# 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.

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

Permanent link:
**https://www.knoppia.net/doku.php?id=pan:cifrado_homomorfico_v2&rev=1766682237**

Last update: **2025/12/25 17:03**