Protocolo para el intercambio de claves criptográficas basado en el problema "learning with rounding"
Key exchange protocol based on learning with rounding problem

Esp. David Ricardo Ledo Baster[1]*, Dr C. Manuel Mariño Betancourt[2], Dr C. Miguel Cruz Ramírez[2]

Resumen La mayoría de los protocolos de intercambio de claves utilizados con mayor frecuencia se basan en la suposición de que los problemas del logaritmo discreto y la factorización de ciertos números son problemas difíciles de resolver. Sin embargo, dicha suposición no se cumple si utilizamos computadoras cuánticas. En este trabajo se propone un protocolo para el intercambio de claves criptográficas basado en el problema Learning with Rounding (LWR), el cual es inmune a la computación cuántica.

Abstract Most of the key exchange protocols used most frequently are based on the assumption that the problems of the discrete logarithm and the factorization of certain numbers they are difficult problems to solve. However, this assumption is not met if we use quantum computers. In this paper is proposed a protocol for the exchange of cryptographic keys based on the Learning with Rounding (LWR) problem, which is immune to quantum computing.

Palabras Clave
protocolos de intercambio de claves, criptografía asimétrica, criptografía postcuántica

[1] *Departamento de Informática, Universidad de Holguín, Holguín, Cuba, dledob@uho.edu.cu*
[2] *Universidad de Holguín, Holguín, Cuba*
***Autor para Correspondencia**

Introducción

La criptografía está presente en muchas partes de nuestra vida diaria, por ejemplo en tarjetas de crédito, comercio electrónico mediante internet, votaciones electrónicas, etc. Un aspecto importante de la criptografía lo constituyen los métodos para intercambiar una clave secreta a través de una canal abierto, posiblemente vigilado, sin tener que intercambiar ningún secreto previamente. Estos métodos son llamados protocolos de intercambio de claves. La mayoría de los protocolos de intercambio de claves utilizados con mayor frecuencia se basan en la suposición de que los problemas del logaritmo discreto y la factorización de ciertos números son problemas difíciles de resolver. Sin embargo, dicha suposición no se cumple si utilizamos computadoras cuánticas y el algoritmo de Shor [18] (ver una excelente explicación en [19]). Teniendo en cuenta lo anterior, muchas organizaciones gubernamentales y privadas han comenzado a estudiar y desarrollar nuevos protocolos para el intercambio de claves. Particularmente, el NIST lanzó un proyecto para crear estándares criptográficos que sean inmunes a la computación cuántica [14].

La criptografía basada en *lattices* constituye una opción atractiva y es una de las más representadas en el proyecto de estandarización del NIST [15]. En particular el problema LWE[1] [17] tiene muchos aspectos interesantes para diversos usos debido a la reducción hacia problemas sobre *lattices* en el peor de los casos y la dificultad para resolverlo aún con computadoras cuánticas. Brevemente se define como la solución a un sistema de ecuaciones de la forma $b_i = a_i s + e_i \pmod{q}$ donde a_i y s son elegidos siguiendo una distribución uniforme y e_i según la distribución de Gauss. El problema LWR [2] es la variante determinística del LWE, donde se reemplaza la distribución de Gauss por el redondeo utilizando un módulo p más pequeño. Esto garantiza mayor eficiencia en los criptosistemas debido a que se elimina la operación de seleccionar números según la distribución de Gauss.

Los protocolos para el intercambio de claves criptográficas se presentan principalmente en dos variantes, en la primera, concida como KEM[2], se utiliza un algoritmo de cifrado asimétrico para cifrar, con la clave pública del receptor, una clave de sesión; en la segunda, conocida como DH[3], ambos

[1] LWE: Learning with Errors
[2] KEM: Key Encapsulation Mechanism
[3] Por ser Diffie y Hellman los primeros en proponer un protocolo de este tipo

participantes intercambian información pública para derivar la clave de sesión. Los protocolos tipo DH tienen la propiedad de que no es posible obtener la clave de sesión conociendo las claves privadas de los usuarios, lo cual se conoce como secreto hacia adelante. Otra propiedad necesaria en los protocolos de intercambio de claves es la autenticidad de la información que se intercambia, para evitar el ataque del hombre en el medio, la cual se puede alcanzar de forma explícita firmando digitalmente la información que se intercambia, o de forma implícita si el protocolo tiene mecanismos propios para garantizarle al receptor que está interactuando con el emisor y viceversa.

Dentro de las opciones basadas en la criptografía sobre *lattices* aparecen los protocolos propuestos en [6, 12, 16, 20, 11, 5, 9, 8, 3, 1, 10] de los cuales [9, 8, 3, 1, 10] utilizan el problema LWR. De estos útlimos, solo el protocolo spKEX propuesto por Bhattacharya et al. en [3] es del tipo DH, y además constituye el menos denso de los cinco. Sin embargo, el mecanismo para derivar la clave secreta no garantiza que sea uniforme en el espacio de claves teniendo en cuenta que es un mecanismo aproximado en el que se debe enviar información extra para que ambos participantes del protocolo puedan derivar la misma clave. Tampoco se demuestra la seguridad en función de la dificultad del problema LWR, solo se analizan los principales ataques conocidos y se estiman los parámetros para que dichos ataques no tengan éxito.

Motivación. Por lo tanto, en este trabajo se desarrolla un protocolo para el intercambio de claves criptográficas tipo DH que utiliza ideas propuestas en los trabajos [3] y [5] para garantizar la uniformidad de las claves generadas en presencia de información extra, y que la seguridad del protocolo se pueda demostrar con respecto a la dificultad del problema LWR.

