TRABAJO DE FIN DE GRADO · INGENIERÍA MATEMÁTICA

Análisis de Learning With Errors e implementación de esquemas seguros

Seguridad en criptografía postcuántica

Alejandro Martínez Ronda

Tutor: Jorge Calvo Martín

Junio de 2026

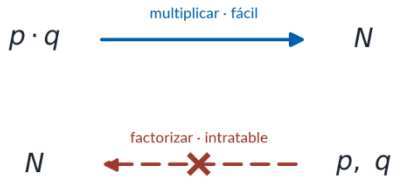
UAX Universidad Alfonso X el Sabio

UAX Universidad Alfonso X el Sabio

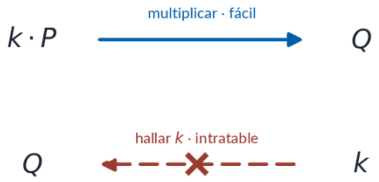
El algoritmo de Shor rompe la clave pública actual

Los dos problemas que hoy la sostienen — y que Shor ataca:

RSA
factorización de enteros



ECC
logaritmo discreto



SHOR · 1994

Convierte ambas inversas en tiempo polinómico – la dureza desaparece en un ordenador cuántico

¿POR QUÉ ACTUAR YA?

01 **Harvest now, decrypt later**

02 **La inercia del despliegue**

03 **La respuesta del NIST**

Retículos: por qué importa la base

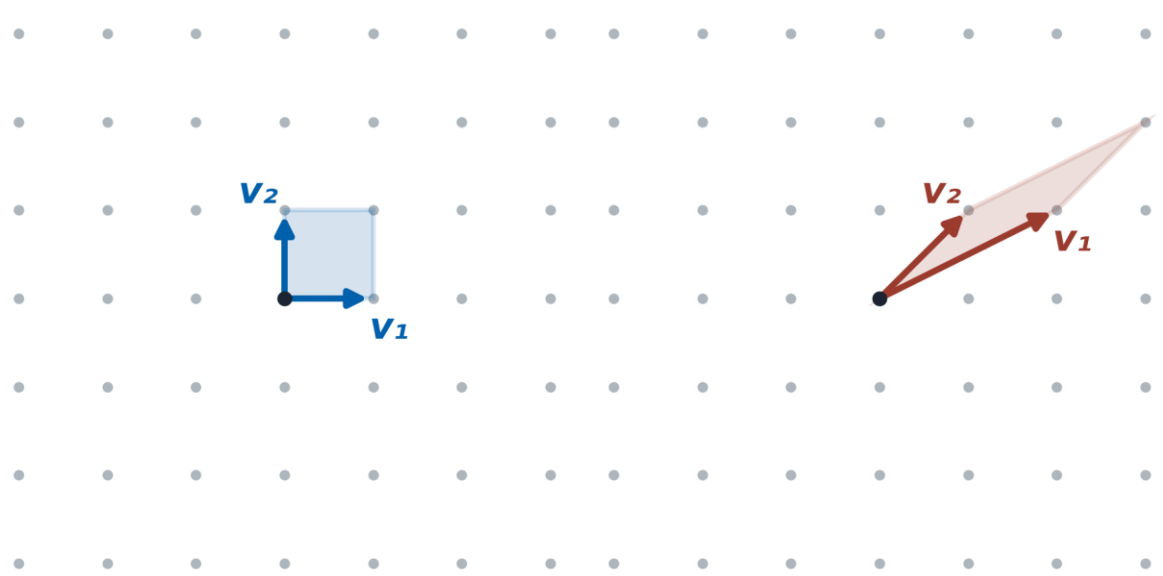
Combinaciones enteras de una base forman una **malla discreta**. Su volumen es invariante: *no se puede acortar todo a la vez.*

SVP el vector no nulo más corto del retículo.

CVP el punto del retículo más cercano a un objetivo externo.

En dimensión alta son difíciles. **LLL y BKZ** son los mejores ataques; el bloque β mide la seguridad.

