Introducción al cifrando homomorfico

- 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 homomorfico

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.

$Dk (X+Y) = DK(c) o Dk(y)$

- Encriptación: Cx = E(x) = X^e mod n; Cy =E(y) = y^e 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 Lambda 1 del vector más corto en el retículo
- Aproximación alfa del SVP: Encontrar cualquier vector con una norma menor de alfa lambda 1, donde alfa es mayor que uno.
- SIVP: Problema del vector independiente más corto. En este caso, lambda 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.

From:
https://www.knoppia.net/ - **Knoppia**

Permanent link:
https://www.knoppia.net/doku.php?id=pan:enchmo&rev=1728489515

Last update: **2024/10/09 15:58**