Cifrado de la información mediante un algoritmo hibrido basado en matrices de rotación cuaterniónica

M. A. Salazar-Ramirez, H. Oviedo-Galdeano, J. A. López-Toledo
Instituto Politécnico Nacional, SEPI Zacatenco, Ciudad de México, México. C.P.07320
msalazarr1401@alumno.ipn.mx

***Resumen*— En el presente trabajo se aborda la construcción de la matriz de rotación cuaterniónica para el desarrollo de un algoritmo hibrido combinado con el protocolo BB84. Se emplea Python para realizar los cálculos de la matriz de rotación cuaterniónica cifrada, el resultado es el mensaje para transmitir en el canal de comunicación. En el receptor se realiza el proceso inverso para el descifrado de la información. Para evaluar y comparar el grado de fiabilidad y seguridad de la información recibida, se programa el coeficiente de correlación.**

***Palabras Clave* — Cuaterniones, Matriz de rotación Cuaterniónica, Criptografia, Seguridad en redes, Protocolo BB84.**

Abstract- This paper is devoted to the construction of the quaternionic rotation matrix for the development of a hybrid algorithm combined with the BB84 protocol. Python is used to perform the calculations of the encrypted quaternionic rotation matrix, the result of which is the message to be transmitted on the communication channel. At the receiver, the reverse process is performed to decrypt the information. In order to evaluate and compare the degree of reliability and security of the information received, the correlation coefficient is programmed.

***Keywords* — Quaternions, Quaternionic Rotation Matrix, Cryptography, Network Security, BB84 Protocol.**

I. INTRODUCCIÓN

La continua evolución en el ámbito de la seguridad en redes impulsa la investigación de técnicas criptográficas más eficientes y resistentes a ataques. Una de las herramientas que se utiliza en este trabajo es el cifrado cuaterniónico para ofrecer una mayor seguridad y posibilidad de combinarse con otros protocolos de seguridad que refuercen la gestión y la distribución segura de claves en un sistema de comunicación [1-3].

Para llevar a cabo el cifrado, se considera inicialmente la transformación de los datos que pueden abarcar desde texto plano hasta imágenes en blanco y negro en una o varias matrices cuaterniónicas [4, 5]. Esta rotación altera la estructura interna de cada elemento cuaterniónico, modificando de manera no lineal la información y dificultando su lectura por parte de agentes no autorizados.

En el proceso de descifrado, se recurre a la matriz cuaterniónica inversa [4,5], utilizando la misma clave se restablece la información a su forma original.

El uso de matriz de rotación cuaterniónica combinada con el protocolo BB84 [6-10], representa una propuesta innovadora que aprovecha las ventajas de ambos dando como resulta un modelo de cifrado hibrido aplicable múltiples tipos de servicios tales como: voz, datos y video.

Los resultados que se presentan en este esquema criptográfico permiten la evaluación de parámetros como el tiempo de procesamiento e integridad de los datos tras ciclos de cifrado/descifrado. Conforme incrementa la demanda de sistemas capaces de proteger datos sensibles, el cifrado cuaterniónico resulta ser un mecanismo prometedor para garantizar la confidencialidad, la autenticidad y la disponibilidad de la información en tránsito y en reposo.

II. METODOLOGÍA/DESARROLLO

Para el desarrollo del trabajo sobre el cifrado de datos para un sistema de comunicación, los cuaterniones son la base de nuestra propuesta [11-14], fueron propuestos en el año de 1843 por William Rowan Hamilton. A continuación, se definen propiedades y operaciones fundamentales necesarias para su aplicación.

2.1. Cuaterniones

También denominados números Hipercomplejos, son considerados una extensión de los números complejos, están compuestos por dos partes: una escalar y una vectorial. Sea $H(\mathbb{R})$ el conjunto de cuaterniones reales, la representación de H es en honor a su creador.

