Lattice based post-quantum encryption

Joel Macías, Marcel Sánchez, Sergio Sanz, Arnau Valls

Mayo 2025

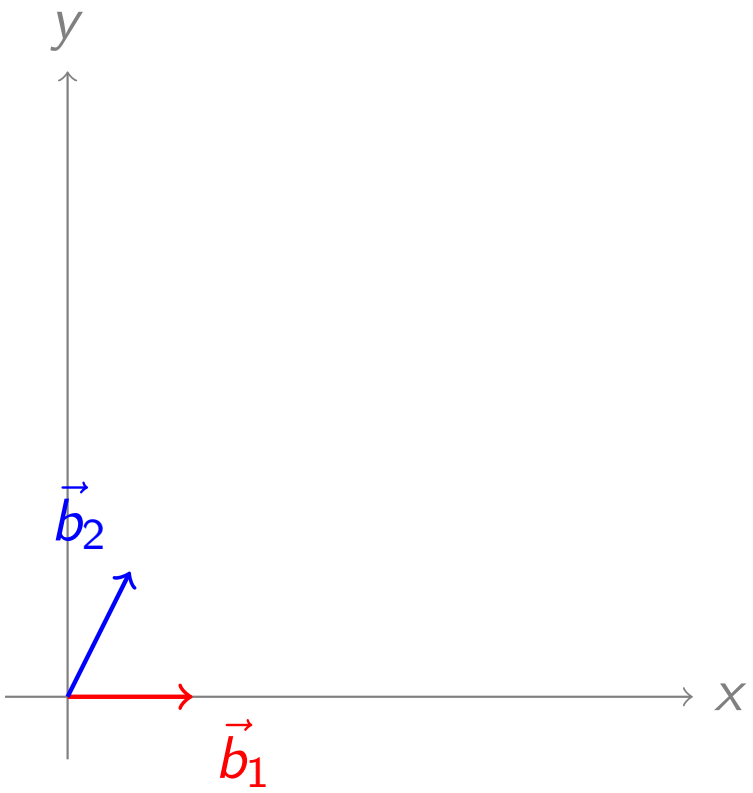
El problema: la amenaza cuántica

- La seguridad digital actual (RSA, ECC) se basa en problemas difíciles para ordenadores **clásicos**.
- **Amenaza cuántica:** Algoritmos como el de Shor (1994) podrían romper RSA y ECC si tuviéramos ordenadores cuánticos potentes.
- Riesgo: "Cosechar ahora, descifrar después". Datos cifrados hoy podrían ser vulnerables mañana.
- **Necesidad Urgente:** Nuevos algoritmos criptográficos resistentes a ataques cuánticos.

