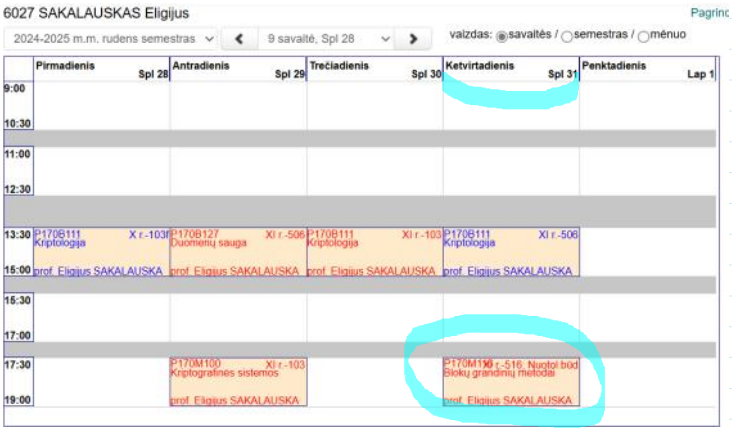
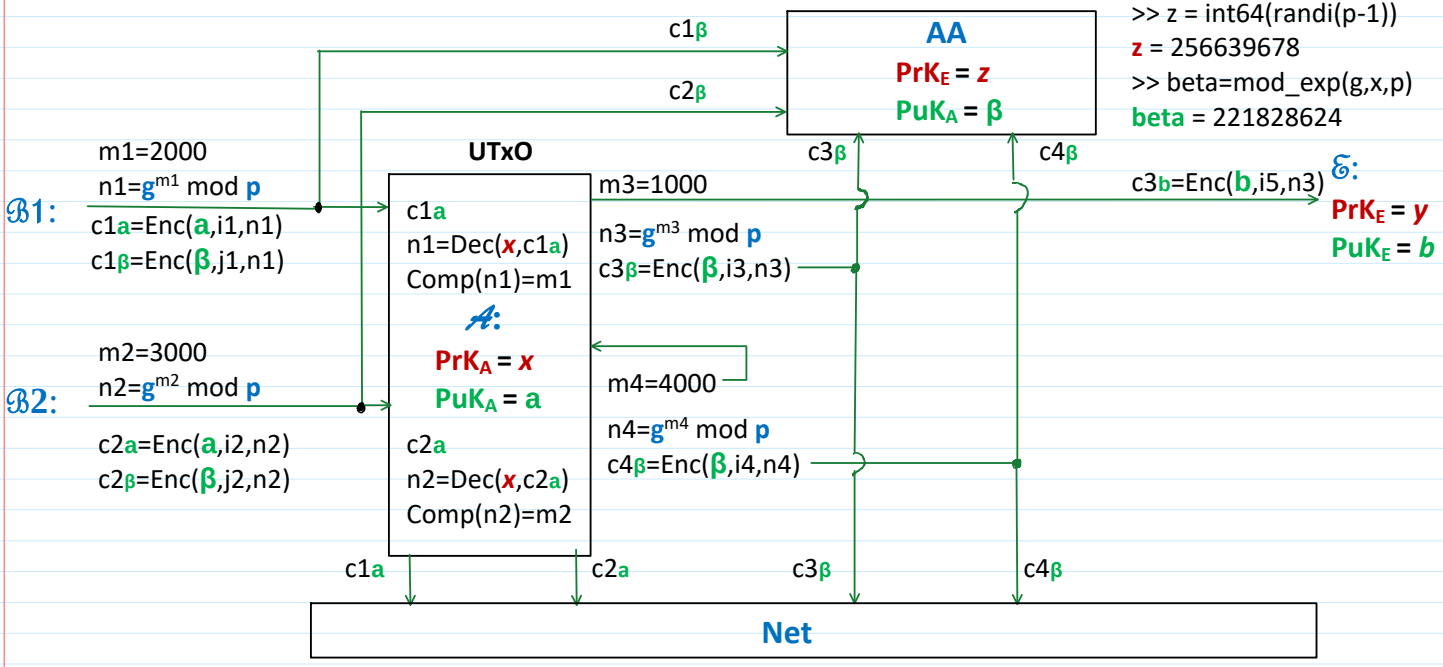
Koliokviumas: Ciphertexts equivqlency proof.
IV-nis, Spalio 31 d., 17:30.