LA MISMA MALLA, DISTINTA BASE



LWE: un sistema lineal con ruido — búsqueda y decisión

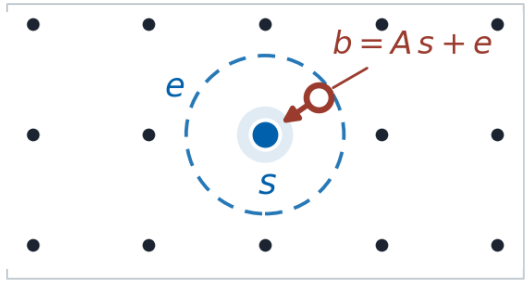
$$b = A \cdot s + e \pmod{q}$$

SIN RUIDO (e = 0)
álgebra lineal resoluble en tiempo polinómico

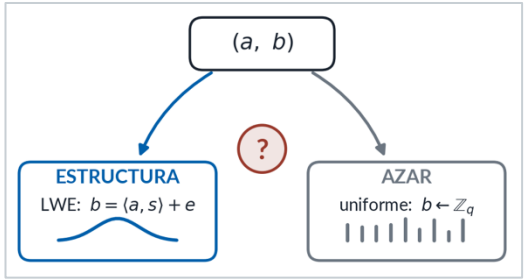
CON RUIDO (e ≠ 0)
sin algoritmo eficiente, clásico ni cuántico

n dimensión → seguridad q módulo → escala σ intensidad del ruido

SEARCH-LWE

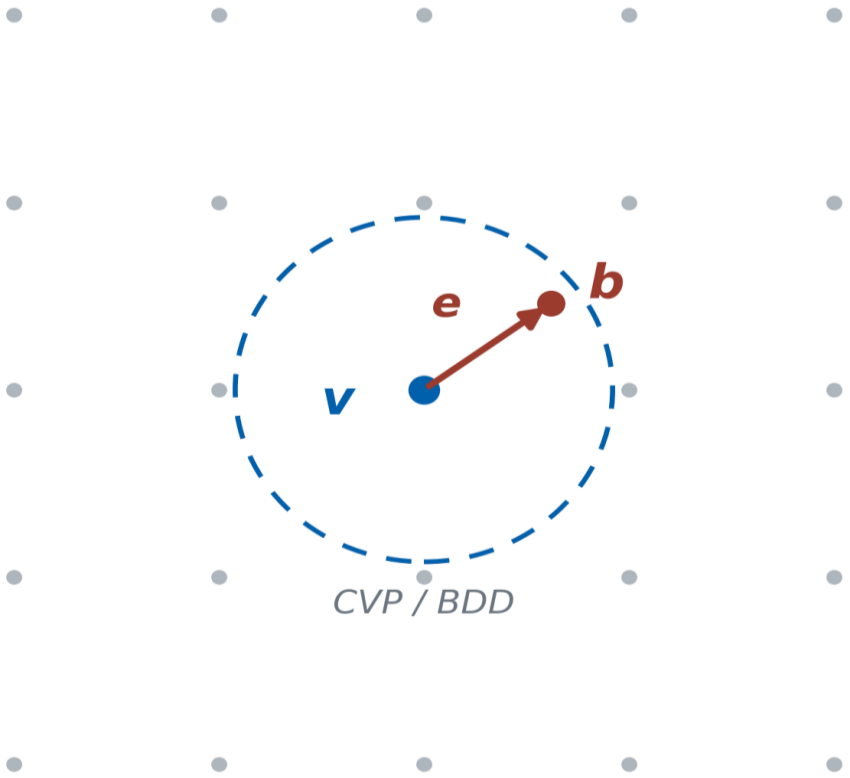


DECISION-LWE



UAX Universidad Alfonso X el Sabio

Interpretación geométrica: recuperar es CVP / BDD



∈ **Punto válido**

Las soluciones exactas $\mathbf{b = A \cdot s \pmod q}$ forman un retículo q-ario.

+e **Desplazamiento por error**

El ruido desplaza la observación: $\mathbf{b = v + e}$, con $v \in L_q(A)$.

min **Recuperación**

Volver a v equivale a hallar el punto del retículo más cercano: **CVP / BDD**.

Lectura dual: $\langle y, b \rangle \equiv \langle y, e \rangle \pmod q$ *— ciertas direcciones cancelan el secreto: base del ataque dual.*

La reducción de Regev (2005)

PEOR CASO

SIVP / GapSVP

retículos · cualquier instancia

PUENTE

Muestreo gaussiano

reducción cuántica

PROMEDIO

Decision-LWE

álgebra · instancia aleatoria

Resolver LWE en promedio resolvería SIVP/GapSVP en cualquier retículo: **la dureza se hereda del peor caso.**

QUÉ GARANTIZA

Un fundamento de dureza sólido, no heurístico.

QUÉ NO

No fija parámetros ni promete seguridad incondicional.

UAX Universidad Alfonso X el Sabio

Cifrado — esquema de Regev

1 Claves

Pública **(A, b)**, $b = A \cdot s + e$

Privada: s.

