· ElG.KG, ElG.Enc, ElG.Dec /* Threshold version */

· ElG.KG(n, λ) /* n: 사용자의 수, λ: prime p의 길이 */

U_1 수행

1. choose a random prime p of λ-bit length such that $p = 2q + 1$ for some prime q
2. Find a generator g of order q
3. Share (p, q, g) with all users
4. Each user U_i chooses a random $x_i \in \{2, \cdots, q-2\}$
5. computes $y_i \leftarrow g^{x_i} \bmod p$
6. sends y_i to all other users
7. After receiving $(y_1, \cdots, y_n)$, compute $y \leftarrow \prod_{i=1}^{n} y_i \bmod p$
8. Set the public key $pk = (p, q, g, y)$ and

the secret key $sk = (p, q, g, \underbrace{x = x_1 + \cdots + x_n}_{\text{실제로 } U_1, \cdots, U_n \text{은 누구도 모름}})$

· ElG.Enc(pk, m)

1. choose a random $r \in \{2, \cdots, q-2\}$
2. Compute a ciphertext $c = (u, v)$ where

$u \leftarrow g^r \bmod p$

$v \leftarrow m \cdot y^r \bmod p$

· ElG.Dec(sk_i, c) ← $U_1, \cdots, U_n$ 중 하나가 암호문 (u, v)를 decrypt 해야 하는 상황에서 시작

1. Each user U_i computes $z_i \leftarrow u^{-x_i} \bmod p$ and sends z_i to all other users.

((u, v)를 받은 사용자가 $U_1, \cdots U_n$ 에게 z_i의 계산을 요청해야 함)

2. After receiving $(z_1, \cdots, z_n)$, computes $v \cdot \left(\prod_{i=1}^{n} z_i\right)$

(2)에서 이 값은 위에 있는 (u, v)의 v임.

$= m \cdot y^r \cdot z_1 \cdots z_n = m \cdot y_1^r \cdots y_n^r z_1 \cdots z_n$

$= m \cdot g^{x_1 r} \cdots g^{x_n r} g^{-r x_1} \cdots g^{-r x_n}$

$= m$

실방학 protocol

- 사용자 : 3명 (U_1, U_2, U_3)
- 각 사용자의 message : m_1, m_2, m_3
- Message encryption의 setup :
  1. ElG.KG(λ, 2048)을 수행하여 $pk=(p, g, g)$를 먼저 공개하고
     - i. U_1은 $x_1 \in \{0, \dots, g-2\}$ 선택후 $y_1 \leftarrow g^{x_1} \bmod p$
     - ii. U_2 : $x_2 \in \{0, \dots, g-2\}$ & $y_2 \leftarrow g^{x_2} \bmod p$
     - iii. U_3 : x_3 선택하고 $y_3 \leftarrow g^{x_3} \bmod p$

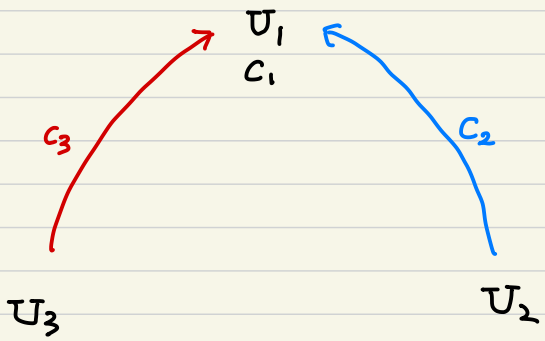
) 각자 계산후
  2. 각자의 y_i를 다른 모든 사용자에게 send
  3. y_1, y_2, y_3를 receive 한 후, $y \leftarrow y_1 \cdot y_2 \cdot y_3 \bmod p$
  4. 각자의 $pk=(p, g, g, y)$이며 $sk_i=(p, g, g, x_i)$이다.

- **step1.**
  1. 각 사용자 U_i는 m_i를 c_i로 encrypt :

     (U_i의 random)

     $$c_i \leftarrow \text{ElG.Enc}(pk, m_i) = (u_i, v_i) = (g^{s_i} \bmod p,\ m \cdot y^{s_i} \bmod p)$$

  2. 각 사용자 U_i는 사용자 U_2에게 c_i를 전송.