1. Preliminares

Notaciones. Los vectores se denotan por letras en minúscula, en negrita y siempre son considerados como vectores columna, por ejemplo $\mathbf{v}$. Las matrices se denotan por letras en mayúscula y en negrita, por ejemplo $\mathbf{M}$. Un vector columna $\mathbf{v_1}$ se transforma en el vector fila $\mathbf{v_1}^\top$. La transpuesta de la matriz $\mathbf{M}$ se denota por $\mathbf{M}^\top$. El producto interno de dos vectores $\mathbf{v_1}$ y $\mathbf{v_2}$ se define por $(\mathbf{v_1},\mathbf{v_2}) = \mathbf{v_1}^\top \cdot \mathbf{v_2}$. La norma de un vector es la euclidiana l_2, a menos que se mencione lo contrario. Se denota por $\|\mathbf{M}\|_\infty$ el máximo valor absoluto de las entradas de la matriz $\mathbf{M}$. Para cada número real x se define $\lfloor x \rceil = max\{n \in \mathbb{Z}\} \mid n \leq x$ y $\lfloor x \rceil = \lfloor x + 1/2 \rfloor$.

Si χ es una distribución de probabilidad sobre un conjunto S, $x \xleftarrow{\$} \chi$ significa elegir $x \in S$ de acuerdo con χ. Si S es un conjunto, entonces $U(S)$ es la distribución uniforme sobre S, y seleccionar un elemento x uniforme y aleatoriamente se denota por $x \xleftarrow{\$} U(S)$ o simplemente $x \xleftarrow{\$} S$. Para una matriz $\mathbf{M}$ o un vector $\mathbf{v}$, la notación $\mathbf{M} \xleftarrow{\$} \chi$ o $\mathbf{v} \xleftarrow{\$} \chi$ significa que todas las entradas de $\mathbf{M}$ y $\mathbf{v}$ son seleccionadas independientemente siguiendo la distribución χ. Para $n, h \in \mathbb{Z}$ y $0 \leq h \leq n$, $\mathscr{HW}_n(h)$ es el conjunto de los vectores $\{-1,0,1\}^n$ con peso de Hamming h.

Función de redondeo. Sean $q, p \in \mathbb{Z}$ tal que $q \geq p \geq 2$. Se define la función $\lfloor \cdot \rceil_p : \mathbb{Z}_q \to \mathbb{Z}_p$ como $\lfloor x \rceil_p = \lfloor (p/q) \cdot \bar{x} \rceil \pmod p$ donde $\bar{x}$ es un número congruente con x módulo q. La función $\lfloor \cdot \rceil_p$ puede extenderse a matrices y vectores en $\mathbb{Z}_q$ aplicando la función componente a componente. En [7] se define la función probabilística $\mathsf{Inv}(\cdot) : \mathbb{Z}_p \to \mathbb{Z}_q$ que toma un elemento $x \in \mathbb{Z}_p$ como entrada y selecciona uniformemente un elemento del conjunto $\{u \in \mathbb{Z}_q | \lfloor u \rceil_p = x\}$ y lo retorna como salida. De manera intuitiva se puede observar que si x es uniforme en $\mathbb{Z}_p$ entonces $\mathsf{Inv}(x)$ es uniforme en $\mathbb{Z}_q$; sin embargo, en [7] no aparece la demostración. Debido a la importancia de la uniformidad de Inv, nosotros proponemos y demostramos el siguiente lema:

Lema 1. *Si $p|q$ y $x \xleftarrow{\$} \mathbb{Z}_p$ entonces $\mathsf{Inv}(x)$ es uniforme en $\mathbb{Z}_q$.*

Demostración. Sea $q = kp$ y $S_x = \{u \in \mathbb{Z}_q | \lfloor u \rceil_p = x\}$. Sea la variable aleatoria S cuyo espacio muestral lo constituyen los $p-1$ subconjuntos S_i con $0 \leq i \leq p-1$. Calculemos la probabilidad de que $\mathsf{Inv}(x) = r$ para $r \in \mathbb{Z}_q$.

$$\begin{aligned} P(\mathsf{Inv}(x) = r) &= P(r \xleftarrow{\$} S \wedge S = S_x) \\ &= P(r \xleftarrow{\$} S | S = S_x) P(S = S_x) \\ &= \frac{1}{k}\frac{1}{p} \\ &= \frac{1}{kp} = \frac{1}{q} \end{aligned}$$

Lo cual se obtiene debido a que si $x \xleftarrow{\$} \mathbb{Z}_p$ entonces $P(S = S_x) = 1/p$ y $P(r \xleftarrow{\$} S | S = S_x) = 1/k$ porque r se selecciona uniformemente de un subconjunto S_x, los cuales tienen k elementos pues $p|q$. □

Mecanismo de reconciliación. Como mecanismo de reconciliacón utilizamos el defindo en [5] el cual establece que

$$[\cdot]_{2^B} : v \to \lfloor 2^{-\bar{B}} v \rceil \pmod{2^B}$$

donde $v \in \mathbb{Z}_q$ y $\bar{B} = \log_2 q - B$. También se establece que

$$\langle \cdot \rangle_{2^B} : v \to \lfloor 2^{-\bar{B}+1} v \rfloor \pmod 2$$

y la función $rec(\cdot,\cdot)$ que tiene como entrada $w \in \mathbb{Z}_q$ y $b \in \{0,1\}$ y retorna $[v]_{2^B}$, donde v es el elemento más cercano a w tal que $\langle v \rangle_{2^B} = b$.

De [5] se tomaron los lemas siguientes:

Lema 2. *Si $v \in \mathbb{Z}_q$ es seleccionado de forma uniforme, entonces $[v]_{2^B}$ es uniforme conociendo $\langle v \rangle_{2^B}$.*

Lema 3. *Si $|v - w| < q/2^{B+2}$, entonces $rec(w, \langle v \rangle_{2^B}) = [v]_{2^B}$.*

Problema LWE y sus variantes.

Definición 1 (Distribución LWE)**.** *Sean n y q enteros positivos. Sea χ una distribución de probabilidad sobre $\mathbb{Z}$. Para un vector $\mathbf{s} \in \mathbb{Z}_q^n$, la distribución LWE $A_{\mathbf{s},\chi}$ sobre $\mathbb{Z}_q^n \times \mathbb{Z}_q$ se obtiene seleccionando $\mathbf{a} \xleftarrow{\$} U(\mathbb{Z}_q^n)$, e $\xleftarrow{\$} \chi$ y retornando $(\mathbf{a}, b = (\mathbf{a},\mathbf{s}) + e \pmod q)$.*

Problema 1 (**LWE**$_{n,q,\chi,m}$ de búsqueda)**.** *Si se tienen m muestras independientes $(\mathbf{a_i}, b_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ seleccionadas de $A_{\mathbf{s},\chi}$ para un $\mathbf{s} \xleftarrow{\$} U(\mathbb{Z}_q^n)$ (fijo para todas las muestras), encontrar* **s**.