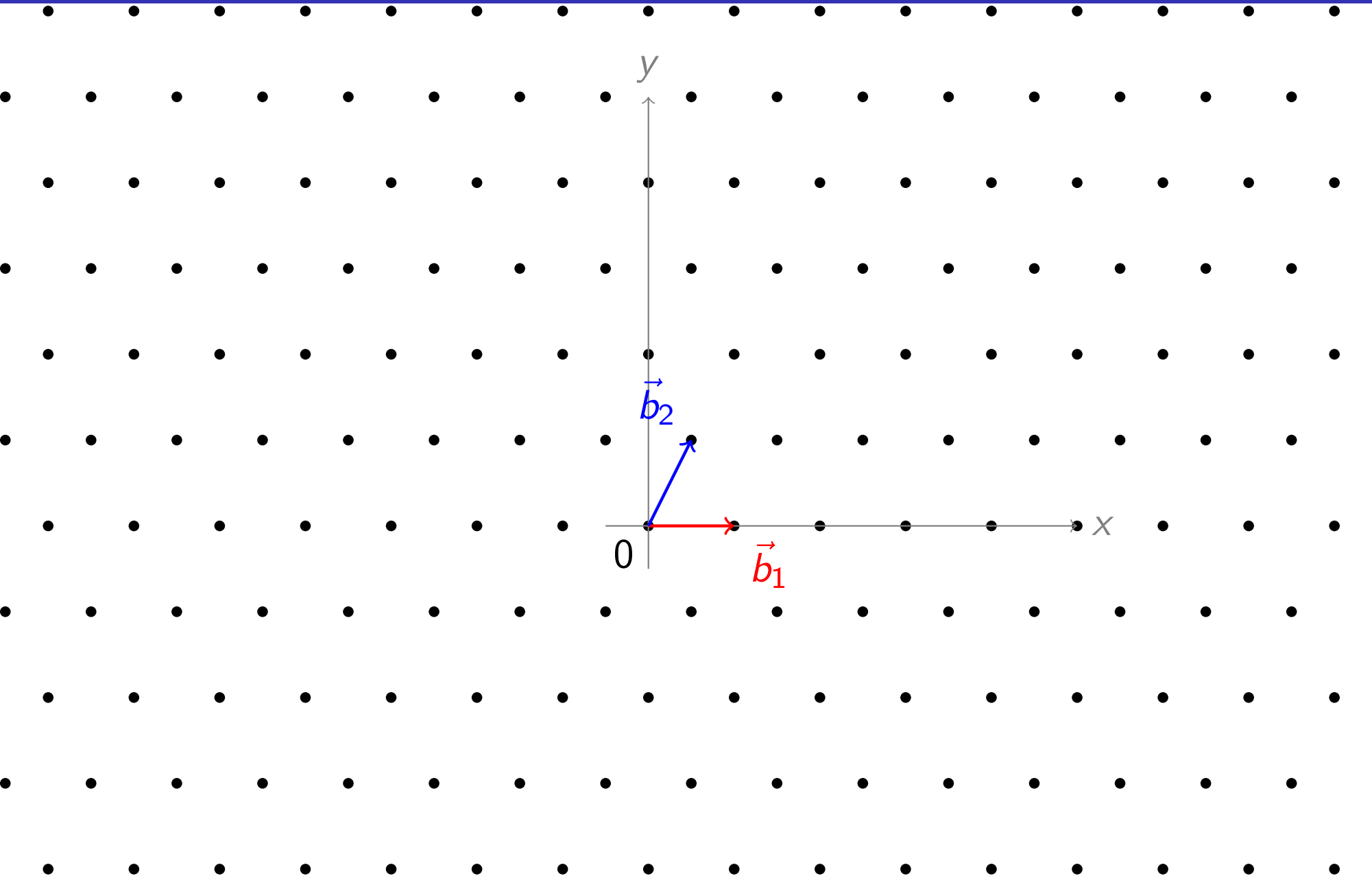
Solución: Criptografía Post-Cuántica (PQC)

- PQC: Desarrollar criptosistemas seguros contra ordenadores **clásicos Y cuánticos**.
- Hoy nos centraremos en una familia líder: **Criptografía Basada en Lattices (Retículos)**.
- ¿Por qué Lattices?
  - Seguridad basada en problemas matemáticos que (creemos) son difíciles incluso para ordenadores cuánticos.
  - Buen rendimiento y versatilidad.

Qué es un lattice



Qué es un lattice



Qué es un lattice

Un lattice (L) se define como el conjunto de todas las combinaciones lineales con coeficientes enteros de un conjunto de vectores base linealmente independientes ($B = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$) en un espacio real m-dimensional ($\mathbb{R}^m$) (usualmente, $m = n$).

$$L = \left\{ \sum_{i=1}^{n} z_i \mathbf{b}_i : z_i \in \mathbb{Z} \right\}$$

Problemas geométricos fundamentales en lattices

- Problemas muy difíciles
- No existen algoritmos cuánticos capaces de resolverlos eficientemente

Problemas geométricos fundamentales en lattices

SVP (Shortest Vector Problem)

- **Objetivo:** En un lattice L, encontrar el vector $\mathbf{v} \in L$, $\mathbf{v} \neq \mathbf{0}$, lo más corto posible.
- **Intuición:** Encontrar el punto del lattice (distinto del origen) más cercano al origen.
- **Dureza:** NP-hard. Incluso aproximarlo bien es difícil.
- **Variantes:**
  - **SIVP (Shortest Independent Vectors Problem):** Encontrar n vectores linealmente independientes lo más cortos posible.
  - **GapSVP$_\gamma$ (Problema de decisión):** Dado un vector y una distancia d, decidir si el vector más corto es $\leq d$ o $> \gamma \cdot d$. Difícil incluso para factores de aproximación γ grandes.
  - **uSVP (unique SVP):** SVP bajo la promesa de que el vector más corto es significativamente más corto que todos los demás vectores no paralelos.

