Ásstery Journal
revistas.educaidscientific.com/index.php/assteryjournal
asstery@educaidscientific.com

Criptografía Post-Cuántica: LWE y Firmas Seguras

Post-Quantum Cryptography: LWE and Secure Signatures

A. Benítez-Rodríguez

0009-0009-5816-8854

Universidad de El Salvador, El Salvador

sebastianbenitez1@protonmail.com

Recibido: 11/12/2024

Aceptado: 10/10/2025

Publicado: 30/12/2025

Citación/como citar este artículo: Benítez-Rodríguez, A. (2025). Criptografía Post-Cuántica: LWE y Firmas Seguras. *Ásstery Journal*, 1(1), 45-51.

Ásstery Journal Vol. 1 Num.1
pp. 45-51

Resumen

Este artículo presenta un análisis del problema Learning with Errors (LWE) en el contexto de la criptografía post-cuántica, destacando su relación con la teoría de reticulados y su aplicabilidad en la construcción de algoritmos seguros frente a la computación cuántica. El artículo examina el uso de LWE en aplicaciones criptográficas clave, como firmas digitales (por ejemplo, BLISS y FALCON). Se discute, además, la resistencia de LWE a los ataques cuánticos, incluyendo el impacto de algoritmos como el de Grover, y se evalúa su robustez en un futuro entorno post-cuántico.

Palabras claves: Learning with Errors, criptografía basada en retículas, criptografía post-cuántica, firmas digitales

Abstract

This article presents an analysis of the Learning with Errors (LWE) problem in the context of post-quantum cryptography, highlighting its relationship with lattice theory and its applicability in constructing algorithms secure against quantum computing. The article examines the use of LWE in key cryptographic applications, such as digital signatures (e.g., BLISS and FALCON). Furthermore, it discusses LWE's resistance to quantum attacks, including the impact of algorithms like Grover's, and evaluates its robustness in a future post-quantum environment.

Keywords: Learning with Errors, lattice-based cryptography, post-quantum cryptography, digital signatures

Introducción

La criptografía post-cuántica (PQC) se ha convertido en un área de investigación crucial debido al potencial de las computadoras cuánticas para romper los sistemas criptográficos actuales. Problemas como Learning with Errors (LWE) son considerados difíciles incluso con el poder de las computadoras cuánticas, lo que los hace adecuados para el diseño de algoritmos resistentes a ataques cuánticos. Diversas investigaciones, como las de Ducas et al. [1] y Howe et al. [2], exploran la aplicabilidad de los reticulados y LWE en el diseño de esquemas de firmas digitales seguros, como BLISS y FALCON, que están siendo considerados como candidatos para la estandarización de la criptografía post-cuántica. En el ámbito cuántico, los avances en algoritmos como el de Grover [3] plantean amenazas significativas para sistemas criptográficos tradicionales, como AES. El trabajo de Grassl [4] analiza cómo el algoritmo de Grover podría reducir la seguridad de los algoritmos de búsqueda no estructurada, lo que afectaría negativamente a los sistemas de cifrado simétrico como AES. Sin embargo, los algoritmos basados en reticulados, como LWE, ofrecen una robustez considerable frente a ataques cuánticos, lo que los posiciona como una alternativa segura. El esquema HAWK [5], desarrollado recientemente, es un ejemplo de firma digital post-cuántica basada en reticulados que muestra un alto grado de seguridad ante potenciales ataques cuánticos, subrayando la viabilidad de la criptografía basada en reticulados para un futuro cuántico.

Definición formal matemática de LWE

A. Lattices

Los lattices o reticulados representan una estructura matemática fundamental que puede visualizarse como una colección infinita de puntos en un espacio, distribuidos de manera regular y ordenada. Imaginemos una red tridimensional perfectamente simétrica que se extiende infinitamente en todas direcciones, donde cada punto está conectado con sus vecinos siguiendo patrones precisos y predecibles. La característica más distintiva de un lattice es que si se toman dos puntos cualquiera de esta estructura y realizamos operaciones básicas como suma o resta de sus coordenadas, invariablemente se llegará a otro punto que también pertenece al mismo lattice.

