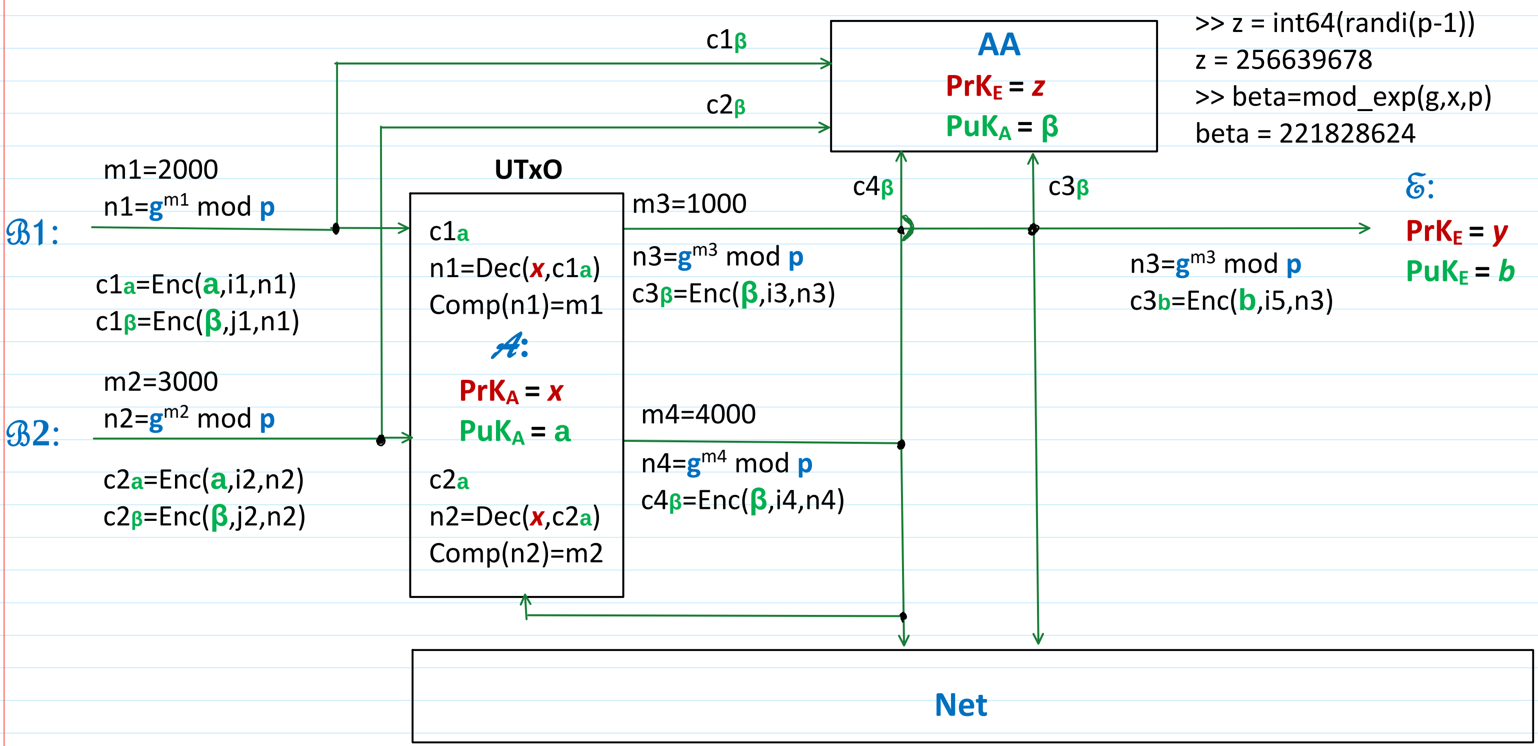

c_{12a} $\quad$ $c_{34\beta}$

$\mathcal{A}$: $c_{12a} = c_{1a} \cdot c_{2a} = (E_{1a}, D_{1a}) \cdot (E_{2a}, D_{2a}) =$

$= (E_{1a} \cdot E_{2a} \bmod p,\ D_{1a} \cdot D_{2a} \bmod p).$

$c_{34\beta} = c_{3\beta} \cdot c_{4\beta} = (E_{3\beta}, D_{3\beta}) \cdot (E_{4\beta}, D_{4\beta}) =$

$= (E_{3\beta} \cdot E_{4\beta} \bmod p,\ D_{3\beta} \cdot D_{4\beta} \bmod p).$

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

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

$c_{12a} \neq c_{34\beta}$

$\mathcal{A}$: must prove that c_{12a} and $c_{34\beta}$ encrypts the same product

$n = n_{12} = n_{34}$

It is named as ciphertexts equivalency proof.

$$c_{12a} = (\overbrace{\overbrace{n_1 a^{i_1} \bmod p}^{E_{1a}} \cdot \overbrace{n_2 a^{i_2} \bmod p}^{E_{2a}}}^{E_{12a}},\ \overbrace{\overbrace{g^{i_1} \bmod p}^{D_{1a}} \cdot \overbrace{g^{i_2} \bmod p}^{D_{2a}}}^{D_{12a}})$$

$$= (n_1 \cdot n_2\ a^{i_1+i_2} \bmod p,\ g^{i_1+i_2} \bmod p) =$$

$$C_{12a} = (n_1 a^{i_1} \bmod p \cdot n_2 a^{i_2} \bmod p,\ g^{i_1} \bmod p \cdot g^{i_2} \bmod p)$$

$$= (n_1 \cdot n_2\, a^{i_1+i_2} \bmod p,\ g^{i_1+i_2} \bmod p) =$$

$$= (\underbrace{n_{12}\, a^{i_1+i_2} \bmod p}_{E_{12a}},\ \underbrace{g^{i_1+i_2} \bmod p}_{D_{12a}})$$

$$C_{34\beta} = (\overbrace{\overbrace{n_3 \beta^{i_3} \bmod p}^{E_{3\beta}} \cdot \overbrace{n_4 \beta^{i_4} \bmod p}^{E_{4\beta}}}^{E_{34\beta}},\ \overbrace{\overbrace{g^{i_3} \bmod p}^{D_{3\beta}} \cdot \overbrace{g^{i_4} \bmod p}^{D_{4\beta}}}^{D_{34\beta}}) = \ldots$$

$$= (\underbrace{n_{34}\, \beta^{i_3+i_4} \bmod p}_{E_{34\beta}},\ \underbrace{g^{i_3+i_4} \bmod p}_{D_{34\beta}})$$

