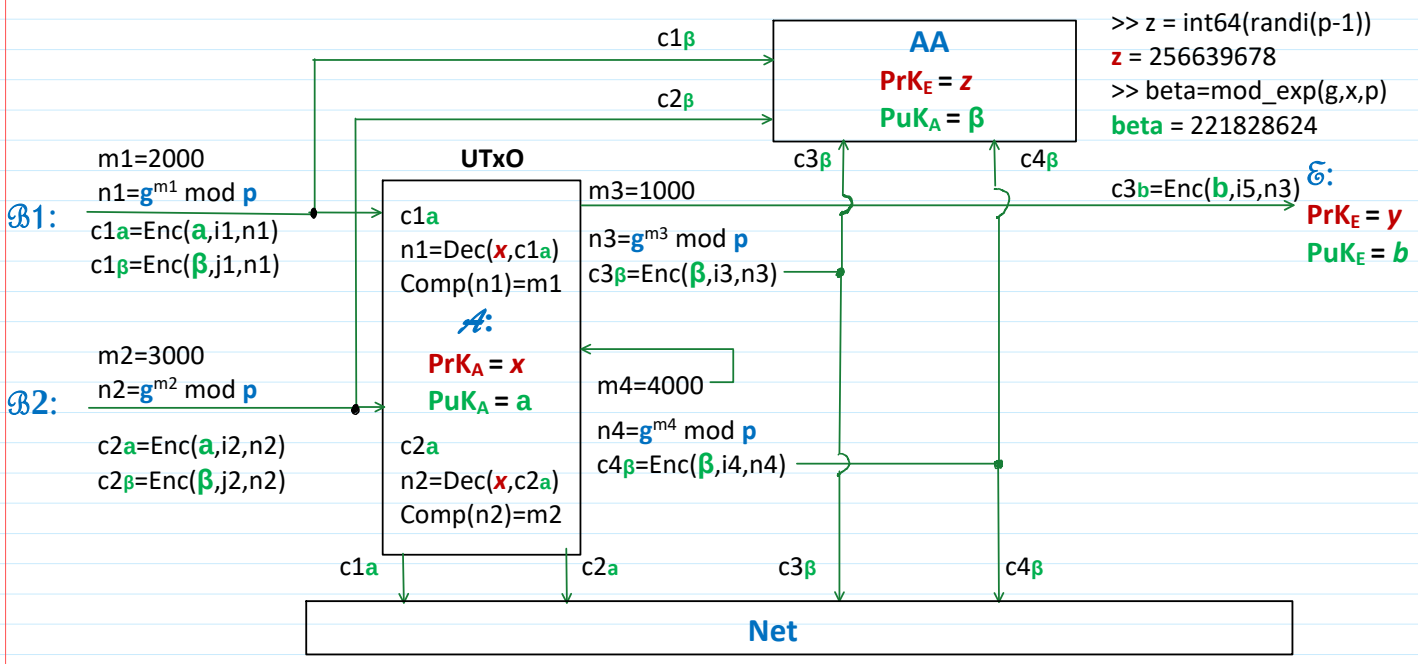
Confidential Verifiable Transactions - 2 PP = (p, g).



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

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

$$c_{3\beta} \cdot c_{4\beta} = c_{34\beta} = Enc(\beta, i_{34}, n_{34}) = (E_{34\beta}, D_{34\beta}) = (n_{34} \cdot \beta^{i_{34}}, g^{i_{34}}) = c_{34\beta}$$
$$i_{34} = (i_3 + i_4) \bmod (p-1)$$
$$n_{34} = n_3 \cdot n_4 \bmod p$$

If transaction balance is valid: $m_1 + m_2 = 2000 + 3000 = 1000 + 4000 = m_3 + m_4$

Then since: $n_{12} = n_1 \cdot n_2 = g^{m_1} \cdot g^{m_2} \bmod p = g^{m_1+m_2} \bmod p$
$n_{34} = n_3 \cdot n_4 = g^{m_3} \cdot g^{m_4} \bmod p = g^{m_3+m_4} \bmod p.$
$\Rightarrow n_{12} = n_{34} = n$

A: must prove to the net, that c_{12a} and $c_{34\beta}$ encrypted the same value $n_{12} = n_{34} = n$; → Ciphertexts Equivalency Proof.

The statement St for this proof is the following:

$St = \{c_{12a}, c_{34\beta}, a, \beta\}$; For example: $a = g^x \bmod p$

PuK = a is a statement for x.