Desde una perspectiva matemática, un lattice puede definirse como un grupo abeliano libre de dimensión n que abarca el espacio vectorial R_n .. Esto significa que podemos tomar cualquier base del espacio y construir un lattice formando todas las posibles combinaciones lineales de los vectores base, siempre y cuando usemos coeficientes enteros. Una propiedad crucial es que los puntos del lattice mantienen una distancia mínima entre sí y, al mismo tiempo, ningún punto del espacio está “demasiado lejos” de algún punto del lattice, lo que matemáticamente se conoce como conjunto de Delone.

Definamos: Un conjunto de vectores linealmente independiente

$\mathbf{b}_1, \ldots, \mathbf{b}_m \in R^n$; Donde $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_m\}$

El lattice correspondiente a esos vectores será:

$$L = \{ \Sigma_{i=1}{}^{m} a_i \boldsymbol{b}_i \mid a_i \in \mathbb{Z}, b_i \in B$$

En donde describiremos los elementos de esta ecuación:

- **B** La base del Lattice.
- a_i Los coeficientes asociados enteros.

B. Learning with Errors (LWE)

El problema de LWE es un desafío matemático que simula la introducción de ruido controlado en un sistema de ecuaciones lineales. Imaginemos un conjunto de ecuaciones donde cada resultado está ligeramente "distorsionado" por un error pequeño pero aleatorio. El objetivo es recuperar un vector secreto s (clave privada) a partir de múltiples observaciones ruidosas, en donde describimos este vector secreto como:

$$\mathbf{s} = (s_1, s_2, \ldots, s_n) \in Z^n{}_q$$

Y sus ecuaciones lineales:

$a_{1,1} \cdot s_1 + a_{1,2} \cdot s_2 + \ldots + a_{1,n} \cdot s_n \approx a$

$a_{2,1} \cdot s_1 + a_{2,2} \cdot s_2 + \ldots + a_{2,n} \cdot s_n \approx b$

⋮

$a_{m,1} \cdot s_1 + a_{m,2} \cdot s_2 + \ldots + a_{m,n} \cdot s_n \approx m$

Donde "≈" simplemente significa que el valor está cerca de la respuesta real dentro de un cierto margen de error agregado e_i.

C. Algorithm

Para codificarlo basándonos en un contexto matemático, generamos una llave pública utilizando una cantidad aleatoria m de vectores $\mathbf{a}_i$ que pertenecen a $\sum^u{}_p$, generándonos:

$$(\mathbf{a}_i, b_i = \langle \mathbf{s}, \mathbf{a}_i \rangle + e_i) \qquad (2)$$

donde $(\mathbf{a}_i, b_i) | \; i \in \{1, \ldots, m\}$ que sería nuestra llave pública (public key).

Encriptación: Para encriptarlo en un bit, ya sea 0 o 1, tomamos un subconjunto aleatorio S de $\{1, 2 \ldots, m\}$ y luego calculamos:

a) $(\sum_{i \in S} a_i, \sum_{i \in S} b_i)$ si el bit es 0,

b) $(\sum_{i \in S} a_i, p \; / \; 2 + \sum_{i \in S} b_i)$ si el bit es 1.

Desencriptación: Para desencriptar basta con calcular b - ⟨s, a⟩ si el resultado es cercano a 0 que [p/2], retorna 0; en caso contrario, retorna 1.

Construcción de digital signature schemes

Los esquemas de firmas digitales basados en retículas, como CRYSTALS-Dilithium, FALCON, BLISS, HAWN, entre otras, están siendo considerados como alternativas seguras frente a la amenaza de los computadores cuánticos. Estos esquemas aprovechan la complejidad matemática de las retículas, por sus estructuras algebraicas de alta dimensión, para generarnos firmas digitales cuya seguridad se basa en problemas computacionales difíciles de resolver, incluso por computadoras cuánticas. En lugar de depender de la factorización de números grandes o el problema del logaritmo discreto, los esquemas de firma basados en retículas confían en la dificultad de resolver problemas como el *Shortest Vector Problem* (SVP) o el *Learning With Errors* (LWE).