2 Cifrado del bit μ

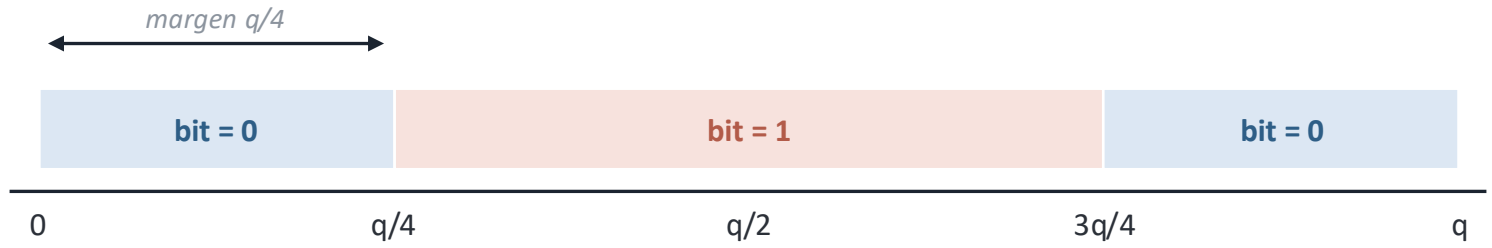
$u = A^T r$

$v = b^T r + \mu \cdot \lfloor q/2 \rfloor$

3 Descifrado

$d = v - \langle u, s \rangle$

aísla el ruido + μ



Si |ruido| < q/4 el bit se recupera; si lo supera, falla.

IDENTIDAD CENTRAL

$$d = e^T r + \mu \cdot \lfloor q/2 \rfloor$$

El secreto se cancela: queda solo el ruido más el bit codificado.

Base conceptual de FrodoKEM y ML-KEM.

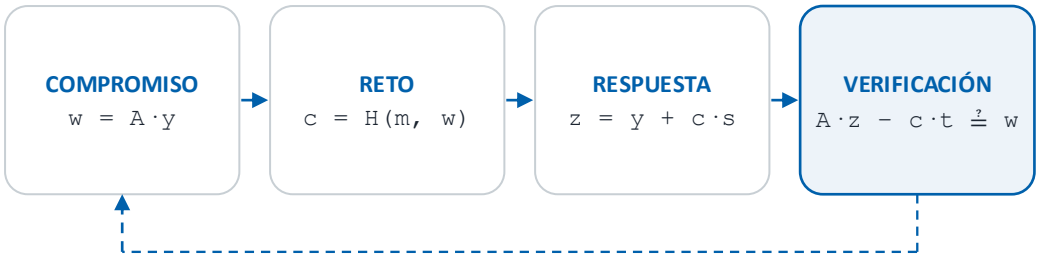
ML-KEM / Kyber y ML-DSA / Dilithium

ML-KEM / KYBER

FIPS 203 · Module-LWE — *encapsulación de claves*

ML-DSA / DILITHIUM

FIPS 204 · Module-SIS — *firma digital*



el reto encadena mensaje y compromiso — falsificar exige resolver Module-SIS

ML-KEM protege el intercambio de claves; **ML-DSA** protege la autenticidad.

UAX Universidad Alfonso X el Sabio

Estado del arte: comparación de KEMs

Todos establecen una clave, así que las cifras son comparables. Tres familias postcuánticas frente a la referencia clásica.

Esquema	Familia	Clave pública	Cifrado / secreto
ECDH P-256	clásico · acuerdo	**≈32 B**	**secreto 32 B**
ML-KEM-768	retículos · Module-LWE	**12KB**	**cifrado 1,1KB**
FrodoKEM-976	retículos · LWE estándar	**15,3KB**	**cifrado ≈15,7KB**
Classic McEliece	códigos	**≈524KB**	**cifrado ≈156B**

ML-KEM y FrodoKEM, cifras del TFG; McEliece, ECDH y RSA, referencia estándar. Las firmas se comparan aparte.

Implementación experimental

OBJETIVO

Observar cómo el **ruido** (σ), el **módulo** (q) y la **dimensión** (n) **afectan a la corrección, al coste y al tamaño de clave** — y por qué eso explica las decisiones de los estándares.

