Notation

- $\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$ for a prime p
- A small letter except p means an element in $\mathbb{Z}_p^*$
- $g \leftarrow \mathbb{Z}_p^*$ denotes sampling from the unifrom distribution on $\mathbb{Z}_p^*$

ElGamal Encryption

ElGamal Encryption consists of $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$:

- $\mathsf{KeyGen}(1^\lambda)$;
  - Choose a large prime p and $g \leftarrow \mathbb{Z}_p^*$
  - Choose a secret key $s \leftarrow \mathbb{Z}_p^*$
  - Compute $y := g^s \mod p$
  - Output $pk := \{p, g, y\}$ and $sk := \{s\}$
- $\mathsf{Enc}(pk, m)$;
  - Choose a random $r \leftarrow \mathbb{Z}_p^*$
  - Compute $c_1 = g^r \mod p$
  - Compute $c_2 = m \cdot y^r \mod p$
  - Output $c := (c_1, c_2)$
- $\mathsf{Dec}(sk, c)$;
  - Parse c as (c_1, c_2)
  - Output $m := c_2 \cdot (c_1^s)^{-1}$

Moreover, ElGamal Encryption supports multiplications.

- $\mathsf{Mult}(c_1, c_2)$;
  - Parse c_1 as (c_{11}, c_{12}).
  - Parse c_2 as (c_{21}, c_{22}).
  - Output $c_{mult} := (c_{11} \cdot c_{21}, c_{12} \cdot c_{22})$

Correctness

- for decryption:
  - $c_2 \cdot (c_1^s)^{-1} = m \cdot y^r \cdot (g^r)^{-s} = m$
- for multiplication:
  - Let $\mathsf{Enc}(pk, m_1) = (c_{11}, c_{12}) = (g^{r_1}, m_1 \cdot y^{r_1})$
  - Let $\mathsf{Enc}(pk, m_2) = (c_{21}, c_{22}) = (g^{r_2}, m_2 \cdot y^{r_2})$
  - Then, $(c_{11} \cdot c_{21}, c_{12} \cdot c_{22}) = (g^{r_1+r_2}, m_1 m_2 \cdot y^{r_1+r_2})$

Distributed ElGamal Encryption

Distributed ElGamal Encryption consists of $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{PartDec}, \mathsf{Reconstruct})$:

- KeyGen(1^λ);
  - Choose a large prime p and $g \leftarrow \mathbb{Z}_p^*$
  - For each player i,
    - choose a secret key $s_i \leftarrow \mathbb{Z}_p^*$
    - compute $y_i := g^{s_i} \mod p$
      - along with zero-knowledge proof
      - Proof of Knowledge of DL of y_i
    - Output $pk_i := \{p, g, y_i\}$ and $sk_i := \{s_i\}$
- Enc($\{pk_i\}, m$);
  - From $\{pk_i\}$, compute $y := \prod y_i$ for all i.
  - Choose a random $r \leftarrow \mathbb{Z}_p^*$
  - Compute $c_1 = g^r \mod p$
  - Compute $c_2 = m \cdot y^r \mod p$
  - Output $c := (c_1, c_2)$
- PartDec(sk_i, c);
  - Parse c as (c_1, c_2)
  - Output $m_i := c_1^{s_i}$
    - along with zero-knowledge proof
    - Proof of Equality of DL for y_i and m_i
- Reconstruct($\{m_i\}, c$);
  - parse c as (c_1, c_2)
  - Compute $d := \prod m_i$
  - Output $m := c_2 \cdot d^{-1}$

Correctness

- $d = \prod m_i = \prod c_1^{s_i} = g^{r \sum s_i}$
- Let $s = \sum s_i$
- $c_2 \cdot d^{-1} = m \cdot y^r \cdot (g^{rs})^{-1} = m \cdot (\prod y_i)^r \cdot (g^{rs})^{-1} = m \cdot (\prod g^{s_i})^r \cdot (g^{rs})^{-1} = m \cdot (g^s)^r \cdot (g^{rs})^{-1} = m$

Remark

- To multiply two ciphertexts, the underlying public key should be the same.
- Every player who has a secret key should take part in the decryption phase.

(t, n)-Threshold ElGamal Encryption

Threshold ElGamal Encryption consists of (KeyGen, Enc, PartDec, Reconstruct):

- KeyGen(1^λ, t, n);
  - Choose a large prime p and $g \leftarrow \mathbb{Z}_p^*$

- Choose a secret $a \leftarrow \mathbb{Z}_p^*$ and compute $y = g^a$
- Set a random polynomial $f(x)$ of degree $t-1$
  - $f(x) = a + \sum_{i=1}^{t-1} a_i x^i$ where $a_i \leftarrow \mathbb{Z}_p^*$ for all i
- Distribute $(x_i, f(x_i))$ to each player i.
- Output $pk := (p, g, y)$ and $sk_i = (f(x_i))$
- $msk := (a)$, however, it is not given to anyone.

- Enc(pk, m);
  - Choose a random $r \leftarrow \mathbb{Z}_p^*$
  - Output $c := (g^r, m \cdot y^r)$
- PartDec(sk_i, c);
  - Parse c as (c_1, c_2)
  - Output $m_i := c_1^{s_i \ell_i(0)}$ where $s_i = f(x_i)$ and $\ell_i(x) = \prod_{k=1, k\neq i}^{n} \frac{x - x_k}{x_i - x_k}$
    - $f(x) = f(x_1)\ell_1(x) + f(x_2)\ell_2(x) + \cdots + f(x_n)\ell_n(x)$
    - $a = f(0) = f(x_1)\ell_1(0) + f(x_2)\ell_2(0) + \cdots + f(x_n)\ell_n(0)$
- Reconstruct$(\{m_i\}, c)$;
  - parse c as (c_1, c_2)
  - Compute $d := \prod m_i$
  - Output $m := c_2 \cdot d^{-1}$

Correctness

- $d = \prod m_i = \prod c_1^{s_i \ell_i(0)} = c_1^{\sum f(x_i)\ell_i(0)} = c_1^a$
- $c_2 \cdot d^{-1} = m \cdot y^r \cdot (g^r)^a = m$