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

Retículos

Un retículo n-dimensional es cualquier combinación de enteros en base n ${a_1, a_2,..., a_n}$. 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
- ∝-Aproximate SVP: Encontrar un vector con una norma más pequeña que $∝λ_1$ donde ∝>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 homomorfico