Paillier 暗号

(1) 準備

Paillier 暗号は，次のような性質を利用している．$n \in \mathbb{N}^+$ のとき，二項定理より，

$$(1+x)^n = \sum_{j=0}^{n} {}_n\mathrm{C}_j x^j \equiv 1 + nx. \pmod{n^2} \tag{1}$$

そこで，$y := (1+x)^n$ とすると，$x = (y-1)/n \pmod{n^2}$ である．ここで，関数 $L(x)$ を次のように定義する．

$$L(x) := \frac{x-1}{n}. \tag{2}$$

この関数は，後で Paillier 暗号の復号の際に使う．

$$L(y \pmod{n^2}) = \frac{y \pmod{n^2} - 1}{n} \pmod{n} \equiv \frac{(1+nx)-1}{n} = x. \tag{3}$$

(2) 鍵生成

- $\gcd(pq, (p-1)(q-1)) = 1$ を満たす大きな素数 p, q を選ぶ．
- 公開鍵 $\boldsymbol{pk}$ は，$n \leftarrow pq,\ g \leftarrow (1+\alpha n)\beta^n$ である．ただし，$\forall\alpha, \forall\beta \in \mathbb{Z}_{n^2}^*$ である．
- 秘密鍵 $\boldsymbol{sk}$ は，$\lambda \leftarrow \mathrm{lcm}(p-1, q-1)$ である．

(3) 暗号化アルゴリズム

公開鍵 $\boldsymbol{pk}$ と $\gcd(r,n) = 1$ を満たす乱数 $r \in \mathbb{Z}_{n^2}^*$ を用いて，次のようにメッセージ $m \in \mathbb{Z}_n$ を暗号化する．つまり，c を暗号文，E を暗号化関数とすると，

$$c = E(m, r) := g^m r^n. \pmod{n^2} \tag{4}$$

(4) 復号化アルゴリズム

秘密鍵 $\boldsymbol{sk}$ と (3) の関数 L を用いて復号する．

$$\frac{L(c^\lambda \pmod{n^2})}{L(g^\lambda \pmod{n^2})} = m. \pmod{n} \tag{5}$$

(6) を計算するために，まず $r^{\lambda n} \equiv 1 \pmod{n^2}$ を示す必要がある．

補題 1　$\gcd(r,n) = 1$ を満たす $r \in \mathbb{Z}_{n^2}^*$ について $r^{\lambda n} \equiv 1 \pmod{n^2}$ が成り立つ．

proof. Euler の整関数より $\varphi(n^2) = n(p-1)(q-1)$ であり，$\gcd(pq, (p-1)(q-1)) = 1$ なので，原始根定理より $\mathbb{Z}_{n^2}^*$ には，位数 n と位数 $(p-1)(q-1)$ の部分群が存在する．したがって，$\gcd(r,n) = 1$ を満たす $r \in \mathbb{Z}_{n^2}^*$ について， Euler の定理の精密化[*1]より，

$$r^\lambda \equiv 1. \pmod{n} \tag{6}$$

つまり，ある整数 Q を用いて $r^\lambda := 1 + nQ$ と表すことができる．よって，

$$r^{\lambda n} = (1+nQ)^n = 1 + n^2(Q + \cdots) \equiv 1. \pmod{n^2} \tag{7}$$

以上より，補題 1 は示された．■

補題 1 を用いて，$L(c^\lambda \pmod{n^2})$ を具体的に計算すると，$\gcd(\alpha, n) = 1, \gcd(\beta, n) = 1$ なので，

$$\begin{aligned} L(c^\lambda \pmod{n^2}) &= L(g^{m\lambda} \cdot r^{\lambda n} \pmod{n^2}) = L(g^{m\lambda} \pmod{n^2}) \\ &= \frac{(1+\alpha n)^{m\lambda}\beta^{nm\lambda} \pmod{n^2} - 1}{n} \\ &\equiv \frac{(1+\alpha nm\lambda)-1}{n} = \alpha m\lambda. \pmod{n} \end{aligned} \tag{8}$$

以上 (6),(9) より，

$$\frac{L(c^\lambda \pmod{n^2})}{L(g^\lambda \pmod{n^2})} = \alpha m\lambda \cdot (\alpha\lambda)^{-1} = m. \pmod{n} \tag{9}$$

[*1] Refined Euler's Theorem

(5) 暗号化関数の準同型性

Paillier 暗号化関数 E は準同型写像である．乱数 $r_1, r_2 \in \mathbb{Z}_n^*$ とメッセージ $m_1, m_2 \in \mathbb{Z}_n$ を暗号化した暗号文 $E(m_1, r_1), E(m_2, r_2)$ の積を考える．

$$\begin{aligned} E(m_1, r_1) \times E(m_2, r_2) &= g^{m_1} r_1^n \times g^{m_2} r_2^n \\ &= g^{m_1+m_2} (r_1 r_2)^n \\ &= E(m_1 + m_2, r_1 r_2). \pmod{n^2} \end{aligned} \tag{10}$$

したがって，メッセージ $m \in \mathbb{Z}_n$ のスカラー倍は次のように表すことができる．$N \in \mathbb{Z}_n$ において，

$$\begin{aligned} \prod_{i=1}^{N} E(m, r_i) &= E(m, r_1) \times E(m, r_2) \times \cdots \times E(m, r_N) \\ &= (g^m)^N \times \prod_{i=1}^{N} r_i = E(N \times m, r_1 r_2 \cdots r_N). \pmod{n^2} \end{aligned} \tag{11}$$

(11),(12) のように暗号化したまま平文の和やスカラー倍を求められる性質を加法準同型性と呼ぶ．