Problema 2 (**LWE**$_{n,q,\chi,m}$ de decisión)**.** *Si se tienen m muestras independientes $(\mathbf{a_i}, b_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ donde cada muestra es seleccionada de (1) $A_{\mathbf{s},\chi}$ para un $\mathbf{s} \xleftarrow{\$} U(\mathbb{Z}_q^n)$ (fijo para todas las muestras), o de (2) la distribución uniforme en $\mathbb{Z}_q^n \times \mathbb{Z}_q$, el problema de decisión consiste en distinguir entre las dos distribuciones de probabilidad.*

En ambos problemas se utiliza un número m de muestras(ecuaciones en la definición 1), por lo que los vectores $\mathbf{a_i}$ se pueden agrupar en una matriz $\mathbf{A}$ de m filas y n columnas. También es posible sustituir los vectores $\mathbf{s}$ y $\mathbf{e}$ por las respectivas matrices $\mathbf{S}$ y $\mathbf{E}$ obteniendo problemas equivalentes, según se demuestra en [13].

Problema LWR y sus variantes.

Definición 2 (Distribución LWR)**.** *Sean n, p y q enteros positivos. Para un vector $\mathbf{s} \in \mathbb{Z}_q^n$, la distribución LWR $O_{\mathbf{s}}$ sobre $\mathbb{Z}_q^n \times \mathbb{Z}_p$ se obtiene seleccionando $\mathbf{a} \xleftarrow{\$} U(\mathbb{Z}_q^n)$ y retornando $(\mathbf{a}, b = \lfloor (\mathbf{a},\mathbf{s}) \rceil_p)$.*

Problema 3 (**LWR**$_{n,p,q,m}$ de búsqueda)**.** *Si se tienen m muestras independientes $(\mathbf{a_i}, b_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_p$ seleccionadas de $O_{\mathbf{s}}$ para un $\mathbf{s} \xleftarrow{\$} U(\mathbb{Z}_q^n)$ (fijo para todas las muestras), encontrar* **s**.

Problema 4 (**LWR**$_{n,p,q,m}$ de decisión)**.** *Si se tienen m muestras independientes $(\mathbf{a_i}, b_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_p$ donde cada muestra es seleccionada de (1) $O_{\mathbf{s}}$ para un $\mathbf{s} \xleftarrow{\$} U(\mathbb{Z}_q^n)$ (fijo para todas las muestras), o de (2) la distribución uniforme en $\mathbb{Z}_q^n \times \mathbb{Z}_p$, el problema de decisión consiste en distinguir entre las dos distribuciones de probabilidad.*

La confiabilidad en los problemas 3 y 4 se debe a que existe una reducción desde el problema LWE hacia el correspondiente problema LWR [4, 2].

Problema 5 (sp-terLWR)**.** *Sean m, n, p, q y h enteros positivos. La variante de **búsqueda** del problema **sp-terLWR** (**ssp-terLWR**) consiste en encontrar $\mathbf{s} \in \{-1,0,1\}^n$ con peso de Hamming h si se tienen m muestras independientes $(\mathbf{a_i}, \lfloor (\mathbf{a_i},\mathbf{s}) \rceil_p)$. La variante de **decisión** del problema **sp-terLWR** (**dsp-terLWR**) consiste en distinguir entre la distribución $(\mathbf{a}, \lfloor (\mathbf{a},\mathbf{s}) \rceil_p)$, dentoda por $O_{\mathbf{s},\mathbf{h}}$, y la uniforme en $\mathbb{Z}_q^n \times \mathbb{Z}_p$ con una ventaja no despreciable, para un valor fijo de $\mathbf{s} \in \{-1,0,1\}^n$ con peso de Hamming h.*

De acuerdo con [9] la dificultad del problema anterior puede obtenerse desde el problema LWE con la misma distribución para el secreto, teniendo en cuenta que la reducción de LWE hacia LWR es independiente de la distribución del secreto. En el caso del problema LWE con peso de Hamming h para el secreto, está demostrada una reducción hacia el problema LWE en [8].

2. Descripción del protocolo

El protocolo propuesto en este trabajo se basa en la dificultad de resolver la siguiente variante del problema 5:

Problema 6 (sp-ter**LWR**$_{m,n,p,q,h,\bar{n}}$)**.** *Sean m, n, $\bar{n}$, p, q y h enteros positivos. La variante de **búsqueda** del problema **sp-ter**LWR$_{m,n,p,q,h,\bar{n}}$ (**ssp-ter**LWR$_{m,n,p,q,h,\bar{n}}$) consiste en encontrar una matriz* $\mathbf{S}$ *formada por vectores columnas con peso de Hamming h, tal que $\lfloor \mathbf{AS} \rceil_p = \mathbf{B}$. La variante de **decisión** del problema **sp-ter**LWR$_{m,n,p,q,h,\bar{n}}$ (**dsp-ter**LWR$_{m,n,p,q,h,\bar{n}}$) consiste en distinguir entre la distribución $(\mathbf{A}, \lfloor \mathbf{AS} \rceil_p)$, dentoda por $O_{\mathbf{S},\mathbf{h}}$, y la uniforme en $\mathbb{Z}_q^{m \times n} \times \mathbb{Z}_p^{m \times \bar{n}}$.*

Esto no es mas que la variante que utiliza matrices para el secreto, donde $\bar{n}$ representa las instancias del problema 5, $\mathbf{A}^{m \times n}$ los coeficientes de las n ecuaciones y $\mathbf{S}^{n \times \bar{n}}$ los $\bar{n}$ vectores secretos.

