TP4 : QO

Non-Interactive Divertible Schnorr Proof

(Prover) (BEFORE ONCE) (Verifier)

Secret $m \in \mathbb{Z}_q$, $h = g^m \% p$

$r = rand(\mathbb{Z}_q)$

$s = g^r \% p$

$c = (r + cm) \% q$

$(G, g, q, h), s$ →

← c

← f

message $m \in \mathbb{Z}_q$

w is a re-randomizing (blinding factor)

$r', w = rand(\mathbb{Z}_q^2)$

$s' = s^w \cdot g^{r'} \% p$; $c' = H(g, h, s', m) \in \mathbb{Z}_q$

$c = c' \cdot w^{-1} \% q = c' \cdot (w^{-1} \% q) \% q$

$f' = (r' + w \cdot f) \% q$

$\Rightarrow G = (s', c', f')$

In practice c' could not be stored as it is easily recomputable

(LATER NTIMES)

Verifier: $m \in \mathbb{Z}_q$, $G = (s', c', f')$

$(s', h'), m$ →

← (G, g, q, h)

$c' = H(g, h, s', m)$

Check :

$g^{f'} \% p \stackrel{?}{=} s' \cdot h^{c'} \% p$

Non-Interactive so c' is not sent as verifier can recompute it !!

(completeness) correctness :

$$\boxed{g^{f'}} = g^{r' + wf} = g^{r'} \cdot g^{w(r + cm)} = g^{r'} \cdot g^{wr} \cdot g^{wc(c' \cdot w^{-1}) \cdot w}$$

$$= g^{r'} \cdot (g^r)^w \cdot (g^m)^{c'} = (s^w \cdot g^{r'}) \cdot h^{c'} = \boxed{s' \cdot h^{c'}}$$

($s^w = g^{rw}$, $h = g^m$, $s' = s^w \cdot g^{r'}$)

TP.4.1

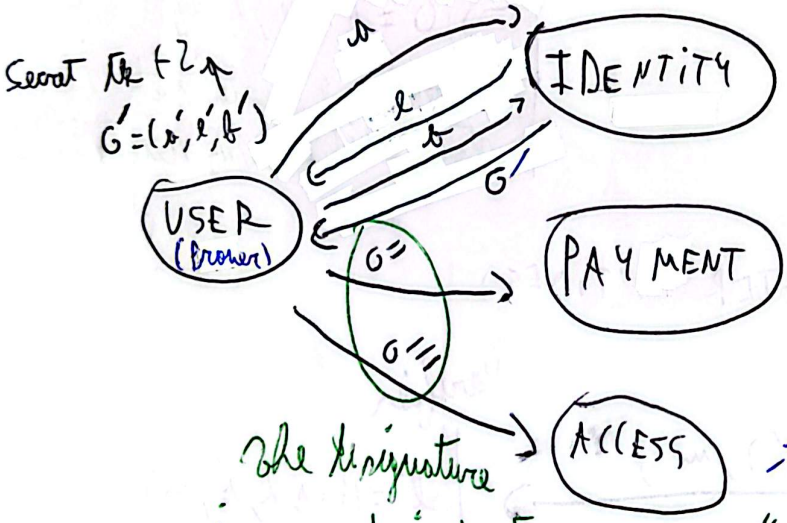
Q1) 1) → Each user is uniquely identified by a token tk.

→ The theater knows the user's identity at payment's time.

→ The theater asks which movie at watching's time.

So the unique token can be used by the theater to link each user identity to the watched movies making privacy totally broken.

2) We can use a Divertible Schnorr Proof with 3 micro-services : IDENTITY, PAYMENT and ACCESS.



The user gets a signature that of its token to anonymously authenticate later.

The signature proves the user is valid without revealing who it is. $gt'' = x''.h^{t''} \pmod{p}$

The re-signature is re-randomized at each transaction to preserve unlinkability.

