TP5:

Q1) If double spending happens we get two transaction T_1, T_2 of the same money. From these two we can recover sk_U.

$$\begin{cases} T_1 = sk_U + R_1 k \\ T_1 = sk_U + R_2 k \end{cases} \Leftrightarrow k = \frac{T_1 - sk_U}{R_1} = \frac{T_2 - sk_U}{R_2} \Leftrightarrow sk_U = \frac{R_2 T_1 - R_1 T_2}{(R_2 - R_1)}$$

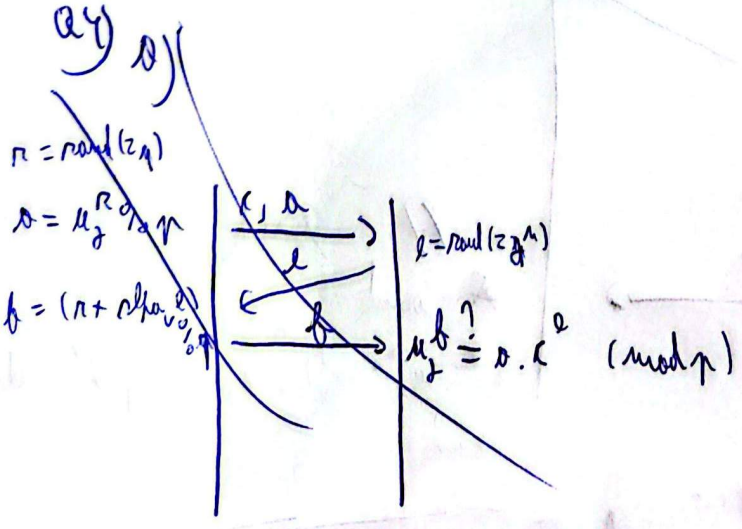
T_1, T_2, R_1, R_2 are accessible by Bank.

Q2) These are two different coins with the same amount of money.

Q3) Now $k = k'$ so we lose the property of unlinkability (= anonimity) from each micro-service as k' exactly the same and can collaborate with others to track an activity list of the user.

Normally, the bank signs $\kappa = u_0^{\pi} \cdot u_1^{m_1} \cdot u_2^{sk} \cdot u_3^{t}$ and under re-randomize $\kappa' = \kappa \cdot u_1^{\pi'}$ also in order to preserve anonimity when doing a transaction with the Bank. Now the bank can fully maps each k' to a key value store $k = k' \rightarrow sk_U$ that is profiting.

Q4)



Q4) $\pi = \pi + \pi'$; $R' = \mu_0^{h+h'} \cdot \mu_1^{\dots} \cdot \mu_2^{\dots} \cdot \mu_3^{k}$

a) $\pi = \text{rand}(z_q)$ $A_{\bar\pi}, A_\pi$ We have always to prove random stuff as π, π.

$h = R / \mu_2^{nk}$

$A = \mu_2^{\pi} \% n$

$A_\pi = \mu_2^{nk} \% n$ $A_0 = \mu_0^{\bar\pi} \% n$

$f_{nk} = (\pi + l_{nk} \cdot nk) \% q$

$A_{\bar\pi} = (\pi + l\pi) \% n$

$A_\pi = (\pi' + l\pi) \% n$

$A_{\bar\pi}, A_{nk}, A_\pi$ → $l_{nk} = \text{rand}(z, m)$

l_{nk} ←

$f_{nk}, \beta_{\bar\pi}, \beta_\pi$ →

$\mu_2^{f_{nk}} \stackrel{?}{=} A_{nk} \cdot h^{l_{nk}} \pmod n$

$\mu_0^{\beta_{\bar\pi}} \cdot \mu_2^{f_{nk}} \cdot \mu_3^{\beta_\pi} \stackrel{?}{=} A_{\bar\pi} \cdot A_{nk} \cdot A_\pi \cdot h^l \pmod n$

Full: $R = \mu_0^{\pi} \cdot \mu_1^{m} \cdot \mu_2^{msk} \cdot \mu_3^{k}$

(Prove all)

User

$\pi_0, \pi_1, \pi_2, \pi_3 = \text{rand}(z_q^4)$

$A_i = \mu_i^{\pi_i} \% n$

$F_0 = (\pi_0 + l \cdot \pi) \% q$

$F_1 = (\pi_1 + l \cdot m) \% q$

$F_2 = (\pi_2 + l \cdot msk) \% q$

$F_3 = (\pi_3 + l \cdot k) \% q$

A_0, A_1, A_2, A_3 →

← l

F_0, F_1, F_2, F_3 →

Bank

$l = \text{rand}(z_m)$

$\mu_0^{F_0} \cdot \mu_1^{F_1} \cdot \mu_2^{F_2} \cdot \mu_3^{F_3} \stackrel{?}{=} A_0 \cdot A_1 \cdot A_2 \cdot A_3 \cdot R^l \pmod n$ *

b) 1) Same thing but this time $\bar\pi = \pi \wedge h = R / \mu_2^{nk}$

2) Add

$T = nk + k$

$R = \mu_0^{\pi} \cdot \mu_1^{m} \cdot \mu_2^{nk} \cdot \mu_3^{k}$

$h = R / \mu_2^{nk}$

$\pi_0, \pi_1, \pi_2, \pi_3 = 2^{\text{rand}(q)}$

$A_0 = \mu_0^{\pi_0} \% n$, $A_1 = \mu_1^{\pi_1} \% n$,

$A_2 = \mu_2^{\pi_2} \% n$, $A_3 = \mu_3^{\pi_3} \% n$

$A_3' = \mu_2^{\pi_3} \% n$

$F_0 = (\pi_0 + l\,\pi) \% q$

$F_1 = (\pi_1 + l\,m) \% q$

$F_3 = (\pi_3 + k \cdot l) \% q$

$F_2 = (\pi_2 + l\,nk\,m) \% q$

User

$h, A_0, A_1, A_2, A_3, R, T, A_3'$ →

← l

F_0, F_1, F_2, F_3 →

Bank

$l = \text{rand}(z_m)$

$\mu_0^{F_0} \cdot \mu_1^{F_1} \cdot \mu_3^{F_3} \stackrel{?}{=} A_0 \cdot A_1 \cdot A_3 \cdot h^l \pmod n$

and

$\mu_2^{F_2 + R \cdot F_3} \stackrel{?}{=} A_2 \cdot A_3^R \cdot \mu_2^{RT} \pmod n$

~~$\mu_2^{F_2} \cdot (\mu_3^{F_3})^R \stackrel{?}{=} A_2 \cdot \mu_2 \cdot A_3^R$~~

SURPASS

Q5) TP.S.2

a) R = Hash(name, birth)

* ~~If we associate (name, birth) to a Transaction T then we know~~ we have to be able to associate a pair to each transaction T that is against privacy and allows profiling, very bad.

b) $R = pk_U = g^{sk_U}$

we cannot profile users but we can link all transactions having the same R that is against unlinkability.

c) R = Time of signature

Still R is constant and make all transactions linkable.

All solutions are bad it is better to have R as random.