> **Implementación deliberadamente simplificada — no es un sistema desplegable.**
>
> *Se omiten anillos, compresión, reconciliación, Fujisaki–Okamoto y canales laterales.*

PARÁMETROS BASE

n	**64**	dimensión del secreto
q	**257**	módulo primo
σ	**3**	desviación del error
m	**$2n = 128$**	nº de muestras

El ruido define una ventana de funcionamiento

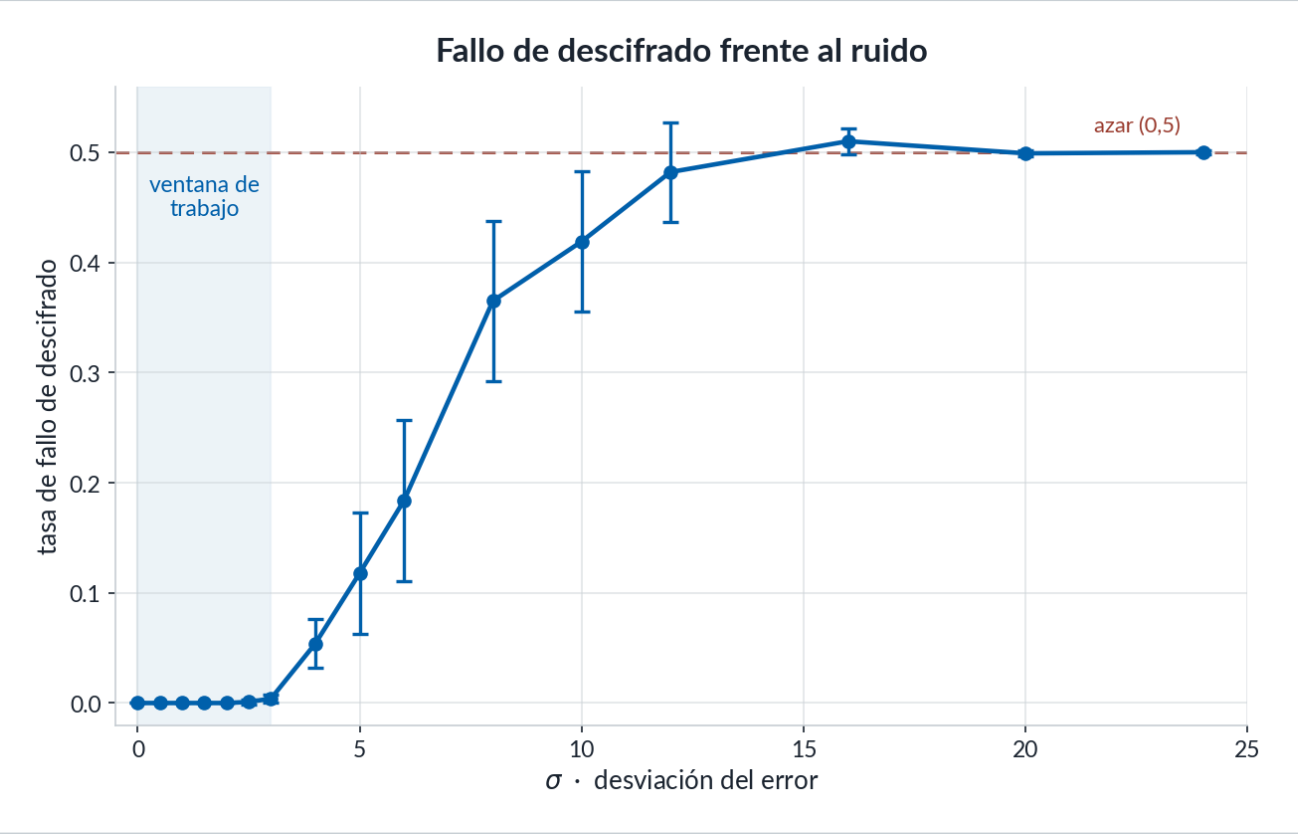
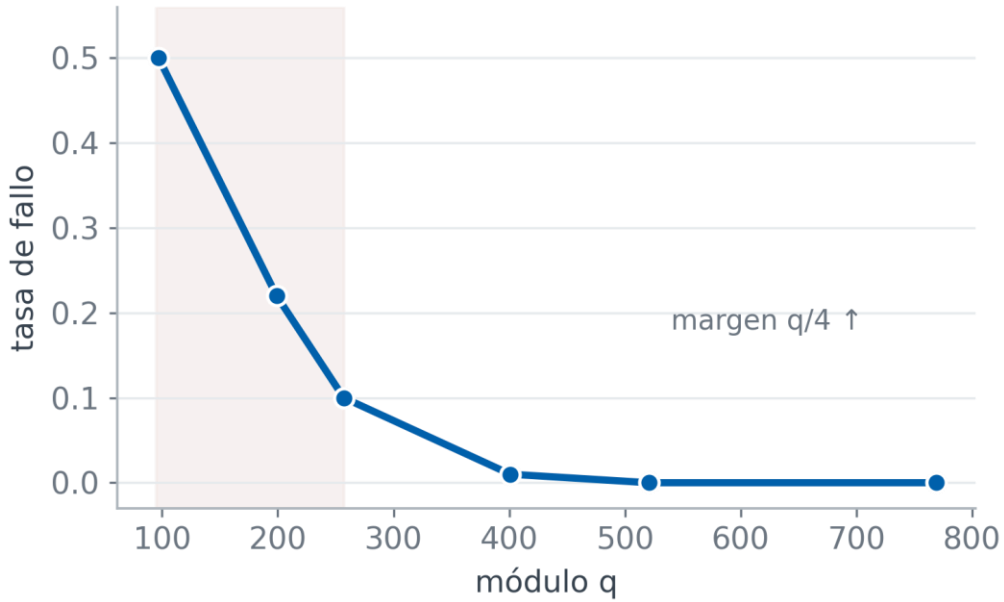


