Additive homomorphic encryption which supports one-time multiplication

Mitsunari Shigeo

July 20, 2016

1 Lifted ElGamal Encryption

Let G be an additive cyclic group generated by P and let $r := |G|$ be a prime.

- KeyGen: Take a random number $x \in \mathbb{Z}/p\mathbb{Z}$ and compute xP. x is a secret key and xP is a public key.
- Encrypt: For a message $m \in \mathbb{Z}/p\mathbb{Z}$, take a random number r and

$$\mathrm{Enc}(m) := (S, T) := (mP + r(xP), rP).$$

- Decrypt: For a ciphertext $c := (S, T)$, compute

$$S - xT = (mP + rxP) - x(rP) = mP$$

and find m by computing the discrete log of mP base P.

We can not take a large plaintext m because we should solve this DLP. We use a notation of $m = \log_P(mP)$.

2 Additive homomorphic encryption

Lifted ElGamal encryption is additively homomorphic as the following:
For two plaintext m_1 and m_2, define

$$c_i := \mathrm{Enc}(m_i) = (S_i, T_i) = (m_i P + r_i(xP), r_i P)$$

where r_i is a random number. Let

$$\mathrm{Add}(c_1, c_2) := (S_1 + S_2, T_1 + T_2).$$

Then, we get

$$\mathrm{Add}(c_1, c_2) = ((m_1 + m_2)P + (r_1 + r_2)xP, (r_1 + r_2)P) = \mathrm{Enc}(m_1 + m_2).$$

3 Pairing

Let G_1 and G_2 be additive cyclic groups generated by P_1 and P_2, and G_T be an multiplicative cyclic group of order r and take a pairing

$$e : G_1 \times G_2 \to G_T.$$

For any $a, b \in \mathbb{Z}/p\mathbb{Z}$, $e(aP_1, bP_2) = e(P_1, P_2)^{ab}$. Let $g := e(P_1, P_2)$.

4 Multiplicative homomorphic encryption

Let x_i be a secret key of an lifted ElGamal encryption for G_i and $\mathrm{Enc}_i(m_i)$ be a ciphertext for m_i according to G_i. We define multiplication of $\mathrm{Enc}_1(m_1)$ and $\mathrm{Enc}_2(m_2)$ as the following:

Let $c_i := \mathrm{Enc}_i(m_i) = (S_i, T_i)$ where $S_i, T_i \in G_i$.

$$\mathrm{Mul}(c_1, c_2) := (s, t, u, v) := (e(S_1, S_2), e(S_1, T_2), e(T_1, S_2), e(T_1, T_2)) \in {G_T}^4.$$

Decrypt of $\mathrm{Mul}(c_1, c_2) := (s, t, u, v)$ is as the following:

$$\begin{aligned} sv^{x_1x_2}/(t^{x_2}u^{x_1}) &= e(S_1, S_2)e(T_1, T_2)^{x_1x_2}/e(S_1, T_2)^{x_2}/e(T_1, S_2)^{x_1} \\ &= e(S_1, S_2)e(x_1T_1, x_2T_2)e(S_1, -x_2T_2)e(-x_1T_1, S_2) \\ &= e(S_1 - x_1T_1, S_2 - x_2T_2) \\ &= e(m_1P_1, m_2P_2) = e(P_1, P_2)^{m_1m_2} = g^{m_1m_2}. \end{aligned}$$

Then we solve a DLP of $\log_g(g^{m_1m_2})$ and get m_1m_2.

So define $Enc(m) := (Enc_1(m), Enc_2(m)) \in {G_1}^2 \times {G_2}^2$, then we get additive homomorphic encryption which supports one multiplication.