Criptografía basada en retículos

Alba Larraya Sancho

Trabajo de fin de grado de Matemáticas
Universidad de Zaragoza

Directores del trabajo: Álvaro Lozano Rojo y Miguel Ángel Marco Buzunariz

Fecha:12-09-2022

Resumen

A lo largo de este trabajo estudiamos una de las ramas de la criptografía post-cuántica, la criptografía basada en retículos. Para ello, veremos en primer lugar un ejemplo de un criptosistema que nos sirve como base para muchos criptosistemas eficientes.

Vamos a ver también los fundamentos de la teoría de retículos, unas definiciones básicas y algunos resultados importantes para la aplicación a la criptografía, veremos también algunos problemas que se consideran difíciles, ya que en ellos se basa la seguridad de los criptosistemas.

A continuación hablaremos sobre la distribución gaussiana discreta, ya que en muchos casos vamos a necesitar obtener muestras en $\mathbb{Z}^n$, y por lo tanto vamos a necesitar una distribución discreta que se comporte como una distribución gaussiana continua.

Luego trataremos el problema LWE (Learning With Errors), que es uno de los principales problemas computacionales, considerado difícil cuando lo aplicamos a retículos, y en el cual se basa el criptosistema que utilizamos de ejemplo.

Después, veremos el criptosistema utilizado más en detalle, probando que es seguro cuánticamente.

Para concluir vamos a hablar de tres algoritmos basados en retículos que han sido aceptados por el NIST para el estándar de criptografía post-cuántica.

Abstract

In this paper we are going to study lattice-based cryptography, a branch of the field of post-quantum cryptography. To do this, we will first see an example of a cryptosystem that serves as basis for many others efficient cryptosystems.

We will explain the fundamentals of lattice theory, some basic definitions and important results for the applications to cryptography. We will also see some of the hard problems in lattices, since the security of the cryptosystems is based on them.

Next, we will talk about the discrete Gaussian distribution, since in many cases we will need to obtain Gaussian samples from $\mathbb{Z}^n$, and then we will need a discrete distribution that behaves like the Gaussian distribution.

We will then talk about the Learning With Errors problem, one of the main computational problems, considered hard when applied to lattices. The cryptosystem in our example is based in this problem.

Next, we will analyse the cryptosystem and we will prove that it is quantum secure.

We will conclude talking about three algorithms based in lattices that have been approved for the post-quantum cryptography standard.

Índice general

Resumen III

Abstract V

1. Introducción 1

2. Teoría de retículos 3
2.1. Bases de teoría de retículos . . . 3
2.1.1. Definiciones . . . 3
2.1.2. Acotaciones de la distancia mínima . . . 6
2.2. Problemas difíciles . . . 10

3. Gaussianos discretos 11

4. Learning With Errors 15
4.1. Definición del problema . . . 15
4.1.1. Búsqueda LWE . . . 15
4.1.2. Decisión LWE . . . 16
4.2. Propiedades de LWE . . . 16
4.2.1. Equivalencia de la búsqueda/decisión de LWE . . . 16
4.2.2. LWE en retículos . . . 17
4.3. Forma hermítica del LWE . . . 17
4.4. Dificultad del problema $\mathrm{LWE}_{s,\bar{\Psi}_\alpha}$ . . . 18

5. Criptosistema de clave pública usando LWE 19
5.1. Presentación del algoritmo . . . 19
5.2. Seguridad del criptosistema . . . 20
5.3. Left Over Hash Lemma . . . 22

6. Conclusiones 25

A. Problemas difíciles en retículos 27
A.1. Problemas . . . 27
A.2. Algoritmo de resolución LLL . . . 28
A.2.1. Algoritmo LLL . . . 29
A.3. Diagrama de relaciones entre los problemas. . . . 29

Bibliografía 31

Capítulo 1

Introducción

Los ordenadores cuánticos, si llegan a desarrollarse, serán capaces de romper los protocolos de cifrado actuales, como el RSA o los algoritmos basados en el problema del logaritmo discreto, mediante una variante del algoritmo de Shor, un algoritmo cuántico para descomponer en factores un número N en tiempo $O((\log N)^3)$. Esto crea la necesidad de desarrollar nuevos algoritmos resistentes frente a los ataques de estos ordenadores, y a todo este conjunto de algoritmos es lo que denominamos criptografía post-cuántica. Una de las ramas de ésta es la criptografía basada en retículos, en la que nos centramos en el trabajo.

Cabe remarcar que el pasado 5 de Julio de 2022 el NIST seleccionó cuatro algoritmos de cifrado que pasarán a formar parte del estándar criptográfico post cuántico, tres de los cuales están basados en la teoría de retículos.

En este trabajo nos centraremos en el algoritmo de clave pública propuesto por Regev, basado en el problema de Learning With Errors, un problema computacional que se considera difícil cuánticamente, ya que se puede reducir a problemas difíciles en retículos. Este problema consiste en encontrar un vector $s \in \mathbb{Z}_q^n$ a partir del par (A,b), donde A es una matriz y b se ha obtenido mediante la ecuación $b^t = s^t A + e^t$. Vemos en primer lugar un ejemplo de este algoritmo:

En primer lugar contamos con una matriz pública, que forma parte del estándar, a la que llamamos A, que es elegida uniformemente en $\mathbb{Z}_q^{n\times m}$. En este ejemplo, por motivos de simplicidad tomamos $n = 3$, $m = 17$ y $q = 17$. Nuestra matriz A es la siguiente:

$$\begin{pmatrix} 14 & 9 & 5 & 14 & 7 & 6 & 8 & 4 & 15 & 9 & 2 & 7 & 14 & 7 & 12 & 4 & 14 \\ 3 & 14 & 7 & 16 & 3 & 15 & 3 & 15 & 4 & 3 & 9 & 9 & 11 & 6 & 8 & 5 & 4 \\ 6 & 3 & 8 & 6 & 5 & 9 & 16 & 9 & 5 & 11 & 15 & 1 & 0 & 13 & 16 & 12 & 14 \end{pmatrix}$$

La clave secreta de Alice es el vector entero $s = \begin{pmatrix} 13 \\ 5 \\ 8 \end{pmatrix} \in \mathbb{Z}_q^n$, y calculamos la clave pública de Alice, $b \in \mathbb{Z}_q^m$, mediante la ecuación:

$$b^t = s^t A + e^t, \tag{1.1}$$

donde e es un vector tomado aleatoriamente en $\mathbb{Z}_q^m$, mediante una distribución que nos da vectores cortos con alta probabilidad. Entendemos que un vector es corto cuando cada coordenada es pequeña, en el caso de vectores en $\mathbb{Z}_q^n$, cuando las coordenadas están en $\left(\frac{-q}{4}, \frac{q}{4}\right)$. Si tomamos el siguiente vector balanceado, esto es, que todos los elementos módulo q están entre $-q/2$ y $q/2$

$$e^t = (-1,-2,1,-1,-3,1,0,-3,-1,0,-2,0,4,2,1,2,2)$$

obtenemos que la clave pública de Alice es:

$$b^t = (6,5,12,3,7,5,9,9,16,16,2,8,3,6,2,5,10)$$

Suponemos que Bob quiere enviarle a Alice un mensaje $bit = 0$, entonces, Bob elige un vector $x \in \{0,1\}^m$ efímero de manera uniformemente aleatoria, y envia a Alice el par (u, u'), donde

$$u = Ax$$

$$u' = b^t x$$

En nuestro caso, si tomamos

$$x = (1,1,1,0,1,1,1,1,0,0,1,1,0,0,0,1,1)$$

obtendremos

$$u = (12,2,13)$$

$$u' = 10$$

Si por el contrario Bob quiere enviarle a Alice un mensaje $bit = 1$, entonces, Bob enviará a Alice el par (u, u'), donde

$$u = Ax$$

$$u' = b^t x + \lfloor \frac{q \cdot bit}{2} \rfloor$$

En este caso,

$$u = (12,2,13)$$

$$u' = 1$$

Entonces, para decodificar el mensaje, Alice calcula $s^t u$ y lo compara con u', si son próximos, el bit codificado es 0.

Cuando Alice calcula $s^t u$ obtiene $s^t u = 15$, luego si recibe $u' = 13$, puede saber que el bit es un 0, ya que la diferencia módulo 17 es pequeña, $s^t u - u' = 2$. Mientras que si recibe $u' = 1$, la diferencia es $s^t u - u' = 14$, luego la diferencia es grande y puede saber que el bit enviado es 1.

A lo largo del trabajo vamos a explicar las bases teóricas en las que se basa este sistema y su seguridad. Vamos a comenzar viendo las bases de la teoría de retículos, ya que la clave pública de Alice, b, es un elemento muy próximo al retículo generado por las columnas de A módulo q, luego la seguridad de la clave secreta se basa en la dificultad de hallar el elemento del retículo más próximo a b.

Capítulo 2

Teoría de retículos

En este capítulo tratamos las bases de la teoría de retículos y vemos cómo se relacionan con el algoritmo explicado en la introducción.

2.1. Bases de teoría de retículos

2.1.1. Definiciones

Definimos un retículo $\mathscr{L}$ como un subgrupo discreto de $\mathbb{R}^n$. Consideramos retículos enteros y de rango completo, por tanto, $\mathscr{L}$ está contenido en $\mathbb{Z}^n$ y recubre $\mathbb{R}^n$ con coeficientes reales, esto es, la clausura lineal sobre $\mathbb{R}$ es $\mathbb{R}^n$. Por tanto, $\dim\mathscr{L} = n$.

Definición 1. (Base de un retículo) Llamamos base de un retículo $\mathscr{L}$ a un conjunto ordenado y minimal $\mathbb{B} = (b_1, ..., b_m)$ de $\mathscr{L}$, tal que

$$\mathscr{L} = \mathscr{L}(\mathbb{B}) = \mathbb{B} \cdot \mathbb{Z}^m = \left\{ \sum_{i=1}^{m} c_i \cdot b_i : c_i \in \mathbb{Z} \right\} \tag{2.1}$$

Dado $k \in \mathbb{R}^m$ un vector columna, escribimos $\mathbb{B} \cdot k = k_1 b_1 + \cdots + k_m b_m$ el elemento de $\mathbb{R}^m$ con coordenadas k respecto a la base $\mathbb{B}$. Si tenemos un sistema generador de un retículo tal que los vectores no son libres, es siempre posible construir otro sistema generador que tenga n vectores libres, esto es, que sea libre, y por tanto, base.

Dada una matriz $A = (a_1 | \cdots | a_m)$ en $\mathbb{Z}^{n \times m}$, definimos el retículo

$$\mathscr{L}_A(s) = \left\{ x \in \mathbb{Z}^m : s^t A \equiv x \mod q \right\} \subset \mathbb{Z}^m \text{ , para algún } s \in \mathbb{Z}_q^n, \tag{2.2}$$

generado por la matriz $\tilde{A} = \left(\frac{A}{qI_n} \right)$, donde añadimos la segunda parte de la matriz porque trabajamos en módulo q. Por tanto, en nuestro ejemplo tenemos que $s^t A$ es un elemento de este retículo, con coordenadas s, y la clave pública de Alice es una perturbación de este elemento.

Definición 2. (Paralelepípedo fundamental) Llamamos paralelepípedo fundamental de una base $\mathbb{B}$ al conjunto

$$P(\mathbb{B}) = \mathbb{B} \cdot \left[-\frac{1}{2}, \frac{1}{2} \right)^m = \left\{ \sum_{i=1}^{m} \alpha_i \cdot b_i : -\frac{1}{2} \leq \alpha_i < \frac{1}{2} \right\} \tag{2.3}$$

Este conjunto no depende únicamente del retículo, sino también de la base $\mathbb{B}$. Intuitivamente, podemos decir que $\mathbb{B}$ es una 'buena' base de $\mathscr{L}$ si el paralelepípedo tiene forma aproximadamente de ortoedro, mientras que una 'mala' base nos da un paralelepípedo delgado. Podemos ver la diferencia ilustrada en las figuras 2.1 y 2.2

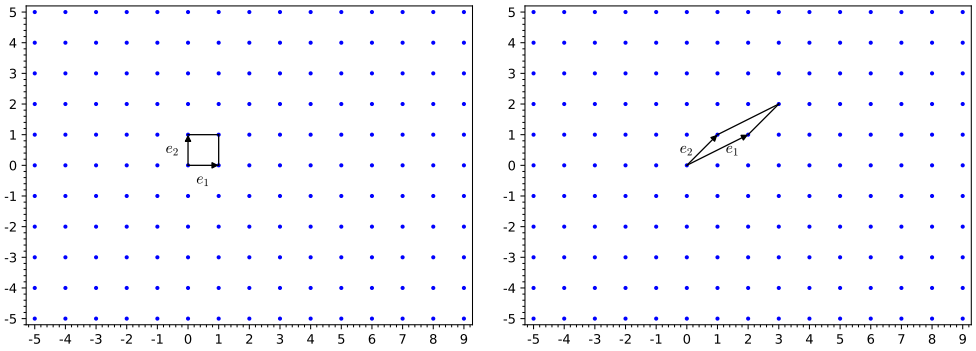


Figura 2.1: Comparación de una base que se puede considerar 'buena' a la izquierda, y una que se puede considerar 'mala' a la derecha, en $\mathbb{Z}^2$

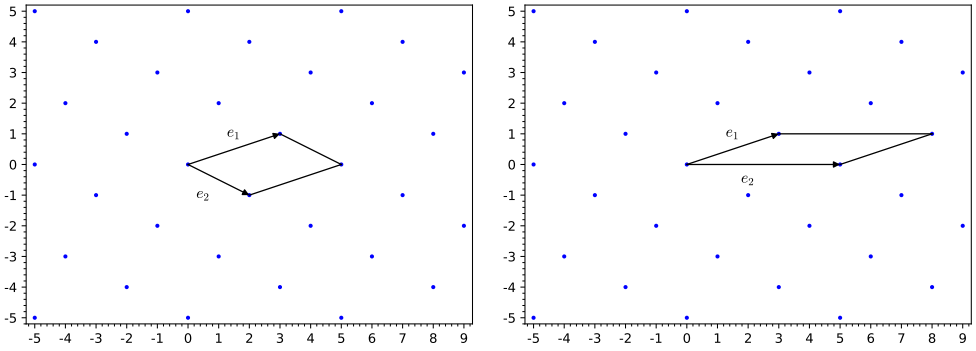


Figura 2.2: Comparación de una base que se puede considerar 'buena' a la izquierda, y una que se puede considerar 'mala' a la derecha, en el retículo generado por los vectores $(3,1),(2,-1)$

En las figuras podemos observar que cuanto más pequeño es el retículo, esto es, cuando tiene menos puntos, más grande es el paralelepípedo fundamental.