Step#2

1. 사용자 U_1은 (C_1, C_2, C_3)를 준비.
2. 사용자 U_1은 3개의 random values $r_i \in \{2, \cdots, g-2\}$ 선택
3. U_1은 각 $c_i = (u_i, v_i)$에 대해서 /* c_i는 3개 */
   i. Compute $\bar{u}_i \leftarrow u_i \cdot g^{r_i} \bmod p$
   ii. Compute $\bar{v}_i \leftarrow v_i \cdot y^{r_i} \bmod p$
   iii Set $\bar{c}_i = (\bar{u}_i, \bar{v}_i)$
4. $(\bar{c}_1, \bar{c}_2, \bar{c}_3)$를 각 $\bar{u}_i$의 크기에 의해 sort하여 $(\tilde{c}_1, \tilde{c}_2, \tilde{c}_3)$로 설정
   ← sort한뒤에 (u_i, v_i)는 함께 이동.
5. U_1이 $(\tilde{c}_1, \tilde{c}_2, \tilde{c}_3)$를 U_2에게 send

Step#3

$(C_1, C_2, C_3) = (\tilde{C}_1, \tilde{C}_2, \tilde{C}_3)$ of U_1

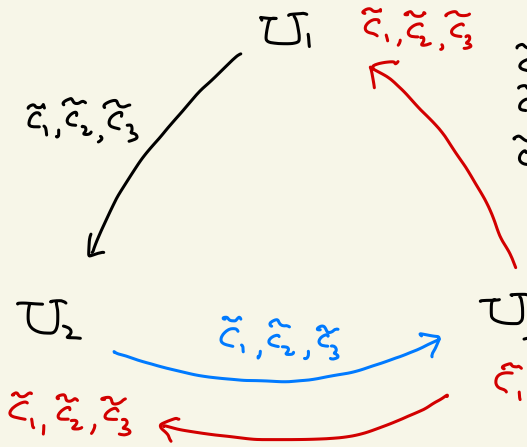
1. 사용자 U_2는 U_1에게 (C_1, C_2, C_3)를 수신하여 준비
2. U_2는 3개의 random values $r_i \in \{2, \cdots, g-2\}$ 선택
3. U_2는 각 $c_i = (u_i, v_i)$에 대해서
   i. Compute $\bar{u}_i \leftarrow u_i \cdot g^{r_i} \bmod p$
   ii. Compute $\bar{v}_i \leftarrow v_i \cdot y^{r_i} \bmod p$
   iii Set $\bar{c}_i = (\bar{u}_i, \bar{v}_i)$
4. $(\bar{c}_1, \bar{c}_2, \bar{c}_3)$를 각 $\bar{u}_i$의 크기에 의해 sort하여 $(\tilde{c}_1, \tilde{c}_2, \tilde{c}_3)$로 설정
   ← sort한뒤에 (u_i, v_i)는 함께 이동.
5. U_2는 $(\tilde{c}_1, \tilde{c}_2, \tilde{c}_3)$를 U_3에게 send

Step#4

$(C_1, C_2, C_3) = (\tilde{c}_1, \tilde{c}_2, \tilde{c}_3)$ of U_2

1. 사용자 U_3는 U_2에게 (C_1, C_2, C_3)를 수신하여 준비
2. U_3은 random values 3개 r_1, r_2, r_3를 선택한다
3. Step#2 & Step#3의 line 3처럼 c_i를 $\bar{c}_i$로 update
4. $(\tilde{c}_1, \tilde{c}_2, \tilde{c}_3)$를 U_1, U_2에게 send

Step#4 까지 완료



$\tilde{c}_1 = (\bar{u}_1, \bar{v}_1) = (g^{s_1+r_1}, m_1 y^{s_1} y^{r_1})$

$\tilde{c}_2 = (\bar{u}_2, \bar{v}_2) = (g^{s_2+r_2}, m_2 \cdot y^{s_2} \cdot y^{r_2})$