Problemas geométricos fundamentales en lattices

CVP (Closest Vector Problem)

- **Objetivo:** Dado un lattice L y un vector objetivo $\mathbf{t} \in \mathbb{R}^n$ (que no está necesariamente en L), encontrar el vector $\mathbf{v} \in L$ más cercano a $\mathbf{t}$.
- **Intuición:** Redondear un punto cualquiera al punto más cercano del lattice.
- **Dureza:** NP-hard.
- **Variantes:**
  - **CVPP (Closest Vector Problem with Preprocessing):** Se permite preprocesar el lattice antes de recibir el vector objetivo $\mathbf{t}$.
  - **GapCVP$_\gamma$ (Problema de decisión):** Dado $\mathbf{t}$ y una distancia d, decidir si el vector del lattice más cercano está a distancia $\leq d$ o si todos están a $> \gamma \cdot d$.
  - **BDD (Bounded Distance Decoding):** Dado $\mathbf{t}$ y la promesa de que existe un vector del lattice a una distancia $\leq d$ (para d suficientemente pequeño), encontrarlo.

La dualidad de las bases en un lattice

Un mismo lattice puede ser descrito por muchas bases diferentes.

Base "buena"

- Compuesta por vectores base:
  - Relativamente **cortos**.
  - Casi **ortogonales** (ángulos $\approx 90°$).
- La estructura geométrica del lattice es más **evidente**.
- Problemas como SVP o CVP pueden ser (relativamente) más fáciles de abordar o visualizar.

Base "mala"

- Compuesta por vectores base:
  - A menudo **largos**.
  - Muy **oblicuos**.
- Aunque genera el *mismo* lattice, la estructura está **ofuscada**.
- Resolver SVP o CVP a partir de esta base es típicamente muy **difícil**.

La dualidad de las bases en un lattice

Idea clave: Si una entidad conoce una **base "buena"** mientras públicamente solo se conoce una **base "mala"**, esto crea una **asimetría computacional**.

- Esto es la esencia de un **trapdoor** en lattices.

Concepto principal: Determinar un secreto s a partir de ecuaciones con "ruido".

Planteamiento del problema:

1. **Secreto:** Existe un valor s (oculto).
2. **Pistas públicas:** Se proporcionan múltiples valores $a_1, a_2, \ldots$.
3. **Resultados ruidosos públicos:** Para cada a_i, se calcula $b_i = (a_i \cdot s) + \text{error pequeño}_i \pmod{q}$.
   - El error es de magnitud pequeña y aleatorio.
   - Se conocen los a_i y los b_i.

Desafío LWE: Dadas múltiples parejas (a_i, b_i), ¿es posible encontrar s? Los errores pequeños hacen que s sea muy difícil de aislar.

- **Variante estructurada de LWE:** En lugar de vectores, se trabaja con polinomios en un anillo.
- Muestras: $(a_i(x), b_i(x))$, con $b_i(x) = a_i(x) \cdot s(x) + e_i(x) \pmod{q, \Phi_n(x)}$.
- **Ventajas:** Mucho más eficiente (claves más pequeñas, operaciones más rápidas) para un nivel de seguridad similar a LWE, gracias a la estructura polinómica.

SIS (Short Integer Solution)

- **Definición:** Dada una matriz pública (aleatoria) $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$ y un módulo q.
- **Objetivo:** Encontrar un vector **no nulo** $\mathbf{z} \in \mathbb{Z}^n$ tal que:
  1. $\mathbf{Az} = \mathbf{0} \pmod{q}$ (el vector $\mathbf{z}$ está en el kernel de $\mathbf{A}$ $(\text{mod } q)$).
  2. Las componentes de $\mathbf{z}$ son "pequeñas" (ej. $0, \pm 1$, o dentro de un rango pequeño), es decir, $\|\mathbf{z}\|_\infty \leq \beta$ para alguna cota β.
- **Dureza:** Difícil si se exige que $\mathbf{z}$ sea suficientemente corto y $n > m \log q$. Relacionado con SVP en el peor caso.