Lema 1. Las traslaciones del paralelepípedo fundamental por vectores de $\mathscr{L}$ son un recubrimiento de $\mathbb{R}^n$ sin superposiciones, esto es,

$$\mathbb{R}^n = \bigcup_{v\in\mathscr{L}} (v + P(\mathbb{B})) \tag{2.4}$$

Demostración. Sabemos que $\mathscr{L}$ recubre $\mathbb{R}^n$ con coeficientes reales, por tanto, para todo $p \in \mathbb{R}^n$, existen coeficientes reales $x_1,\ldots,x_n \in \mathbb{R}$ tales que

$$p = \sum_i x_i b_i = \sum_i \lceil x_i \rfloor b_i + \sum_i (x_i - \lceil x_i \rfloor) b_i$$

donde $\lceil a \rfloor$ es el redondeo de a, esto es, el único número entero tal que $-\frac{1}{2} \leq a - \lceil a \rfloor < \frac{1}{2}$.
Luego tenemos que $\sum_i \lceil x_i \rfloor b_i \in \mathscr{L}$ y $\sum_i (x_i - \lceil x_i \rfloor) b_i \in P(\mathbb{B})$.

Por tanto, p está en $\mathbb{R}^n = \bigcup_{v\in\mathscr{L}} (v + P(\mathbb{B}))$. Solo falta probar que no hay superposiciones entre las distintas traslaciones del paralelepípedo fundamental. Si existen $v_1, v_2 \in \mathscr{L}$ distintos tales que

$$(v_1 + P(\mathbb{B})) \cap (v_2 + P(\mathbb{B})) \neq \emptyset$$

obtenemos que $v_1 + \alpha = v_2 + \beta$ para ciertos α y β en $P(\mathbb{B})$, luego $v_1 - v_2 = \beta - \alpha$, y como $v_1 - v_2$ es combinación $\mathbb{Z}$-lineal de los vectores de la base mientras que $\beta - \alpha$ es combinación $(-1,1)-$lineal, necesariamente ambos deben ser nulos. Obtenemos por lo tanto el resultado. □

Notemos que se puede considerar una clase de $\mathbb{R}^n/\mathscr{L}$ como $v+\mathscr{L}$ una traslación del retículo $\mathscr{L}$ por un vector v de $\mathbb{R}^n$.

Lema 2. Cada clase de $\mathbb{R}^n/\mathscr{L}$ tiene un único representante en el paralelepípedo fundamental.

Demostración. Tomamos v como representante de la clase $v+\mathscr{L}$. Como hemos probado que

$$\mathbb{R}^n = \bigcup_{w\in\mathscr{L}} (w+P(\mathbb{B}))$$

cubre $\mathbb{R}^n$ sin superposiciones, existe un único $w \in \mathscr{L}$ tal que $v \in w+P(\mathbb{B})$, luego $v-w \in P(\mathbb{B})$ y por tanto,

$$v+\mathscr{L} = (v-w)+\mathscr{L}+w = (v-w)+\mathscr{L}$$

ya que $w \in \mathscr{L}$. Así, $v-w$ es un representante de la clase $v+\mathscr{L}$ y está en $P(\mathbb{B})$. Por tanto, solo nos queda probar que es único. Suponemos que existen $v_1, v_2 \in P(\mathbb{B})$ tales que

$$v_1+\mathscr{L} = v_2+\mathscr{L}$$

donde

$$v_1 = \sum_j c_{1j}b_j, \quad v_2 = \sum_j c_{2j}b_j$$

y $-1/2 \le c_{ij} < 1/2$ para $i = 1,2$. Así obtenemos que

$$v_1 - v_2 = \sum (c_{1j}-c_{2j})b_j \in \mathscr{L}.$$

Por tanto, $c_{1j}-c_{2j} \in \mathbb{Z}$ para todo j, y entonces, como $-1 < c_{1j}-c_{2j} < 1$, necesariamente $c_{1j}-c_{2j} = 0$ para todo j. Así, $v_1 = v_2$, y el representante es único. □

Por tanto, el paralelepípedo fundamental es un dominio fundamental de $\mathbb{R}^n/\mathscr{L}$. Como podemos encontrar muchas bases de $\mathscr{L}$, podemos obtener muchos dominios fundamentales.

Un retículo $\mathscr{L}$ puede estar generado por muchas bases distintas, pero el valor absoluto del determinante de los vectores de la base es constante, ya que el cambio de base debe pertenecer a $SL_n(\mathbb{Z})$, luego tenemos que si $\mathbb{B}'$ es otra base de $\mathscr{L}$, existe una matriz $U \in SL_n(\mathbb{Z})$ tal que $\mathbb{B} = \mathbb{B}'U$. DE manera que $\det(\mathbb{B}) = \det(\mathbb{B}')\cdot\det(U) = \det(\mathbb{B}')$. Por tanto, el valor absoluto del determinante no depende de la base. Así, podemos definir el determinante de $\mathscr{L}$ como dicho valor absoluto. Además, se puede ver que este determinante también es igual al número de clases de $\mathbb{Z}^n/\mathscr{L}$ por la forma normal de Smith, y al volumen del paralelepípedo fundamental.

$$\det(\mathscr{L}) := |\det\mathbb{B}| = |\mathbb{Z}^n/\mathscr{L}| = vol(P(\mathbb{B})) \tag{2.5}$$

Podemos encontrar la demostración de esta igualdad en [1]. La demostración de que $|\det\mathbb{B}| = |\mathbb{Z}^n/\mathscr{L}|$ se basa en escribir la matriz $\mathbb{B}$ como $\mathbb{B} = P\cdot S\cdot Q$, con P, Q invertibles y de determinante ± 1, y S la forma normal de Smith, explicada en [7]. Se utiliza además el Teorema de Estructura de los módulos sobre DIP para ver que el cardinal del cociente coincide con el valor absoluto del determinante de $\mathbb{B}$.

Definición 3. Si $\mathscr{L} \subset \mathbb{Z}^n$ es un retículo, definimos su dual como

$$\mathscr{L}^* = \{x \in \mathbb{R}^n : x\cdot y \in \mathbb{Z}, \forall y \in \mathscr{L}\} \tag{2.6}$$

Podemos notar que $\det(\mathscr{L}^*) = (\det(\mathscr{L}))^{-1}$. Si $\mathscr{L}$ es un retículo de rango completo con base $\mathbb{B}$,

$$y \in \mathscr{L}^* \Leftrightarrow \mathbb{B}^T y \in \mathbb{Z}^n \Leftrightarrow y \in (\mathbb{B}^T)^{-1}\mathbb{Z}^n,$$

luego $(\mathbb{B}^T)^{-1}$ es una base del retículo dual.

Así, obtenemos $\det(\mathscr{L}^*) = \det((\mathbb{B}^T)^{-1}) = \frac{1}{\det(\mathbb{B}^T)} = \frac{1}{\det(\mathbb{B})} = \det(\mathbb{B})^{-1} = \det(\mathscr{L})^{-1}$.

Por ejemplo, para todo $t > 0$ el retículo dual de $t\mathbb{Z}^n$ es $\frac{1}{t}\mathbb{Z}^n$.

Si tenemos el retículo $\mathscr{L}$ generado por los vectores $(2,-1,0),(0,1,2),(-1,0,2)$, entonces el retículo dual está generado por los vectores $(\frac{1}{3},\frac{2}{3},\frac{1}{6}),(0,1,0),(0,0,\frac{1}{2})$.

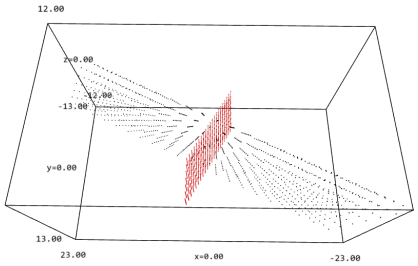


Figura 2.3: En negro tenemos $\mathscr{L}$ y en rojo, su dual.

2.1.2. Acotaciones de la distancia mínima

Nos interesamos ahora en la norma de los vectores del retículo, ya que varios de los problemas más difíciles en retículos se basan en la dificultad de encontrar el vector con norma mínima.

Mínimos sucesivos

Podemos definir los mínimos sucesivos de vectores del retículo $\mathscr{L}$ como sigue:

- $\lambda_1(\mathscr{L}) := \text{mín}_{v\in\mathscr{L}\setminus\{0\}} ||v|| = \text{mín}_{x\neq y\in\mathscr{L}} ||x-y||$
- $\lambda_i(\mathscr{L}) := \text{mín}\{r : \mathscr{L}$ contiene i vectores linealmente independientes de longitud $\leq r\}$

Entonces tenemos que:

$$\lambda_1(\mathscr{L}) \leq \lambda_2(\mathscr{L}) \leq \cdots \leq \lambda_n(\mathscr{L})$$

Tomamos $v_1,\ldots,v_n$ elementos de $\mathscr{L}$ tales que $\|v_i\| = \lambda_i(\mathscr{L})$. Esta familia no es necesariamente una base.

Por ejemplo, si tomamos $n > 4$ y el retículo definido por

$$\mathscr{L} = \left\{ \sum_{i=1}^{n} \mu_i 2e_i + \mu(1,1,\ldots,1), \mu_i \in \mathbb{Z} \forall i, \mu \in \mathbb{Z} \right\} \tag{2.7}$$

Entonces, $v \in \mathscr{L}$ si y solo si $v_1 = v_2 = \cdots = v_n \mod 2$, ya que si $\mu = 0$, $v_1 = v_2 = \cdots = v_n = 0 \mod 2$, y si $\mu \neq 0$, $v_1 = v_2 = \cdots = v_n = 1 \mod 2$ para todo vector del retículo.
Vamos a ver que podemos tomar n vectores de $\mathscr{L}$ independientes y tales que $\|u_i\| = \lambda_i(\mathscr{L})$ pero que no forman una base del retículo. En primer lugar calculamos los mínimos sucesivos:

$\lambda_1(\mathscr{L}) = \text{mín}_{0\neq v\in\mathscr{L}} \|v\| = 2$ ya que $\|2e_i\| < \|(1,1,\ldots,1)\|$ y para todo vector que sea combinación lineal de los vectores $(1,1,\ldots,1), 2e_i$ para todo $i = 1,\ldots,n$, la norma euclídea será mayor.

Como todos los vectores $2e_1,\ldots,2e_n$ son independientes y de norma 2, obtenemos $\lambda_i(\mathscr{L}) = 2$ para i de 2 hasta n.

No podemos tener λ_{n+1} ya que la base del retículo en $\mathbb{Z}^n$ tiene $n+1$ vectores, luego no son independientes.

Por tanto, los vectores correspondientes a los mínimos sucesivos son $\{2e_1,\ldots,2e_n\}$, que sin embargo no son una base de $\mathscr{L}$, ya que $(1,\ldots,1)$ es un elemento de $\mathscr{L}$ y sin embargo no se puede escribir como combinación lineal de $\{2e_1,\ldots,2e_n\}$.

Gracias a este ejemplo podemos observar también una diferencia entre los espacios vectoriales y los retículos, ya que en un espacio vectorial, un sistema generador minimal es también un sistema de vectores libres maximal, mientras que en este ejemplo tenemos una base del retículo, sistema generador

minimal, que no es un sistema de vectores libres maximal, ya que los vectores del sistema generador no son independientes.

A continuación, vamos a acotar tanto superiormente como inferiormente los mínimos sucesivos, en particular λ_1, ya que esto puede ayudarnos a conocer la norma del vector más corto en nuestro retículo.