Un cuaternión $q \in H(\mathbb{R})$ es representado por la expresión:

$$q = q_0 + \sum_{j=1}^{3} q_j i_j = q_0 + q_1 i_1 + q_2 i_2 + q_3 i_3, \quad (1)$$

donde $q_0, q_1, q_2, q_3 \in \mathbb{R}$ y i_1, i_2, i_3 son unidades imaginarias cuaterniónicas. Otra manera de representar un cuaternión real o complejo es como la suma de un escalar y un vector:

$$q = q_0 + \vec{q}, \quad (2)$$

$$\vec{q} = \sum_{k=1}^{3} q_k i_k, \tag{3}$$

donde q_0 representa la parte escalar y $\vec{q}$ representa la parte vectorial.

El producto de las unidades imaginarias debe cumplir con las siguientes igualdades:

$$i_1^2 = i_2^2 = i_3^2 = -1, \tag{4}$$

$$i_1 i_2 = -i_2 i_1 = i_3, \tag{5}$$

$$i_2 i_3 = -i_3 i_2 = i_1, \tag{6}$$

$$i_3 i_1 = -i_1 i_3 = i_2. \tag{7}$$

Se enlistan las operaciones fundamentales con los cuaterniones. Considérese un segundo cuaternión denominado $p = p_0 + p_1 i_1 + p_2 i_2 + p_3 i_3$, donde $p \in H(\mathbb{R})$.

Suma y resta

$$q \pm p = (q_0 \pm p_0) + \sum_{k=1}^{3} (q_k \pm p_k) i_k. \tag{8}$$

Producto

$$qp = q_0 p_0 + p_0 \vec{q} + q_0 \vec{p} - \langle \vec{q}, \vec{p} \rangle + [\vec{q} \times \vec{p}]. \tag{9}$$

Nota: el producto entre dos cuaterniones no es conmutativo $qp \neq pq$, como se puede observar en (5 – 7).

Cociente

$$qp^{-1} = \frac{p\bar{q}}{|q|^2}, pq^{-1} = \frac{p\bar{q}}{|q|^2}. \tag{10}$$

Producto Vectorial

$$\vec{q} \times \vec{p} = \begin{vmatrix} i_1 & i_2 & i_3 \\ q_1 & q_2 & q_3 \\ p_1 & p_2 & p_3 \end{vmatrix}. \tag{11}$$

Producto Escalar

$$\langle \vec{q}, \vec{p} \rangle = q_0 p_0 + q_1 p_1 + q_2 p_2 + q_3 p_3. \tag{12}$$

2.2. Propiedades

La norma de un cuaternión está dada por:

$$|q| = \sqrt{q_0^2 + q_1^2 + q_2^2 + q_3^2} = \sqrt{q\bar{q}}, \tag{13}$$

el conjugado cuaternionico de $q = q_0 + \vec{q}$, se define como el cambio de signo solo en la parte vectorial, está dado por:

$$\bar{q} = q_0 - q_1 i_1 - q_2 i_2 - q_3 i_3 = q_0 - \vec{q}, \tag{14}$$

el inverso de un cuaternión es considerado el inverso multiplicativo de q, dado que el producto de cuaterniones no es conmutativo, está dado por la expresión:

$$q^{-1} = \frac{\bar{q}}{|q|^2}. \tag{15}$$

2.3. Construcción de la matriz de rotación cuaterniónica $R(q)$.

El cifrado y descifrado de datos, se realiza a través de la aplicación de la matriz de rotación cuaterniónica $R(q)$. Mediante este proceso, la información a encriptar es distribuida en bloques binarios de 24 bits de tal forma que formen los puntos $\vec{p}$, esto garantiza que su contenido resulte incomprensible para cualquier agente externo que intente interceptarla en el canal de comunicación.

Considérense los cuaterniones p y q, con $p_0 = 0$, por lo que $p = \vec{p}$ y q unitario.

