Voting

Voting

(Distributed) Key Generation

→ T_i : $x_i \xleftarrow{\$} \mathbb{Z}_q$, publish $h_i := g^{x_i}$

Public key is general (aggregation) :

$$pk = (G, q, g, h := \prod h_i = g^{\sum x_i})$$

Issue : if last T_t picks x and computes

$h_t := g^{x_t} = \frac{g^x}{\prod^{t-1} h_i}$ ⇒ $pk = \prod^t h_i = g^x$ so

T_t knows private key

Solution : T_i each prove NI-ZK proof that they have x ! Let $H(a)$ random fct (to simulate challenge)

Proof T_i : → $r_i \xleftarrow{\$} \mathbb{Z}_q$

→ Send $(a_i = g^{r_i}, e_i = H(g, h_i, a_i), f_i = r_i + e_i x_i)$

Verif (a_i, e_i, f_i) : 1) $H(g, h_i, a_i)$

2) $g^{f_i} = a_i h_i^{e_i}$

From this :

→ T_i has a part of the key x_i

→ Each voter can compute pk

→ T_i cannot cheat in key gen

Encryption

→ Each voter has $pk = (G, q, g, h = \prod h_i)$

→ Voter has $m \in \{0, 1\}$.

→ $Enc_{pk}(m)$:

one encryption/candidate/voter

1) $r \xleftarrow{\$} \mathbb{Z}_q$

2) Send $(c_1, c_2) = (g^r, g^m h^r)$

Issue : One could encrypt bad msg

Solution : Do a dysjonctive proof :

$V_i = (c_1, c_2)$ encrypts $m_0 = 0$ OR $m_1 = 1$

$= (g^r, g^m h^r)$

if $m = 0$: V_i must prove he has r st $\begin{cases} c_2 = h^r \\ g^r = c_1 \end{cases}$

$m = 1$: V_i must prove he has r st $\begin{cases} c_1 = g^r \\ c_2/g = h^r \end{cases}$

Chaum Pedersen

Idea : 2 proofs in //, one simulated the other one real. Only one challenge ⇒ challenge for real proof must be computed from $e - e_1$

Proof : if $v_i = Enc_{pk}(0)$:

1) P: runs simulation of CP protocol that v_i encr 1

⇒ has (a_1, e_1, f_1)

↳ is the CP pair

2) P : $s \xleftarrow{\$} \mathbb{Z}_p$ $a_0 = (g^s, h^s)$

3) P : sends (a_0, a_1) and get e

4) P : → $e_0 = e - e_1$

→ $f_0 = s + e_0 r$ → my secret r_i →

→ send (e_0, e_1), (f_0, f_1)

5) V checks :

→ $e = e_0 + e_1$

→ (a_0, e_0, f_0) is valid CP

→ (a_1, e_1, f_1) is valid CP

From this :

v_i has sent (c_1, c_2) his encrypted vote which IS either 0/1

Tally

We have many $Enc_{pk}(m_i) = (g^{r_i}, g^{m_i} h^{r_i})$

1) For each candidate : $\prod Enc_{pk}(m_i) = (g^{\sum r_i}, g^{\sum m_i} h^{\sum r_i}) = (C_1, C_2)$

2) Each T_i publishes decryption factor $d_i = c_1^{x_i} = (g^{r_i})^{x_i}$ *

and can compute $d = \prod d_i$

3) $(d, C) \rightarrow g^{\sum m_i} = \frac{g^{\sum m_i} g^{\sum r_i \cdot \sum r_i}}{d}$ which can be computed for small m (ok here I guess)

* Prove with CP that (NI I think)

They have x_i st $h_i = g^{x_i}$, $d = c_1^{x_i}$

Chaum Pederson

Proof x st $h_1 = g_1^x$, $h_2 = g_2^x$

P $\xrightarrow{(a_1, a_2) := (g_1^r, g_2^r)}$ V

$\xleftarrow{e}$

$\xrightarrow{f : r + ex \bmod (q)}$

V accepts if $\begin{cases} g_1^f = a_1 (h_1)^e \\ g_2^f = a_2 (h_2)^e \end{cases}$