Cifrado Homomorfico

Cuando un tercero tiene que operar con nuestros datos y no queremos que los vea, se aplica cifrado homomorfico, que permite realizar operaciones sobre datos cifrados.

A la hora de operar con cifrado homomorfico se usan los siguientes componentes:

- **n** → Tamaño de los vectores
- **q** → Valor del módulo (módulo q)
  - Trabajamos con módulos en potencias de 2 (2^x)
- **e** → Error
  - Dsitribución normal N(0,γ*q) → r = γ*q
    - Media 0
    - Valor relacionado con q
    - El valor debe estar redondeado
    - Valor entre 0 y q
- **a** → Vector de soporte
  - Vector de tamaño n con valores entre 0 y q-1
- **S** → Secreto o clave privada
  - Solo la conoce el dueño de los datos a operar
  - Valores aleatorios del conjunto {-1,0,1}

Sabiendo esto, sabemos que la clave pública (a,b) del cifrado homomorfico es:

$$(a,b = S^T*a+e \ $ \MOD q) \in Z^n_q * Z_q$$

Esta fórmula es solo la clave pública, si queremos proceder a realizar el cifrado utilizando esta, debemos introducir otros 2 elementos:

- **m** → Mensaje a Cifrar
- **Δ** → Constante (Normalmente su valor es una potencia de 2)

El cifrado homomórfico se vería de la siguiente forma:

$$(a,b = S^T*a+e+Δ*m \ $ \MOD q)$$

- Clave pública → S^T*a+e
- Texto Cifrado → $b = S^T*a+e+Δ*m \ $ \MOD q$
- **OJO**: a y b son necesarios para poder descrifrar el mensaje

Cuando se mandan datos a un tercero para operar con ellos, se madan a y b

$$Δ*m+e = b+S^T*a$$

- $m' = Δ*m+e$ → Mensaje aproximado con error

$$m+e = (b+S^T*a)/Δ \ MOD\ q$$

- $m' = m+e$

$$m = ||(b+S^T*a)/Δ - e \ MOD\ q||$$

- Redondeamos el resultado para el descifrado
- Si todo va bien, al realizar el redondeo desaparece el error aplicado y el valor final obtenido es el mensaje inicial.

Ejemplo de Cifrado Homomórfico

DATOS

$n = 2$

$q = 4 = 2^2$

$Δ = 1 = 2^0$

$e = 0$ (no hay error)

$S = \begin{pmatrix}1\\0\end{pmatrix}$

$a = \begin{pmatrix}2\\3\end{pmatrix}$

$m = 1$

Cifrado

$(a = \begin{pmatrix}2\\3\end{pmatrix}, b = S^T * a + e + Δ*m) \bmod q$

$b = (1\ 0) * \begin{pmatrix}2\\3\end{pmatrix} + 0 + 1*1$

$b = 2 + 0 + 0 + 1*1 = 3$

$\boxed{b = 3}$

Descifrado

$(a = \begin{pmatrix}2\\3\end{pmatrix}, b = 3)$

$$m' = \frac{b - S^T * a - e}{Δ} \bmod q$$

$$m' = \frac{3 - (1\ 0) * \begin{pmatrix}2\\3\end{pmatrix} - 0}{1} \bmod 4$$

$$m' = \frac{3 - 2}{1} \bmod 4$$

$\boxed{m = 1}$

Sumas sobre cifrado Homomórfico

Ejemplo de suma con cifrado homomórfico

Datos

$n = 2$
$q = 4 = 2^2$
$Δ = 1 = 2^0$
$e = 0$
$S = \begin{pmatrix}1\\0\end{pmatrix}$
$m_1 = 1$
$m_2 = 2$
$a_1 = \begin{pmatrix}2\\3\end{pmatrix}$
$a_2 = \begin{pmatrix}3\\2\end{pmatrix}$

$(a_1, b_1 = S^T * a_1 + e_1 + Δ * m_1 \ MOD q)$

$(a_2, b_2 = S^T * a_2 + e_2 + Δ * m_2 \ MOD q)$

$$m1 = \frac{b_1 - S^T * a_1 - e_1}{Δ}$$

$$m2 = \frac{b_2 - S^T * a_2 - e_2}{Δ}$$

$$m1 + m2 = \frac{b_1 - S^T * a_1 - e_1}{Δ} + \frac{b_2 - S^T * a_2 - e_2}{Δ} =$$

