

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:

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

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

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

- $m' = \Delta * m + e \rightarrow$ Mensaje aproximado con error

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

- $m' = m + e$

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

- 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

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

Cifrado

$$\begin{aligned} (a &= \begin{pmatrix} 2 \\ 3 \end{pmatrix}, b = S^T * a + e + \Delta * m) \bmod q \\ b &= (1 \ 0) * \begin{pmatrix} 2 \\ 3 \end{pmatrix} + 0 + 1 * 1 \\ b &= 2 + 0 + 0 + 1 * 1 = 3 \\ b &= 3 \end{aligned}$$

Descifrado

$$\begin{aligned} (a &= \begin{pmatrix} 2 \\ 3 \end{pmatrix}, b = 3) \\ m' &= \frac{b - S^T * a - e}{\Delta} \bmod q \\ m' &= \frac{3 - (1 \ 0) * \begin{pmatrix} 2 \\ 3 \end{pmatrix} - 0}{1} \bmod 4 \\ m' &= \frac{3 - 2}{1} \bmod 4 \\ m' &= 1 \end{aligned}$$

Sumas sobre cifrado Homomórfico

Multiplicación de cifrado homomórfico contra una pequeña constante

Descomposición gadget

From:

<https://www.knoppia.net/> - Knoppia

Permanent link:

https://www.knoppia.net/doku.php?id=pan:cifrado_homomorfico_v2&rev=1766684194

Last update: 2025/12/25 17:36



