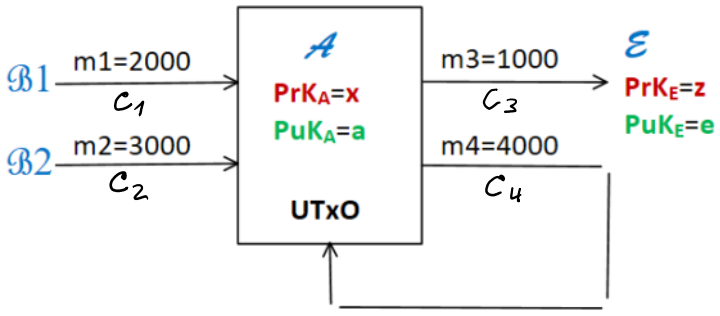
Zero Knowledge Proof (ZKP) of equivalence of 2 ciphertexts *c*3, *c*3*e* corresponding to the same plaintext *m* obtained by encryption with different Puks



How to provide anonymity of transaction amounts and to verify the **balance**: **m1+m2 = m3+m4** ?

n1= g^{m1} mod **p** **n3**= g^{m3} mod **p**

n2= g^{m2} mod **p** **n4**= g^{m4} mod **p**

If **(m1+m2) mod (p -1) = (m3+m4) mod (p-1)**,
Then **(n1*n2) mod p = (n3*n4) mod p**.

$n_1 \cdot n_2 \bmod p = g^{m_1+m_2} \bmod p$ $\quad$ $n_3 \cdot n_4 = g^{m_3+m_4} \bmod p$

If $n_1 \cdot n_2 \bmod p = n_3 \cdot n_4 \bmod p$

$c_1 \cdot c_2 = c_3 \cdot c_4$

$c_1 = Enc(a, i_1, n_1) = (E_1, D_1)$ $\quad$ $c_3 = Enc(a, i_3, n_3) = (E_3, D_3)$

$c_2 = Enc(a, i_2, n_2) = (E_2, D_2)$ $\quad$ $c_4 = Enc(a, i_4, n_4) = (E_4, D_4)$

A: Enc(**e**, n3) =
c3e=(E3e,D3e)
E3e= n3*e^{i3} mod **p**
D3e= g^{i3} mod **p** } c_{3e}
Enc(**e**, i3) = ci3e
j3e <-- randi(**p**-1)
Ei3e= i3*e^{j3} mod **p**
Di3e= g^{j3} mod **p** } c_{i3e}

c3e=(E3e,D3e)
ci3e=(Ei3e,Di3e) → **E**: PrK=**z**; PuK=**e**.

E: Dec(**z**, c3e) = n3 & verifies if n3=g^{m3} mod **p**
Dec(**z**, ci3e) = i3

Net:

A: c3=(E3,D3)
E3= n3*a^{i3} mod **p**
D3= g^{i3} mod **p** } $c_3 = (E_3, D_3)$

A: c3e=(E3e,D3e)
E3e= n3*e^{i3} mod **p**
D3e= g^{i3} mod **p** } $c_{3e} = (E_{3e}, D_{3e})$

$c_3 \neq c_{3e}$

Let **E** knows i_3, then **E** can verify that c_3 and c_{3e} encrypts the same number $n_3 = g^{m_3} \bmod p$, when $m_3 = 1000$.

E takes a ratio

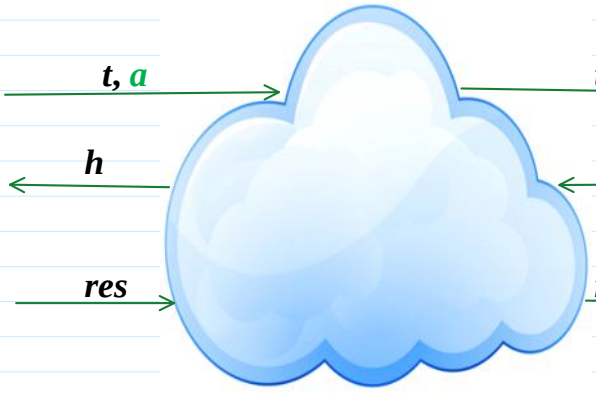
$$\frac{E_3}{\quad} = \frac{n_3 \cdot a^{i_3} \bmod p}{\quad} = \left(\frac{a}{\quad}\right)^{i_3} \bmod p$$

$$\frac{E_3}{E_{3e}} = \frac{n_3 \cdot a^{i_3} \bmod p}{n_3 \cdot e^{i_3} \bmod p} = \left(\frac{a}{e}\right)^{i_3} \bmod p$$

Schnorr Identification: Zero Knowledge Proof - ZKP

Schnorr Id scenario: **Alice** wants to prove **Bank** that she knows her Private Key - $PrK_A = x$ which corresponds to her Public Key - $PuK_A = a = g^x \bmod p$ not revealing $PrK_A = x$.

$\mathcal{A}$: ZKP of knowledge x:
$PrK_A = x =$ randi(p-1)
$PuK_A = a = g^x \bmod p$
1.Computes commitment ***t*** for ***i***:
i=randi(p-1)
$t=g^i \bmod p$
3.Computes response ***res***:
$res=i+xh \bmod (p-1)$



$\mathcal{B}$: $PuK_A = a = g^x \bmod p$
2.Generates challenge ***h***:
h=randi(p-1)
Verifies:
$g^{res} = ta^h \bmod p$

t
h
res
Time

Correctness:
$g^{res} \bmod p = g^{i+xh} \bmod p = g^i g^{xh} \bmod p = t(g^x)^h \bmod p = ta^h \bmod p$.

$r \leftarrow randi(\mathcal{I}_p^*)$; $\mathcal{I}_p^* = \{1, 2, 3, \ldots, p-1\}$; $*$ mod p; / mod p

$u = g^r \bmod p$; $v = \left(\frac{a}{e}\right)^r \bmod p$.

$h = H(u \| v)$

$w = (i_3 \cdot h + r) \bmod (p-1)$ —u, v, w / a, e→ Ver: $h = H(u \| v)$

Ver1: $g^w = (D_3)^h \cdot u \bmod p =$

Ver2: $\left(\frac{a}{e}\right)^w = \left(\frac{E_3}{E_{3e}}\right)^h \cdot v \bmod p =$

Correctness:

Ver1: $g^w = g^{(i_3 \cdot h + r) \bmod (p-1)} \bmod p = (g^{i_3})^h \cdot g^r \bmod p = (D_3)^h \cdot u \bmod p.$

Ver2: $\left(\frac{a}{e}\right)^w \bmod p = \left(\frac{a}{e}\right)^{(i_3 \cdot h + r) \bmod (p-1)} \bmod (p-1) =$

Ver 2 : $\left(\frac{a}{e}\right)^{} \bmod p = \left(\frac{}{e}\right)^{}$ $\quad mod(p-1) =$

$$= \left(\frac{a}{e}\right)^{i_3 \cdot h} \cdot \left(\frac{a}{e}\right)^{r} \bmod p = \left(\frac{a^{i_3}}{e^{i_3}}\right)^{h} \cdot v \bmod p =$$

$$= \left(\frac{n_3 a^{i_3}}{n_3 e^{i_3}}\right)^{h} \cdot v \bmod p = \left(\frac{E_3}{E_{3e}}\right)^{h} \cdot v \bmod p.$$

Till this place

A: Net