Acotación inferior

Vamos a ver en primer lugar cómo podemos acotar inferiormente $\lambda_1(\mathscr{L})$, esto es, cómo podemos encontrar una cota inferior para la norma más pequeña de los vectores del retículo.

Una manera de obtener dicha cota de λ_1 consiste en utilizar la ortogonalización de Gram-Schmidt $\tilde{\mathbb{B}}$ de una base $\mathbb{B}$ de $\mathscr{L}$. Notar que no usamos la ortonormalización de Gram-Schmidt, por lo que los vectores de $\tilde{\mathbb{B}}$ son ortogonales entre sí pero no tienen norma 1. Si $\tilde{\mathbb{B}}$ es esta ortogonalización de la base $\mathbb{B}$ tenemos:

$$\mathbb{B} = \tilde{\mathbb{B}} \begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \tag{2.8}$$

Lema 3. *$P(\tilde{\mathbb{B}})$ es un dominio fundamental de $\mathscr{L}$.*

Demostración. Solo necesitamos probar que no hay superposiciones, ya que $vol(P(\tilde{\mathbb{B}})) = vol(P(\mathbb{B}))$. Hacemos una demostración por reducción al absurdo. Suponemos que hay superposición, esto es,

$$\mathbb{B}x + \tilde{\mathbb{B}}\alpha = \mathbb{B}y + \tilde{\mathbb{B}}\beta \tag{2.9}$$

para algún $x, y \in \mathbb{Z}^n$ y $\alpha, \beta \in [-1/2, 1/2)^n$. Entonces,

$$\mathbb{B}(x-y) = \tilde{\mathbb{B}}(\beta - \alpha). \tag{2.10}$$

Si llamamos $z = x - y$ y por (2.8)

$$\tilde{\mathbb{B}} \begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix} z = \tilde{\mathbb{B}}(\beta - \alpha) \tag{2.11}$$

luego

$$\begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix} z = (\beta - \alpha) \tag{2.12}$$

Tenemos entonces que, como z es un vector entero, y

$$-1 \lneq \beta_i - \alpha_i \lneq 1$$

Por (2.12) obtenemos

$$z_n = \beta_n - \alpha_n, \tag{2.13}$$

y así, $z_n = 0$. Igualmente, por (2.12) tenemos

$$z_{n-1} + *z_n = \beta_{n-1} - \alpha_{n-1}, \tag{2.14}$$

$$z_{n-1} = \beta_{n-1} - \alpha_{n-1}, \tag{2.15}$$

luego $z_{n-1} = 0$.
Repitiendo este mismo argumento sucesivamente obtenemos $z_1 = 0$ y así, $x = y$. □

Entonces, vemos ahora que podemos acotar λ_1 por el mínimo de la norma de los vectores $\tilde{b_i}$:

Si $\mathbb{B}$ es una base de $\mathscr{L}$, todo vector no nulo del retículo se puede escribir como $\mathbb{B}x$, con $x \in \mathbb{Z}^n$ no nulo. Sea k el mayor índice tal que $x_k \neq 0$.
Entonces, tomamos el producto escalar con $\tilde{b_k}$, y por la ortogonalidad de $\tilde{b_k}$ y de b_i cuando $i < k$, obtenemos que

$$\langle \mathbb{B}x, \tilde{b_k} \rangle = \sum_{i \leq k} \langle b_i x_i, \tilde{b_k} \rangle = x_k \langle b_k, \tilde{b_k} \rangle = x_k ||\tilde{b_k}||^2 \tag{2.16}$$

Por Cauchy-Schwarz, tenemos:

$$||\mathbb{B}x|| \cdot ||\tilde{b_k}|| \geq |\langle \mathbb{B}x, \tilde{b_k} \rangle| \geq |x_k| \cdot ||\tilde{b_k}||^2$$

Como $|x_k| \geq 1$, y dividiendo por $||\tilde{b_k}||$, obtenemos que $||\mathbb{B}x|| \geq ||\tilde{b_k}|| \geq \text{mín}_i ||\tilde{b_i}||$

Acotación superior

A continuación vamos a demostrar los teoremas de Minkowski, que podemos encontrar en [1] y cuyas demostraciones hemos completado. El primero nos permitirá obtener una cota superior de $\lambda_1(\mathscr{L})$ y por tanto de la norma del vector más corto del retículo, mientras que el segundo nos da información sobre todos los mínimos sucesivos.

Teorema 1. (Teorema de Minkowski 1) Sea un retículo $\mathscr{L}$ con determinante $\det(\mathscr{L})$. Entonces, todo subconjunto S convexo y simétrico respecto al origen de $\mathbb{R}^n$, con volumen mayor a $2^n \det(\mathscr{L})$, contiene un punto no nulo de $\mathscr{L}$. Además, si x es dicho punto, como S es simétrico, tenemos que $-x$ también está en el subconjunto.

Demostración. Sea $S' = \frac{1}{2}S$, entonces tenemos que, como $vol(S) > 2^n \det(\mathscr{L})$, $vol(S') > \det(\mathscr{L})$. Para cada $v \in \mathscr{L}$, definimos:

$$P_v := ((v + P(\mathbb{B})) \cap S') \setminus \{v\}$$

Hemos probado antes que los trasladados de $P(\mathbb{B})$ son disjuntos, luego

$$vol(S') = \sum vol(P_v) > vol(P(\mathbb{B})). \tag{2.17}$$

Por tanto, existen $v_1 \neq v_2 \in \mathscr{L}$, tales que

$$P_{v_1} \cap P_{v_2} \neq \emptyset. \tag{2.18}$$

Así, obtenemos:

$$(v_1 + S') \cap (v_2 + S') \neq \emptyset. \tag{2.19}$$

Luego existe z en la intersección, y $x, y \in S'$ tal que $z = v_1 + x = v_2 + y$. Por lo tanto

$$x - y = v_2 - v_1 \neq 0 \in \mathscr{L}. \tag{2.20}$$

Por definición de S', $2x, -2y \in S$, luego

$$x - y = \frac{1}{2}(2x) + \frac{1}{2}(-2y) \in S. \tag{2.21}$$

Con $x \neq y$ porque en otro caso $v_1 = v_2$, así, S contiene un punto del retículo no nulo. □

Corolario 1. $\sqrt{n}(\det(\mathscr{L}))^{1/n} \geq \lambda_1(\mathscr{L})$

Demostración. Una bola cerrada de radio mayor a $\sqrt{n}(\det(\mathscr{L}))^{\frac{1}{n}}$ es convexa y centralmente simétrica y además, $B(0,\sqrt{n}(\det(\mathscr{L}))^{1/n})$ contiene un cubo de lado $2(\det(\mathscr{L}))^{\frac{1}{n}}$, ya que dist((1,...,1),(0,...,0))=$\sqrt{n}$ Por tanto,

$$vol(B(0,\sqrt{n}(\det(\mathscr{L}))^{1/n})) > 2^n \det(\mathscr{L}) \tag{2.22}$$

Así, por el teorema de Minkowski, obtenemos que $B(0,\sqrt{n}(\det(\mathscr{L}))^{1/n})$ contiene un punto no nulo de $\mathscr{L}$, y por tanto, $\lambda_1(\mathscr{L}) \leq ||v||$ para algún $v \in \mathscr{L}$, y de aquí obtenemos $\lambda_1(\mathscr{L}) \leq \sqrt{n}(\det(\mathscr{L}))^{1/n}$.

□

Teorema 2. (Teorema de Minkowski 2) $(\prod_{i=1}^{n}\lambda_i(\mathscr{L}))^{\frac{1}{n}} \leq \sqrt{n}(\det(\mathscr{L}))^{\frac{1}{n}}$

Demostración. Podemos asumir que $||b_i|| = \lambda_i(\mathscr{L})$ para $i = 1,...,n$, y consideramos el retículo generado por $b_1,...,b_n$, que es posiblemente un subretículo de $\mathscr{L}$. Consideramos el elipsoide

$$T := \left\{ y \in \mathbb{R}^n : \sum_{i=1}^{n} \left(\frac{\langle y, \tilde{b_i} \rangle}{||\tilde{b_i}||\lambda_i} \right)^2 < 1 \right\},$$

donde $\tilde{b_i}$ son los vectores de la base ortogonalizada de $\mathbb{B}$.

En primer lugar probamos que no hay ningún punto no nulo del retículo en T. Sean $0 \neq y \in \mathscr{L}$ y $1 \leq k \leq n$ maximal tal que

$$\lambda_{k+1}(\mathscr{L}) \gneq ||y|| \geq \lambda_k(\mathscr{L}) \tag{2.23}$$

Podemos suponer que y está en $span(b_1,...,b_k) = span(\tilde{b_1},...,\tilde{b_k})$, con coeficientes enteros, ya que en otro caso $b_1,...,b_k,y$ son $k+1$ vectores linealmente independientes y sus normas son menores que λ_{k+1}, lo que es una contradicción. Por tanto, tenemos:

$$\sum_{i=1}^{n} \left(\frac{\langle y, \tilde{b_i} \rangle}{||\tilde{b_i}||\lambda_i} \right)^2 = \sum_{i=1}^{k} \left(\frac{\langle y, \tilde{b_i} \rangle}{||\tilde{b_i}||\lambda_i} \right)^2 \geq \sum_{i=1}^{k} \frac{1}{\lambda_k^2} \left(\frac{\langle y, \tilde{b_i} \rangle}{||\tilde{b_i}||} \right)^2 = \frac{||y||^2}{\lambda_k^2} \geq 1 \tag{2.24}$$

Luego $y \neq T$, i.e, T no contiene ningún punto del retículo. Por tanto, tenemos que

$$2^n \det(\mathscr{L}) \geq vol(T) = \left(\prod_{i=1}^{n} \lambda_i \right) vol(B(0,1)) \geq \left(\prod_{i=1}^{n} \lambda_i \right) \left(\frac{2}{\sqrt{n}} \right)^n, \tag{2.25}$$

Si nos quedamos con

$$2^n det(\mathscr{L}) \geq \left(\prod_{i=1}^{n} \lambda_i \right) \left(\frac{2}{\sqrt{n}} \right)^n \tag{2.26}$$

y despejamos $(\prod_{i=1}^{n}\lambda_i)$ obtenemos

$$\left(\prod_{i=1}^{n} \lambda_i \right)^{\frac{1}{n}} \leq \sqrt{n}(\det(\mathscr{L}))^{\frac{1}{n}}$$

□

Lema 4. Para todo retículo n-dimensional $\mathscr{L}$, tenemos

$$1 \leq \lambda_1(\mathscr{L}) \cdot \lambda_n(\mathscr{L}^*) \leq n$$

2.2. Problemas difíciles

En esta sección enumeramos algunos de los problemas que encontramos en retículos. Se ha probado que estos problemas son difíciles de resolver, clásica o cuánticamente, por lo que vamos a poder utilizarlos para probar la dificultad del problema Learning With Errors. Esto nos ayudará a su vez a ver que el algoritmo de cifrado que hemos introducido en el capítulo 1 es seguro.

Todos estos problemas son bastante similares entre sí, basados principalmente en minimizar la distancia o encontrar vectores cortos.

1. **Problema del vector más corto (SVP, SVP_γ y $GapSVP_\gamma$)**
   El problema SVP consiste en encontrar el vector $v \in \mathscr{L}$ tal que $||v|| = \lambda_1(\mathscr{L})$. Una variante de este problema es SVP_γ, que consiste en encontrar un vector $v \in \mathscr{L}$ tal que $||v|| \leq \gamma\lambda_1(\mathscr{L})$. Este problema es más sencillo cuanto mayor es γ.
   La versión de decisión del problema SVP_γ es $GapSVP_\gamma$, que consiste en, dado un numero real d, decidir entre $\lambda_1(\mathscr{L}) \leq d$ y $\lambda_1(\mathscr{L}) > \gamma d$. Esto es, buscamos aproximar $\lambda_1(\mathscr{L})$ dentro de un factor multiplicativo de γ.
   El problema SVP es NP-complejo con respecto a la norma uniforme $||\cdot||_\infty$. Con respecto a la norma $L2$ el problema es NP-complejo para reducciones aleatorias, como se puede ver en [4]

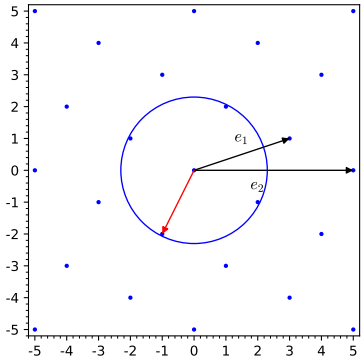


Figura 2.4: En la imagen vemos en rojo el vector más corto

2. **Problema de los vectores independientes más cortos ($SIVP_\gamma$)**
   El problema consiste en encontrar n vectores independientes $v_1, ..., v_n$ tales que $||v_i|| \leq \gamma\lambda_n$ para todo i.
3. **Bounded Distance Decoding (BDD)**
   Dados una base $\mathbb{B}$ del retículo, un vector $\vec{t}$ y un número real $d < \lambda_1/2$ tal que la distancia entre $\vec{t}$ y el retículo es menor que d, el problema consiste en encontrar el vector v del retículo que minimiza la distancia a $\vec{t}$.
4. **Short Integer Solution (SIS)**
   El problema consiste en encontrar un vector $v \in \mathbb{Z}^m$ tal que $\|v\| < \beta$ para $\sqrt{n \log q} \leq \beta < q$ en el retículo $\mathscr{L}(A)^\perp := \{x \in \mathbb{Z}^n : Ax = 0 \mod q\}$ donde A es una matriz en $\mathbb{Z}_q^{n \times m}$. Las condiciones sobre β se toman para asegurar que la ecuación $Ax = 0 \mod q$ tiene soluciones no triviales.
   Se puede ver que resolver SIS es tan difícil como resolver con probabilidad no despreciable los problemas $GapSVP_\gamma$ y $SIVP_\gamma$
5. **Learning With Errors (LWE)**
   El problema consiste en encontrar un vector $s \in \mathbb{Z}_q^n$ dados m vectores $\vec{a}_i \in \mathbb{Z}_q^n$ y m enteros $b_i \in \mathbb{Z}_q$ tales que $b_i = \langle s, \vec{a}_i \rangle + e_i$ para ciertos e_i enteros pequeños. Estudiaremos este problema más a fondo en el capítulo 4.
6. **Problema del muestre gaussiano discreto (DGS)**
   El problema consiste en obtener muestras de un retículo siguiendo una distribución, que denominamos distribución gaussiana discreta, y que trataremos en el capitulo siguiente.

