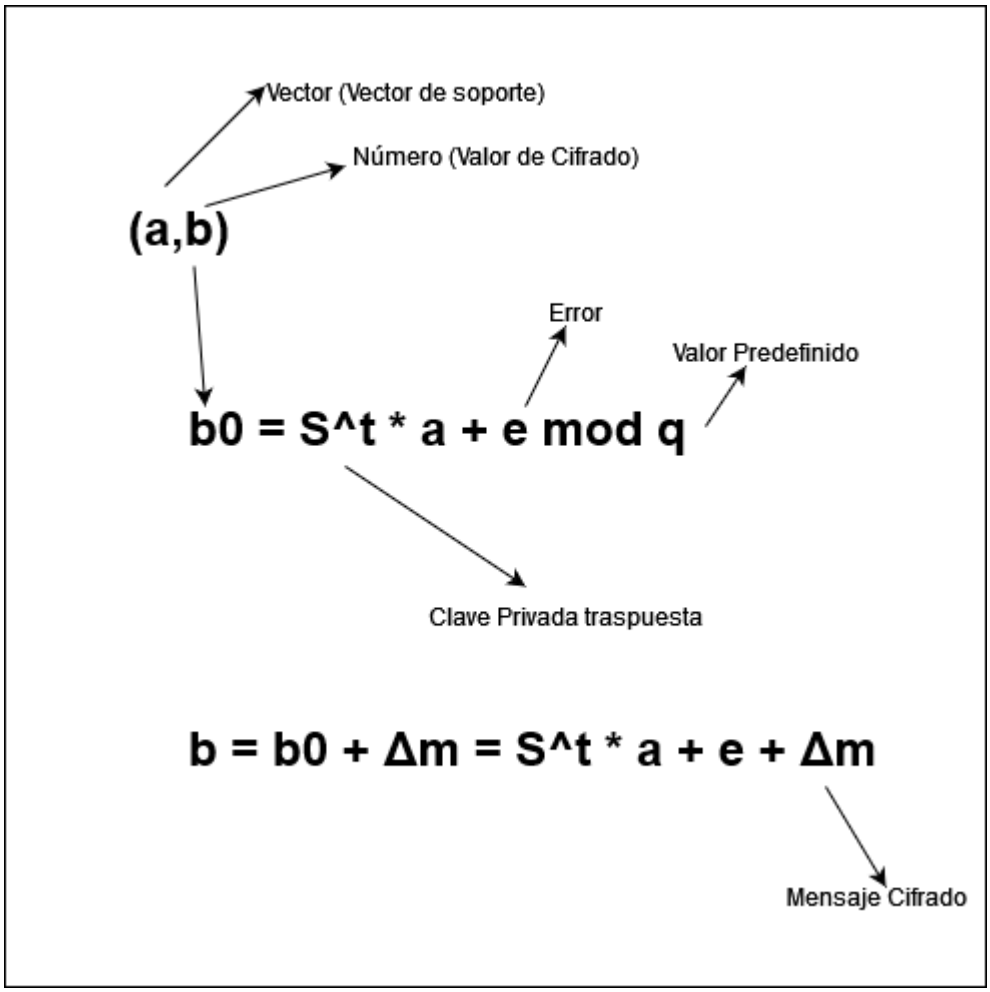
Homomórfico

Encriptación Simétrica LWE



Desencriptado

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

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

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

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

$$\overbrace{(S^t * a1 + \Delta m1)}^{b1} + \overbrace{(S^t * a2 * \Delta m2)}^{b2} = S^t(a1+a2) + L + \Delta(m1+m2)$$

Longitud 1 + Longitud 2

Descomposición Gadget

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