

# Cifrado Homomorfo

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

A la hora de operar con cifrado homomorfo 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  $N(0, \gamma^2 q) \rightarrow r = \gamma^2 q$ 
    - 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 homomorfo es:

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

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

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

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

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

- $m' = m + e$

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

Permanent link:  
[https://www.knoppia.net/doku.php?id=pan:cifrado\\_homomorfico\\_v2&rev=1766681882](https://www.knoppia.net/doku.php?id=pan:cifrado_homomorfico_v2&rev=1766681882)

Last update: **2025/12/25 16:58**