Capítulo 3

Gaussianos discretos

En este capítulo vamos a definir la distribución gaussiana discreta. Esta distribución nos ayudará a demostrar la dureza del problema del Learning with Errors, que definiremos más adelante. Además, introduciremos la distribución del error que utilizamos en el criptosistema de nuestro ejemplo en el capítulo 1.

La distribución gaussiana que vamos a introducir depende de un parámetro s, que elegiremos según otro parámetro, ε, que nos indica la probabilidad del origen en el retículo dual, que buscaremos que sea muy pequeña. En muchos casos tomaremos $\varepsilon = 2^{-n}$.

Definición 4. La distribución gaussiana discreta sobre la clase $c+\mathscr{L}$ se define como

$$D_{c+\mathscr{L},s}(x) = \frac{\rho_s(x)}{\rho_s(c+\mathscr{L})} \tag{3.1}$$

para todo $x \in c+\mathscr{L}$, donde

$$\rho_s(x) = \exp\left(-\frac{\pi\|x\|^2}{s^2}\right) \tag{3.2}$$

y

$$\rho_s(c+\mathscr{L}) = \sum_{x\in\mathscr{L}} \rho_s(c+x) = \sum_{x\in\mathscr{L}} \exp\left(-\frac{\pi\|x+c\|^2}{s^2}\right) \tag{3.3}$$

Además, definimos

$$\rho_{s,-c}(x) := \exp\left(-\frac{\pi\|x-c\|^2}{s^2}\right) \tag{3.4}$$

la traslación a la clase de equivalencia de 0.

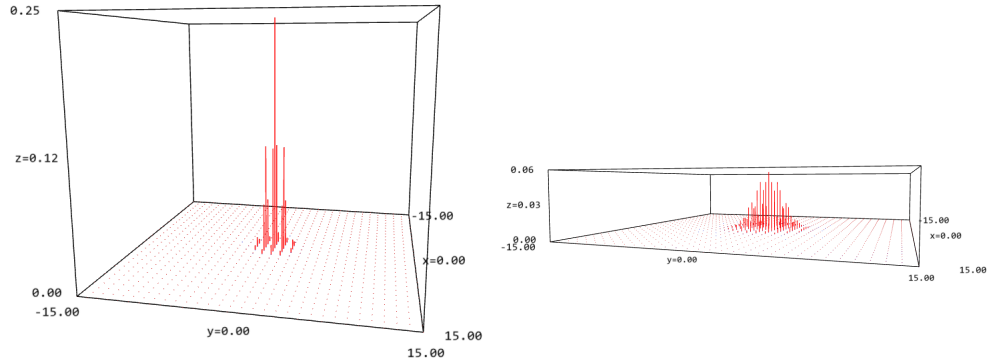


Figura 3.1: En esta gráfica podemos comparar las distribuciones gaussianas discretas sobre $\mathbb{Z}^2$ $D_{\mathbb{Z}^2,2}$ y $D_{\mathbb{Z}^2,4}$

Parámetro de suavizado

A continuación definimos un parámetro real positivo, denominado parámetro de suavizado, asociado al retículo. Intuitivamente, este parámetro nos da el menor s tal que la distribución $D_{\mathscr{L},s}$ 'se comporta como una distribución gaussiana continua'.

Definición 5. Para un retículo $\mathscr{L}$ y un número real positivo $\varepsilon > 0$, definimos el parámetro de suavizado $\eta_\varepsilon(\mathscr{L})$, dependiente de ε, como el menor s tal que $\rho_{1/s}(\mathscr{L}^* \setminus \{0\}) \leq \varepsilon$.

Esto es, ε es un parámetro que elegimos que nos da información sobre la probabilidad del origen en el retículo dual. Entonces, en la práctica, nosotros elegiremos el valor del parámetro ε y a continuación buscaremos $s \geq \eta_\varepsilon(\mathscr{L})$.

Contamos con dos acotaciones para el parámetro de suavizado, que podemos encontrar en [3].

Acotación superior

Lema 5. $\eta_\varepsilon(\mathscr{L}) \leq \frac{\sqrt{n}}{\lambda_1(\mathscr{L}^*)}$ cuando $\varepsilon = 2^{-n}$

Demostración. La demostración se basa en otro lema que podemos encontrar en [3], que nos dice que, para todo $c > \frac{1}{\sqrt{2\pi}}$, $\mathscr{L}$ retículo $n-$dimensional y $v \in \mathbb{R}^n$,

$$\rho_1(\mathscr{L} \setminus c\sqrt{n}\mathbb{B}) < C^n \rho_1(\mathscr{L}), \text{ con } \mathbb{B} \text{ una base de } \mathscr{L}.$$

Entonces, si tomamos $c = 1, C = \sqrt{2\pi e} \cdot e^{-\pi} < \frac{1}{4}$ y separamos el lado derecho de la ecuación anterior como la suma de los puntos en $\sqrt{n}\mathbb{B} =$ y la suma de los puntos fuera de este conjunto. Entonces, al reordenar, obtenemos

$$\rho_1(\mathscr{L} \setminus c\sqrt{n}\mathbb{B}) < \frac{C^n}{1-C^n} \rho_1(\mathscr{L} \cap c\sqrt{n}\mathbb{B})$$

Así, si tomamos $s > \frac{\sqrt{n}}{\lambda_1(\mathscr{L}^*)}$, como el vector más corto de $s\mathscr{L}^*$ tiene norma mayor que $\sqrt{n}$ y por tanto $s\mathscr{L}^* \setminus \sqrt{n}\mathbb{B} = s\mathscr{L}^* \setminus \{0\}$ y $s\mathscr{L}^* \cap \sqrt{n}\mathbb{B} = \{0\}$, obtenemos

$$\rho_{\frac{1}{s}}(\mathscr{L}^* \setminus \{0\}) = \rho_1(s\mathscr{L}^* \setminus \sqrt{n}\mathbb{B}) < \frac{C^n}{1-C^n} \rho_1(\mathscr{L} \cap c\sqrt{n}\mathbb{B}) = \frac{C^n}{1-C^n} < 2^{-n}$$

□

Acotación inferior

Lema 6.

$$\eta_\varepsilon(\mathscr{L}) \geq \sqrt{\frac{\ln\frac{1}{\varepsilon}}{\pi}}\frac{1}{\lambda_1(\mathscr{L}^*)} \tag{3.5}$$

Demostración. Sea $v \in \mathscr{L}^*$ un vector de longitud $\lambda_1(\mathscr{L}^*)$ y $s = \eta_\varepsilon(\mathscr{L})$. Entonces, tenemos

$$\varepsilon \geq \rho_{1/s}(\mathscr{L}^* \setminus 0) \geq \rho_{1/s}(v) = \exp(-\pi(s\lambda_1(\mathscr{L}^*)^2) \tag{3.6}$$

Obtenemos la desigualdad despejando en la ecuación. □

Gaussianos discretos

Si $s > \eta_\varepsilon(\mathscr{L})$, $\rho_s(c+\mathscr{L})$ es muy cercano a $s^n \det(\mathscr{L}^*)$. Si $\varepsilon = 2^{-n}$, $s > \sqrt{n}/\lambda_1(\mathscr{L}^*)$, y $\rho_s(x)$ es la restricción de la distribución gaussiana ρ_s a $c+\mathscr{L}$.

Para justificar esta afirmación probamos el siguiente resultado, que podemos encontrar en [1].

Lema 7.

$$\rho_s(c+\mathscr{L}) \in [s^n(1-\varepsilon)\det(\mathscr{L}^*), s^n(1+\varepsilon)\det(\mathscr{L}^*)]$$

Demostración. Sea $\hat{\rho}_s(y)$ la transformada de Fourier de $\rho_s(w)$, definida como

$$\hat{\rho}_s(w) = \int_{\mathbb{R}^n} \rho_s(w) e^{-2\pi i\langle x,w\rangle} dx \tag{3.7}$$

Por lo que se cumple la siguiente relación:

$$\hat{\rho}_s(y) = \int_{\mathbb{R}^n} \rho_s(x) e^{-2\pi i x\cdot y} dx = \int_{\mathbb{R}^n} e^{-\pi(\frac{||x||^2}{s^2} + 2ix\cdot y)} dx = \int_{\mathbb{R}^n} e^{-\pi\sum_j(\frac{x_j}{s} + iy_j s)^2} e^{-\pi(s||y||)^2} dx = s^n \rho_{1/s}(y)$$

Así, podemos probar nuestro resultado calculando

$$\rho_s(c+\mathscr{L}) = \sum_{x\in\mathscr{L}} \rho_s(x+c) = \sum_{x\in\mathscr{L}} \rho_{s,-c}(x) = \det(\mathscr{L}^*) \sum_{y\in\mathscr{L}^*} \hat{\rho}_{s,-c}(y) = \tag{3.8}$$

$$= \det(\mathscr{L}^*) \sum_{y\in\mathscr{L}^*} \hat{\rho}_{s,-c}(y) = \det(\mathscr{L}^*) s^n \sum_{y\in\mathscr{L}^*} e^{2\pi i\langle c,y\rangle} \rho_{1/s}(y) \in [s^n(1-\varepsilon)\det(\mathscr{L}^*), s^n(1+\varepsilon)\det(\mathscr{L}^*)]$$

□

Así, $\rho_s(c+\mathscr{L})$ es casi uniforme respecto a c cuando s es suficientemente grande. Y por lo tanto, la distribución gaussiana discreta se puede considerar invariante respecto a las traslaciones. Como consecuencia, obtenemos muy poca información sobre $c+\mathscr{L}$ cuando sacamos las muestras de $D_{c+\mathscr{L},s}$ si $s \sim \sqrt{n}/\lambda_1(\mathscr{L}^*)$.

Más formalmente, sea la distribución $D_{\mathbb{Z}^n,s}$ con $s > \eta_\varepsilon(\mathscr{L})$, esta distribución es casi uniforme sobre $\mathbb{Z}^n/\mathscr{L}$, esto es, si elegimos $x \in \mathbb{Z}^n$ de $D_{\mathbb{Z}^n,s}$ y revelamos la clase $x+\mathscr{L}$, entonces cada clase $c+\mathscr{L}$ es prácticamente igual de probable, esto es, $|\mathbb{P}(c_1+\mathscr{L}) - \mathbb{P}(c_2+\mathscr{L})| < \varepsilon$ para $\varepsilon > 0$ muy pequeño. Dado $x \in c+\mathscr{L}$, tiene la distribución condicional $D_{c+\mathscr{L},s}$. Probamos esto en el siguiente lema.

Lema 8. Para todo $s > 0$, $c \in \mathbb{R}^n$ y retículo $\mathscr{L}$ con base $\mathbb{B}$, la distancia estadística entre $D_{s,c} \mod P(\mathbb{B})$ y la distribución uniforme sobre $P(\mathbb{B})$ es como mucho $\frac{1}{2}\rho_{1/s}(\mathscr{L}(\mathbb{B})^* \setminus \{0\})$.
En particular, para todo $\varepsilon > 0$ y cualquier $s \geq \eta_\varepsilon(\mathbb{B})$, la distancia estadística es como mucho $\varepsilon/2$.