El triple producto está definido

$$\vec{r} = q\vec{p}\bar{q}, \tag{16}$$

obsérvese que:

$$\langle \vec{q}, \vec{p} \rangle = \langle \vec{p}, \vec{q} \rangle = q_1 p_1 + q_2 p_2 + q_3 p_3, \tag{17}$$

$$\vec{q}\vec{p} = -\langle \vec{q}, \vec{p} \rangle + [\vec{q} \times \vec{p}], \tag{18}$$

$$\vec{p}\vec{q} = -\langle \vec{p}, \vec{q} \rangle + [\vec{p} \times \vec{q}], \tag{19}$$

$$[\vec{q} \times \vec{p}] = -[\vec{p} \times \vec{q}], \tag{20}$$

$$\begin{aligned} -q[\vec{p} \times \vec{q}] &= -[-\langle \vec{q}, [\vec{p} \times \vec{q}] \rangle + [\vec{q} \times [\vec{p} \times \vec{q}]]] \\ &= \langle \vec{q}, [\vec{p} \times \vec{q}] \rangle, \end{aligned} \tag{21}$$

$$\langle \vec{q}, \vec{q} \rangle = |\vec{q}|^2. \tag{22}$$

Desarrollando el triple producto (16) mediante la expresión (2) y considerando (14) como propiedad de los cuaterniones, resulta

$$\vec{r} = q\vec{p}\bar{q} = (q_0 + \vec{q})\vec{p}(q_0 - \vec{q}) = (q_0 + \vec{q})(\vec{p}q_0 - \vec{p}\vec{q}), \tag{23}$$

realizando el producto de (23) se tiene

$$\vec{r} = q_0^2 \vec{p} + q_0 \vec{p}\vec{q} - q_0 \vec{q}\vec{p} - \vec{q}\vec{p}\vec{q}, \tag{24}$$

$$\begin{aligned} \vec{r} &= q_0^2 \vec{p} + q_0 \langle \vec{p}, \vec{q} \rangle - q_0 [\vec{p} \times \vec{q}] - q_0 \langle \vec{q}, \vec{p} \rangle + q_0 [\vec{q} \times \vec{p}] - \vec{q}\vec{p}\vec{q} \\ &= q_0^2 \vec{p} + q_0 [\vec{q} \times \vec{p}] + q_0 [\vec{q} \times \vec{p}] - \vec{q}\vec{p}\vec{q} \\ &= q_0^2 \vec{p} + 2q_0 [\vec{q} \times \vec{p}] - \vec{q}(\vec{p}\vec{q}) \end{aligned}$$

$$= q_0{}^2\vec{p} + 2q_0[\vec{q} \times \vec{p}] - q(-\langle \vec{p}, \vec{q}\rangle + [\vec{p} \times \vec{q}])$$
$$= q_0{}^2\vec{p} + 2q_0[\vec{q} \times \vec{p}] - (-q\langle \vec{p}, \vec{q}\rangle + q[\vec{p} \times \vec{q}])$$
$$= q_0{}^2\vec{p} + 2q_0[\vec{q} \times \vec{p}] + q\langle \vec{p}, \vec{q}\rangle - q[\vec{p} \times \vec{q}]), \quad (25)$$

aplicando (17-22) en (25), resulta

$$\vec{r} = q_0{}^2\vec{p} + 2q_0[\vec{q} \times \vec{p}] + q\langle \vec{p}, \vec{q}\rangle - p\langle \vec{q}, \vec{q}\rangle + q\langle \vec{q}, \vec{p}\rangle$$
$$= q_0{}^2\vec{p} + 2q_0[\vec{q} \times \vec{p}] + 2q\langle \vec{p}, \vec{q}\rangle - p|q|^2$$
$$= (q_0{}^2 - |q|^2)\vec{p} + 2q_0[\vec{q} \times \vec{p}] + 2q\langle \vec{p}, \vec{q}\rangle,$$

finalmente se tiene

$$\vec{r} = q\vec{p}\bar{q} = (q_0{}^2 - |q|^2)\vec{p} + 2q_0[\vec{q} \times \vec{p}] + 2q\langle \vec{p}, \vec{q}\rangle, \quad (26)$$

de la expresión (26) se observa que el resultado del triple producto de dos cuaterniones por un vector es otro vector, además si el cuaternión q es unitario, la norma del producto es la norma de $\vec{p}$, es decir

$$|\vec{r}| = |q\vec{p}\bar{q}| = |q||\vec{p}||\bar{q}| = 1|\vec{p}|1| = |\vec{p}|, \quad (27)$$

desarrollando la expresión (26) se tiene

$$\vec{r} = (2q_0{}^2 - q_0{}^2 - |q|^2)\vec{p} + 2q_0[\vec{q} \times \vec{p}] + 2q\langle \vec{p}, \vec{q}\rangle$$
$$= (2q_0{}^2 - |q|^2)\vec{p} + 2q_0[\vec{q} \times \vec{p}] + 2q\langle \vec{p}, \vec{q}\rangle$$
$$= (2q_0{}^2 - 1)\vec{p} + 2q\langle \vec{p}, \vec{q}\rangle + 2q_0[\vec{q} \times \vec{p}]. \quad (28)$$

