

1. (Cifrado Homomórfico): Si queremos multiplicar un mensaje  $m$  por un valor  $c$ , tenemos la expresión base:

$$a, b = S^T * a + e + \Delta n \pmod{q} \rightarrow c * a \pmod{q}, c * b \pmod{q}$$

Se propone la siguiente expresión alternativa:

$$a_i, b_i = S^T * a_i + e_i + \Delta n \pmod{q} \rightarrow a' = \sum_{i=1}^n X^2_i$$

¿Tienen ambas la misma varianza?

2.

From:

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

Permanent link:

<https://knoppia.net/doku.php?id=pan:examen2025&rev=1736596492>

Last update: **2025/01/11 11:54**