Demostración. La demostración de este lema, que podemos encontrar en [3], se basa en calcular la función de densidad sobre $P(\mathbb{B})$ definida por $D_{s,c}$ y utilizar la transformada de Fourier para obtener $Y(x) = \det(\mathscr{L}(\mathbb{B})^*)\left(1 - \sum_{w\in\mathscr{L}(\mathbb{B})^*\setminus\{0\}} \exp 2\pi i\langle x-c, w\rangle \rho_{\frac{1}{s}}(w)\right)$. La densidad sobre $P(\mathbb{B})$ de la distribución uniforme es $U(x) = \frac{1}{vol(P(\mathbb{B}))} = \det(\mathscr{L}(\mathbb{B})^*)$.
Entonces acotamos la distancia estadística hasta obtener:

$$\Delta(Y,U) = \frac{1}{2}\int_{x\in P(\mathbb{B})} |Y(x) - U(x)|dx \leq \frac{1}{2}\rho_{\frac{1}{s}}(\mathscr{L}(\mathbb{B})^* \setminus \{0\})$$

□

Sea A una matriz muestreada uniformemente en $\mathbb{Z}_q^{n\times m}$, y sea x una muestra de la distribución $D_{\mathbb{Z}^m,s}$. Definimos $f_A(x) := Ax \in \mathbb{Z}_q^n$. Sea $u = f_A(x)$, entonces, invertir f_A es equivalente a resolver el problema SIS para A. La distribución condicionada a $Ax = u$ es $D_{\mathscr{L}_u^\perp(A),s}$, donde

$$\mathscr{L}_u^\perp(A) = \{x \in \mathbb{Z}^n : Ax = u \mod q\}$$

Luego tenemos que obtener una muestra de $D_{\mathbb{Z}^m,s}$ en el retículo $\mathscr{L}_u^\perp(A)$ es un problema difícil. Más generalmente tenemos:

Definición 6. El problema del muestreo gaussiano discreto, denotado DGS_r, consiste en obtener una muestra en un retículo $n-$dimensional$\mathscr{L}$ según la distribución $D_{\mathscr{L},r}$

Es importante remarcar que el muestreo gaussiano discreto sobre un retículo es un problema difícil de resolver, ya que, como se puede ver en [2], podemos reducir algunos problemas difíciles en retículos, como el $SIVP_\gamma$ y el $GapSVP_\gamma$ a este problema.

Debido a esta dificultad de realizar el muestreo, en la práctica utilizamos otra distribución, $\bar{\Psi}_\alpha$, que es una distribución en $\mathbb{Z}_q$ con forma gaussiana, centrada en torno a 0 y con amplitud αq, y tal que la probabilidad de 0 es aproximadamente $\frac{1}{q\alpha}$.

Más concretamente, se define la distribución Ψ_α como la distribución en $\mathbb{R}/\mathbb{Z}$ obtenida muestreando una variable normal de media 0 y desviación típica $\frac{\alpha}{\sqrt{2\pi}}$ y luego reduciendo el resultado módulo 1,

$$\forall r \in [0,1), \Psi_\alpha(r) := \sum_{k=-\infty}^{\infty} \frac{1}{\alpha}\cdot \exp\left(-\pi\left(\frac{r-k}{\alpha}\right)^2\right) \tag{3.9}$$

Entonces, $\bar{\Psi}_\alpha$ es la discretización $\mathbb{Z}_q \to \mathbb{R}^+$ de la distribución $\Psi_\alpha : \mathbb{R}/\mathbb{Z} \to \mathbb{R}^+$, obtenida muestreando de Ψ_α, multiplicando por q y luego redondeando al entero más próximo módulo q.

Esta distribución también tiene forma gaussiana, y es más sencillo realizar el muestreo.

Capítulo 4

Learning With Errors

Vamos a tratar en este capítulo el problema de Learning With Errors, el problema computacional en el que se basa la seguridad del algoritmo de cifrado utilizado en la introducción.

4.1. Definición del problema

El Learning With Errors es un problema computacional que trata de encontrar una función en n variables, lineal, sobre un anillo finito, a partir de m muestras dadas, que tienen pequeños errores.

Vamos a definir el problema dependiente de una distribución χ sobre $\mathbb{Z}_q$, de la que proviene el error en cada muestra. Normalmente tomaremos χ^n como la distribución gaussiana discreta o $\bar{\Psi}_\alpha$.

Existen dos variantes de este problema, que definimos a continuación.

4.1.1. Búsqueda LWE

En la búsqueda LWE$_{s,\chi}$ el objetivo es encontrar el vector $s \in \mathbb{Z}_q^n$ tal que, dados m vectores de $\mathbb{Z}_q^n$, $\vec{a}_i$, elegidos independiente e uniformemente, y m escalares de $\mathbb{Z}_q$, b_i, se cumplan los productos escalares, $b_i = \langle s, a_i \rangle + e_i$, donde e_i son muestras de la distribución χ sobre $\mathbb{Z}_q$ de amplitud αq. Esto es, buscamos invertir la función:

$$\begin{array}{rccc} f: & \mathbb{Z}_q^n \times \mathbb{Z}^m & \to & \mathbb{Z}_q^m \\ & (s,e) & \mapsto & b^t = s^t A + e. \end{array}$$

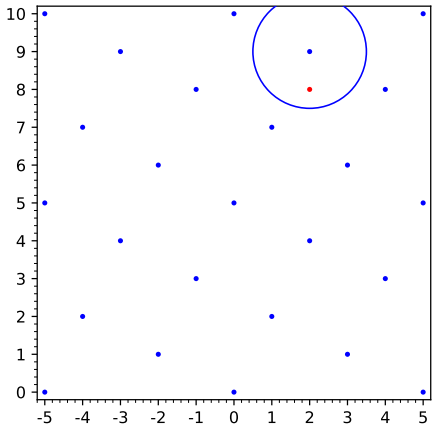


Figura 4.1: En la figura se ilustra el problema de búsqueda LWE

En la figura 4.1, podemos ver el retículo generado por las filas de la matriz $A = \begin{pmatrix} 3 & 1 \\ 2 & -1 \end{pmatrix}$. El punto rojo está obtenido como en el problema LWE, esto es, es de la forma $s^t A + e$, y entonces, el problema consiste en encontrar el punto del retículo más cercano a él, que sería s, en este caso es el punto dentro de la circunferencia.
Si no tuviéramos el término del error, el problema se podría resolver de manera sencilla mediante eliminación gaussiana.

En el ejemplo del capítulo 1, la clave pública de Alice b^t se calcula mediante esta función f, con s siendo la clave secreta de Alice. Por tanto, si un atacante fuera capaz de obtener la clave secreta de Alice a partir de la pública, también sería capaz de resolver el problema de búsqueda LWE.

4.1.2. Decisión LWE

En esta versión del LWE el objetivo es encontrar un algoritmo que distinga entre $(A, b^t = s^t A + e^t)$ y (A, b^t), donde (A, b^t) es uniforme, con alta probabilidad de acertar. Esto es, buscamos distinguir entre las distribuciones uniforme y $A_{s,\chi}$, donde $A_{s,\chi}$ es la distribución sobre $\mathbb{Z}_q^n \times \mathbb{Z}_q$ obtenida eligiendo un vector $a \in \mathbb{Z}_q^n$ uniformemente aleatorio, eligiendo $e \in \mathbb{Z}^n$ según la distribución χ y calculando $(a, \langle a, s \rangle + e)$, donde la suma se realiza módulo q.

La seguridad de nuestro algoritmo está basada en la dificultad de esta versión del problema, ya que demostraremos que si podemos diferenciar entre el cifrado de 0 y de 1, entonces también podemos resolver este problema.

4.2. Propiedades de LWE

1. Es fácil comprobar si un vector $s' \in \mathbb{Z}_q^n$ es solución: Es suficiente comprobar si $b - \langle s', \vec{a} \rangle$ es pequeño, esto es, si está en $(-q/4, q/4)$. Si $s \neq s'$, entonces $b - \langle s', \vec{a} \rangle = \langle s - s', \vec{a} \rangle + e$ está bien extendido en $\mathbb{Z}_q$, esto es, algunos de las componentes de $b - \langle s', \vec{a} \rangle$ serán grandes y otras serán pequeños. Como trabajamos en $\mathbb{Z}_q$, consideramos que un número es pequeño si está en el intervalo $(-q/4, q/4)$ y que es grande si está en $(-q/2, -q/4) \cup (q/4, q/2)$.

2. Podemos obtener nuevos LWE que tienen esencialmente las mismas soluciones trasladando el secreto s por cualquier $t \in \mathbb{Z}_q^n$. Sea $t \in \mathbb{Z}_q^n$, entonces hacemos la traslación

$$(\vec{a}, b = \langle s, \vec{a} \rangle + e) \rightarrow (\vec{a}, b' = b + \langle t, \vec{a} \rangle = \langle s + t, \vec{a} \rangle + e) \tag{4.1}$$

Gracias a estas dos propiedades, si tuviéramos un algoritmo que resolviera el problema de búsqueda-LWE con probabilidad de acertar p, podemos trasladar el secreto s por un vector $t \in \mathbb{Z}_q^n$ y a continuación obtener nuevas muestras como hemos hecho arriba. Después aplicamos el algoritmo y comprobamos si la solución obtenida es correcta. En caso de no ser correcta reiteramos el proceso, y como nuestro algoritmo tiene p probabilidad de acertar, si lo aplicamos suficientes veces acabaremos encontrando una solución correcta.

4.2.1. Equivalencia de la búsqueda/decisión de LWE

Para ver que ambos problemas son equivalentes, probamos que podemos resolver la búsqueda LWE sabiendo resolver la decisión y que podemos resolver la decisión LWE sabiendo resolver la búsqueda.
En primer lugar vemos cómo resolver la búsqueda sabiendo resolver la decisión.

Suponemos que tenemos un oráculo $\mathscr{D}$ que sabe resolver la decisión LWE, esto es, que sabe distinguir entre $(\vec{a}, b = \langle s, \vec{a} \rangle + e)$ y $(\vec{a}, b)$ uniforme. Entonces, dados los pares $(\vec{a}, b)$, queremos hallar s.

Buscamos cada componente por separado:

Para encontrar $s_1 \in \mathbb{Z}_q$, tomamos $k \in \mathbb{Z}_q$ y transformamos los pares en $(\vec{a}+(l,0,\ldots,0), b+l\cdot k)$ para algún $l \in \mathbb{Z}_q$. Esta transformción lleva la distribucion uniforme a sí misma, y si $k = s_1$, entonces los pares transformados siguen siendo LWE, pero si $k \neq s_1$, entonces los pares pasan a una distribución uniforme.

Por tanto, utilizamos $\mathscr{D}$ con los pares transformados y comprobamos si $k = s_1$. Solo hay q posibilidades para s_1, luego las probamos todas.
Repetimos el proceso con el resto de componentes de s y al final hallamos el secreto s.

A continuación probamos el recíproco. Supongamos que tenemos un oráculo para resolver la búsqueda LWE. Entonces, si tenemos muestras $(\vec{a}_i, b_i)$, aplicamos el oráculo a estas muestras, y si obtenemos s, para todo i, calculamos $\{e_i\} = \{\langle \vec{a}_i, s\rangle - b_i\}$. Si las muestras eran LWE, entonces $\{e_i\}$ estarán distribuidos según χ, en otro caso, estarán distribuidos uniformemente.

4.2.2. LWE en retículos

Sea el retículo

$$\mathscr{L}(A) := \{z \in \mathbb{Z}^m : z^t = s^t A \mod q \text{ para algún } s \in \mathbb{Z}_q^n\} = \pi^{-1}(\operatorname{im} A),$$

que es el retículo formado por las combinaciones lineales de las filas de $A \mod q$.
Entonces, LWE nos da un punto b de la forma $b^t = s^t A + e$, luego, como el error e es un término pequeño, y $s^t A$ es un punto del retículo, obtenemos que resolver LWE sería resolver BDD en este retículo dado el punto b.

4.3. Forma hermítica del LWE

Llamamos χ^n a una distribución cualquiera sobre $\mathbb{Z}_q^n$.

Definición 7. Decimos que el problema LWE está en forma hermítica normal cuando el secreto s sigue la misma distribución que el error χ^n

Podemos notar que en este caso el secreto es un vector corto.

Demostramos a continuación que el problema LWE no es más fácil cuando el secreto se obtiene de la distribución del error χ^n.

Teorema 3. Sea χ^n una distribución de la que obtenemos el error para el problema LWE, y sean $s_1 \in \mathbb{Z}_q^n$ obtenido de la misma distribución del error, y $s_2 \in \mathbb{Z}_q^n$ obtenido de manera uniforme. Entonces, si podemos resolver el problema $\mathrm{LWE}_{s_1,\chi^n}$, podemos resolver $\mathrm{LWE}_{s_2,\chi^n}$.

