operaciones honomórficas

tipo de criptografia para proteger la informacion

aplicaciones: sanidad, finanzas, cloud computing, ia y machine learning (necesitan muchos datos y debemos asegurar su proteccion y privacidad. aportar datos cifrados). gobiernos y defensa.

problemas: lento, necesita muchos recursos.

* estion del ruido: hay datos que no pueden ser descifrados con la informacion original por las operaciones añadiendo un ruido.
* hardware: lsa cpus tradicoinales no son lo suficientemente rapidas.es necesario un hw escpecializado.
* complejidad de sitribucion. es un reto la distribucion de claves seguras.

Estandarización

HomomorphicEncryption.org está intentando hacer el Homomorphic Encrption EStandard (HES), últmo workship en 2018.

en 2019 un draft par aactualizar el HES.

Futuro

Debe pasra de un punto teorico a uno mas practico y continuar con las estandarizaciones. si se tratan los problemas que tiene es muy factible que salga adelante.