Entre los candidatos oficiales basados en lattices para la estandarización en criptografía post-cuántica del Instituto Nacional de Estándares y Tecnología (NIST) se incluyen CRYSTALS-Dilithium (ML-DSA) y FALCON (FN-DSA) [6], los cuales fueron seleccionados debido a su robustez matemática, eficiencia computacional y seguridad frente a amenazas cuánticas.

A. Firma digital (BLISS)

BLISS (Bimodal Lattice Signature Scheme) utiliza distribuciones gaussianas bimodales para generar un conjunto de valores que aseguren la integridad y autenticidad del mensaje. Matemáticamente, BLISS aprovecha la dificultad de encontrar un vector corto en un retículo, específicamente utilizando una variante del *Shortest Vector Problem* (SVP). Durante la generación de la firma, se utiliza un muestreo gaussiano sobre retículos para crear una firma compacta, mientras que la verificación de la firma es eficiente gracias a la estructura algebraica de los retículos.

B. Firma digital (FALCON)

FALCON (Fast Fourier Lattice-based Compact Signatures over NTRU) es un esquema de firma digital avanzado que se basa en la estructura matemática del algoritmo NTRU para la encriptación asimétrica. Este esquema se destaca por su eficiencia computacional y por la compacidad de las firmas generadas, lo que lo hace adecuado para su implementación en entornos con recursos limitados. Además, su seguridad se fundamenta en problemas difíciles de resolver dentro de la teoría de los retículos, ofreciendo resistencia a ataques cuánticos.

C. Firma digital (HAWN)

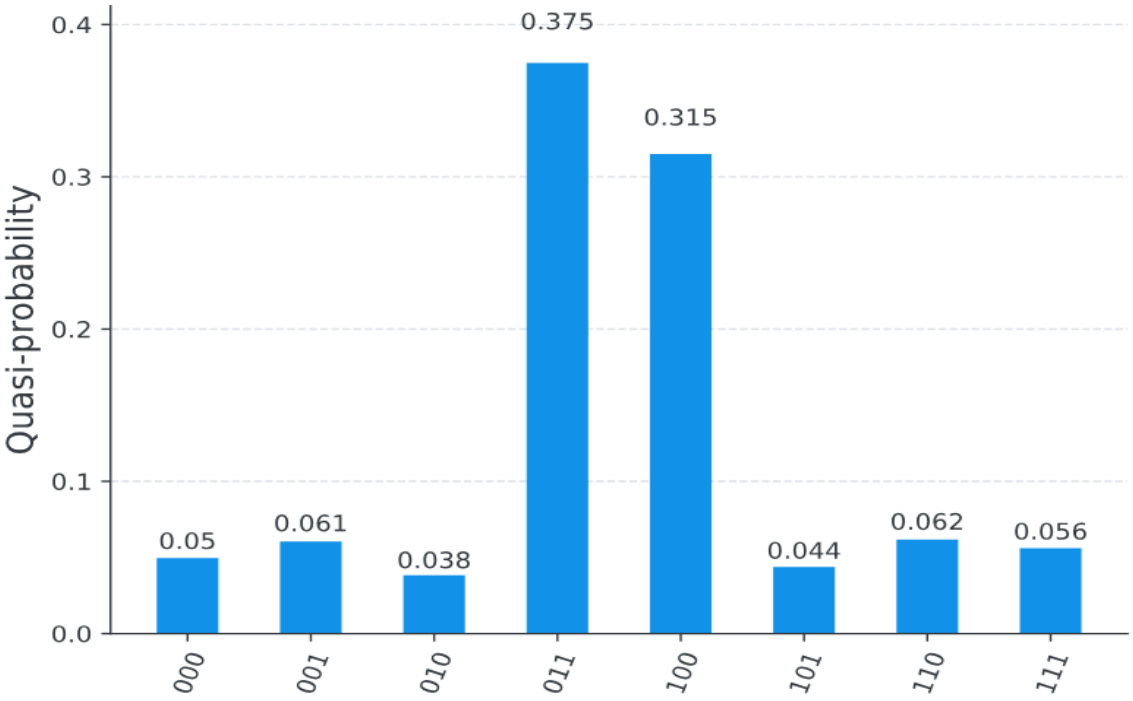
HAWN es un esquema de firma digital basado en transformaciones algebraicas no lineales. Su seguridad se deriva de problemas computacionales complejos, como el *Shortest Vector Problem* (SVP), que proporcionan una base sólida frente a ataques,

