Optimización de Circuitos Cuánticos para la Implementación de Criptología Cuántica

Jorge Garcia-Diaz
Universidad de La Laguna
Tenerife, Spain
jorgegardiaz@gmail.com

Francisco Costa-Cano
Universidad Internacional de La Rioja
Logroño, Spain
podxboq@gmail.com

Pino Caballero-Gil
Universidad de La Laguna
Tenerife, Spain
pcaballe@ull.edu.es

Daniel Escanez-Exposito
Universidad de La Laguna
Tenerife, Spain
jescanez@ull.edu.es

***Resumen*—Actualmente la computación cuántica es uno de los temas de investigación que más atención está captando en diversas instituciones. Esto se debe a que constituye un novedoso modo de computación que tiene el potencial de resolver varios problemas complejos, algunos de los cuales son intratables con ordenadores clásicos. Este potencial supone un gran peligro para la criptografía actual, pero a la vez también abre la posibilidad de definir una nueva base para los futuros algoritmos criptográficos. Este trabajo explora la aplicación de técnicas algebraicas para optimizar los circuitos cuánticos, con el objetivo de mejorar su eficiencia, reducir las tasas de error y allanar el camino para el desarrollo de nuevos sistemas cuánticos que permitan la implementación de algoritmos, tanto para proteger la información como para romper algunos cifrados actuales.**

***Index Terms*—Computación cuántica, Circuitos cuánticos, Criptología, Criptografía cuántica, Ciberseguridad**

Tipo de contribución: *Investigación en desarrollo*

I. Introducción

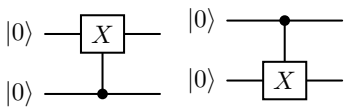
La computación cuántica contempla un candente paradigma de cómputo que ofrece ventajas bastantes notorias con respecto a la computación clásica para ciertos problemas. Entre otras, una de estas ventajas es su potencial para romper algunos algoritmos criptográficos actuales, como el sistema RSA [1] [2]. Sin embargo, no se debe considerar solo una amenaza sino también una aliada para el futuro de la ciberseguridad, pues permite sentar las bases para nuevos y revolucionarios algoritmos criptográficos cuánticos [3] [4] [5].

La realización de computadoras cuánticas escalables y tolerantes a fallos sigue siendo un desafío debido sobre todo a dos motivos: que los circuitos cuánticos, bloques fundamentales de los algoritmos cuánticos, son susceptibles a errores e ineficiencias que obstaculizan la implementación práctica de estos algoritmos [6]; y que el hardware cuántico actual no está lo suficientemente desarrollado como para poder implementar dichos circuitos [7]. Por ello, no sólo se debe investigar en hardware y algoritmos cuánticos, sino también en cómo hacer posible de la mejor manera la implementación de dichos algoritmos cuánticos con el hardware actual. En este trabajo se presenta una alternativa a este problema desde un novedoso punto de vista, que es la optimización de los circuitos cuánticos mediante técnicas algebraicas. Las técnicas algebraicas proporcionan un marco poderoso para analizar y manipular los circuitos cuánticos y por tanto los algoritmos cuánticos, ofreciendo un enfoque sistemático para identificar redundancias, explotar simetrías y simplificar las computaciones cuánticas. Esto ayudará en la optimización crucial de los circuitos cuánticos para superar las limitaciones inherentes del hardware cuántico actual. Por tanto, el objetivo de este trabajo es mostrar una nueva notación algebraica y demostrar varios resultados que puedan ayudar a optimizar los circuitos cuánticos con objeto de hacer posible la implementación de distintos algoritmos cuánticos. Además, se han creado diagramas de diferentes circuitos cuánticos a partir de la librería *Quantikz* [8].

Este artículo sigue la siguiente estructura. En la Sección II se introducen los diagramas de circuitos cuánticos y su respectiva notación tradicional, además de dos ejemplos para entender las debilidades de esta notación tradicional. En la Sección III se muestra la nueva notación algebraica junto con varios ejemplos para entenderla de mejor manera. En la Sección IV se reflexiona sobre tres circuitos cuánticos a modo de ejemplos para poder comparar la nueva notación con la notación tradicional. En la Sección V se exponen y demuestran distintos resultados obtenidos utilizando la nueva notación. Para finalizar, en la Sección VI se culmina este artículo con algunas conclusiones y trabajos futuros.

