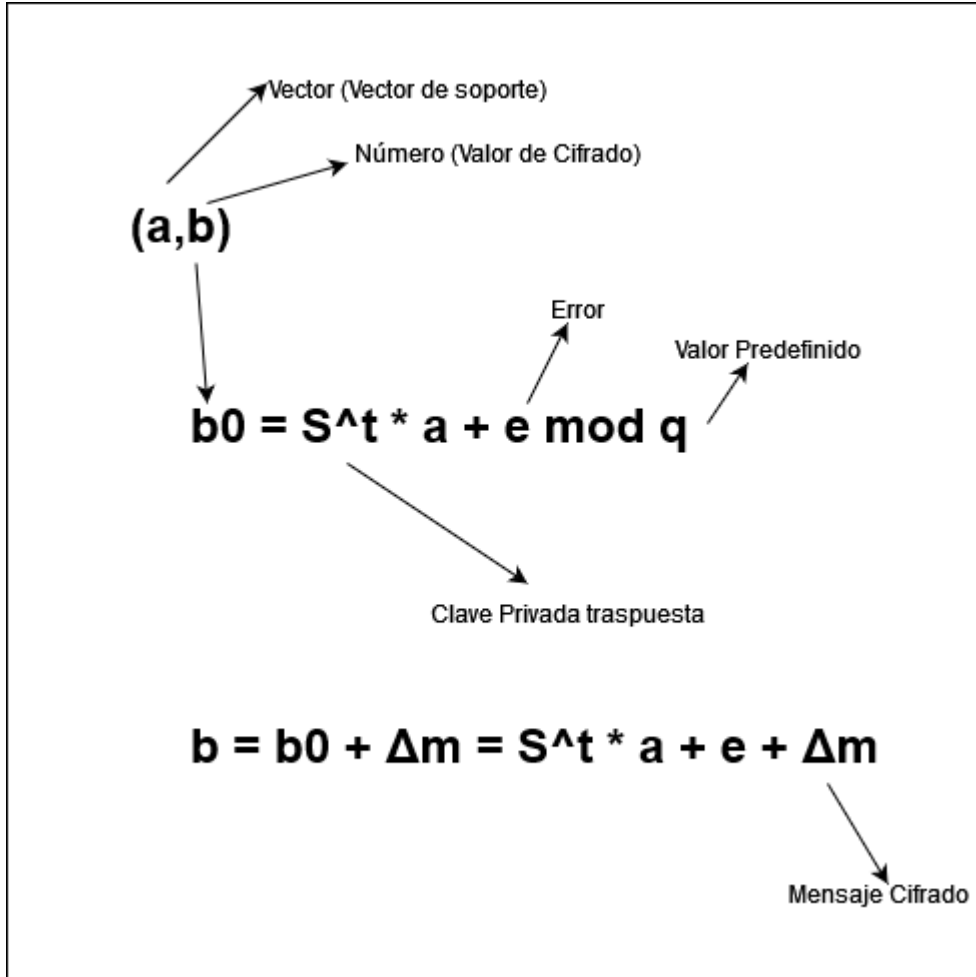


Homomórfico

Encriptación Simétrica LWE



Desencriptado

$$b = S^t + e + \Delta m$$



$$\Delta m = (b - S^t * a - e) / \Delta$$



$$m = (b - S^t * a - e) / \Delta \text{ mod } q$$

Si el error es tal que $|e| < \Delta/2$ entonces el mensaje se ha recuperado correctamente
 En cambio, si no se cumple la condición no se ha podido recuperar el mensaje.
 Hay que tener en cuenta que no siempre se va a poder descifrar.

Cifrando varios mensajes

$$\overbrace{(S^t * a_1 + \Delta m_1)}^{b_1} + \overbrace{(S^t * a_2 + \Delta m_2)}^{b_2} = S^t(a_1+a_2) + L + \Delta(m_1+m_2)$$

Longitud 1 + Longitud 2

Descomposición Gadget

Se quiere dividir un número en B bloques y cada bloque tienen P bits.

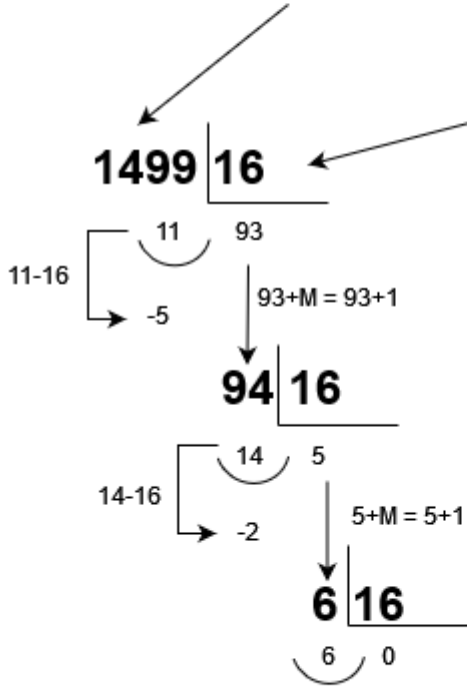
M = 1 → Mensaje

B = 3 → Bloques

P = 4 → Bits

Número = 1499

$2^P = 2^4 = 16$



$1499 = 6 \cdot 2^{(4 \cdot 2)} + 2 \cdot 2^{(4 \cdot 1)} - 5 \cdot 2^{(4 \cdot 0)}$

From:

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

Permanent link:

<https://knoppia.net/doku.php?id=pan:phomo&rev=1730216286>

Last update: **2024/10/29 15:38**