La representación matricial de $\vec{r}$ es

$$(2q_0{}^2 - 1)\vec{p} = \begin{bmatrix} (2q_0{}^2 - 1) & 0 & 0 \\ 0 & (2q_0{}^2 - 1) & 0 \\ 0 & 0 & (2q_0{}^2 - 1) \end{bmatrix} \begin{bmatrix} p_1 \\ p_2 \\ p_3 \end{bmatrix}, \quad (29)$$

$$2q\langle \vec{p}, \vec{q}\rangle = \begin{bmatrix} 2q_1{}^2 & 2q_1q_2 & 2q_1q_3 \\ 2q_1q_2 & 2q_2{}^2 & 2q_2q_3 \\ 2q_1q_3 & 2q_2q_3 & 2q_3{}^2 \end{bmatrix} \begin{bmatrix} p_1 \\ p_2 \\ p_3 \end{bmatrix}, \quad (30)$$

$$2q_0[\vec{q} \times \vec{p}] = \begin{bmatrix} 0 & -2q_0q_3 & 2q_0q_2 \\ 2q_0q_3 & 0 & -2q_0q_1 \\ -2q_0q_2 & 2q_0q_1 & 0 \end{bmatrix} \begin{bmatrix} p_1 \\ p_2 \\ p_3 \end{bmatrix}. \quad (31)$$

Al sumar las tres componentes (29-31) obtenemos la siguiente expresión de forma comprimida

$$R(q) = \begin{bmatrix} R_{11} & R_{12} & R_{13} \\ R_{21} & R_{22} & R_{23} \\ R_{31} & R_{32} & R_{33} \end{bmatrix}, \quad (32)$$

donde las componentes R_{ij} de la expresión (32) están dadas por

$$R_{11} = (2q_0{}^2 - 1) + 2q_1{}^2,\ R_{12} = 2q_1q_2 - 2q_0q_3,$$
$$R_{13} = 2q_1q_3 + 2q_0q_2,\ R_{21} = 2q_1q_2 + 2q_0q_3,$$
$$R_{22} = (2q_0{}^2 - 1) + 2q_2{}^2,\ R_{23} = 2q_2q_3 - 2q_0q_1,$$
$$R_{31} = 2q_1q_3 - 2q_0q_2,\ R_{32} = 2q_2q_3 + 2q_0q_1,$$
$$R_{33} = (2q_0{}^2 - 1) + 2q_3{}^2,$$

se expresa la rotación de un vector denominado $\vec{p}$ rotado hacia un vector denominado $\vec{r}$ mediante $R(q)$. Esto es: $\vec{r} = R(q)\vec{p} = q\vec{p}\bar{q}$ donde se sustituye R_{ij} en (32) se obtiene

$$R(q) = \begin{bmatrix} (2q_0{}^2 - 1) + 2q_1{}^2 & 2q_1q_2 - 2q_0q_3 & 2q_1q_3 - 2q_0q_2 \\ 2q_1q_2 + 2q_0q_3 & (2q_0{}^2 - 1) + 2q_2{}^2 & 2q_2q_3 - 2q_0q_1 \\ 2q_1q_3 - 2q_0q_2 & 2q_2q_3 + 2q_0q_1 & (2q_0{}^2 - 1) + 2q_3{}^2 \end{bmatrix}.$$

A continuación, en las figuras 1 y 2 se presentan los diagramas de flujo para el desarrollo del algoritmo propuesto, para el cifrado se considera la expresión anterior $R(q)$, y para el descifrado se realiza el proceso inverso.

