(t, n) - Threshold ElGamal Encryption

- KeyGen $(1^\lambda, n, t)$; choose a large prime p and $g \xleftarrow{\$} \mathbb{Z}_p^*$.

  choose $a \xleftarrow{\$} \mathbb{Z}_p^*$ and compute $y = g^a$

  set $f(x) = a + \sum_{i=1}^{t-1} a_i x^i$ where $a_i \xleftarrow{\$} \mathbb{Z}_p^*$.

  distribute $f(x_i)$ to each player i. (not given to anyone.)

  output $pk = (p, g, y)$ and $sk_i = (f(x_i))$. $msk = (a)$.

- Enc(pk, m); choose a random $r \xleftarrow{\$} \mathbb{Z}_p^*$

  output $(g^r, m \cdot y^r)$

$$\ell_i(x) = \prod_{k \neq i} \frac{x - x_k}{x_i - x_k}$$

- Dec(sk_i, c); (partial decryption) parse c as (c_1, c_2).

  For each player i, compute $d_i = c_1^{s_i \ell_i(0)}$ where $\ell_i(x) = \begin{cases} 1 & \text{if } x = x_i \\ 0 & \text{if } x \neq x_i \end{cases}$

  (msg reconstruction) output $c_2 \cdot (\prod d_i)^{-1}$

$$\hookrightarrow \prod d_i = \prod g^{r s_i \ell_i(0)} = \prod g^{r f(x_i) \ell_i(0)}$$

$$= g^{r \sum f(x_i) \ell_i(0)}$$

$$= g^{r f(0)} = g^{ra}.$$

$$m \cdot y^r \cdot (g^{ra})^{-1} = m \cdot (g^a)^r \cdot (g^{ra})^{-1} = m$$

$$\hookrightarrow f(x) = \sum_{k=1}^{t} \left(y_k \cdot \prod_{j \neq k}^{n} \frac{-x_j}{x_k - x_j} \right)$$

Think thing