Demostración. En primer lugar tomamos muestras hasta obtener $(\bar{A}, \bar{b}^t = s^t\bar{A} + \bar{e}^t)$ para $\bar{A}$ cuadrada e invertible, y para s obtenido de manera uniforme. Luego, obtenemos muestras adicionales del LWE $(\vec{a}, b = \langle s, \vec{a}\rangle + e)$ y las transformamos a $\vec{a'} = -\bar{A}^{-1}\vec{a}$. Entonces tenemos

$$\begin{aligned} b' &= b + \langle \bar{b}, \vec{a'}\rangle \\ &= \langle s, \vec{a}\rangle + e + \langle \bar{A}^t s + \bar{e}^t, \vec{a'}\rangle \\ &= \langle s, \vec{a}\rangle + \langle \bar{A}^t s, \vec{a'}\rangle + \langle \bar{e}^t, \vec{a'}\rangle + e \\ &= \langle s, \vec{a}\rangle + \langle s, \bar{A}(-\bar{A}^{-1})\vec{a}\rangle + \langle \bar{e}^t, \vec{a'}\rangle + e \\ &= \langle \bar{e}^t, \vec{a'}\rangle + e \end{aligned}$$

Entonces, $(\vec{a'}, b')$ es LWE con secreto $\bar{e}$, que está obtenido de la distribución χ^n. Por hipótesis del enunciado, podemos resolver $\text{LWE}_{\bar{e},\chi^n}$. Luego obtenemos s de $\bar{b}^t = s^t\bar{A} + \bar{e}^t$. □

4.4. Dificultad del problema $\text{LWE}_{s,\bar{\Psi}_\alpha}$

La demostración de la dureza de este problema se puede encontrar en [2], y está basada en la dificultad del muestreo en la distribución gaussiana discreta. Se puede probar que si tuviéramos acceso a un oráculo que resuelve $LWE_{s,\bar{\Psi}_\alpha}$, entonces existiría un algoritmo cuántico para resolver $DGS_{\sqrt{2n}\cdot\eta_\varepsilon(\mathscr{L})/\alpha}$. A su vez, se puede ver que el problema $DGS_{\sqrt{2n}\cdot\eta_\varepsilon(\mathscr{L})/\alpha}$ se reduce al problema $SIVP_\gamma$ y al problema $GapSVP_\gamma$, lo que nos asegura su dureza cuántica.

Por tanto, hasta este punto hemos visto unas bases de la teoría de retículos y ciertos problemas que son difíciles de resolver en estos espacios, pero que serían más sencillos si trabajáramos en espacios vectoriales. Además, hemos estudiado la distribución gaussiana discreta y definimos otra distribución,$\bar{\Psi}_\alpha$, con forma gaussiana y también discreta, pero que es más sencilla de muestrear. Por último, hemos estudiado el problema LWE, para el cuál necesitábamos la distribución $\bar{\Psi}_\alpha$ y cuya seguridad está asegurada por la dificultad de obtener muestras de la distribución gaussiana discreta.

En el capítulo siguiente, vamos a estudiar el criptosistema propuesto por Regev, donde se aplica todo lo que hemos visto hasta aquí.

Capítulo 5

Criptosistema de clave pública usando LWE

En esta sección vamos a presentar el criptosistema de clave pública presentado por Regev en [2], que hemos utilizado en nuestro ejemplo en el capítulo 1, en el que se muestra como utilizamos la teoría de retículos y el problema LWE para cifrar y descifrar información. Vamos a explicar el funcionamiento del algoritmo y demostraremos que es seguro.

5.1. Presentación del algoritmo

En primer lugar, sea n el parámetro de seguridad del sistema. Entonces tomamos $q \geq 2$ un número primo entre n^2 y $2n^2$, y $m = (1+\varepsilon)(1+n)\log q$ para algún $\varepsilon > 0$ arbitrario. Contamos con una matriz publica $A \in \mathbb{Z}_q^{n\times m}$, uniformemente aleatoria sobre $\mathbb{Z}_q$, esto es, las columnas de A están elegidas independientemente de una distribución uniforme.
Tomamos $\bar{\Psi}_\alpha$ como distribución para el error, e, donde $\alpha < \frac{1}{n\log n}$

Clave secreta
La clave secreta de Alice es un vector $s \in \mathbb{Z}_q^n$ elegido uniformemente.

Clave pública
La clave pública de Alice se calcula a partir de la clave secreta de la siguiente manera:

$$b^t = s^t A + e^t, \text{ donde } e \text{ se elige según la distribución } \bar{\Psi}_\alpha. \tag{5.1}$$

Cifrado
Bob toma una clave secreta efímera $x \in \{0,1\}^m$ y cifra un bit de la siguiente manera:

$$u = Ax \tag{5.2}$$

$$u' = b^t x + \lfloor \frac{bit \cdot q}{2} \rfloor \tag{5.3}$$

Descifrado
Alice calcula $s^t u = s^t Ax = (b^t - e)x = u' - ex$ y a continuación estudia la diferencia

$$d = u' - s^t u = ex + \lfloor \frac{bit \cdot q}{2} \rfloor \mod q \tag{5.4}$$

expresada en el intervalo $[-\frac{q-1}{2}, \frac{q-1}{2}]$. Si

$$\frac{-q}{4} \leq d \leq \frac{q}{4} \tag{5.5}$$

entonces el bit encriptado era un 0.
En caso contrario, el bit era un 1.

5.2. Seguridad del criptosistema

Para probar la seguridad del criptosistema, tenemos que ver que un atacante no puede llegar a conocer el mensaje que Bob envía a Alice. Hay diversas maneras en las que esto puede suceder:

1. El atacante obtiene la clave secreta de Alice, s y puede por lo tanto descifrar el mensaje que envía Bob.
2. El atacante no puede obtener s pero obtiene x y puede por tanto calcular $b^t x$ y compararlo con u'. Si obtiene $u' = b^t x$, el bit enviado es 0, en caso contrario el bit es 1.
3. El atacante puede distinguir de alguna manera entre los cifrados de 0 y 1, conociendo solo $(u,u'),(A,b)$.

Vamos a tratar cada uno de estos casos por separado:

En primer lugar, como hemos remarcado anteriormente, sabemos que la clave secreta de Alice es segura ya que para obtener s, un atacante debería poder resolver el problema de búsqueda LWE, conociendo A y b^t, para obtener s a partir de la ecuación $b^t = s^t A + e^t$.

Para el segundo caso, suponemos que el atacante si que puede calcular x. Sabemos que es posible encontrar una solución entera arbitraria t del sistema de ecuaciones lineales $At = u \mod q$, mediante álgebra lineal. Entonces, todas las soluciones de $Ax = u \mod q$ son de la forma $t + \mathscr{L}^{\perp}(A)$, donde $\mathscr{L}^{\perp}(A) = \{x \in \mathbb{Z}^m : Ax = 0\}$. Y así el x buscado es un vector corto en $t + \mathscr{L}^{\perp}(A)$, equivalentemente, buscamos un vector en el retículo, $v \in \mathscr{L}^{\perp}(A)$, tal que sea cercano a t.
Por tanto, encontrar x es una instancia media del problema del vector más corto, que ya hemos visto que es un problema difícil.

Por último, tratamos el tercer caso, esto es, que el atacante sea capaz de distinguir entre los cifrados de 0 y 1, conociendo solo $(u,u'),(A,b)$.
Como $m \geq n \log q$, el par (u,u') es uniformemente aleatorio por el Left-over Hash lemma, que explicaremos más adelante, por lo que no da información sobre s, y tampoco es posible distinguir entre el cifrado de 0 y 1 a partir de (u,u'). Por otro lado, contamos con el siguiente lema, que nos dice que para m suficientemente grande no podemos distinguir entre los cifrados de 0 y 1, demostrado por Regev en [2].

Lema 9. Para cualquier $\varepsilon > 0$ y $m \geq (1+\varepsilon)(n+1)\log q$, si existe un algoritmo, $\mathscr{W}$ que distingue entre los cifrados de 0 y 1 en tiempo polinomial en n, podemos resolver eficientemente el problema de decisión-LWE para $(A, b^t = s^t A + e)$ para una fracción no despreciable de todos los posibles $s \in \mathbb{Z}_q^n$.

Demostración. Decimos que $\mathscr{W}$ acepta cuando dice que el bit encriptado era 0. Entonces definimos:

- $p_0(\mathscr{W})$ la probabilidad de que $\mathscr{W}$ acepte $((a_i,b_i)_{i=1}^m,(u,u'))$, donde (u,u') es el cifrado de 0 con clave pública $(a_i,b_i)_{i=1}^m$.
- $p_1(\mathscr{W})$ la probabilidad de que $\mathscr{W}$ acepte $((a_i,b_i)_{i=1}^m,(u,u'))$, donde (u,u') es el cifrado de 1 con clave pública $(a_i,b_i)_{i=1}^m$.
- $p_u(\mathscr{W})$ la probabilidad de que $\mathscr{W}$ acepte $((a_i,b_i)_{i=1}^m,(u,u'))$, donde (u,u') es elegido uniformemente sobre $\mathbb{Z}_q^n \times \mathbb{Z}_q$.

Con esta notación, la hipótesis de que $\mathscr{W}$ distingue entre los encriptados de 0 y 1 se puede escribir de la siguiente manera:

$$|p_0(\mathscr{W}) - p_1(\mathscr{W})| \geq \frac{1}{n^c}, \text{ donde } c > 0 \tag{5.6}$$

Entonces, vamos a contruir otro oráculo $\mathscr{W}'$ que pueda distinguir entre el cifrado de 0 y (u,u') uniforme, esto es, tal que

$$|p_0(\mathscr{W}') - p_u(\mathscr{W}')| \geq \frac{1}{2n^c} \tag{5.7}$$

Sabemos que $|p_0(\mathscr{W}) - p_u(\mathscr{W})| \geq \frac{1}{2n^c}$ o $|p_1(\mathscr{W}) - p_u(\mathscr{W})| \geq \frac{1}{2n^c}$ (en otro caso, si $|p_0(\mathscr{W}) - p_u(\mathscr{W})| < \frac{1}{2n^c}$ y $|p_1(\mathscr{W}) - p_u(\mathscr{W})| < \frac{1}{2n^c}$ entonces tendríamos $|p_0(\mathscr{W}) - p_1(\mathscr{W})| \leq |p_0(\mathscr{W}) - p_u(\mathscr{W})| + |p_1(\mathscr{W}) - p_u(\mathscr{W})| < \frac{1}{n^c}$).

Por tanto, si $|p_0(\mathscr{W}) - p_u(\mathscr{W})| \geq \frac{1}{2n^c}$, podemos tomar $\mathscr{W} = \mathscr{W}'$.

Si $|p_1(\mathscr{W}) - p_u(\mathscr{W})| \geq \frac{1}{2n^c}$, construimos $\mathscr{W}'$ como sigue:
La entrada de $\mathscr{W}'$ es el par $((a_i,b_i)_i,(u,u'))$, y $\mathscr{W}'$ aplica $\mathscr{W}$ pero con entrada $((a_i,b_i)_i,(u,u'+\frac{q-1}{2}))$. Esto lleva la distribución de cifrados de 0 a la distribución de cifrados de 1, y la distribución uniforme a sí misma, luego W' es el oráculo requerido.

Por último, construimos un oráculo $\mathscr{Z}$ que pueda distinguir entre una distribución uniforme y la distribución $A_{s,\chi}$ del problema LWE para un número no despreciable de $s \in \mathbb{Z}_q^n$.

Sea $s \in \mathbb{Z}_q^n$ y definimos

- $p_0(s)$ la probabilidad de que $\mathscr{W}'$ acepte $((a_i,b_i)_{i=1}^m,(u,u'))$, donde (u,u') es el cifrado de 0 con clave pública $(a_i,b_i)_{i=1}^m$, y $(a_i,b_i)_{i=1}^m$ están elegidos de $A_{s,\chi}$.
- $p_u(s)$ la probabilidad de que $\mathscr{W}'$ acepte $((a_i,b_i)_{i=1}^m,(u,u'))$, donde (u,u') está elegido uniformemente sobre $\mathbb{Z}_q^n \times \mathbb{Z}_q$, y $(a_i,b_i)_{i=1}^m$ están elegidos de $A_{s,\chi}$.

Entonces, nuestra suposición sobre $\mathscr{W}'$ implica que $|\mathbb{E}_s[p_0(s)] - \mathbb{E}_s[p_u(s)]| \geq \frac{1}{2n^c}$ y podemos definir $Y = \left\{s : |p_0(s) - p_u(s)| \geq \frac{1}{4n^c}\right\}$, entonces, al menos $\frac{1}{4n^c}$ de todos los s están en Y, ya que en caso contrario tenemos

$$\begin{aligned}
|\mathbb{E}_s[p_0(s)] - \mathbb{E}_s[p_u(s)]| &= |\mathbb{E}_s[p_0(s) - p_u(s)]| \\
&= \frac{|\sum_{s\in\mathbb{Z}_q^n} p_0(s) - p_u(s)|}{|\mathbb{Z}_q^n|} \\
&\leq \frac{\sum_{s\in\mathbb{Z}_q^n} |p_0(s) - p_u(s)|}{|\mathbb{Z}_q^n|} \\
&= \frac{\sum_{s\in Y} |p_0(s) - p_u(s)|}{|\mathbb{Z}_q^n|} + \frac{\sum_{s\in\mathbb{Z}_q^n\setminus Y} |p_0(s) - p_u(s)|}{|\mathbb{Z}_q^n|} \\
&< \frac{\sum_{s\in Y} 1}{|\mathbb{Z}_q^n|} + \frac{\sum_{s\in\mathbb{Z}_q^n\setminus Y} 1}{4n^c|\mathbb{Z}_q^n|} \\
&< \frac{|\mathbb{Z}_q^n|}{4n^c|\mathbb{Z}_q^n|} + \frac{|\mathbb{Z}_q^n|}{4n^c|\mathbb{Z}_q^n|} \\
&= \frac{1}{2n^c}
\end{aligned}$$

lo que contradice nuestra hipótesis sobre $\mathscr{W}'$. Por tanto, al menos $\frac{1}{4n^c}$ de todos los s están en Y, y nos basta con encontrar un oráculo $\mathscr{Z}$ que distinga entre ambas distribuciones para todos los $s \in Y$. Describimos $\mathscr{Z}$ a continuación:

Se nos da una distribución R sobre $\mathbb{Z}_q^n \times \mathbb{Z}_q^m$, que puede ser la distribución uniforme, U, o $A_{s,\chi}$ para $s \in Y$. Entonces tomamos m muestras $(a_i,b_i)_{i=1}^m$ de R y definimos:

- $p_0((a_i,b_i)_i)$ la probabilidad de que $\mathscr{W}'$ acepte $((a_i,b_i)_{i=1}^m,(u,u'))$, donde la probabilidad se toma en la elección de (u,u') como cifrado de 0 con clave pública $(a_i,b_i)_{i=1}^m$.
- $p_u((a_i,b_i)_i)$ la probabilidad de que $\mathscr{W}'$ acepte $((a_i,b_i)_{i=1}^m,(u,u'))$, donde la probabilidad se toma en la elección de (u,u') uniforme sobre $\mathbb{Z}_q^n \times \mathbb{Z}_q$.