Lema 4. *Existe una reducción polinomial del problema 5 (**sp-terLWR**) hacia el problema 6 (**sp-ter**LWR$_{m,n,p,q,h,\bar{n}}$).*

Esta reducción se puede demostrar siguiendo un razonamiento similar a [13]. (está escrita pero no digital.....)
El protocolo comienza con la definición de los siguientes parámetros públicos:

- q: el módulo mayor del problema LWR.
- p: el módulo utilizado para redondear, el cual es una potencia de 2 y divide a q.
- n: la dimensión del problema LWR, y también la dimensión de la matriz pública $\mathbf{A} \in \mathbb{Z}_q^{n \times n}$.
- h: el peso de Hamming del secreto.
- $\bar{n}, \bar{m}$: número de intancias del problema LWR creadas por Alice y Bob respectivamente.
- B: cantidad de bits que se extraen por cada coeficiente.
- **seed**$_{\mathbf{A}}$: semilla con la que se inicializa un generador de números pseudoaleatorios para obtener la matriz $\mathbf{A}$.
- s: tamaño en bits de la semilla.

Basados en los parámetros públicos anteriores, Alice y Bob utilizan el protocolo descrito en la Figura 1 para acordar la clave secreta $\mathbf{K}$.

Ambas partes siempre puedan calcular el mismo valor de $\mathbf{K}$, lo cual lo establece el siguiente teorema:

Alice		Bob
$\mathbf{seed_A} \xleftarrow{\$} U(\{0,1\}^s)$		
$\mathbf{A} \leftarrow Gen(\mathbf{seed_A})$		
$\mathbf{S} \xleftarrow{\$} \mathscr{HW}_n(h)^{\bar{n}}$		
$\mathbf{B} \leftarrow \lfloor \mathbf{AS} \rceil_p$	$\xrightarrow[\in \{0,1\}^s \times \mathbb{Z}_q^{n\times\bar{n}}]{\mathbf{seed_A},\mathbf{B}}$	$\mathbf{A} \leftarrow Gen(\mathbf{seed_A})$
		$\mathbf{S'} \xleftarrow{\$} \mathscr{HW}_n(h)^{\bar{m}}$
		$\bar{\mathbf{V}} \leftarrow \lfloor \mathbf{S'}^\top \mathsf{Inv}(\mathbf{B}) \rceil_p$
		$\mathbf{V} \leftarrow \mathsf{Inv}(\bar{\mathbf{V}})$
		$\mathbf{C} \leftarrow \langle \mathbf{V} \rangle_{2^B}$
$\mathbf{V'} \leftarrow \mathsf{Inv}(\mathbf{B'})\mathbf{S}$	$\xleftarrow[\in \mathbb{Z}_q^{\bar{m}\times n} \times \mathbb{Z}_2^{\bar{m}\times\bar{n}}]{\mathbf{B'},\mathbf{C}}$	$\mathbf{B'} \leftarrow \lfloor \mathbf{S'}^\top \mathbf{A} \rceil_p$
$\mathbf{K} \leftarrow rec(\mathbf{V'}, \mathbf{C})$		$\mathbf{K} \leftarrow [\mathbf{V}]_{2^B}$

Figura 1. El protocolo de intercambio de claves basado en el problema LWR con parámetros (n, p, q) y los parámetros $\bar{n}, \bar{m}, h, B \in \mathbb{Z}$ propios de la instancia del protocolo. La matriz $\mathbf{A}$ se genera utilizando un generador de números pseudoaleatorios *Gen* con semilla $\mathbf{seed_A}$.

Teorema 1. *Si se cumple la relación* $2h+1 < p/2^{B+2}$*, entonces ambas partes obtienen el mismo valor de* $\mathbf{K}$*.*

Demostración. Calculemos los valores de $\mathbf{V'}$ y $\mathbf{V}$.

$$\mathbf{V'} = \mathsf{Inv}(\mathbf{B'})\mathbf{S} = (\mathbf{S'}^\top \mathbf{A} + \mathbf{E_1})\mathbf{S} = \mathbf{S'}^\top \mathbf{AS} + \mathbf{E_1 S}$$

$$\mathbf{V} = \mathsf{Inv}(\bar{\mathbf{V}}) = \mathbf{S'}^\top \mathsf{Inv}(\mathbf{B}) + \mathbf{E_2} = \mathbf{S'}^\top (\mathbf{AS} + \mathbf{E_3}) + \mathbf{E_2} = \mathbf{S'}^\top \mathbf{AS} + \mathbf{S'}^\top \mathbf{E_3} + \mathbf{E_2}$$

Como $\|\mathbf{E_1}\|_\infty < q/p, \|\mathbf{E_2}\|_\infty < q/p, \|\mathbf{E_3}\|_\infty < q/p$ y $\mathbf{S}, \mathbf{S'}$ tienen h entradas $\in \{-1, 1\}$ entonces $\|\mathbf{E_1 S}\|_\infty < hq/p$ y $\|\mathbf{S'}^\top \mathbf{E_3}\|_\infty < hq/p$ por lo que

$$\|\mathbf{V} - \mathbf{V'}\|_\infty = \|\mathbf{S'}^\top \mathbf{E_3} + \mathbf{E_2} - \mathbf{E_1 S}\|_\infty < 2hq/p + q/p$$

y hacemos $2hq/p + q/p < q/2^{B+2}$, aplicando el lema 3 obtenemos el resultado esperado. □

3. Análisis de la seguridad

Nuestro análisis de la seguridad utiliza los mismos mecanismos que [3] en cuanto a:

- Ataques utilizando los algoritmos de reducción en *lattices*.
- Ataques especializados que explotan el uso del secreto con un peso de Hamming determinado.
- Consideraciones para el cálculo de la matriz $\mathbf{A}$.

y agregamos la demostración de la uniformidad de la clave obtenida $\mathbf{K}$ y la propiedad IND-CPA del protocolo.