$\mathcal{A}$: $\xrightarrow{PuK_A = a}$ $\mathcal{B}$: is able to encrypt m to $\mathcal{A}$: $m < p$

$\mathcal{B}$: $r \leftarrow randi(\mathbb{Z}_p^*)$; $\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$

$$\left.\begin{array}{l} E = m \cdot a^r \bmod p \\ D = g^r \bmod p \end{array}\right\} c = (E, D) \longrightarrow$$

$\mathcal{A}$: is able to decrypt $c = (E, D)$ using her $PrK_A = x$.

1. $D^{-x \bmod (p-1)} \bmod p$
2. $E \cdot D^{-x} \bmod p = m$

$$(-x) \bmod (p-1) = (0 - x) \bmod (p-1) =$$
$$= (p - 1 - x) \bmod (p-1)$$

```
>> m1=2000
m1 = 2000
>> n1=mod_exp(g,m1,p)
n1 = 28125784
>> i1 = int64(randi(p-1))
i1 = 237208612
>> a_i1=mod_exp(a,i1,p)
a_i1 = 225539744
>> E1a=mod(n1*a_i1,p)
E1a = 236913646
>> D1a=mod_exp(g,i1,p)
D1a = 157143772
```

```
>> m2=3000
m2 = 3000
>> n2=mod_exp(g,m2,p)
n2 = 222979214
>> i2 = int64(randi(p-1))
i2 = 202826700
>> a_i2=mod_exp(a,i2,p)
a_i2 = 89867164
>> E2a=mod(n2*a_i2,p)
E2a = 243880762
>> D2a=mod_exp(g,i2,p)
D2a = 12682290
```

```
>> E12a=mod(E1a*E2a,p)
E12a = 103086800
>> D12a=mod(D1a*D2a,p)
D12a = 239766142
```

C12a

```
>> m3=1000
m3 = 1000
>> n3=mod_exp(g,m3,p)
n3 = 260099963
>> i3 = int64(randi(p-1))
```

```
>> m4=4000
m4 = 4000
>> n4=mod_exp(g,m4,p)
n4 = 246637967
>> i4 = int64(randi(p-1))
i4 = 225960178
```

```
>> E34beta=mod(E3beta*E4beta,p)
E34beta = 84122191
>> D34beta=mod(D3beta*D4beta,p)
D34beta = 198671542
```

C34beta

```
>> n3=mod_exp(g,m3,p)
n3 = 260099963
>> i3 = int64(randi(p-1))
i3 = 158270313
>> beta_i3=mod_exp(beta,i3,p)
beta_i3 = 152293358
>>  E3beta=mod(n3*beta_i3,p)
E3beta = 239879038
>> D3beta=mod_exp(g,i3,p)
D3beta = 226571899
```

```
n4 = 246637967
>> i4 = int64(randi(p-1))
i4 = 225960178
>> beta_i4=mod_exp(beta,i4,p)
beta_i4 = 28521928
>> E4beta=mod(n4*beta_i4,p)
E4beta = 214072649
>>  D4beta=mod_exp(g,i4,p)
D4beta = 229603826
```

```
D34beta = 198671542
```

$\mathcal{A}$: must prove that ciphertexts $c_{12\alpha}$ and $c_{34\beta}$ encrypted the same textogram $n = n_{12} = n_{34}$ ➡

➡ balance $= (m_1 + m_2) \bmod (p-1) = (m_3 + m_4) \bmod (p-1)$

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

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

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

3) $\mathcal{A}$ proves to the Net that she knows her random parameter $i_{34} = (i_3 + i_4) \bmod (p-1)$ for n_3 and n_4 encryption.

Random parameters i_3 and i_4 must be secret otherwice encrypted values n_3 and n_4 can be decrypted without a knowledge of her $PrK = x$.

For example. Let i_3 is known to the Net. Tada by having $E_{3\beta}$ one can decrypt n_3:

a) the inverse element of $i_3 \bmod (p-1)$ is computed and having $-i_3 \bmod (p-1)$, $E_{3\beta}$ is multiplied by $\beta^{-i_3} \bmod p$.

$$nn_3 = E_{3\beta} * \beta^{-i_3} \bmod p = n_3 \cdot \beta^{i_3} * \beta^{-i_3} \bmod p = n_3\, \beta^{i_3 - i_3} \bmod p =$$
$$= n_3\, \beta^0 \bmod p = n_3.$$

```
>> mi3 = mod(-i3, p-1)
>> beta_mi3 = mod_exp(beta, mi3, p)
>> nn3 = mod(E3beta * a_mi3, p)
```

```
>> mi3=mod(-i3,p-1)
mi3 = 110164705
>> mod(i3+mi3,p-1)
ans = 0

>> beta_mi3=mod_exp(beta,mi3,p)
beta_mi3 = 150721861
>> nn3=mod(E3beta*beta_mi3,p)
nn3 = 260099963
>>  n3 = int64(260099963)
n3 = 260099963
```

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:

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