Problemas algebraicos con seguridad basada en Lattices

Con esto se construyen:

- **KEMs (Key Encapsulation Mechanisms):** Para establecer claves secretas compartidas.
- **Firmas digitales:** Para autenticidad e integridad de mensajes.

Estado del Arte: NIST confía en lattices

- El Instituto Nacional de Estándares y Tecnología de EE.UU. lanzó un proceso mundial para estandarizar la PQC (desde 2016).
- Los algoritmos basados en lattices han dominado la selección
- **Estándares ya publicados (2024):**
  - **ML-KEM (CRYSTALS-Kyber):** Para intercambio de claves (KEM). Basado en LWE.
  - **ML-DSA (CRYSTALS-Dilithium):** Para firmas digitales. Basado en LWE/SIS.
- **Próximo estándar:**
  - **FN-DSA (Falcon):** Otra firma digital, firmas muy compactas. Basado en SVP.
- Esto demuestra la madurez y confianza en la seguridad y eficiencia de los lattices.

Basada en Códigos Correctores de Errores

- **Principio:** Dificultad de decodificar códigos lineales aleatorios.
- **Ventajas:** Operaciones muy rápidas.
- **Desventajas:** Claves públicas muy grandes.
- **vs. Lattices:** Lattices suelen ofrecer mejor equilibrio tamaño/velocidad.

Basada en Funciones Hash

- **Principio:** Firmas de un solo uso (OTS) + árboles de Merkle para firmas múltiples.
- **Ventajas:** Seguridad basada en la robustez bien entendida de las funciones hash.
- **Desventajas:** Esquemas *stateful* (riesgo si se reutiliza clave) o *stateless* (firmas grandes y lentas).
- **vs. Lattices:** Lattices son *stateless*, firmas más pequeñas y rápidas.

Criptografía Multivariada

- **Principio:** Dificultad de resolver sistemas de ecuaciones polinómicas.
- **Ventajas:** Firmas muy rápidas.
- **Desventajas:** Claves públicas muy grandes, historial de seguridad con altibajos.
- **vs. Lattices:** Lattices ofrecen mejor equilibrio general y seguridad más estable.

Basada en Isogenias Supersingulares

- **Principio:** Dificultad de encontrar isogenias entre curvas elípticas.
- **Ventajas:** Claves públicas extremadamente pequeñas.
- **Desventajas:** Muy lentas; propuestas clave (SIDH/SIKE) rotas recientemente.
- **vs. Lattices:** Lattices son más maduras, eficientes y actualmente más seguras.

Lattices: Una Solución Equilibrada

- Los sistemas basados en *lattices* emergen como una opción muy versátil.
- **Fortalezas Clave:**
  - **Seguridad:** Basada en problemas (LWE, SIS) considerados difíciles, incluso para cuánticos.
  - **Eficiencia:** Tamaños de clave/texto cifrado moderados y alta velocidad.
  - **Flexibilidad:** Aplicables a encapsulamiento de claves (KEMs) y firmas digitales.
- Se posicionan como una de las mejores opciones PQC por este equilibrio.

Desafíos Actuales de los Lattices

A pesar de sus ventajas, enfrentan desafíos:

- **Eficiencia Computacional:**
  - Operaciones pueden ser más costosas que en criptografía clásica.
  - Impacto en dispositivos con recursos limitados. Mejora continua en algoritmos y hardware.

Desafíos Actuales de los Lattices

A pesar de sus ventajas, enfrentan desafíos:

- **Eficiencia Computacional:**
  - Operaciones pueden ser más costosas que en criptografía clásica.
  - Impacto en dispositivos con recursos limitados. Mejora continua en algoritmos y hardware.
- **Tamaño de Claves y Firmas:**
  - Generalmente mayores que en sistemas clásicos.
  - *Structured lattices* ayudan a reducir tamaños.

Desafíos Actuales de los Lattices

A pesar de sus ventajas, enfrentan desafíos:

- **Eficiencia Computacional:**
  - Operaciones pueden ser más costosas que en criptografía clásica.
  - Impacto en dispositivos con recursos limitados. Mejora continua en algoritmos y hardware.
- **Tamaño de Claves y Firmas:**
  - Generalmente mayores que en sistemas clásicos.
  - *Structured lattices* ayudan a reducir tamaños.
- **Complejidad de Implementación Segura:**
  - Elección crítica de parámetros (dimensión, módulo, error).
  - Encontrar el balance entre seguridad robusta y eficiencia.