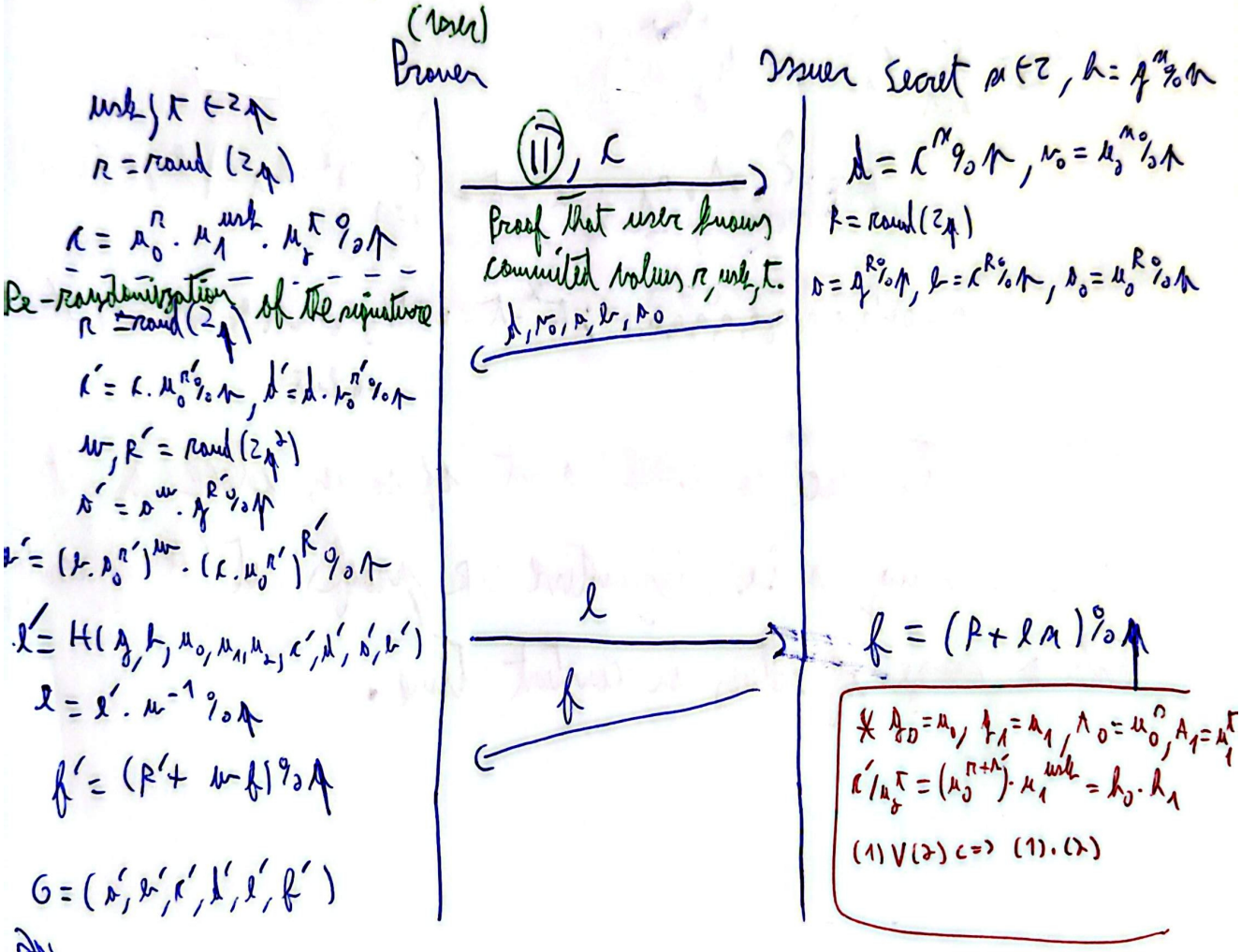
$r'' = rand(Z_q) \pmod{q}$ $\pmod{p}$

$G'' = (x'.g^{r''} = x'', t'' = Hash(g, h, b'', m), f'' = f' + r'')$ $\pmod{q}$

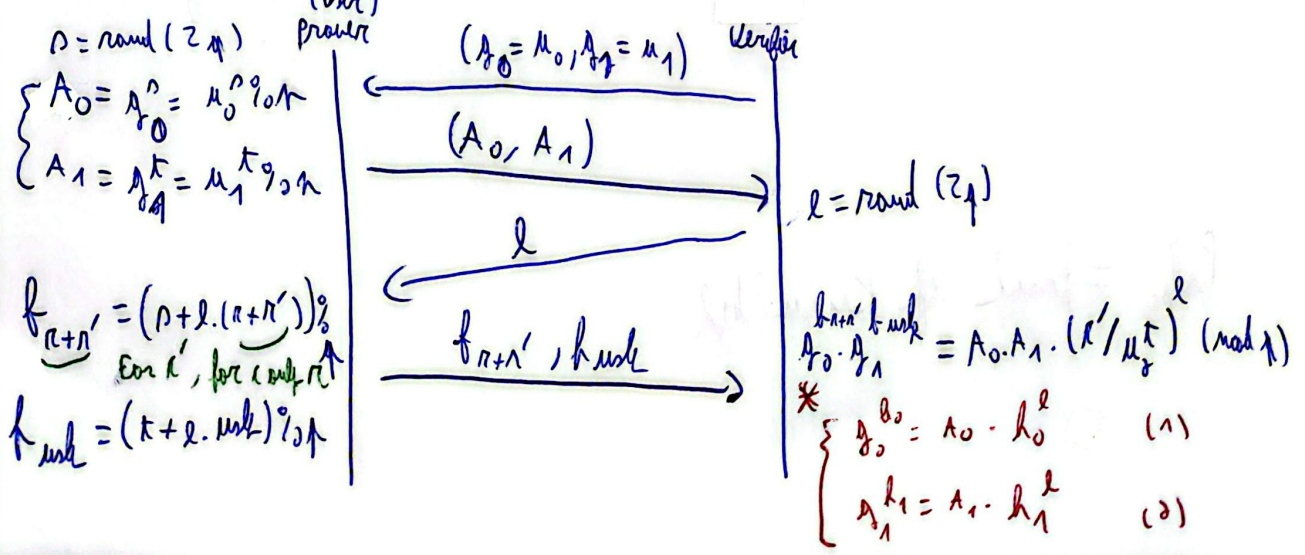
Q2)

