

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
 - Distribución normal $N(0, \gamma * q) \rightarrow r = \gamma * q$
 - 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:

$$(a, b = S^T * a + e \pmod q) \in \mathbb{Z}^n_q * \mathbb{Z}_q$$

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:

$$(a, b = S^T * a + e + \Delta * m \pmod q)$$

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

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

$$\Delta * m + e = b + S^T * a$$

- $m' = \Delta * m + e \pmod q$ → Mensaje aproximado con error

$$m + e = (b + S^T * a) / \Delta \pmod q$$

- $m' = m + e$

$$m = \lfloor (b + S^T * a) / \Delta - e \pmod q \rfloor$$

- 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

$n = 2$
 $q = 4 = 2^2$
 $\Delta = 1 = 2^0$
 $e = 0$ (no hay error)
 $S = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$
 $a = \begin{pmatrix} 2 \\ 3 \end{pmatrix}$
 $m = 1$

Cifrado

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

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

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

$$b = 3$$

Descifrado

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

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

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

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

$$m = 1$$

Sumas sobre cifrado Homomórfico

Ejemplo de suma con cifrado homomórfico

Datos

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

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

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

$$m_1 = \frac{b_1 - S^T * a_1 - e_1}{\Delta}$$

$$m_2 = \frac{b_2 - S^T * a_2 - e_2}{\Delta}$$

$$m_1 + m_2 = \frac{b_1 - S^T * a_1 - e_1}{\Delta} + \frac{b_2 - S^T * a_2 - e_2}{\Delta} =$$

$$= \frac{b_+ - S^T * a_+ - e_+}{\Delta} \pmod q$$

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

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

$$m_1 + m_2 = (a_+ = a_1 + a_2, b_+ = b_1 + b_2) \pmod q =$$

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

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

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

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

Multiplicación de cifrado homomórfico contra una pequeña constante

Multiplicación por una constante pequeña con homomórfico

$$b = S^T * a + e + \Delta * m \pmod q$$

↓

$$\hat{m} = \frac{b - S^T * a - e}{\Delta} \pmod q$$

$$c * \hat{m} = c * \left(\frac{b - S^T * a - e}{\Delta} \right) \pmod q =$$

$$= \frac{\boxed{c * b} - \boxed{c * S^T * a} - \boxed{c * e}}{\Delta} \pmod q$$

↓

$$(a^* = a * c, b^* = b * c) \pmod q$$

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_homomorfo_v2&rev=1767041051

Last update: 2025/12/29 20:44