Principales Vectores de Ataque a Lattices

Los ataques buscan resolver problemas difíciles subyacentes (SVP, CVP).

- **Reducción de Bases (LLL, BKZ):**
  - Fundamentales en muchos criptoanálisis.

Principales Vectores de Ataque a Lattices

Los ataques buscan resolver problemas difíciles subyacentes (SVP, CVP).

- **Reducción de Bases (LLL, BKZ):**
  - Fundamentales en muchos criptoanálisis.
- **Ataques Primales:**
  - Intentan encontrar un vector corto específico en el *lattice*.

Principales Vectores de Ataque a Lattices

Los ataques buscan resolver problemas difíciles subyacentes (SVP, CVP).

- **Reducción de Bases (LLL, BKZ):**
  - Fundamentales en muchos criptoanálisis.
- **Ataques Primales:**
  - Intentan encontrar un vector corto específico en el *lattice*.
- **Ataques Hibridos:**
  - Adivinanza parcial
  - Ataque lattice tradicional

Soluciones propuestas y optimizaciones recientes

Eficiencia computacional y optimizaciones de hardware

- Procesadores especializados para operaciones en lattices.
- Uso de instrucciones SIMD para paralelizar cálculos.
- Reducción del consumo energético en dispositivos IoT.

Ejemplo destacado

Zewen Ye et al. presentan un procesador eficiente para criptografía post-cuántica en IoT, utilizando instrucciones SIMD y unidades de hardware para operaciones polinómicas y Keccak.

Soluciones propuestas y optimizaciones recientes

Eficiencia computacional y optimizaciones de hardware

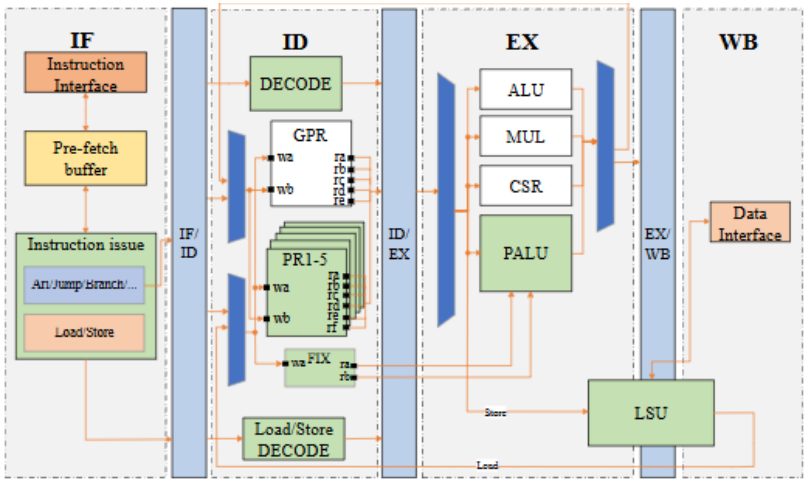
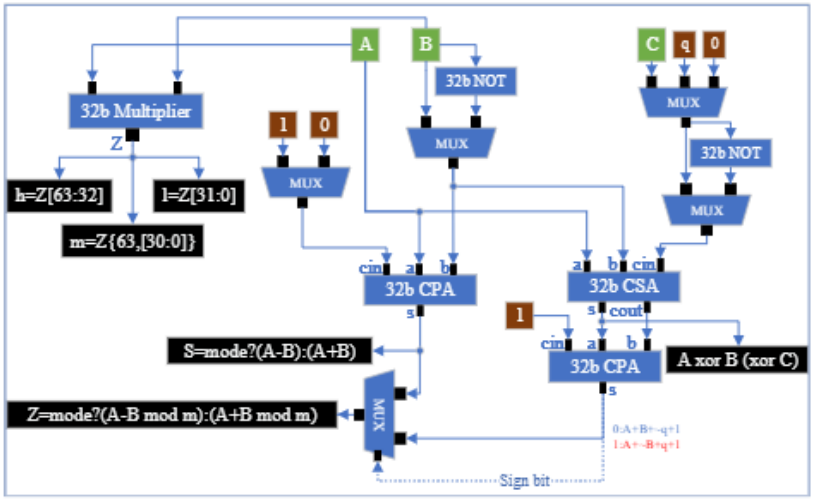


Figure 1: Proposed SIMD Processor Architecture.