1) The commitment c contains three informations, the user's token usk and the date of the creation of the commitment t.

$$c = u_0^r \cdot u_1^{usk} \cdot u_2^t \bmod n \quad | \quad r = rand(\mathbb{Z}_q) \wedge t = day \in \mathbb{Z}_q \wedge usk = secret \in \mathbb{Z}_q$$



2) To check if G is still valid uses a Chaum-Pedersen proof:



(Parallel Chaum-Pedersen) TP.4.3

2) make a Disjunctive proof to prove that a the commitment t is in a set $\{x, x-1, \ldots, x-d+1\}$.

A lot of $g_2 = u_1^{x-d_i}$ and $h_0 \cdot h_1 = x' / u_2^{x-d_i} = u_0^{r} \cdot u_1^{wk}$

3) $c_\Delta = \prod_{i=1}^{g} c_i^{2^i} = u_2^{x^*-x} u_0^{r}$

$$n = \sum_{i=1}^{g} 2^i \cdot n_i \; ; \; x^*-x = \sum_{i=1}^{g} 2^i \cdot b_i \;\Big|\; b_i \in \{0;1\}$$

$n = 0x'n_9 n_8 n_7 n_6 n_5 n_4 n_3 n_2 n_1 0'$; $x^*-x = 0x' b_9 b_8 b_7 b_6 b_5 b_4 b_3 b_2 b_1 0'$

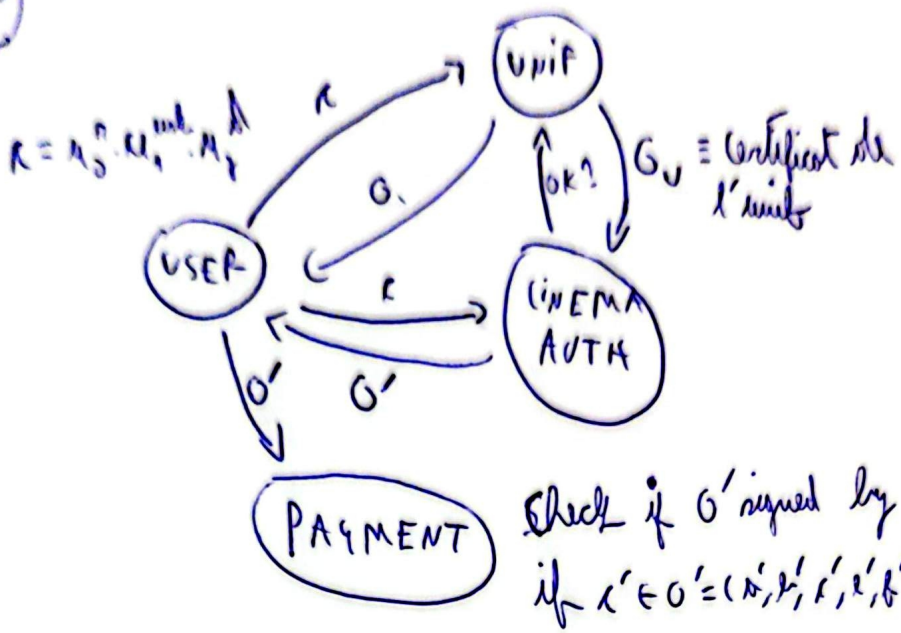
10 bits

Idea: at the place to check a set of values check a bit pattern using a Dez Disjunctive OR proof, it'll efficiently test a range of values in constant time.

Pok = Proof of Knowledge

TP 4.4

Q 3)



Check if σ' signed by cinema unit and if $x' \in \sigma' = (s', k', r', t', \beta')$ committed to σ'.

Check if $d = 1$: Chaum - Pedersen

If yes and $10000 \leq x \leq 0$ sum applicate discount.

D . D'