$$= \frac{b_+ - S^T * \boxed{a_+} - \boxed{e_+}}{Δ} \bmod q$$

$(a_1 = \begin{pmatrix}2\\3\end{pmatrix}, b_1 = 3)$

$(a_2 = \begin{pmatrix}3\\2\end{pmatrix}, b_2 = 1)$

$m1 + m2 = (a_+ = a_1 + a_2,\ b_+ = b_1 + b_2) \bmod q =$

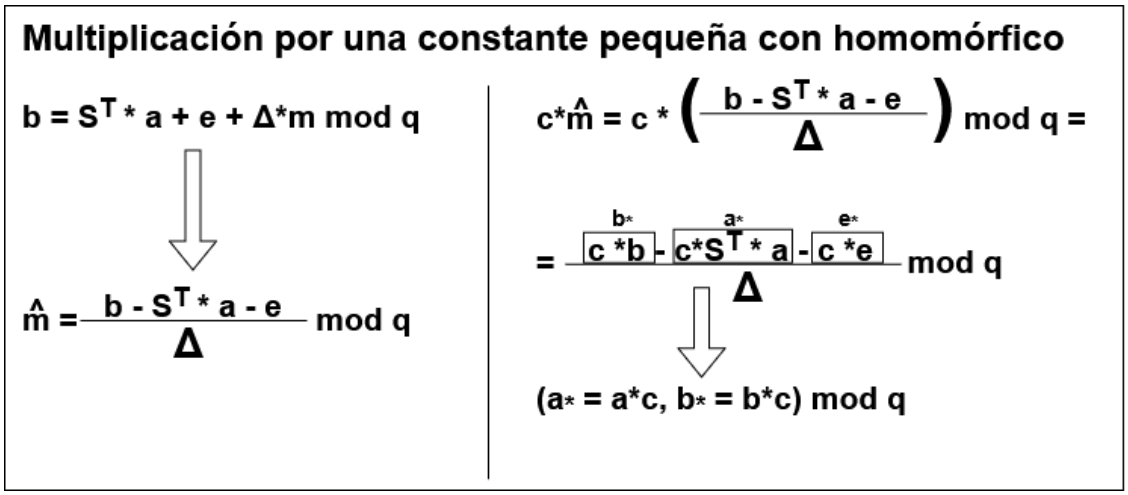
$= (a_+ = \begin{pmatrix}2\\3\end{pmatrix} + \begin{pmatrix}3\\2\end{pmatrix},\ b_+ = 3 + 1) \bmod 4 =$

$= (a_+ = \begin{pmatrix}1\\1\end{pmatrix},\ b_+ = 0)$

$$\hat{m}_+ = \frac{b_+ - S^T * a_+ - e_+}{Δ} \bmod q = \frac{0 - (1\ 0) * \begin{pmatrix}1\\1\end{pmatrix} - e_+}{1} \bmod 4 = -1/1 \bmod 4 = 3$$

$m_1 + m_2 = \hat{m}_+ = 3$

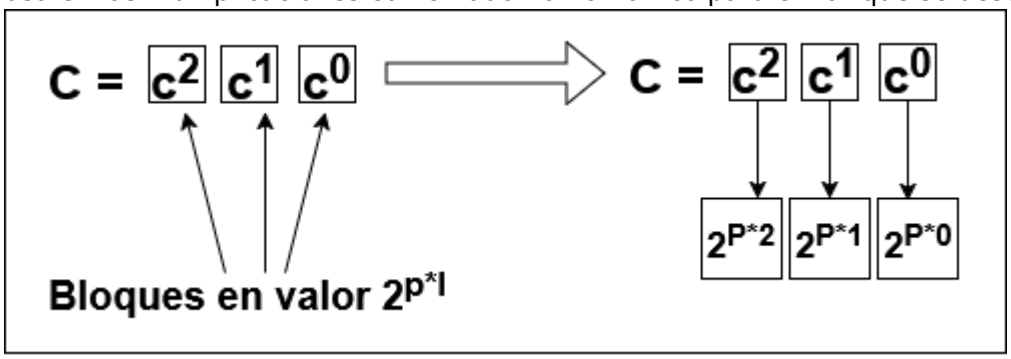
Multiplicación de cifrado homomórfico contra una pequeña constante



NOTA: Si el valor de C es muy grande puede descuadrarse todo al multiplicarse el error.

Descomposición gadget

La descomposición gadget consiste en tomar un número grande y descomponerlo en bloques. Esto se usa en las multiplicaciones con cifrado homomórfico para evitar que se descuadren los valores.



From:
https://knoppia.net/ - **Knoppia**

Permanent link:
https://knoppia.net/doku.php?id=pan:cifrado_homomorfico_v2&rev=1767041051

Last update: **2025/12/29 20:44**