Entonces, $\mathscr{Z}$ utiliza $\mathscr{W}'$ un número polinomial en n de veces para estimar $p_0((a_i,b_i)_i)$ y $p_u((a_i,b_i)_i)$ con un error esperado máximo de $\frac{1}{64n^c}$. Si las estimaciones difieren en más de $\frac{1}{16n^c}$, $\mathscr{Z}$ acepta, esto es, la distribución sería $A_{s,\chi}$, y en caso contrario, $\mathscr{Z}$ rechaza. Por último, demostramos que si R es la

distribución uniforme, $\mathscr{Z}$ rechaza con probabilidad alta, y que si R es $A_{s,\chi}$, $\mathscr{Z}$ acepta con probabilidad $\frac{1}{poly(n)}$.

En primer lugar asumimos que R es una distribución uniforme, entonces $(a_i,b_i)_i$ son muestras tomadas de una distribución uniforme sobre $\mathbb{Z}_q^n \times \mathbb{Z}_q$. Utilizamos el siguiente resultado, que podemos encontrar en [2], cuya demostración omitimos por razones de espacio:

Lema 10. Sea G un grupo abeliano finito y l un entero. Entonces, para l elementos cualesquiera de G, $g_1,...,g_l$ consideramos la distancia estadística entre la distribución uniforme y la distribución dada por la suma de un subconjunto aleatorio de $g_1,...,g_l$. Entonces, la esperanza de esta distancia estadística sobre la elección uniforme de $g_1,...,g_l \in G$ es como mucho $\sqrt{|G|/2^l}$.

Entonces, tomando $G = \mathbb{Z}_q^n \times \mathbb{Z}_q$, obtenemos que con probabilidad exponencialmente cercana a 1, la distribución de (u,u') es exponencialmente cercana a la distribución uniforme sobre $\mathbb{Z}_q^n \times \mathbb{Z}_q$. Por tanto, excepto con probabilidad exponencialmente pequeña,

$$|p_0((a_i,b_i)_i^m) - p_u((a_i,b_i)_i^m)| \leq 2^{-\Omega(n)} \tag{5.8}$$

donde $\Omega(n)$ es una función $h = h(n)$ tal que $\limsup \frac{|h(n)|}{n} > 0$, luego nuestras dos estimaciones difieren como mucho en $\frac{1}{32n^c} + 2^{-\Omega(n)}$, y $\mathscr{Z}$ rechaza.

Ahora asumimos que R es la distribución $A_{s,\chi}$ para $s \in Y$, entonces, notamos primero que $p_0(s)$ y $p_u(s)$ son las medias respectivas de $p_0((a_i,b_i)_i^m)$ y $p_u((a_i,b_i)_i^m)$ tomadas sobre la elección de $(a_i,b_i)_i^m$ en $A_{s,\chi}$. De $|p_0(s) - p_u(s)| \geq \frac{1}{4n^c}$ obtenemos que:

$$|p_0((a_i,b_i)_i^m) - p_u((a_i,b_i)_i^m)| \geq \frac{1}{8n^c} \tag{5.9}$$

con probabilidad al menos $\frac{1}{8n^c}$ sobre la elección de $(a_i,b_i)_i^m$ de $A_{s,\chi}$. Por lo tanto, nuestras estimaciones difieren en más de $\frac{1}{16n^c}$ y $\mathscr{Z}$ acepta. □

5.3. Left Over Hash Lemma

Antes de introducir el lema necesitamos dos definiciones.

Definición 8. Se define una familia de funciones hash 2-universal $H = \{h : \mathscr{S} \times \mathscr{X} \to \{0,1\}^m\}$ como una familia de funciones tales que para 2 claves cualesquiera $(x_1,x_2) \in (\mathscr{S} \times \mathscr{X})^2$ y para dos imágenes $(y_1,y_2) \in \{0,1\}^m \times \{0,1\}^m$ se cumple

$$\Pr[h(x_1) = y_1 \wedge h(x_2) = y_2] = m^{-2} \tag{5.10}$$

Definición 9. Se define la mínima entropía H_∞ como menos el logaritmo de la probabilidad del resultado más probable.

Lema 11. Sea X una variable aleatoria sobre $\mathscr{X}$ y sea $m > 0$. Sea $h : \mathscr{S} \times \mathscr{X} \to \{0,1\}^m$ una función hash 2-universal. Si se cumple

$$m \leq H_\infty + 2\log(\varepsilon) \tag{5.11}$$

entonces para S uniforme sobre $\mathscr{S}$ e independiente de X tenemos

$$\delta[(h(S,X),S),(U,S)] \leq \varepsilon \tag{5.12}$$

donde δ es la distancia estadística y U es uniforme sobre $\{0,1\}^m$ e independiente de S.

Este lema implica que, si nuestra clave secreta tiene n bits y un adversario consigue $m < n$ bits, podemos fabricar otra clave que tenga $n-m$ bits y de la cual el adversario no conoce ninguna información.

En nuestro caso vamos a tomar la familia de funciones Hash

$$h_s(x) = (Ax, b_s x + \frac{q \cdot bit}{2})$$

definidas sobre $\mathscr{X} = \{0,1\}^m \times \{0,1\}$ Entonces, obtenemos que $(u,u') = h_{(A,b)}(x, bit)$ es uniformemente aleatorio, cuando $m \geq n \log q$.

La condición anterior es necesaria ya que nuestra función está definida con dominio e imagen

$$h_s(x) : \{0,1\}^m \to \mathbb{Z}_q^n \times \mathbb{Z}_q \tag{5.13}$$

y el resultado no puede ser uniforme si la función no es sobreyectiva. Para que la función sea sobreyectiva es necesario que

$$|\{0,1\}^m| \geq |\mathbb{Z}_q^n \times \mathbb{Z}_q| \tag{5.14}$$

por tanto,

$$2^m \geq q^{n+1} \tag{5.15}$$

y tomando el logaritmo en base 2, obtenemos $m \geq (n+1)\log q > n \log q$.

Capítulo 6

Conclusiones

En este trabajo hemos estudiado las bases de la teoría de retículos, después de lo cual introducimos varios problemas que son considerados cuánticamente difíciles. A continuación definimos la distribución gaussiana discreta y el problema del muestreo gaussiano discreto, que podemos reducir a algunos de los problemas difíciles en retículos y que es, por tanto, difícil de resolver cuánticamente. Hemos introducido también el problema de Learning With Errors, en el que se basa el criptosistema de clave pública de Regev, y cuya seguridad demostramos basándonos en la dificultad de resolver el LWE.
Podemos remarcar que este criptosistema no es eficiente, ya que, cuando $q = 401, n = 3$, que es un número primo relativamente pequeño, para enviar un solo bit de información necesitamos enviar la pareja $(u, u') \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ que ocupará al menos $3 \cdot 2^9 + 2^9$ bits, que son aproximadamente 36 bits. Por tanto, el mensaje cifrado es 36 veces más grande que el original. En la practica se usan primos mucho mayores, por lo que el sistema no es eficiente. Sin embargo, este algoritmo es la base para criptosistemas más eficientes.

Como hemos comentado en la introducción, el pasado 5 de Julio, el NIST aprobó tres algoritmos de cifrado basados en la teoría de retículos que pasaron a formar parte del Estándar de criptografía post-cuántica:

Para encriptación general, han seleccionado el algoritmo CRYSTAL-Kyber. Entre sus ventajas se cuentan la velocidad de cálculo y el uso de claves de encriptado relativamente pequeñas, que las dos partes interesadas pueden intercambiar fácilmente. La seguridad de este algoritmo está basada en la dificultad de resolver el problema Learning With Errors sobre retículos modulares. El diseño del algoritmo se basa en el algoritmo de Regev, y se aumenta la eficacia del sistema al observar que el secreto s del LWE se puede sacar de la misma distribución que el error y que se puede utilizar matrices cuadradas en vez de rectangulares a la hora de construir el algoritmo. Otra mejora ha sido utilizar anillos de polinomios en vez de enteros.

Para firmas digitales, el NIST ha aprobado los algoritmos CRYSTALS-Dilithium y FALCON. En el algoritmo Dilithium, la seguridad se basa en la dificultad de encontrar vectores cortos en retículos. Entre las ventajas del algoritmo tenemos que el tamaño de la clave pública y de la firma es de los más pequeños, y que utiliza muestreo uniforme, ya que es más fácil de implementar de forma segura y eficiente que el muestreo gaussiano.
La seguridad de FALCON está basada en el problema Short Integer Solution en retículos NTRU. La principal ventaja del algoritmo es su compacidad, esto es, la suma de los tamaños de la firma y de la clave pública es pequeña.
Todos estos algoritmos trabajan con anillos de polinomios en vez de con retículos enteros, lo que les permite una mayor eficacia tanto en la velocidad de cálculo como en el tamaño de los mensajes.

Todos estos avances que se están realizando y estos algoritmos que han sido aprobados para el Estándar de criptografía post-cuántica justifican el interés en el estudio de la teoría de retículos.

Apéndice A

Problemas difíciles en retículos

Vamos a ver ahora con un poco más de detalle los problemas difíciles que encontramos en la teoría de retículos. Además, veremos el algoritmo LLL (Lenstra-Lenstra-Lovaz), que nos permite reducir el tamaño de la base de un retículo. Por último, veremos un diagrama en el que se observan las relaciones entre los distintos problemas, indicando qué problemas podemos reducir a otros.

A.1. Problemas

Problema del vector más corto (*SVP*)

El problema del vector más corto (SVP) de un retículo $\mathscr{L}$ consiste en encontrar un vector $v \in \mathscr{L}$ tal que $||v|| = \lambda_1(\mathscr{L})$.

Derivado de este problema podemos definir otro problema también difícil de resolver pero más débil que el SVP, introduciendo un parámetro $\gamma \geq 1$.
Dados $\gamma \geq 1$ y una base $\mathbb{B}$ de $\mathscr{L}$, el problema SVP_γ consiste en buscar un vector no nulo del retículo tal que $||v|| \leq \gamma\lambda_1(\mathscr{L})$

Existe otra versión del problema, denominada $GapSVP_\gamma$, en la que, dados la base $\mathbb{B}$ y un numero real d, tenemos que decidir entre $\lambda_1(\mathscr{L}) \leq d$ y $\lambda_1(\mathscr{L}) > \gamma d$. Esto es, buscamos aproximar $\lambda_1(\mathscr{L})$ dentro de un factor multiplicativo de γ.

Podemos remarcar que $GapSVP_\gamma$ se reduce al SVP_γ ya que SVP_γ consiste en encontrar un vector $v \neq 0 \in \mathscr{L}$ tal que $\lambda_1(\mathscr{L} \leq ||v|| \leq \gamma\lambda_1(\mathscr{L}))$. Si encontramos v tal que $\lambda_1(\mathscr{L})||v|| \leq \gamma\lambda_1(\mathscr{L})$ entonces $\lambda_1 \leq \gamma d$. Asi, como necesariamente $\lambda_1 \leq d$ o $\lambda_1 > d$ obtenemos que $\lambda_1 < d$. Y si $||v|| > \gamma d$ tenemos $\gamma d < ||v|| \leq \gamma\lambda_1$, luego $d < \lambda_1$ y asi, $\lambda_1 > \gamma d$.

Cabe remarcar que la dificultad de los problemas SVP_γ y $GapSVP_\gamma$ disminuye cuanto mayor sea γ.

Problema de los vectores independientes más cortos ($SIVP_\gamma$)

Dada una base $\mathbb{B}$ buscamos n vectores linealmente independientes $v_1, \ldots, v_2$ tales que $||v_i|| \leq \gamma\lambda_n$ para todo i

Bounded-Distance Decoding (*BDD*)

Dados una base $\mathbb{B}$, un vector $\vec{t}$ y un real $d < \lambda_1/2$ tal que dist$(\vec{t}, \mathscr{L}) \leq d$, queremos encontrar el único vector $v \in \mathscr{L}$ que minimiza la distancia.
Este problema equivale a encontrar un vector en la clase de $\vec{t}$ con norma menor o igual a d.