Se describen los pasos a seguir del algoritmo de la figura 1.

1. Se solicita al usuario que ingrese los valores del cuaternión q ($q0, q1, q2, q3$).
2. Se verifica que se haya cumplido el paso anterior.
3. Se calcula la norma del cuaternión usando la expresión (13).
4. Se verifica que el valor de la norma no sea muy pequeña o cercana a 0, evita divisiones por este último, lo cual generaría errores numéricos.
5. Se normaliza el cuaternión, es decir, se divide cada componente de este último entre la norma obtenida en el paso 3 para asegurar que el cuaternión sea unitario.
6. Se construye la matriz de rotación 3 x 3 R(q).
7. Se verifica la ortogonalidad de la matriz, de acuerdo con las siguientes condiciones.

- Si el producto de la matriz R por su matriz transpuesta T, es igual a matriz identidad I entonces la matriz es ortogonal y representa una rotación válida.
- Si el producto de la matriz R por su matriz transpuesta T no es igual la matriz identidad I resulta una matriz inválida, lo que indica un error en los datos de entrada o en los cálculos realizados.

8. Se calcula el determinante, debe ser igual a 1 para que sea una matriz de rotación válida.
9. Finalmente se imprime la matriz de rotación cuaterniónica R(q).

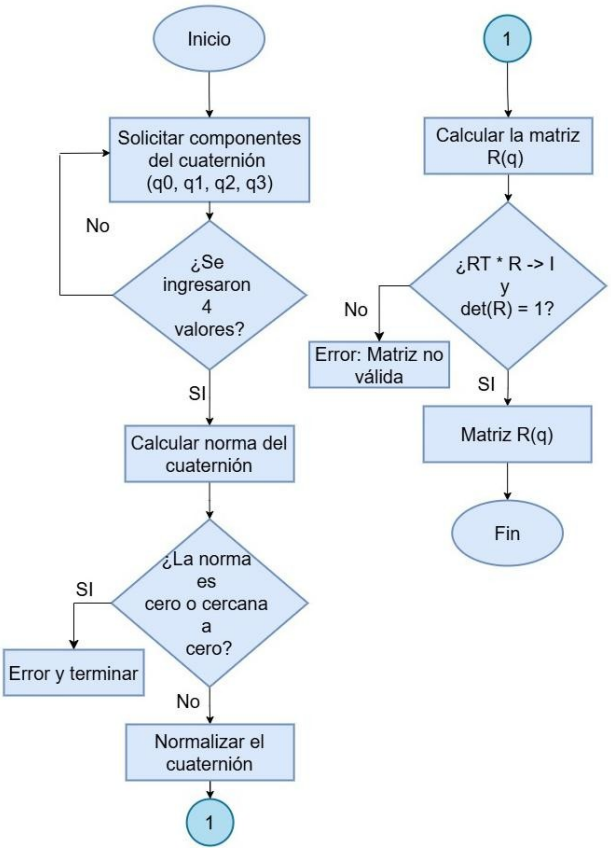

Figura. 1- Diagrama de flujo algoritmo construcción matriz de rotación cuaternionica.

A continuación, se describen los pasos a seguir del algoritmo hibrido de encriptación el cual está compuesto de dos fases fundamentales: la primera fase es la de distribución de claves mediante el protocolo BB84 y la segunda fase es la del cifrado y descifrado tal como se muestra en el diagrama de flujo de la figura 2.