3.1 Uniformidad de la clave

Teorema 2. *En el protocolo mostrado en la Figura 1, el valor de* $[\mathbf{V}]_{2^B}$ *es uniforme conociendo* $\langle \mathbf{V} \rangle_{2^B}$*.*

Demostración. Por el lema 1 si $x \in \mathbb{Z}_p$ es uniforme, entonces lo es también $\mathsf{Inv}(x)$. Asumiendo que el problema **dsp-terLWR**$_{n,p,q,h,\bar{n}}$ es difícil, entonces $\mathbf{B} \leftarrow \lfloor \mathbf{AS} \rceil_p$ es uniforme en $\mathbb{Z}_p$ por lo que $\mathsf{Inv}(\mathbf{B})$ también lo es en $\mathbb{Z}_p$ y por consiguiente $\bar{\mathbf{V}} \leftarrow \lfloor \mathbf{S'}^\top \mathsf{Inv}(\mathbf{B}) \rceil_p$ constituye una instancia del problema **dsp-terLWR**$_{n,p,q,h,\bar{n}}$ lo que implica que $\bar{\mathbf{V}}$ sea uniforme. Aplicando el lema 2 a $\mathbf{V} = \mathsf{Inv}(\bar{\mathbf{V}})$, que es uniforme también, se obtiene el resultado esperado. □

3.2 Demostración de la propiedad IND-CPA

Para probar la seguridad del protocolo se considera a un adversario que intenta distinguir entre una clave de sesión K y una uniforme K' conociendo los valores públicos del protocolo. Formalmente se define la ventaja de tal adversario $\mathscr{A}$ como

donde los valores de $\mathbf{A}, \mathbf{B}, \mathbf{B'}, \mathbf{C}, K$ se muestran en la Figura 1.

El siguiente teorema implica que bajo la suposición de que el problema 5 (de decisión) es difícil, todos los adversarios eficientes obtienen una ventaja infinitesimal con respecto al protocolo mostrado en la Figura 1.

Teorema 3. *Sean n, $\bar{n}$, $\bar{m}$, p, q y h enteros positivos. Si el problema* ***dsp-ter*LWR** *(ver problema 5) es difícil, entonces el protocolo desarrollado genera claves con una distribución indistinguible de la uniforme. De forma más exacta,*

$$\mathsf{Adv}^{ddh-like}_{n,p,q,h,\bar{n},B}(\mathscr{A}) \leq \bar{n} \cdot \mathsf{Adv}^{dsp-terLWR}_{n,p,q,h}(\mathscr{A} \circ \mathscr{B}_1) + \bar{m} \cdot \mathsf{Adv}^{dsp-terLWR}_{n,p,q,h}(\mathscr{A} \circ \mathscr{B}_2)$$

donde $\mathscr{B}_1$ *y* $\mathscr{B}_2$ *se muestran en la Figura 3.*

Experimento 1

$\mathbf{A} \xleftarrow{\$} U(\mathbb{Z}_q^{n\times n})$
$\mathbf{S} \xleftarrow{\$} \mathscr{HWT}_n(h)^{\bar{n}}$
$\mathbf{B} \leftarrow \lfloor \mathbf{AS} \rceil_p$
$\mathbf{S}' \xleftarrow{\$} \mathscr{HWT}_n(h)^{\bar{m}}$
$\mathbf{B}' \leftarrow \lfloor \mathbf{S}'^{\top}\mathbf{A} \rceil_p$
$\bar{\mathbf{V}} \leftarrow \lfloor \mathbf{S}'^{\top}\mathsf{Inv}(\mathbf{B}) \rceil_p$
$\mathbf{C} \leftarrow \langle \mathsf{Inv}(\bar{\mathbf{V}}) \rangle_{2^B}$
$\mathbf{K} \leftarrow [\mathsf{Inv}(\bar{\mathbf{V}})]_{2^B}$
$\mathbf{K}' \xleftarrow{\$} U(\{0,1\}^{\bar{n}\cdot\bar{m}\cdot B})$
$b^* \xleftarrow{\$} U(\{0,1\})$
if $b^* = 0$
return $(\mathbf{A},\mathbf{B},\mathbf{B}',\mathbf{C},\mathbf{K})$
else
return $(\mathbf{A},\mathbf{B},\mathbf{B}',\mathbf{C},\mathbf{K}')$

Experimento 2

$\mathbf{A} \xleftarrow{\$} U(\mathbb{Z}_q^{n\times n})$
$\mathbf{B} \xleftarrow{\$} U(\mathbb{Z}_p^{n\times \bar{n}})$
$\mathbf{S}' \xleftarrow{\$} \mathscr{HWT}_n(h)^{\bar{m}}$
$\mathbf{B}' \leftarrow \lfloor \mathbf{S}'^{\top}\mathbf{A} \rceil_p$
$\bar{\mathbf{V}} \leftarrow \lfloor \mathbf{S}'^{\top}\mathsf{Inv}(\mathbf{B}) \rceil_p$
$\mathbf{C} \leftarrow \langle \mathsf{Inv}(\bar{\mathbf{V}}) \rangle_{2^B}$
$\mathbf{K} \leftarrow [\mathsf{Inv}(\bar{\mathbf{V}})]_{2^B}$
$\mathbf{K}' \xleftarrow{\$} U(\{0,1\}^{\bar{n}\cdot\bar{m}\cdot B})$
$b^* \xleftarrow{\$} U(\{0,1\})$
if $b^* = 0$
return $(\mathbf{A},\mathbf{B},\mathbf{B}',\mathbf{C},\mathbf{K})$
else
return $(\mathbf{A},\mathbf{B},\mathbf{B}',\mathbf{C},\mathbf{K}')$

Experimento 3

$\mathbf{A} \xleftarrow{\$} U(\mathbb{Z}_q^{n\times n})$
$\mathbf{B} \xleftarrow{\$} U(\mathbb{Z}_p^{n\times \bar{n}})$
$\mathbf{S}' \xleftarrow{\$} \mathscr{HWT}_n(h)^{\bar{m}}$
$[\mathbf{B}'\|\bar{\mathbf{V}}] \leftarrow \lfloor \mathbf{S}'^{\top}[\mathbf{A}\|\mathsf{Inv}(\mathbf{B})] \rceil_p$
$\mathbf{C} \leftarrow \langle \mathsf{Inv}(\bar{\mathbf{V}}) \rangle_{2^B}$
$\mathbf{K} \leftarrow [\mathsf{Inv}(\bar{\mathbf{V}})]_{2^B}$
$\mathbf{K}' \xleftarrow{\$} U(\{0,1\}^{\bar{n}\cdot\bar{m}\cdot B})$
$b^* \xleftarrow{\$} U(\{0,1\})$
if $b^* = 0$
return $(\mathbf{A},\mathbf{B},\mathbf{B}',\mathbf{C},\mathbf{K})$
else
return $(\mathbf{A},\mathbf{B},\mathbf{B}',\mathbf{C},\mathbf{K}')$