Problema del vector más corto (*CVP*)

Dado un retículo $\mathscr{L}$ y un vector $v \in \mathbb{R}^n$ que no está necesariamente en el retículo, el problema consiste en encontrar el vector de $\mathscr{L}$ más cercano a v.

Tenemos también la versión de decisión de este problema, denominada $GapCVP_\beta$, que consiste en encontrar un algoritmo que, dado un retículo $\mathscr{L}$ y un vector $v \in \mathbb{R}^n$, nos diga si uno de los dos casos siguientes es cierto o si ninguno lo es:

- O bien existe un vector del retículo tal que la distancia a v es menor que 1.
- O bien todos los vectores del retículo están a distancia mayor que β de v.

Short-Integer Solution (*SIS*)

Tomamos $\mathbb{Z}_q^n$ el espacio de los vectores n-dimensionales modulo q. Y tomamos m vectores $\vec{a_1}, \ldots, \vec{a_m}$ de este espacio. Entonces buscamos m enteros pequeños y no triviales tales que:

$$z_1\vec{a_1} + \cdots + z_m\vec{a_m} = 0 \tag{A.1}$$

en $\mathbb{Z}_q^n$, esto es:

$$Az = 0 \mod q \tag{A.2}$$

con A la matriz formada por los vectores columna $\vec{a_1}, \ldots, \vec{a_m}$. Esto es, si definimos el retículo $\mathscr{L}(A)^\perp := ker\left(\mathbb{Z}^m \xrightarrow[z \longrightarrow Az]{A \in \mathbb{Z}_q^{n \times m}} \mathbb{Z}_q^n\right) = \{x \in \mathbb{Z}^m : Ax = 0 \mod q\}$, queremos encontrar en este retículo un vector corto.

A.2. Algoritmo de resolución LLL

El algoritmo LLL se utiliza para reducirla norma de los vectores de la base de un retículo.

Definición 10. Sea $\tilde{B}$ una base ortonormal de $\mathscr{L}$, entonces, una base δ-LLL reducida es una base $\mathbb{B} = (b_1, \ldots, b_n)$ tal que

1. Para $1 \leq j < i \leq n$, tenemos $|\mu_{i,j}| \leq \frac{1}{2}$
2. Para $1 \leq i < n$, tenemos

$$\delta||\tilde{b_i}||^2 \leq ||\mu_{i+1,i}\tilde{b_i} + \tilde{b_{i+1}}||^2 = |\mu_{i+1,i}|^2||\tilde{b_i}||^2 + ||\tilde{b_{i+1}}||^2 \tag{A.3}$$

donde

$$\mu_{i,j} = \frac{\langle b_i, \tilde{b_j}\rangle}{||\tilde{b_j}||^2} \tag{A.4}$$

$$\tilde{b_i} = b_i - \sum_{j=1}^{i-1} \mu_{i,j}\tilde{b_j} \tag{A.5}$$

En particular, si $1 \geq \delta > \frac{1}{4}$ tenemos, por A.3

$$||\tilde{b_{i+1}}||^2 \geq \delta||\tilde{b_i}||^2 - |\mu_{i+1,i}|^2||\tilde{b_i}||^2 = (\delta - |\mu_{i+1,i}|^2)||\tilde{b_i}||^2 \tag{A.6}$$

y como tenemos que $|\mu_{i,j}| \leq \frac{1}{2}$, obtenemos

$$||\tilde{b_{i+1}}||^2 \geq (\delta - |\mu_{i+1,i}|^2)||\tilde{b_i}||^2 \geq \left(\delta - \frac{1}{4}\right)||\tilde{b_i}||^2 \tag{A.7}$$

Así, si elegimos $\delta = \frac{3}{4}$ obtenemos:

$$||b_i|| = ||\tilde{b_i}|| \leq 2^{\frac{(n-1)}{2}} min||\tilde{b_i}|| \leq 2^{\frac{(n-1)}{2}} \lambda_1(\mathscr{L}) \tag{A.8}$$

Ya que tenemos:

$$\|\tilde{b_1}\| \leq 2^{\frac{1}{2}} \|\tilde{b_2}\| \leq (2^{\frac{1}{2}})^2 \|\tilde{b_3}\| \leq \cdots \leq (2^{\frac{1}{2}})^{n-1} \|\tilde{b_n}\| = 2^{\frac{n-1}{2}} \|\tilde{b_n}\| \tag{A.9}$$

Luego en particular, si $\|\tilde{b_k}\| = min_i \|\tilde{b_i}\|$ tenemos que

$$\|\tilde{b_i}\| \leq 2^{\frac{k-1}{2}} \|\tilde{b_k}\| \leq 2^{\frac{n-1}{2}} \|\tilde{b_k}\| = 2^{\frac{n-1}{2}} min_i \|\tilde{b_i}\| = 2^{\frac{(n-1)}{2}} \lambda_1(\mathscr{L}) \tag{A.10}$$

A.2.1. Algoritmo LLL

- La entrada del algoritmo es una base $b_1, \ldots, b_n$ del retículo $\mathscr{L}$, y la salida es una base δ-LLL reducida de $\mathscr{L}$

- Empezamos calculando la ortogonalización de Gram-Schmidt $\tilde{b_1}, \ldots, \tilde{b_n}$ de la base.

- Paso de reducción:
  Para $i = 2, ..., n$:
  Para $j = i - 1$ hasta 1

$$c_{ij} = \left\lceil \frac{\langle b_i, \tilde{b_j} \rangle}{\langle \tilde{b_j}, \tilde{b_j} \rangle} \right\rfloor \tag{A.11}$$

$$b_i \longleftarrow b_i - c_{ij} b_j \tag{A.12}$$

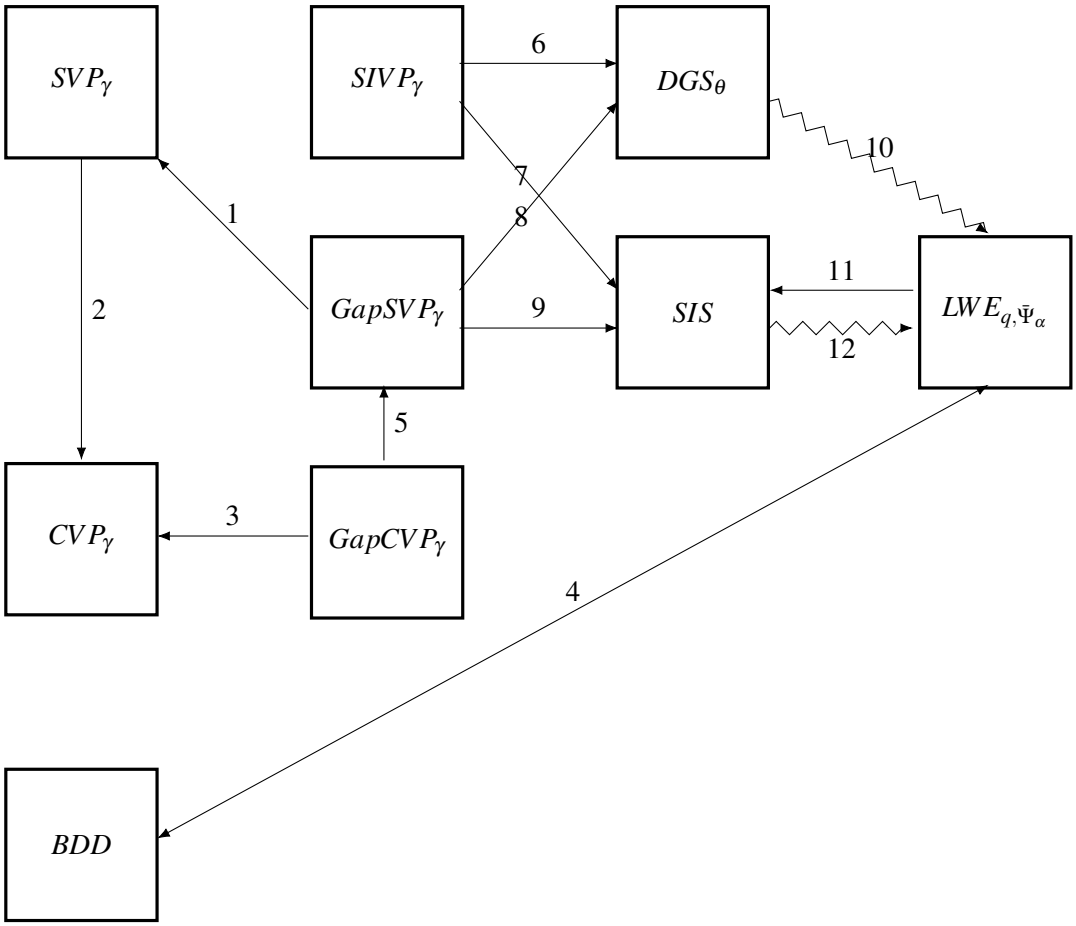
- Paso de intercambio:
  Si existe i tal que $\delta \|\tilde{b_i}\|^2 > \|\mu_{i+1,i} \tilde{b_i} + \tilde{b_{i+1}}\|^2$
  $b_i \longleftrightarrow b_{i+1}$
  Volvemos a empezar.

- La salida son los nuevos $b_1, \ldots, b_n$

Cabe remarcar que las bases que obtenemos mediante el algoritmo LLL no son grandes, pero no son lo suficientemente pequeñas como para resolver el problema *SVP*.

A.3. Diagrama de relaciones entre los problemas.

En esta sección vamos ver un diagrama que relaciona los distintos problemas entre sí, indicando qué problemas se pueden reducir a cuáles. En el diagrama, tenemos $A \longrightarrow B$ si el problema A se puede reducir al problema B. Las líneas rectas indican una reducción clásica, mientras que las líneas en zigzag nos indican una reducción cuántica.



A continuación vamos a ver cada una de las reducciones:

1. El problema $GapSVP_\gamma$ se puede reducir al problema SVP_γ, como se puede ver en [1].
2. Podemos observar en [5] que el problema SVP_γ se puede reducir al problema CVP_γ.
3. La reducción de $GapCVP_\gamma$ a CVP_γ es equivalente a la reducción de $GapSVP_\gamma$ a SVP_γ .
4. Podemos ver la equivalencia entre BDD y LWE en retículos en [1].
5. En [5] se demuestra que hay una reducción en tiempo polinomial en n de $GapSVP_\gamma$ a $GapCVP_\gamma$.
6. En [2] se prueba que hay una reducción de $SIVP_{2\sqrt{n}\phi}$ a DGS_ϕ
7. En [1] podemos ver la reducción de $SIVP_{\beta\sqrt{n}}$ a SIS, donde β es el parámetro de SIS.
8. En [2] se prueba que hay una reducción de $GapCVP_{100\sqrt{n}\gamma}$, y por tanto de $GapSVP_{100\sqrt{n}\gamma}$ a $DGS_{\frac{\sqrt{n}\gamma}{\lambda_1(\mathscr{L}^*)}}$
9. En [1] podemos ver la reducción de $GapSVP_{\beta\sqrt{n}}$ a SIS, donde β es el parámetro de SIS.
10. Podemos ver la reducción cuántica de DGS_θ a $LWE_{q,\bar{\Psi}_\alpha}$ en [2], esta reducción es la que prueba la dificultad de resolver el problema $LWE_{q,\bar{\Psi}_\alpha}$.
11. Podemos ver la reducción de $LWE_{q,\bar{\Psi}_\alpha}$ a SIS en [2].
12. Podemos ver la reducción cuántica de SIS a $LWE_{q,\bar{\Psi}_\alpha}$ en [6].

Bibliografía

[1] DONG PYO CHI, JEONG WOON CHOI, JEONG SAN KIM, TAEWAN KIM , *Lattice Based Cryptography for Beginners*. `https://eprint.iacr.org/2015/938.pdf`

[2] ODED REGEV, *On Lattices, Learning With Errors, Random Linear Codes and Cryptography*. J. ACM, 56(6):1-40, 2009. Versión preliminar en STIC 2005

[3] ODED REGEV, DANIELE MICCIANCIO, *Worst-case to average-case reductions based on Gaussian measures*. SIAM J. Comput. 37, 1, 267–302. 2007

[4] MIKLÓS AJTAI *The Shortest Vector Problem in L2 is NP-hard for Randomized Reductions.Extended Abstract*, In STOC, pages 10–19. 1998.

[5] ODED GOLDREICH ET AL. *Approximating shortest lattice vectors is not harder than approximating closest lattice vectors*, Inf. Process. Lett. 71 (2): 55–61. 1999. url:10.1016/S0020-0190(99)00083-6

[6] DAMIEN STEHLÉ, RON STEINFELD, KEISUKE TANAKA Y KEITA XAGAWA *Efficient Public Key Encryption Based on Ideal Lattices*, ASIACRYPT 2009: Advances in Cryptology – ASIACRYPT 2009 pp 617–635

[7] KEITH MATTHEWS *Smith normal form* MP274: Linear Algebra, Lecture Notes, University of Queensland, 1991