Arquitectura del procesador SIMD



Diseño y flujo de datos de la ALU propuesta

Soluciones propuestas y optimizaciones recientes

Reducción del tamaño de claves y firmas

- Uso de estructuras algebraicas como los *module lattices*.
- Representaciones más compactas de claves y firmas.
- Mejora en la eficiencia de almacenamiento y transmisión.

Ejemplo destacado

Banerjee et al. desarrollan Sapphire, un procesador configurable que optimiza operaciones en lattices, reduciendo el tamaño de las claves mediante técnicas avanzadas de muestreo y transformadas numéricas.

Soluciones propuestas y optimizaciones recientes

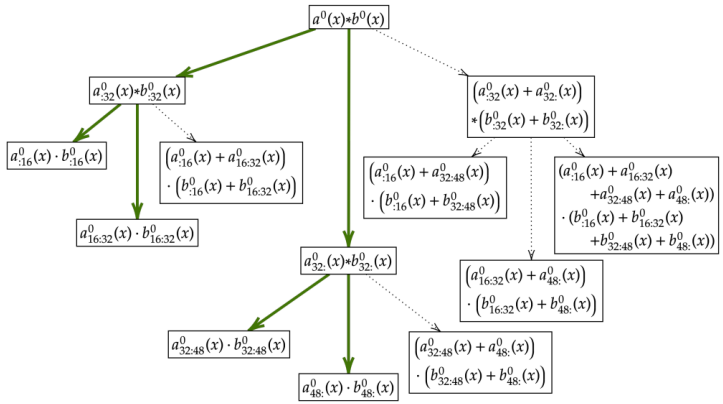
Mejoras en la seguridad y resistencia a ataques

- Mitigación de ataques de canal lateral.
- Análisis de potencia y técnicas de inyección de fallos.
- Implementación de contramedidas en hardware y software.

Ejemplo destacado

Mujdei et al. analizan vulnerabilidades en multiplicaciones polinómicas, proponiendo estrategias para proteger implementaciones de criptografía basada en lattices contra ataques de canal lateral.

Mejoras en la seguridad y resistencia a ataques



Estructura de división de polinomios de 64 coeficientes en Saber

Soluciones propuestas y optimizaciones recientes

Estándares y algoritmos seleccionados por NIST

- Proceso de estandarización iniciado en 2016.
- Selección de algoritmos resistentes a ataques cuánticos.
- Consideración de seguridad y eficiencia en diversas plataformas.

Ejemplo destacado

NIST ha seleccionado algoritmos como CRYSTALS-Kyber para encapsulación de claves y CRYSTALS-Dilithium para firmas digitales, ambos basados en problemas de lattices.

Soluciones propuestas y optimizaciones recientes

Implementaciones eficientes en dispositivos con recursos limitados

- Adaptación de algoritmos post-cuánticos a microcontroladores.
- Desarrollo de bibliotecas y aceleradores criptográficos.
- Optimización del consumo energético y uso de memoria.

Ejemplo destacado

La plataforma OpenTitan ha sido adaptada para soportar criptografía basada en lattices, integrando aceleradores de hardware y contramedidas contra ataques físicos.

Aplicaciones prácticas y adopción en el mercado

- Integración en protocolos como TLS, VPN y SSH.
- Uso en dispositivos IoT y sistemas embebidos.
- Aplicación en blockchain y criptomonedas.

Ejemplo destacado

Empresas como Google, Microsoft, IBM y Cloudflare están adoptando criptografía basada en lattices en sus productos y servicios, impulsando la transición hacia estándares post-cuánticos.

Protocolos de seguridad en Internet

- **TLS**: privacidad, integridad y autenticación.
- **VPN**: IPsec, SSL/TLS.
- **SSH**: acceso remoto seguro.

Integración post-cuántica

- TLS: uso de KEMs (Kyber, NTRU) y firmas híbridas.
- VPN: strongSwan + liboqs, TLS-VPN, WireGuard KEM.
- SSH: OpenSSH + liboqs, impacto en latencia (0.5–50 %).