II. Notación tradicional

La forma más extendida y usada de describir la computación cuántica es mediante los circuitos cuánticos [9]. Dichos circuitos cuánticos tienen dos formas principales de representarse, mediante diagramas de los circuitos o mediante la notación tradicional para circuitos cuánticos [10]. Los diagramas tienen la ventaja de ser muy gráficos, por lo que ayudan a entender y visualizar el funcionamiento del circuito. Sin embargo, esta forma de representación tiene también grandes inconvenientes como el hecho de manipular los estados de los cúbits a lo largo del circuito. La notación tradicional sí que permite manejar de mejor manera los estados de los cúbits a lo largo del circuito, pero aún así es bastante mejorable pues no es nada cómoda de usar. Además tiene la gran desventaja de que se lee de forma inversa que los circuitos cuánticos. Una buena manera de entender estos problemas es mediante ejemplos, como los incluidos en la figura 1, donde se muestran dos circuitos cuánticos, representados con sus respectivos diagramas.



(a) Circuito 1 (b) Circuito 2

Figura 1: Ejemplos de circuitos

En la figura 2 se exponen las notaciones tradicionales correspondientes a los circuitos mostrados en la figura 1.

Circuito 1: $\boxed{CX\,|0\rangle^{\otimes 2}}$

Circuito 2: $\boxed{CX\,|0\rangle^{\otimes 2}}$

Figura 2: Ejemplos de notaciones tradicionales

Como se puede observar, las notaciones de ambos circuitos son idénticas. De hecho, en la literatura, dependiendo del autor, la notación tradicional expuesta en la figura 2 se emplea para hacer referencia tanto al Circuito 1 como al Circuito 2, aunque dichos circuitos sean distintos. Esto puede llevar fácilmente a confusiones y errores. Esto es un ejemplo muy básico de uno de los mayores defectos de la notación tradicional: las puertas cuánticas de varios cúbits no están bien definidas en la mayoría de los casos. Esto es un fallo de la notación tradicional, ya que para saber de qué forma y en qué cúbits actúa una puerta cuántica de varios cúbits, hace falta siempre comparar con el diagrama del circuito. En otras palabras, la notación tradicional no es autosuficiente, pues en la mayoría de los casos es necesario leer el diagrama junto con la notación tradicional para poder entender el efecto de las puertas sobre los kets o simplemente para saber la forma de la matriz asociada a la puerta cuántica en cuestión.
Para mostrar más inconvenientes de la notación tradicional, se introduce en la figura 3 un nuevo ejemplo algo más complejo.

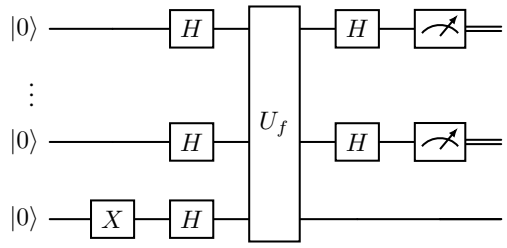


Figura 3: Circuito de Deutsch-Jozsa

La notación tradicional correspondiente al circuito de Deutsch-Jozsa de la figura 3 se muestra en la figura 4.

$$\boxed{(I\otimes M^{\otimes n-1})(I\otimes H^{\otimes n-1})U_f H^{\otimes n}(X\otimes I^{\otimes n-1})|0\rangle^{\otimes n}}$$

Figura 4: Notación tradicional del circuito de Deutsch-Jozsa

El circuito y notación tradicional mostrados en las figura 3 y 4 es el perteneciente al algoritmo de Deutsch-Jozsa [11], uno de los primeros algoritmos que se ve cuando se empieza a estudiar computación cuántica. Como se puede observar, la notación tradicional no es para nada fácil de entender ni de leer. Para empezar, el diagrama del circuito se lee de izquierda a derecha y de arriba abajo (el primer cúbit es el cúbit superior), mientras que la notación tradicional se lee de derecha a izquierda y el primer cúbit es el que está más a la derecha. Estas diferencias entre los métodos actuales de representación hacen que no sea cómodo trabajar con ellos y pueden conducir a cometer varios errores. Por ello, como se mencionó anteriormente, en este trabajo se introduce una nueva notación algebraica que elimina estas desventajas y además añade algunas ventajas. Además, en este trabajo se demuestran varios resultados interesantes que pueden ser utilizados para reducir el número de cúbits y puertas cuánticas necesarias y por tanto optimizar distintos algoritmos cuánticos.

III. Notación Optimizada

A continuación se introduce la notación optimizada utilizada en este trabajo tanto para cúbits como para puertas cuánticas. Se añaden varios ejemplos a lo largo de la explicación para entender mejor cómo se utiliza la notación introducida.

III-A. Cúbits

La forma más extendida de representar los cúbits es la notación bra-ket, también conocida como notación de Dirac [10]. Para esta nueva notación se utiliza la notación bra-ket.