Experimento 4

$\mathbf{A} \xleftarrow{\$} U(\mathbb{Z}_q^{n\times n})$
$\mathbf{B} \xleftarrow{\$} U(\mathbb{Z}_p^{n\times \bar{n}})$
$[\mathbf{B}'\|\bar{\mathbf{V}}] \xleftarrow{\$} U(\mathbb{Z}_p^{\bar{m}\times(n+\bar{n})})$
$\mathbf{C} \leftarrow \langle \mathsf{Inv}(\bar{\mathbf{V}}) \rangle_{2^B}$
$\mathbf{K} \leftarrow [\mathsf{Inv}(\bar{\mathbf{V}})]_{2^B}$
$\mathbf{K}' \xleftarrow{\$} U(\{0,1\}^{\bar{n}\cdot\bar{m}\cdot B})$
$b^* \xleftarrow{\$} U(\{0,1\})$
if $b^* = 0$
return $(\mathbf{A},\mathbf{B},\mathbf{B}',\mathbf{C},\mathbf{K})$
else
return $(\mathbf{A},\mathbf{B},\mathbf{B}',\mathbf{C},\mathbf{K}')$

Figura 2. Secuencia de experimentos para la prueba del Teorema 3.

$$\mathsf{Adv}^{ddh-like}_{n,p,q,h,\bar{n},B}(\mathscr{A}) \quad = \quad |Pr[\mathscr{A}(\mathbf{A},\mathbf{B},\mathbf{B}',\mathbf{C},K)=1] - Pr[\mathscr{A}(\mathbf{A},\mathbf{B},\mathbf{B}',\mathbf{C},K')=1]|,$$

Demostración. La demostración sigue la metodología basada en experimentos ampliamente utilizada en la criptografía basada en *lattices* [5, 16, 6]. Sea S_i el evento de adivinar el bit b^* en el **Experimento** i de la Figura 2.

Experimento 1. Este es el experimento real, donde los mensajes son generados honetsamente según la Figura 1. En el experimento 1 los pares LWR son $(\mathbf{A},\mathbf{B})$ con secreto $\mathbf{S}$; y $(\mathbf{A},\mathbf{B}')$ y $(\mathbf{B},\mathbf{V})$ con secreto $\mathbf{S}'$. Por lo tanto

$$\mathsf{Adv}^{ddh-like}_{n,p,q,h,\bar{n},B}(\mathscr{A}) = |Pr(S_1) - 1/2| \tag{1}$$

Experimento 2. En este experimento la clave pública de Alice es generada de manera aleatoria. Los pares LWR son $(\mathbf{A},\mathbf{B}')$ y $(\mathbf{B},\mathbf{V})$ con secreto $\mathbf{S}'$.

Diferencias entre el Experimento 1 y el Experimento 2. En el Experimento 1, $(\mathbf{A},\mathbf{B})$ es elegido según $O_{\mathbf{S},\mathbf{h}}$. En el Experimento 2, $(\mathbf{A},\mathbf{B})$ es elegido según $\mathscr{U}(\mathbb{Z}_q^{n\times n}) \times \mathscr{U}(\mathbb{Z}_p^{n\times\bar{n}})$. Suponiendo que el problema **dsp-terLWR** es difícil, entonces las dos distribuciones son indistinguibles con un factor $\bar{n}$ según lo demostrado en el lema 4.

Sea el algoritmo $\mathscr{B}_1$ de la Figura 3 que toma como entrada el par $(\mathbf{A},\mathbf{B})$. Cuando $(\mathbf{A},\mathbf{B})$ es elgido de $O_{\mathbf{S},\mathbf{h}}$ donde $\mathbf{S} \xleftarrow{\$} \mathscr{HWT}_n(h)^{\bar{n}}$, entonces la salida de $\mathscr{B}_1$ se distribuye exactamente como en el Experimento 1. Cuando $(\mathbf{A},\mathbf{B})$ es elgido de $\mathscr{U}(\mathbb{Z}_q^{n\times n}) \times \mathscr{U}(\mathbb{Z}_p^{n\times\bar{n}})$, entonces la salida de $\mathscr{B}_1$ se distribuye exactamente como en el Experimento 2. Por lo tanto, si $\mathscr{A}$ puede distinguir entre los experimentos 1 y 2, entonces $\mathscr{A}\circ\mathscr{B}_1$ puede distinguir las distribuciones $O_{\mathbf{S},\mathbf{h}}$ o $\mathscr{U}(\mathbb{Z}_q^{n\times n}) \times \mathscr{U}(\mathbb{Z}_p^{n\times\bar{n}})$. Entonces,

$$\begin{aligned} |Pr(S_1) - Pr(S_2)| \leq \quad & \mathsf{Adv}^{dsp-terLWR}_{n,p,q,h,\bar{n}}(\mathscr{A}\circ\mathscr{B}_1) \\ \mathsf{Adv}^{dsp-terLWR}_{n,p,q,h,\bar{n}}(\mathscr{A}\circ\mathscr{B}_1) \leq \quad & \bar{n}\cdot\mathsf{Adv}^{dsp-terLWR}_{n,p,q,h}(\mathscr{A}\circ\mathscr{B}_1) \end{aligned} \tag{2}$$

Experimento 3. El Experimento 3 es una simple reescritura del Experimento 2. La clave pública de Bob $\mathbf{B}'$ y el secreto $\bar{\mathbf{V}}$ son simultaneamente generados de $\mathbf{S}'$. El par LWR es $([\mathbf{A}\|\mathsf{Inv}(\mathbf{B})],[\mathbf{B}'\|\bar{\mathbf{V}}])$ con secreto $\mathbf{S}'$, lo que constituye una instancia del problema 6 con parámetros $(n+\bar{n}),p,q,h,\bar{m}$.