For proof A randomely generates integers u, v and $(-v) \bmod (p-1)$

$u \leftarrow randi(\mathcal{I}_{p-1})$; $\mathcal{I}_{p-1} = \{0, 1, 2, \dots, p-2\}$

$v \leftarrow randi(\mathcal{I}_{p-1})$

$-v \bmod (p-1)$ $\longrightarrow$ >> $mv = mod(-v, p-1)$

1. The following commitments $\{t_1, t_2, t_3\}$ are computed:

$$t_1 = g^u \bmod p$$

$$t_2 = g^v \bmod p$$

$$t_3 = (D_{12}a)^u \cdot \beta^{-v} \bmod p$$

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

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

3. A having her PrK x and $i_{34} = (i_3 + i_4) \bmod (p-1)$ computes r and s

$$r = (x \cdot h + u) \bmod (p-1)$$

$$s = (i_{34} \cdot h + v) \bmod (p-1)$$

and declares the following set of data to the Net

$\{C_{1a}, C_{2a}, C_{3\beta}, C_{4\beta}\} \cup \{a, \beta, t_1, t_2, t_3, r, s\}$ $\longrightarrow$ Net

Net computes h-value defined above

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

Net verifies transaction correctness by verifying the following identities

$$g^r = a^h \cdot t_1 \bmod p$$

$$g^s = (D_{34\beta})^h \cdot t_2 \bmod p$$

$$(E_{34\beta})^h \cdot (E_{12a})^{-h} \cdot (D_{12a})^r \cdot \beta^{-s} = t_3 \bmod p$$

Declare **Public Parameters** to the network PP = (p, g); p= 268435019; g=2;

$PrK_A = x$ <-- randi ==> $PuK_A = a = g^x \bmod p$ $PrK_A = x$ <-- randi ==> $PuK_A = a = g^x \bmod p$

>> p=int64(268435019)
p = 268435019
>> g=2;

>> x=int64(randi(p-1))
x = int64(220099152)
>> a=mod_exp(g,x,p)
a = 174059961

>> z=int64(randi(p-1))
z = int64(49750938)
>> beta=mod_exp(g,z,p)
beta = int64(213338364)

Incomes

>> m1=2000;
>> n1=mod_exp(g,m1,p)
n1 = 28125784
>> i1=int64(randi(p-1))
i1 = int64(207414820)
>> a_i1=mod_exp(a,i1,p)
a_i1 = 192148999
>> E1a=mod(n1*a_i1,p)
E1a = 207347548
>> D1a=mod_exp(g,i1,p)
D1a = 202537833

c1***a*** = (E1***a***, D1***a***)

Verification: Dec(***x***, c1***a***) = nn1
>> mx=mod(-x,p-1)
mx = 48335866
>> D1a_mx=mod_exp(D1a,mx,p)
D1a_mx = 75547583
>> nn1=mod(E1a*D1a_mx,p)
nn1 = 28125784

>> m2=3000;
>> n2=mod_exp(g,m2,p)
n2 = 222979214
>> i2=int64(randi(p-1))
i2 = int64(67446699)
>> a_i2=mod_exp(a,i2,p)
a_i2 = 211790072
>> E2a=mod(n2*a_i2,p)
E2a = 77938423
>> D2a=mod_exp(g,i2,p)
D2a = 82080815

C2***a*** = (E2***a***, D2***a***)

Verification: Dec(***x***, c2***a***) = nn2
>> mx=mod(-x,p-1)
mx = 48335866
>> D2a_mx=mod_exp(D2a,mx,p)
D2a_mx = 57701660
>> nn2=mod(E2a*D2a_mx,p)
nn2 = 222979214

>> E12a=mod(E1a*E2a,p)
E12a = 52532683
>> D12a=mod(D1a*D2a,p)
D12a = 32918394

C12a = (E12a, D12a)

Expenses

>> m3=1000;
>> n3=mod_exp(g,m3,p)
n3 = 260099963
>> i3=int64(randi(p-1))
i3 = int64(137379932)
>> beta_i3=mod_exp(beta,i3,p)
beta_i3 = 14259017
>> E3beta=mod(n3*beta_i3,p)
E3beta = 167897317
>> D3beta=mod_exp(g,i3,p)
D3beta = 65145889

Verification: Dec(***z***, c3**beta**) = nn3
>> mz=mod(-z,p-1)
mz = 218684080
>> D3beta_mz=mod_exp(D3beta,mz,p)
D3beta_mz = 258869169
>> nn3=mod(E3beta*D3beta_mz,p)
nn3 = 260099963

>> m4=4000;
>> n4=mod_exp(g,m4,p)
n4 = 246637967
>> i4 = int64(randi(p-1))
i4 = int64(225960178)
>> beta_i4=mod_exp(beta,i4,p)
beta_i4 = 159771180
>> E4beta=mod(n4*beta_i4,p)
E4beta = 195130083
>> D4beta=mod_exp(g,i4,p)
D4beta = 229603826

Verification: Dec(***z***, c3**beta**) = nn3
>> mz=mod(-z,p-1)
mz = 218684080
>> D4beta_mz=mod_exp(D4beta,mz,p)
D4beta_mz = 218460911
>> nn4=mod(E4beta*D4beta_mz,p)
nn4 = 246637967

>> E34beta=mod(E3beta*E4beta,p)
E34beta = 57420210
>> D34beta=mod(D3beta*D4beta,p)
D34beta = 107062668

C34beta = (E34beta, D34beta)

The modification of the existing NIZKP to prove the equivalency of two cophertexts.

Namely c_{12a} and Ca,I in (18), (19), and $C\beta,E$ in (20), (21). Recall that Ca,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:

$$g^r = a^h \cdot t_1; \quad (30)$$

$$g^s = (\delta_{\beta,E})^h \cdot t_2; \quad (31)$$

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

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

$$g^r = a^h \cdot t_1; \quad (30)$$

$$g^s = (\delta_{\beta,E})^h \cdot t_2; \quad (31)$$

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