Notación III-A.1: Sea $|a\rangle = |a_1 \dots a_n\rangle$ un estado producto de n cúbits, entonces se escribe:

$$\begin{aligned}|a\rangle = \alpha_{k0}\,|a_1\dots a_{k-1}0a_{k+1}\dots a_n\rangle \\ +\,\alpha_{k1}\,|a_1\dots a_{k-1}1a_{k+1}\dots a_n\rangle\end{aligned} \tag{1}$$

Ejemplo 1: Sean $|a_1a_2\rangle$ dos cúbits en estado producto, entonces aplicando la notación mencionada se obtiene:

$$\begin{aligned}|a_1a_2\rangle &= \alpha_{10}\,|0a_2\rangle + \alpha_{11}\,|1a_2\rangle \\ &= \alpha_{10}\alpha_{20}\,|00\rangle + \alpha_{10}\alpha_{21}\,|01\rangle \\ &+ \alpha_{11}\alpha_{20}\,|10\rangle + \alpha_{11}\alpha_{21}\,|11\rangle\end{aligned}$$

Notación III-A.2: Fijados n cúbits $|a\rangle = |a_1 \dots a_n\rangle$ en estado producto, se utilizará la siguiente notación:

$$|a\rangle_j^k = |a_1\dots a_{k-1}ja_{k+1}\dots a_n\rangle\,;\ k\in\{1,\dots,n\} \tag{2}$$

Ejemplo 2: Sea $|a\rangle = |a_1\dots a_n\rangle$ y $k \in \{1,\dots,n\}$, entonces se tiene:

$$|a\rangle = \alpha_{k0}\,|a\rangle_0^k + \alpha_{k1}\,|a\rangle_1^k$$

III-B. Puertas Cuánticas

Notación III-B.1: Sea A una puerta cuántica con cúbit objetivo $|a_j\rangle$, entonces se usa la siguiente notación:

$$|a_1\dots a_{j-1}\rangle\otimes A\,|a_j\rangle\otimes|a_{j+1}\dots a_n\rangle = |a_1\dots a_jAa_{j+1}\dots a_n\rangle \tag{3}$$

Notación III-B.2: Si A es una puerta cuántica con cúbit objetivo $|a_k\rangle$, donde $k\in\{1,\dots,n\}$, entonces se escribe:

$$|a_1\dots a_kAa_{k+1}\dots a_n\rangle = |a\rangle\,A_k = |a\rangle_A^k \tag{4}$$

Ejemplo 3:

$$\begin{aligned}|101\rangle\,H_2 &= |10H1\rangle = |101\rangle_H^2 \\ &= |1\rangle\otimes H\,|0\rangle\otimes|1\rangle \\ &= |1\rangle\otimes\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\otimes|1\rangle \\ &= \frac{|101\rangle+|111\rangle}{\sqrt{2}}\end{aligned}$$

Se denotan $|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$ y $|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$.

Notación III-B.3: Sea $R \subseteq \{1, \ldots, n\}$ y A una puerta cuántica cualquiera con un cúbit objetivo, entonces se denota:

$$A_R = \prod_{k \in R} A_k \tag{5}$$

Para que esta notación tenga sentido, hay que probar que $|a\rangle\, A_i A_k = |a\rangle\, A_k A_i$ para cualquier estado $|a\rangle = |a_1 \ldots a_n\rangle$ y $i, k \in \{1, \ldots, n\}$ con $i \neq k$. Supongamos sin pérdida de generalidad que $i < k$:

$$\begin{aligned} |a\rangle\, A_i A_k &= |a_1 \ldots a_n\rangle\, A_i A_k \\ &= |a_1 \ldots a_i A \ldots a_k A \ldots a_n\rangle \\ &= |a_1 \ldots a_i A \ldots a_n\rangle\, A_k \\ &= |a_1 \ldots a_n\rangle\, A_k A_i \\ &= |a\rangle\, A_k A_i \end{aligned}$$

Notación III-B.4: El conjunto $\{j, j+1, \ldots, k\}$, donde $j, k \in \{1, \ldots, n\}$ y $j < k$ se escribirá como:

$$j : k = \{j, j+1, \ldots, k\} \tag{6}$$

Ejemplo 4:

$$|100011\rangle\, X_{1:3} = |011011\rangle$$

III-C. Puertas Cuánticas Controladas

Notación III-C.1: Sean $|a\rangle$ un estado de n cúbits y A una puerta cuántica con cúbit de control $|a_k\rangle$ y cúbit objetivo $|a_j\rangle$, entonces se utiliza la siguiente notación:

$$|a\rangle\, A_j^k \tag{7}$$

Ejemplo 5:

$$\frac{|00\rangle + |10\rangle}{\sqrt{2}} X_2^1 = \frac{|10\rangle + |10\rangle_X^2}{\sqrt{2}} = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

IV. Ejemplos de Circuitos

En esta sección se muestran diversos ejemplos de circuitos cuánticos con su respectiva notación algebraica optimizada.