Diferencias entre el Experimento 2 y el Experimento 3. Como el Experimento 3 es una reescritura del Experimento 2 se tiene que

$$Pr(S_2) = Pr(S_3) \tag{3}$$

Experimento 4. En el Experimento 4 no hay pares LWR, los valores de $\mathbf{B}'$ y $\bar{\mathbf{V}}$ son generados de forma uniforme.

Diferencias entre el Experimento 3 y el Experimento 4. En el Experimento 3, $([\mathbf{A}\|\mathsf{Inv}(\mathbf{B})],[\mathbf{B}'\|\bar{\mathbf{V}}])$ es elegido según $O_{\mathbf{S},\mathbf{h}}$ con parámetros$(n+\bar{n}),p,q,h,\bar{m}$. En el Experimento 4, $([\mathbf{A}\|\mathsf{Inv}(\mathbf{B})],[\mathbf{B}'\|\bar{\mathbf{V}}])$ es elegido según $\mathscr{U}(\mathbb{Z}_q^{n\times(n+\bar{n})}) \times \mathscr{U}(\mathbb{Z}_p^{\bar{m}\times(n+\bar{n})})$. Suponiendo que el problema **dsp-terLWR** es

$\underline{\mathscr{B}_1(\mathbf{A},\mathbf{B})}$

1: $\mathbf{S}' \xleftarrow{\$} \mathscr{HWT}_n(h)^{\bar{m}}$
2: $\mathbf{B}' \leftarrow \lfloor \mathbf{S}'^{\top}\mathbf{A} \rceil_p$
3: $\bar{\mathbf{V}} \leftarrow \lfloor \mathbf{S}'^{\top}\mathsf{Inv}(\mathbf{B}) \rceil_p$
4: $\mathbf{C} \leftarrow \left\langle \mathsf{Inv}(\bar{\mathbf{V}}) \right\rangle_{2^B}$
5: $\mathbf{K} \leftarrow [\mathsf{Inv}(\bar{\mathbf{V}})]_{2^B}$
6: $\mathbf{K}' \xleftarrow{\$} U(\{0,1\}^{\bar{n}\cdot\bar{m}\cdot B})$
7: $b^* \xleftarrow{\$} U(\{0,1\})$
8: **if** $b^* = 0$ **return** $(\mathbf{A},\mathbf{B},\mathbf{B}',\mathbf{C},\mathbf{K})$
9: **else return** $(\mathbf{A},\mathbf{B},\mathbf{B}',\mathbf{C},\mathbf{K}')$

$\underline{\mathscr{B}_2(\mathbf{Y},\mathbf{Z})}$

1: $\begin{bmatrix}\mathbf{A}^{\top}\\ \mathbf{B}^{\top}\end{bmatrix} \leftarrow \mathbf{Y}$
2: $\begin{bmatrix}\mathbf{B}'^{\top}\\ \bar{\mathbf{V}}^{\top}\end{bmatrix} \leftarrow \mathbf{Z}$
3: $\mathbf{C} \leftarrow \left\langle \mathsf{Inv}(\bar{\mathbf{V}}) \right\rangle_{2^B}$
4: $\mathbf{K} \leftarrow [\mathsf{Inv}(\bar{\mathbf{V}})]_{2^B}$
5: $\mathbf{K}' \xleftarrow{\$} U(\{0,1\}^{\bar{n}\cdot\bar{m}\cdot B})$
6: $b^* \xleftarrow{\$} U(\{0,1\})$
7: **if** $b^* = 0$ **return** $(\mathbf{A},\mathbf{B},\mathbf{B}',\mathbf{C},\mathbf{K})$
8: **else return** $(\mathbf{A},\mathbf{B},\mathbf{B}',\mathbf{C},\mathbf{K}')$

Figura 3. Reducciones para la prueba del Teorema 3.

difícil, entonces las dos distribuciones son indistinguibles con un factor $\bar{m}$ según lo demostrado en el lema 4.

Sea el algoritmo $\mathscr{B}_2$ de la Figura 3 que toma como entrada el par $(\mathbf{Y},\mathbf{Z})$. Cuando $(\mathbf{Y},\mathbf{Z})$ es elgido de $O_{\mathbf{S}'^{\top},\mathbf{h}}$ donde $\mathbf{S}' \xleftarrow{\$} \mathscr{HWT}_n(h)^{\bar{m}}$, entonces la salida de $\mathscr{B}_2$ se distribuye exactamente como en el Experimento 3. Cuando $(\mathbf{Y},\mathbf{Z})$ es elgido de $\mathscr{U}(\mathbb{Z}_q^{n\times n}) \times \mathscr{U}(\mathbb{Z}_p^{n\times\bar{n}})$, entonces la salida de $\mathscr{B}_2$ se distribuye exactamente como en el Experimento 4. Por lo tanto, si $\mathscr{A}$ puede distinguir entre los experimentos 3 y 4, entonces $\mathscr{A}\circ\mathscr{B}_2$ puede distinguir las distribuciones $O_{\mathbf{S}'^{\top},\mathbf{h}}$ o $\mathscr{U}(\mathbb{Z}_q^{n\times n}) \times \mathscr{U}(\mathbb{Z}_p^{n\times\bar{n}})$. Entonces,

$$\begin{aligned} |Pr(S_3) - Pr(S_4)| &\leq \mathsf{Adv}^{dsp-terLWR}_{n+\bar{n},p,q,h,\bar{m}}(\mathscr{A}\circ\mathscr{B}_2) \\ \mathsf{Adv}^{dsp-terLWR}_{n+\bar{n},p,q,h,\bar{m}}(\mathscr{A}\circ\mathscr{B}_2) &\leq \bar{m}\cdot\mathsf{Adv}^{dsp-terLWR}_{n+\bar{n},p,q,h}(\mathscr{A}\circ\mathscr{B}_2) \end{aligned} \quad (4)$$

Sumando las desigualdades 2 y 4, queda

que después de sustituir la ecuación 3 nos

Partiendo de que en el Experimento 4 se cumple $Pr(S_4) = 1/2$ y con la ecuación 1 obtenemos el resultado esperado. □

4. Conclusiones y trabajo futuro

En el presente trabajo se desarrolló un protocolo para el intercambio de claves criptográficas del tipo DH que basa su seguridad en una variante del problema LWR. Con respecto a [3], se utilizó un mecanismo de reconciliacón similar pero garantizando la uniformidad de la clave acordada y la demostración de la propiedad IND-CPA. Con respecto a [5], se obtuvo una variante más eficiente debido a que no se necesita la generación de números gaussianos.
Como trabajo futuro queda:

1. Reducción más ajustada del problema **LWE** hacia el **sp-terLWR**.
2. Cálculo de los parámetros.
3. Implementación y cálculo del rendimiento.

