**Lattices**

1. **Introducción**

Lattice se puede explicar como un vector en un plano 2D, donde en este espacio hay muchos más lattices posibles.

1. **Problemas de computación de un lattice**

* SIVP: encontrar vectores linealmente independientes lo más cortos posibles. NP-hard
* CVP: dado un lattice, encontrar el vector que se aproxime más a él. NP-hard

Un lattice puede ser hecho por infinitas bases, hay de dos tipos:

* **buena:** vectores base, cortos, cercanos a 90º.
* **mala:** vectores largos y oblicuos. Resolver problemas con estos es muy difícil.

**Asimetría computacional**: la clave pública tiene malas bases, mientras que la privada tiene las buenas permitiendo su cálculo. Se conoce como ***trapdoor*** de lattices.

* Learning with Errors (LWE): secreto con ecuaciones que añaden un poco de ruido. El problema acaba computándose a NP-heard
* El ring-LWE es muy parecido pero mas eficiente
* SIS: encontrar vector no nulo en una matriz pública.

1. **Futuro**

NIST confia en lattices.

Ya hay estándares mostrando cierta madurez en el tema.

Códigos correctores de errores

son muy rápidas.

Funciones de hash (arboles de merkle)

ventajas: robustez bien entenida en las funcoines de hash. desventajas: esquemas stateful.

criptografia multivariada: ecuaciones polinomicas

ventajas: muy rapidas

descentajas: claves pubkicas muy grandes

isogenias supersinglares:

ventajas: claves publicas muy pequeñas

Lentas y ya han sido vulneradas.

1. **Retos de los lattices**

Lattices es un buen equilibrio de todas las alternativas que hay.

Desafíos: eficiencia computacional, tamaño de claves y firmas, complejidad de implementación segura (la seguridad depende de los parámetros que le pongamos nosotros mismos)

Vectores de ataque:

* LLL y BKS: hacer mas simplificado para encontrar vulnerabilidades
* primales: encontrar vector corto especifico en el lattice
* hibridos: adivinanza parcial y ataque lattice tradicional

Soluciones de retos para lattices:

* Falta de coputacion: procesadores especializados o uso de SIMD,
* reduccion del teamaño de claves y firmas
* seguridad y resistencia a ataques:

estan apareciendo estandares aprobados por el NIST

1. **Adopción del mercado**

* integracion con TLS, VPN y SSH
* blockchain

1. **Conclusión**

* La seguridad no es un estado, es un proceso.
* amenaza cuántica real: los sistemas actuales son vulnerables.
* LBC es el algoritmo más viable.