IoT y sistemas embebidos

- Restricciones: memoria, energía y CPU.
- Plataformas: microcontroladores, ASICs, SoCs.

Avances recientes

- NXP: reducción de requisitos RAM/ROM.
- STMicroelectronics: aceleradores PQC en MCU.
- Crypto Quantique: plataforma QuarkLink híbrida.

Blockchain y criptomonedas

- Vulnerabilidad: ECDSA/EdDSA frente a Shor.
- Redes: Bitcoin, Ethereum y contratos inteligentes.

Firmas post-cuánticas

- Dilithium: 2.7 KB, equilibrio seguridad/eficiencia.
- Falcon: 0.7 KB, FFT sobre NTRU, compacta.

Empresas y proyectos involucrados

- Google: TLS 1.3 híbrido.
- Microsoft: PQCrypto-VPN, OpenVPN.
- IBM: propuestas de Lattice Signatures.
- Cloudflare: pruebas de Kyber en TLS híbrido.

Impacto y perspectivas

- Integración gradual en infraestructuras críticas.
- Desafíos: compatibilidad, rendimiento, estándares.
- Futuro: migración masiva a esquemas PQC.

Futuro de LBC (I): Campo dinámico y estandarización

- **LBC no es estática:** Evoluciona con investigación y necesidades cuánticas.
- **Estandarización continua y global**
  - NIST: Nuevos algoritmos a parte de Kyber y Dilithium. PQSC
  - Se esperan más algoritmos (KEMs, firmas) para diversificar opciones.
  - Otros candidatos (ej. NTRU) siguen siendo relevantes.
  - Organismos internacionales (ISO/IEC) impulsan adopción global.
- **Impacto económico de la estandarización**
  - Reduce incertidumbre y costes de desarrollo.
  - Fomenta interoperabilidad y mercado competitivo.

Futuro de LBC: Transición

- **Transición progresiva a PQC puro**
  - *Actual:* Enfoques híbridos (PQC + clásico) para seguridad y confianza gradual.
  - *Objetivo a largo plazo:* Sistemas 100% basados en PQC.

Futuro de LBC: Nuevas primitivas

- **Expansión a primitivas criptográficas avanzadas**
  - Retículos: Buena base más allá de cifrado/firma estándar.
  - **Cifrado homomórfico (FHE)**
    - "Computar sobre datos cifrados" sin revelarlos.
    - Clave para privacidad en la nube, análisis genómico, IA segura.
    - Avances en eficiencia y usabilidad.
  - *Otras:* Criptografía basada en atributos (ABE), pruebas de conocimiento cero (ZKPs) cuántico-resistentes.

Futuro de LBC: Seguridad

- **Evolución continua del análisis de seguridad**
  - La seguridad no es un estado, es un proceso.
  - Búsqueda constante de vulnerabilidades (clásicas/cuánticas).
  - Vigilancia de ataques de canal lateral (fugas de información física).
  - Refinamiento de parámetros para mantener niveles de seguridad.

Futuro de LBC: Adaptabilidad

- **Interoperabilidad y agilidad criptográfica**
  - *Interoperabilidad:* Necesidad de que sistemas PQC diversos se comuniquen fluidamente.
  - *Agilidad criptográfica:* Capacidad de los sistemas para migrar fácilmente entre algoritmos y responder a nuevas amenazas o adoptar mejores estándares sin disrupción.
  - Esencial para la gestión de riesgos y costes a largo plazo.

Conclusión (I)

- **Amenaza cuántica real:** Impulsa la urgencia de PQC ("Cosechar ahora, descifrar después"). Los sistemas actuales (RSA/ECC) serán vulnerables.
- **LBC: El líder ahora mismo**
  - Robusta, eficiente y con fuerte respaldo (NIST: Kyber, Dilithium). $\rightarrow$ PQSC (ML-KEM, ML-DSA)
  - Seguridad basada en problemas matemáticos que resisten ataques cuánticos.

Conclusión (II)

- **Innovación con LBC**
  - Base para primitivas avanzadas como cifrado homomórfico (FHE).
  - Potencial para revolucionar la privacidad y el análisis seguro de datos.
- **En definitiva, LBC es clave para la seguridad y la innovación en las próximas décadas.**