Referencias

[1] Hayo Baan, Sauvik Bhattacharya, Oscar Garcia-Morchon, Ronald Rietman, Ludo Tolhuizen, Jose-Luis Torre-Arce, and Zhenfei Zhang. Round2: Kem and pke based on glwr. Cryptology ePrint Archive, Report 2017, 2017. http://eprint.iacr.org/2017.

[2] Abhishek Banerjee, Chris Peikert, and Alon Rosen. Pseudorandom functions and lattices. Cryptology ePrint Archive, Report 2011/401, 2011. http://eprint.iacr.org/2011/401.

[3] Sauvik Bhattacharya, Oscar Garcia-Morchon, Ronald Rietman, and Ludo Tolhuizen. spkex: An optimized lattice-based key-exchange. Cryptology ePrint Archive, Report 2017, 2017. http://eprint.iacr.org/2017.

[4] Andrej Bogdanov, Siyao Guo, Daniel Masny, Silas Richelson, and Alon Rosen. On the hardness of learning with rounding over small modulus. Cryptology ePrint Archive, Report 2015, 2015. http://eprint.iacr.org/2015.

[5] Joppe Bos, Craig Costello, Leo Ducas, Ilya Mironov, Michael Naehrig, Valeria Nikolaenko, Ananth Raghunathan, and Douglas Stebila. Frodo: Take off the ring! practical, quantum-secure key exchange from lwe. Cryptology ePrint Archive, Report 2016/659, 2016. http://eprint.iacr.org/2016/659.

[6] Joppe W. Bos, Craig Costello, Michael Naehrig, and Douglas Stebila. Post-quantum key exchange for the tls protocol from the ring learning with errors problem. Cryptology ePrint Archive, Report 2014/599, 2014. http://eprint.iacr.org/.

[7] Long Chen, Zhenfeng Zhang, and Zhenfei Zhang. On the hardness of the computational ring-lwr problem and its applications. Cryptology ePrint Archive, Report 2018, 2018. http://eprint.iacr.org/2018.

$$|Pr(S_1) - Pr(S_4)| \quad \leq \quad \bar{n} \cdot \mathsf{Adv}^{dsp-terLWR}_{n,p,q,h}(\mathscr{A} \circ \mathscr{B}_1) + \bar{m} \cdot \mathsf{Adv}^{dsp-terLWR}_{n,p,q,h}(\mathscr{A} \circ \mathscr{B}_2)$$

[8] Jung Hee Cheon, Kyoo Hyung Han, Jinsu Kim, Changmin Lee, and Yongha Son. A practical post-quantum public-key cryptosystem based on splwe. Cryptology ePrint Archive, Report 2016/1055, 2016. http://eprint.iacr.org/2016/1055.

[9] Jung Hee Cheon, Duhyeong Kim, Joohee Lee, and Yongsoo Song. Lizard: Cut off the tail! practical post-quantum public-key encryption from lwe and lwr. Cryptology ePrint Archive, Report 2016/1126, 2016. http://eprint.iacr.org/2016/1126.

[10] Jan-Pieter D'Anvers, Angshuman Karmakar, Sujoy Sinha Roy, and Frederik Vercauteren. Saber: Module-lwr based key exchange, cpa-secure encryption and cca-secure kem. Cryptology ePrint Archive, Report 2018, 2018. http://eprint.iacr.org/2018.

[11] Jintai Ding, Xiang Xie, and Xiaodong Lin. A simple provably secure key exchange scheme based on the learning with errors problem. Cryptology ePrint Archive, Report 2012/688, 2012. http://eprint.iacr.org/2012/688.

[12] Atsushi Fujioka, Koutarou Suzuki, Keita Xagawa, and Kazuki Yoneyama. Strongly secure authenticated key exchange from factoring, codes, and lattices. Cryptology ePrint Archive, Report 2012/211, 2012. http://eprint.iacr.org/.

[13] Daniele Micciancio. On the hardness of learning with errors with binary secrets. Cryptology ePrint Archive, Report 2018, 2018. http://eprint.iacr.org/2018.

[14] National Institute of Standards and Technology. Proposed submission requirements and evaluation criteria for thepost-quantum cryptography standardization process, 2016. http://csrc.nist.gov/groups/ST/post-quantum-crypto/documents/call-for-proposals-draft-aug-2016.pdf.

[15] National Institute of Standards and Technology. Proposed submission for the post-quantum cryptography standardization process, 2017. https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions.

[16] Chris Peikert. Lattice cryptography for the internet. Cryptology ePrint Archive, Report 2014/070, 2014. http://eprint.iacr.org/.

[17] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In ACM, editor, *Thirty-seventh Annual ACM Symposium on Theory of Computing*, pages 84–93, 2005.

[18] Peter W. Shor. Polynominal time algorithms for discrete logarithms and factoring on a quantum computer. In *Lecture Notes in Computer Science*, volume 877, page 289. Springer, 1994.

[19] Song Y. Yan. *Quantum Attacks on Public-Key Cryptosystems*. Springer, 2013.

[20] Jiang Zhang, Zhenfeng Zhang, Jintai Ding, Michael Snook, and Özgür Dagdelen. Authenticated key exchange from ideal lattices. Cryptology ePrint Archive, Report 2014/589, 2014. http://eprint.iacr.org/.