$\tilde{c}_3 = (\bar{u}_3, \bar{v}_3) = (g^{s_3+r_3}, m_3 \cdot y^{s_3} \cdot y^{r_3})$

$\tilde{c}_1 = (\bar{u}_1, \bar{v}_1) = (g^{s_1+r_1+r_1}, m_1 y^{s_1} y^{r_1} y^{r_1} y^{r_1})$

$\tilde{c}_2 = (\bar{u}_2, \bar{v}_2) = (g^{s_2+r_2+r_2+r_2}, m_2 y^{s_2} y^{r_2} y^{r_2} y^{r_2})$

$\tilde{c}_3 = (\bar{u}_3, \bar{v}_3) = (g^{s_3+r_3+r_3+r_3}, m_3 \cdot y^{s_3} y^{r_3} y^{r_3} y^{r_3})$

$\tilde{c}_1 = (\bar{u}_1, \bar{v}_1) = (g^{s_1+r_1+r_1}, m_1 y^{s_1} y^{r_1} y^{r_1})$

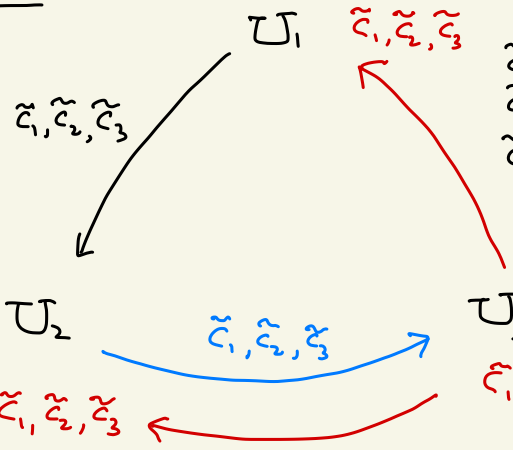
$\tilde{c}_2 = (\bar{u}_2, \bar{v}_2) = (g^{s_2+r_2+r_2}, m_2 y^{s_2} y^{r_2} y^{r_2})$

$\tilde{c}_3 = (\bar{u}_3, \bar{v}_3) = (g^{s_3+r_3+r_3}, m_3 y^{s_3} y^{r_3} y^{r_3})$

Step#5

1. 사용자 U_1은 receive한 $(\tilde{C}_1, \tilde{C}_2, \tilde{C}_3)$에 대해서,
   - i. $\tilde{C}_1 = (\tilde{u}_1, \tilde{v}_1)$에 대해서
     - Compute $z_1 \leftarrow (\tilde{u}_1)^{-x_1} \mod p$
     - Compute $\omega_1 \leftarrow \tilde{v}_1 \cdot z_1 \mod p$
     - Set $d_1 = (z_1, \omega_1)$
   - ii. $\tilde{C}_2 = (\tilde{u}_2, \tilde{v}_2)$에 대해서
     - Compute $z_2 \leftarrow (\tilde{u}_2)^{-x_1} \mod p$
     - Compute $\omega_2 \leftarrow \tilde{v}_2 \cdot z_2 \mod p$
     - Set $d_2 = (z_2, \omega_2)$
   - iii. $\tilde{C}_3 = (\tilde{u}_3, \tilde{v}_3)$에 대해서
     - Compute $z_3 \leftarrow (\tilde{u}_3)^{-x_1} \mod p$
     - Compute $\omega_3 \leftarrow \tilde{v}_3 \cdot z_3 \mod p$
     - Set $d_3 = (z_3, \omega_3)$
2. 사용자 U_1은 U_2, U_3에게
   - i. $z_1 \leftarrow (\tilde{u}_1)^{-x_2} \mod p$, /* U_2에게 */
     $z_1 \leftarrow (\tilde{u}_1)^{-x_3} \mod p$ /* U_3에게 */
     각각 계산을 요청하셔서 수신
   - ii. 비슷하게 z_2, z_2'를 U_2, U_3에게 각각 받고
   - iii. z_3, z_3'도 U_2, U_3에게 receive