incluyendo los cuánticos. HAWN genera firmas compactas y eficientes mediante operaciones vectoriales en espacios de alta dimensionalidad. Su proceso de firma incluye técnicas probabilísticas, como el muestreo gaussiano sobre retículos y perturbaciones controladas, que incrementan la imprevisibilidad de la firma. Este diseño matemático asegura una verificación computacionalmente eficiente, al tiempo que mantiene niveles elevados de seguridad.

Ataques cuánticos y robustez: Resistencia al algoritmo de Grover

Definición: El algoritmo de Grover es un algoritmo cuántico diseñado para resolver problemas de búsqueda no estructurada de manera más eficiente que los algoritmos clásicos. En esencia, ofrece una mejora cuadrática al reducir el número de operaciones necesarias para encontrar un elemento específico en una base de datos no ordenada. Clásicamente, una búsqueda no estructurada de N elementos requiere O(N) operaciones, pero el algoritmo de Grover puede realizar la misma tarea en O(√{N}) operaciones. [3]

Figura 1. *Resultados de la implementación del algoritmo de Grover en formato clásico utilizando Python.*



Conclusión

Finalmente, la criptografía basada en retículos, especialmente a través de problemas como *Learning with Errors* (LWE), ofrece una robustez significativa frente a los desafíos que plantea la computación cuántica. A medida que los avances en computación cuántica continúan, es crucial desarrollar esquemas de criptografía que

puedan resistir los ataques cuánticos, y los algoritmos basados en retículos se presentan como una solución prometedora. Investigaciones recientes, como las que exploran el impacto de algoritmos como Grover y el desarrollo de esquemas de firmas digitales post-cuánticas como HAWK, demuestran que las técnicas basadas en LWE y retículos no solo son seguras en el entorno cuántico, sino también eficientes en términos de computación. Así, la criptografía post-cuántica está bien posicionada para jugar un papel clave en la protección de la información en un futuro dominado por algoritmos cuánticos, computadoras cuánticas o computadoras híbridas (cuántico-clásicas).

Referencias

Ducas, L., Durmus, A., Lepoint, T., & Lyubashevsky, V. (2013). *Lattice signatures and bimodal Gaussians*. Cryptology ePrint Archive, Paper 2013/383.

Howe, J., Pöppelmann, T., O'Neill, M., O'Sullivan, E., & Güneysu, T. (2023). *Practical lattice-based digital signature schemes*. In *Cryptography Conference* (Horst Görtz Institute for IT-Security, Ruhr-University Bochum). Belfast, UK & Bochum, Germany.

IBM. (2024). *Grover's algorithm*. In *Fundamentals of quantum algorithms*. https://learning.quantum.ibm.com/course/fundamentals-of-quantum-algorithms/grovers-algorithm

Grassl, M., Langenberg, B., Roetteler, M., & Steinwandt, R. (2016). Applying Grover's algorithm to AES: Quantum resource estimates. In T. Takagi (Ed.), *Post-quantum cryptography*. Springer International Publishing.

Bos, J. W., Bronchain, O., Ducas, L., Fehr, S., Huang, Y.-H., Pornin, T., Postlethwaite, E. W., Prest, T., Pulles, L. N., & van Woerden, W. (2024). *Hawk: A post-quantum signature scheme* (Version 1.0.2, September 26, 2024).

National Institute of Standards and Technology. (2024). *Post-quantum cryptography: Additional digital signature schemes*. https://csrc.nist.gov/projects/pqc-dig-sig

asecuritysite.com. (2024). *Public key encryption with Learning With Errors (LWE)*. https://asecuritysite.com/encryption/lwe2