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

$a,b=S^T*a+e+Δn$ mod q → $c*a$ mod $q, c*b$ mod q

Se propone la siguiente expresión alternativa:

$a_i,b_i=S^T*a_i+e_i+Δn$ mod q → $a' = Σ^n_{i=1} X^2_i$

¿Tienen ambas la misma varianza?

2.