Step4까지 완료



$\tilde{c}_1 = (\tilde{u}_1, \tilde{v}_1) = (g^{s_1+r_1}, m_1 y^{s_1} y^{r_1})$
$\tilde{c}_2 = (\tilde{u}_2, \tilde{v}_2) = (g^{s_2+r_2}, m_2 \cdot y^{s_2} \cdot y^{r_2})$
$\tilde{c}_3 = (\tilde{u}_3, \tilde{v}_3) = (g^{s_3+r_3}, m_3 \cdot y^{s_3} \cdot y^{r_3})$

$\tilde{c}_1 = (\tilde{u}_1, \tilde{v}_1) = (g^{s_1+r_1+r_1}, m_1 y^{s_1} y^{r_1} y^{r_1} y^{r_1})$

$\tilde{c}_2 = (\tilde{u}_2, \tilde{v}_2) = (g^{s_2+r_2+r_2+r_2}, m_2 y^{s_2} y^{r_2} y^{r_2} y^{r_2})$

$\tilde{c}_3 = (\tilde{u}_3, \tilde{v}_3) = (g^{s_3+r_3+r_3+r_3}, m_3 \cdot y^{s_3} y^{r_3} y^{r_3} y^{r_3})$

① U1이 $\tilde{c}_1, \tilde{c}_2, \tilde{c}_3$ decrypt 해서 U2, U3 에게 (z_1, z_2, z_3) 전송

$z_1 = \tilde{u}_1^{-x_1} = (g^{s_1+r_1+r_1})^{-x_1} = g^{-x_1(s_1+r_1+r_1+s_1)}$

$w_1 = \tilde{v}_1 \cdot z_1 = m_1 y^{s_1} y^{r_1} y^{r_1} y^{r_1} g^{-x_1(s_1+r_1+r_1+s_1)}$

$z_2 = \tilde{u}_2^{-x_1} = (g^{s_2+r_2+r_2+r_2})^{-x} = g^{-x_1(s_2+r_2+r_2+r_2)}$

$w_2 = \tilde{v}_1 z_2 = m_2 y^{s_2} y^{r_2} y^{r_2} y^{r_2} g^{-x_1(s_2+r_2+r_2+r_2)}$

$z_3 = \tilde{u}^{-x_1} = (g^{s_3+r_3+r_3+r_3})^{-x_1} = g^{-x_1(s_3+r_3+r_3+r_3)}$

$w_3 = \tilde{v} z_3 = m_3 y^{s_3} y^{r_3} y^{r_3} y^{r_3} \cdot g^{-x(s_3+r_3+r_3+r_3)}$

② U_1은 U_2, U_3에게 $\tilde{c}_1, \tilde{c}_2, \tilde{c}_3$에 대한 각각의 decryption을 receive하도록, 아래 처럼

① U_2에게 (z_1, z_2, z_3) receive

$$z_1 = \tilde{u}_1^{-x_2} = \left(g^{s_1+r_1+r_1+r_1}\right)^{-x_2} = g^{-x_2(s_1+r_1+r_1+r_1)}$$

$$z_2 = \tilde{u}_2^{-x_2} = \left(g^{s_2+r_2+r_2+r_2}\right)^{-x_2} = g^{-x_2(s_2+r_2+r_2+r_2)}$$

$$z_3 = \tilde{u}_3^{-x_2} = \left(g^{s_3+r_3+r_3+r_3}\right)^{-x_2} = g^{-x_2(s_3+r_3+r_3+r_3)}$$

① U_3에게 (z_1, z_2, z_3) receive

$$z_1 = \tilde{u}_1^{-x_3} = \left(g^{s_1+r_1+r_1+r_1}\right)^{-x_3} = g^{-x_3(s_1+r_1+r_1+r_1)}$$

$$z_2 = \tilde{u}_2^{-x_3} = \left(g^{s_2+r_2+r_2+r_2}\right)^{-x_3} = g^{-x_3(s_2+r_2+r_2+r_2)}$$

$$z_3 = \tilde{u}_3^{-x_3} = \left(g^{s_3+r_3+r_3+r_3}\right)^{-x_3} = g^{-x_3(s_3+r_3+r_3+r_3)}$$