1. Se realiza las polarizaciones, cálculos y operaciones sobre Qubits para la generación de llaves privadas en un canal de comunicación mediante el protocolo BB84.
2. Se debe generar una llave privada binaria de al menos 128 bits.
3. Tanto Emisor y Receptor obtienen la llave respectivamente.
4. Se ingresa una cadena de texto.
5. Se imprime la representación binaria (8 bits) y ASCII de cada carácter.
6. Se generan tantos cuaterniones p por cada 3 caracteres o bloques de 24 bits, se establece desde el inicio que la parte escalar $p0 = 0$ y $p1, p2, p3$ son la representación ASCII de dichos caracteres.
7. Se solicita la llave privada de 128 bits previamente generada, se convertirá en un cuaternión q este definirá el ángulo θ de rotación.
8. Se normaliza el cuaternión q.
9. Encriptacion de cuaterniones, por cada cuaternión p generado en el paso 3, se procede al cálculo del triple producto cuaternionico $\vec{r} = q\vec{p}\bar{q}$
10. Se generan una lista de cuaterniones encriptados, denominados r.
11. Se transmite la información encriptada a través del canal de comunicación.
12. Se recibe la información, se procede a la desencriptación mediante el cálculo de la matriz inversa.
13. Se obtienen los cuaterniones desencriptados y su equivalente en código ASCII.
14. Finalmente se calcula el parámetro matemático coeficiente de correlación entre el texto original y desencriptado, si el resultado es igual 1.0, esto indica que el proceso ha sido exitoso.

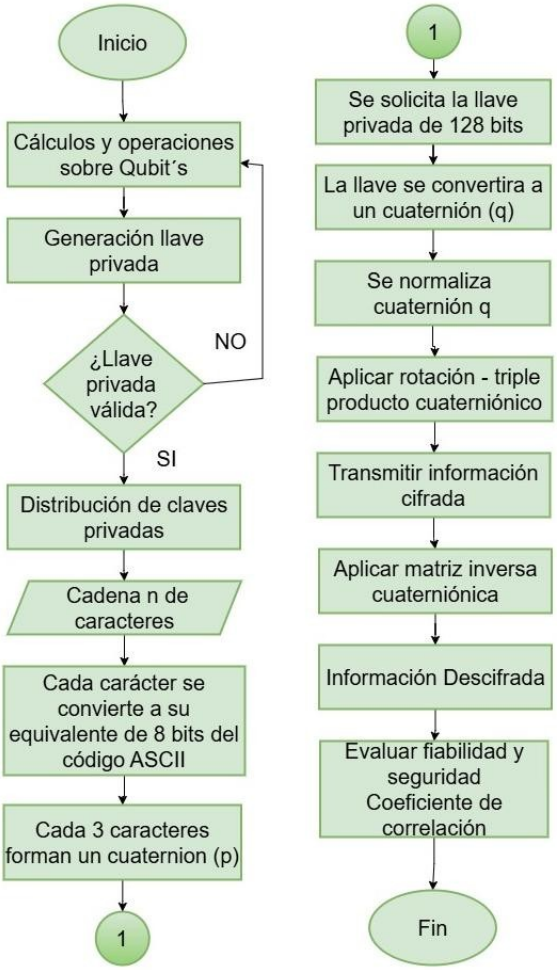

Figura. 2- Diagrama de flujo algoritmo hibrido basado en protocolo BB84 y matriz de rotación cuaterniónica.

III. Resultados y Discusión

A continuación, se muestra la implementación del protocolo de encriptación hibrido y se presenta las primeras iteraciones para el cálculo de los cuaterniones.

1. Se transmite texto plano: Telecomunicaciones!

'T': binario=01010100, ASCII=84
'e': binario=01100101, ASCII=101
'l': binario=01101100, ASCII=108
'e': binario=01100101, ASCII=101
'c': binario=01100011, ASCII=99
'o': binario=01101111, ASCII=111
'm': binario=01101101, ASCII=109
'u': binario=01110101, ASCII=117

para los demás caracteres faltantes del texto plano se realiza de manera análoga.

2. Cuaterniones p generados por cada bloque de 24 bits

Cuaternion 1 -> p0=0, p1=84, p2=101, p3=108
Cuaternion 2 -> p0=0, p1=101, p2=99, p3=111
Cuaternion 3 -> p0=0, p1=109, p2=117, p3=110

3. La llave binaria de 128 bits generada en BB84
00010100101101111011011110000000011001110011000101
01100010010000111111010000110101010101100100000000
01010010001100010011011000 11

4. Cuaternión q generado a partir del paso 3
q0=0.5484652444011794, q1=0.6161853748942223,
q2=0.4689891051101551, q3=0.31551652688630605.