Figura 1 del TFG · tasa de fallo en función de σ (n=64, q=257)

- **σ ≤ 3 fallo ~0 %**
  el ruido 8σ queda bajo q/4 ≈ 64.
- **σ ∈ [4, 8] transición**
  más variabilidad entre claves.
- **σ ≥ 16 fallo ≈ 0,5**
  indistinguible del azar.

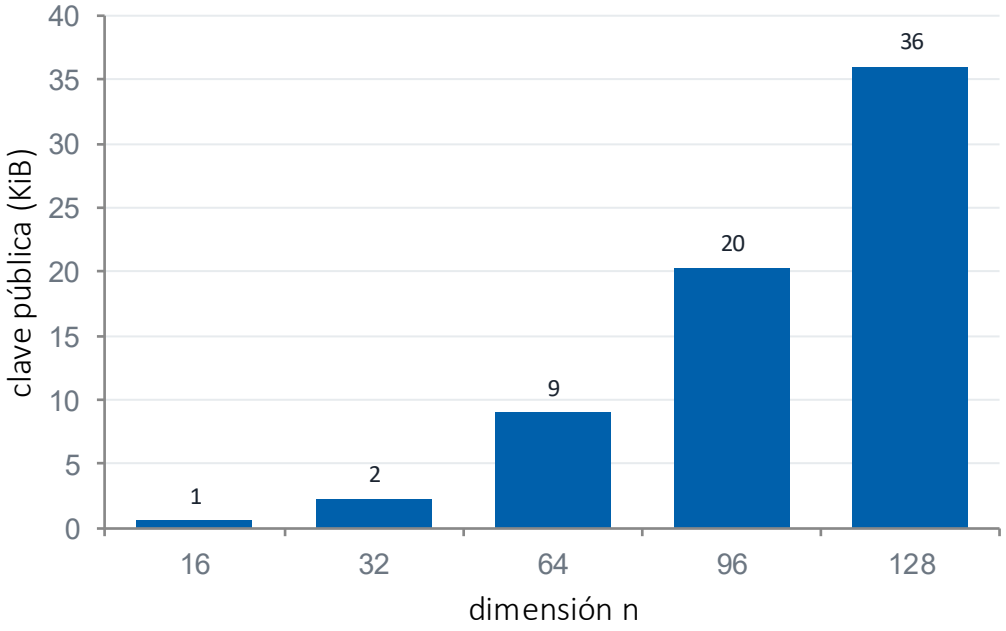
El módulo amplía el margen; la dimensión dispara el coste

FALLO DE DESCIFRADO vs. MÓDULO q



Más q ⇒ más margen q/4 y menos fallo (σ·√(m/2) ≪ q/4).

CLAVE PÚBLICA vs. DIMENSIÓN n



Crecimiento ≈ n^2: por eso los estándares usan Module-LWE con NTT, O(n log n).

Seguridad postcuántica — seguridad cuántica

	PQC · retículos	QKD · BB84
Hardware	✓ Solo software	✗ Canales y HW físicos
Qué cubre	✓ Claves, cifrado y firma	✗ Solo claves
Coste	✓ Bajo	✗ Alto
Distancia	✓ Sin límite práctico - Internet	✗ Limitada – física y canal
Garantía principal	✓ Seguridad computacional postcuántica	✓ Detección física de interceptación

UAX Universidad Alfonso X el Sabio

Conclusiones

1 **Seguridad y corrección comparten parámetros**

2 **El ruido no es un defecto**

3 **Recorrido coherente y desplegable**

> ***Una pequeña cantidad de incertidumbre, introducida en una ecuación matemática exacta, se convierte en unos de los cimientos de la criptografía postcuántica.***

Limitaciones: parámetros ilustrativos · implementación simplificada · ataques a nivel conceptual.

Thank you!
Gracias!

Soy Innovación
Soy Maker
Soy UAX