

[PAN] Cifrado Homomórfico (Resumen)

Se utiliza cuando se quieren realizar computaciones en una entidad que no es de confianza. Se realiza el uso de grupos de homomorfismos: $D_K(x+y) = D_K(x) \{ o \} D_K(y)$

- Cifrado: $Cx = E(X) = X^e \text{ mod}(n)$; $Cy = E(y) = y^e \text{ mod}(n)$
- Descifrado: $X = D(Cx) = c_x^d \text{ mod}(n)$; $Y = D(Cy) = c_y^d \text{ mod}(n)$
- Multiplicación: $Cx * Cy = (x^e \text{ mod}(n)) * (y^e \text{ mod}(n)) = X^e * y^e \text{ mod}(n) = (x*y)^e \text{ mod}(n) = E(x*y)$
- Por lo tanto $D(C_x * C_y) = x*y$

Retículos

Un retículo n-dimensional es cualquier combinación de enteros en base n $\{a_1, a_2, \dots, a_n\}$. Una base es buena si todos los vectores son cortos o es mala si son largos.

Problemas de los retículos de grandes dimensiones

En los retículos es muy difícil calcular:

- SVP (Shortest Vector Problem): Encontrar la norma euclídea λ_1 del vector más corto en el retículo
- α -Aproximate SVP: Encontrar un vector con una norma más pequeña que $\alpha \lambda_1$ donde $\alpha > 1$ puede depender del número de dimensiones.
- SIVP (Shortest Independent Vectors Problem): λ_n es la longitud del n-vector más corto en profundidad.

Por que se usa cifrado basado en Retículos

- Resistencia cuántica
- Relativamente fácil de implementar
- Permite cifrado homomorfo

From:

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

Permanent link:

https://knoppia.net/doku.php?id=pan:res_cifrado_homomorfo&rev=1736286366

Last update: 2025/01/07 21:46