5. Cuaterniones r encriptados
r0=0.0, r1=151.2969322829, r2=40.7800267744, r3=66.0850035792
r0=0.0, r1=159.6799905089, r2=55.2662310663, r3=61.4080152327
r0=0.0, r1=165.8383229973, r2=63.78627777, r3=78.0958474804
Tiempo encriptación: 0.000279 seg.

6. Texto desencriptado: Telecomunicaciones!
Tiempo desencriptación: 0.000461 seg.

7. Correlación entre el texto original y el desencriptado: 1.0

IV. Conclusiones

En este trabajo, se ha propuesto un algoritmo hibrido de cifrado basado en cuaterniones. En la primera fase se implementa un esquema de distribución de llaves privadas mediante el protocolo BB84 que utiliza como principio fundamental estados de polarizacion de fotones, esto es un proceso totalmente aleatorio, generando de esta forma llaves privadas cuya longitud es de 128 bits de acuerdo con las recomendaciones de la NIST [National Institute of Standards and Technology]. Posteriormente en la Fase 2, el texto plano a trasmitir se convierte carácter a carácter con su equivalente del código ASCII y de esta manera representar cada componente de cuaternión, se realiza la rotación cuaterniónica de acuerdo con un ángulo determinado por la llave privada, el cifrado y descifrado se generan de manera exitosa, esto de acuerdo con el parámetro matemático coeficiente de correlación.

Agradecimientos

Los autores agradecen al Conahcyt y a la Secretaría de Investigación y Posgrado por el financiamiento otorgado para la realización de la presente investigación.

Referencias

[1] Introduccion a la Criptología. https://www.um.es/adelrio/Docencia/Criptografia/Criptografia.pdf

[2] CISCO. (2023). Seguridad en terminales. https://skillsforall.com/

[3] CISCO. (2020). CCNAv7: Introduction to Networks Español.https://www.netacad.com/es

[4] Solis Ornelas, C. (2017). Propuesta de un algoritmo de cifrado hibrido basado en matrices de rotacion cuaternionica y el estandar RSA. Tesis de Maestria. IPN, Mexico.

[5] Contreras Cortés, D. (2017). Cifrado de firma electronica mediante el sistema criptografico NTRU basado en cuaterniones. Tesis de Maestria. IPN, Mexico.

[6] Urrego Urrego, J. J. (2019). Método criptográfico para cifrar información usando los estados cuánticos de polarización de fotones individuales. (Tesis de Maestria). Institución Universitaria ITM, Colombia. http://hdl.handle.net/20.500.12622/2090.

[7] Rojas Aguado, C., Vargas Jimenez, A. M., & Corzo Trejo, N. V. (2023). Diseño y construccion de un experimento automatizado de Criptografia Cuantica basado en el protocolo BB84. Tesis Licenciatura. Universidad Autonoma de Queretaro, Queretaro. https://ri-ng.uaq.mx/handle/123456789/7901 del Rio Mateos, A. (2021).

[8] Sanchez Diaz, V. (2015). Implementacion del protocolo de distribucion cuantica de claves, protocolo BB84. Tesis de Maestria. UNAM, Mexico. https://repositorio.unam.mx/contenidos/384095

[9] Molina Vilchis, M. A., Silva Ortigoza, R., & Bracho Molina, E. (2007). Criptografía Cuántica: Un Nuevo Paradigma. Polibits(36), 30-35. https://www.redalyc.org/articulo.oa?id=402640449006

[10] Elkouss, D., & Garcia Lopez, J. (2008). Protocolos de distribucion cuantica de claves. U. Politecnica de Madrid, 1-8.

[11] Rodriguez Bouza, V. (2012). Sobre los cuaterniones, álgebras de Lie, y matrices de Pauli.

[12] Vince, J. (2011). Quaternions for Computer Graphics (Vol. XV). Springer London. doi:https://doi.org/10.1007/978-1-4471-7509-4

[13] Favieri, A. (2008). Introducción a los Cuaterniones.Editorial de la Universidad Tecnológica Nacional: https://www.edutecne.utn.edu.ar/cuaterniones/cuaterniones.pdf

[14] Kamlofsky, J. A., & Bergamini, M. L. (s.f.). Los cuaterniones en visión robotica. Vaneduc, 4.