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



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

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

$$Enc(\beta, i_3, n_3) = c_{3\beta} = (E_{3\beta}, D_{3\beta}) = (n_3 \cdot \beta^{i_3}, g^{i_3}) \bmod p$$
$$Enc(\beta, i, n) = c_{4\beta} = (E_{4\beta}, D_{4\beta}) = (n_4 \cdot \beta^{i_4}, g^{i_4}) \bmod p$$

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

$$n_{34} = n_3 \cdot n_4 \bmod p$$

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

Then since: $n_{12} = n_1 \cdot n_2 = g^{m_1} \cdot g^{m_2} \bmod p = g^{m_1+m_2} \bmod p$

$n_{34} = n_3 \cdot n_4 = g^{m_3} \cdot g^{m_4} \bmod p = g^{m_3+m_4} \bmod p.$ } $n_{12} = n_{34} = n$

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

PrK_A = *x* <-- randi ==> PuK_A = *a* = g^x mod p **PrK_A = *x* <-- randi ==> PuK_A = *a* = g^x mod 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)
```

```
>> m4=4000;
>> n4=mod_exp(g,m4,p)
```

```
>> E34beta=mod(E3beta*E4beta,p)
E34beta = 57420210
```

```
>> 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)

```
>> nn12=mod(nn1*nn2,p)
nn12 = 143845522
```

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

```
>> nn34=mod(nn3*nn4,p)
nn34 = 143845522
```

A: must prove to the net, that $C_{12\alpha}$ 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:

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

$PuK = \alpha$ is a statement for x.

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

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

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

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

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

$t_1 = g^u \bmod p$

$t_2 = g^v \bmod p$

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

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

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

```
>> u = int64(randi(p-1))
u = 234711265
>> t1=mod_exp(g,u,p)
t1 = 160710747

>> v=int64(randi(p-1))
v = 223454508
>> t2=mod_exp(g,v,p)
t2 = 131605032
```

```
>> D12a
D12a = 32918394
>> D12a_u=mod_exp(D12a,u,p)
D12a_u = 190889544
>> mv=mod(-v,p-1)
mv = 44980510
>> beta_mv=mod_exp(beta,mv,p)
beta_mv = 81562027
>> t3=mod(D12a_u*beta_mv,p)
t3 = 202608126
```

```
>> hsym = hd28('a||beta||t1||t2||t3')
>> hsym='174059961||213338364||
160710747||131605032||202608126'
hsym = 174059961||213338364||
160710747||131605032||202608126
>> h=hd28('hsym')
h = 67517394
>>
>> h=hd28(hsym)
h = 264802094
```

```
>> hsym='174059961||213338364||160710747||131605032||202608126'
hsym = 174059961||213338364||160710747||131605032||202608126
>> h=hd28(hsym)
h = 264802094
```

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

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

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

```
>> xh=mod(x*h,p-1)
xh = 2537232
>> r=mod(xh+u,p-1)
r = 237248497
```

```
>> i3
i3 = 137379932
>> i4
i4 = 225960178
>> i34=mod(i3+i4,p-1)
i34 = 94905092
```

```
>> i34h=mod(i34*h,p-1)
i34h = 50935534
>> s=mod(i34h+v,p-1)
s = 5955024
```

and declares the following set of data to the Net

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

Net computes

$$C_{12\alpha} = C_{1\alpha} * C_{2\alpha} \qquad C_{34\beta} = C_{3\beta} * C_{4\beta}$$

$$C_{12\alpha} = (E_{1\alpha} \cdot E_{2\alpha}, D_{1\alpha} \cdot D_{2\alpha}) \qquad C_{34\beta} = (E_{3\beta} \cdot E_{4\beta}, D_{3\beta} \cdot D_{4\beta})$$

Net computes h-value defined above

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

Till this place

Net verifies transaction correctness by verifying the following identities

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

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

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