

Introducción al cifrado homomorfo

- Se pasa la computación a una entidad no confiada, como un ordenador en la nube
- La idea es que el ordenador en la nube vea todo cifrado y sea capaz de hacer operaciones sobre los datos cifrados.
- Un ejemplo de esto sería un sistema de acceso biométrico: Tanto los datos del usuario como la base de datos están encriptados. El sistema de autenticación es capaz de verificar si los datos están en la base sin saber nada sobre estos datos cifrados.

Cifrado homomorfo

Lo que busca es que si se opera sobre las versiones cifradas, al descifrar el resultado se obtiene el resultado de la suma. Por ejemplo, si se realiza una suma sobre lo cifrado, al descifrar el resultado, se obtiene la suma.

$$Dk(X+Y) = Dk(c) \text{ o } Dk(y)$$

- Encriptación: $Cx = E(x) = X^e \text{ mod } n$; $Cy = E(y) = y^e \text{ mod } n$

Retículos

Es una disminución regular y discreta de puntos en el espacio y que de una manera formal se puede escribir como una fase de vectores que general todas las posibles combinaciones como un sumatorio. Las bases de los retículos no son únicas. Pueden ser descritos en términos de dos bases diferentes.

- Una base es buena si los vectores son cortos
- Una base es mala cuando algunos de los vectores son largos

Problemas difíciles con retículos

- SVP: El vector más corto sin ceros: Encontrar la norma euclídea λ_1 del vector más corto en el retículo
- Aproximación α del SVP: Encontrar cualquier vector con una norma menor de $\alpha \lambda_1$, donde α es mayor que uno.
- SIVP: Problema del vector independiente más corto. En este caso, λ_n es la longitud del vector n más corto en profundidad.

Criptografía basada en retículos

- Tiene resistencia cuántica
- Relativamente fácil de implementar
- Permite cifrado homomórfico
- Se les llama la navaja suiza de la criptografía

Problema del aprendizaje con errores (LWE)

Dado un número de ecuaciones lineales módulo q entero, se deben encontrar vectores que las puedan resolver aproximadamente.

Cifrado simétrico de clave usando LWE

Cuando queremos cifrar un mensaje M lo hacemos generando un vector aleatorio de n componentes de forma uniforme sobre los números módulo q

From:

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

Permanent link:

<http://knoppia.net/doku.php?id=pan:enchmo>

Last update: **2024/10/16 16:17**

