

Examen PAN Enero 2025

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

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

Se propone la siguiente expresión alternativa:

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

¿Tienen ambas la misma varianza?

2.

From:

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

Permanent link:

<https://www.knoppia.net/doku.php?id=pan:examen2025>

Last update: **2025/01/11 12:01**