Step#7

1. U_2는 U_1, U_3에게

i. $z_1 \leftarrow (\tilde{u}_1)^{-x_1} \bmod p$, /* U_1에게 */

$z_1 \leftarrow (\tilde{u}_1)^{-x_3} \bmod p$ /* U_3에게 */

ii. 유사하게 z_2, z_2를 U_1, U_3 에게 receive

iii. z_3, z_3를 U_1, U_3에게 receive

Step#8

1. U_3는 U_1, U_2에게

i. $z_1 \leftarrow (\tilde{u}_1)^{-x_1} \bmod p$, /* U_1에게 */

$z_1 \leftarrow (\tilde{u}_1)^{-x_2} \bmod p$ /* U_2에게 */

ii. z_2, z_2
iii. z_3, z_3) 비슷하게 U_1, U_2에게 receive

Step#9

1. 각 사용자는 각자.

i. $m_1 \leftarrow \tilde{v}_1 \cdot z_1 \cdot z_1 \cdot z_1$

$= (m_1 \cdot y^{s_1}) \cdot y_1^{r_1} \cdot y_2^{r_2} \cdot y_3^{r_3} \cdot (\tilde{u}_1)^{-x_1} (\tilde{u}_1)^{-x_2} (\tilde{u}_1)^{-x_3}$

$= (m_1 \cdot y^{s_1}) g^{x_1 r_1 + x_2 r_2 + x_3 r_3} \cdot (g^{s_1} \cdot g^{r_1})^{-x_1} (g^{s_1} \cdot g^{r_2})^{-x_2} (g^{s_1} \cdot g^{-r_3})^{x_3}$

$= (m_1 \cdot y^{s_1}) g^{x_1 r_1 + x_2 r_2 + x_3 r_3} \cdot g^{-s_1 x_1 - s_1 x_2 - s_1 x_3 - r_1 x_1 - r_2 x_2 - r_3 x_3}$

$= m_1 \cdot g^{x s_1} \cdot g^{-s_1 (x_1 + x_2 + x_3)} = m \cdot g^{x s_1} \cdot g^{-s_1 x}$

$= m_1$

m_1의 msg가 아니라 random 값이 됨

Step #9 완료

CT_1은 (z_1, z_2, z_3) & (z_1, z_2, z_3)를 받아서

① $w_1 \cdot z_1 \cdot z_1$

$= (\tilde{v}_1 \cdot z_1) z_1 z_1$

$= m_1 y^{s_1} y^{r_1} y^{r_1} y^{r_1} g^{-\alpha_1(s_1+r_1+r_1+s_1)} g^{-\alpha_2(s_1+r_1+r_1+r_1)} g^{-\alpha_3(s_1+r_1+r_1+r_1)}$

$= m_1 y^{s_1+r_1+r_1+r_1} g^{-s_1(\alpha_1+\alpha_2+\alpha_3)-r_1(\alpha_1+\alpha_2+\alpha_3)-r_1(\alpha_1+\alpha_2+\alpha_3)-r_1(\alpha_1+\alpha_2+\alpha_3)}$

$= m_1 y^{s_1+r_1+r_1+r_1} g^{-s_1 x - r_1 x - r_1 x - r_1 x}$

$x = (\alpha_1+\alpha_2+\alpha_3)$

$= m_1 y^{s_1+r_1+r_1+r_1} g^{x(-s_1-r_1-r_1-r_1)} = m_1 y^{s_1+r_1+r_1+r_1} y^{-(s_1+r_1+r_1+r_1)}$

$y = g^x$

$= m_1$

(*) m_2, m_3도 동일하게 계산해서 decrypt

(**) CT_2는 (z_1, z_2, z_3) & (z_1, z_2, z_3) 받아서 decrypt.

(***) CT_3는 (z_1, z_2, z_3) & (z_1, z_2, z_3) 받아서 decrypt.