

[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: $\text{D}_K(x+y) = \text{D}_k(x) \oplus \text{D}_k(y)$

- Cifrado: $C_x = E(X) = X^e \pmod{n}$; $C_y = E(Y) = Y^e \pmod{n}$
- Descifrado: $X = D(C_x) = c_x X^d \pmod{n}$; $Y = D(C_y) = c_y Y^d \pmod{n}$
- Multiplicación: $C_x * C_y = (X^e \pmod{n}) * (Y^e \pmod{n}) = X^e * Y^e \pmod{n} = (X * Y)^e \pmod{n} = E(X * Y)$
- 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 homomórfico

From:

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

Permanent link:

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



Last update: 2025/01/07 21:46