IV-A. Algoritmo de Deutsch-Jozsa

Reconsiderando el circuito de Deutsch-Jozsa del Ejemplo 3 mostrado en la figura 3, se puede comparar la notación tradicional mostrada en la figura 4 con la nueva notación optimizada mostrada en la figura 5. Dicho circuito permite averiguar si una función es constante o balanceada con un coste menor que cualquier algoritmo clásico.

$$\boxed{|0\rangle^{\otimes n}\, X_n H_{1:n} (U_f)_{1:n} H_{1:n-1} M_{1:n-1}}$$

Figura 5: Notación optimizada del circuito de Deutsch-Jozsa

Como se puede observar en la figura 5 con respecto al circuito de la figura 3, la nueva notación algebraica optimizada se lee de derecha a izquierda, al igual que el diagrama del circuito. Además, el primer cúbit es el cúbit superior del diagrama. Adicionalmente, esta nueva notación consume mucho menos espacio, y por tanto es más fácil de manejar.

IV-B. Teleportación Cuántica

En esta sección se considera el ejemplo de la teleportación cuántica entre dos cúbits [12] para mostrar el potencial de la nueva notación algebraica optimizada introducida.

En el circuito de la figura 6, cuyas notaciones tradicional y optimizada se muestran en las figura 7 y 8, se parte de un estado cualquiera $|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$, mientras se entrelazan otros dos cúbits inicializados ambos en el estado $|0\rangle$. Al ejecutar este circuito, se logra transferir el estado de $|\psi\rangle$ al tercer cúbit sin conocer exactamente el estado de $|\psi\rangle$.

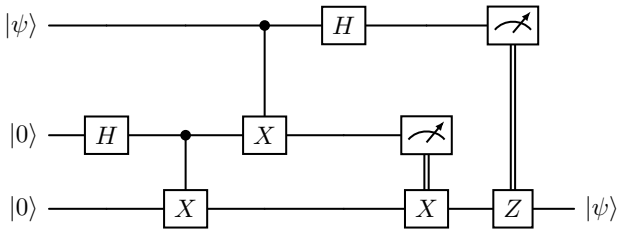


Figura 6: Circuito para la teleportación cuántica

$$\boxed{\begin{array}{c}(CZ \otimes I)(CX \otimes I)(I \otimes M^{\otimes 2})(I^{\otimes 2} \otimes H)(I \otimes CX) \\ (CX \otimes I)(I \otimes H \otimes I)\left(|0\rangle^{\otimes 2} \otimes |\psi\rangle\right)\end{array}}$$

Figura 7: Notación tradicional de la teleportación cuántica

$$\boxed{\left(|\psi\rangle \otimes |0\rangle^{\otimes 2}\right) H_2 X_3^2 X_2^1 H_1 M_{1:2} X_3^2 Z_3^1}$$

Figura 8: Notación optimizada de la teleportación cuántica

Como se aprecia en la figura 2, la notación tradicional no resulta muy adecuada para representar los cúbits de control y objetivo de las puertas controladas. En cambio, como se ha mencionado, en concreto en la *Notación (III-A.1)*, con la nueva notación optimizada sí que es posible.

IV-C. Algoritmo de Shor

En esta sección se muestra como ejemplo de aplicación de la notación optimizada introducida, uno de los algoritmos más importantes de la computación cuántica, el algoritmo de Shor [1]. Este algoritmo debe su fama a que permite resolver el problema de la factorización del producto de dos números enteros $N = p \cdot q$, siendo p y q números primos, con un coste polinomial. Obsérvese que hoy en día con la computación clásica, la resolución de este problema tiene un coste sub-exponencial pero super-polinomial (algoritmo GFNS [13] [14]). El algoritmo de Shor puede llegar a representar un grave peligro para la criptografía actual, ya que por

ejemplo permite romper el sistema criptográfico RSA [15]. Por culpa de algoritmos como el de Shor, se hace cada vez más urgente invertir esfuerzos en desarrollar nuevos protocolos seguros para las comunicaciones dado que hay que sustituir los criptosistemas como el RSA. Aún así, el algoritmo de Shor está todavía lejos de poder ser implementado en un ordenador cuántico real para los tamaños de clave utilizados actualmente [16] [17] [18] [19]. El algoritmo de Shor se basa esencialmente en el circuito de estimación de fase, cuyo circuito y notaciones tradicional y optimizada se muestran en las figuras 9, 10 y 11.

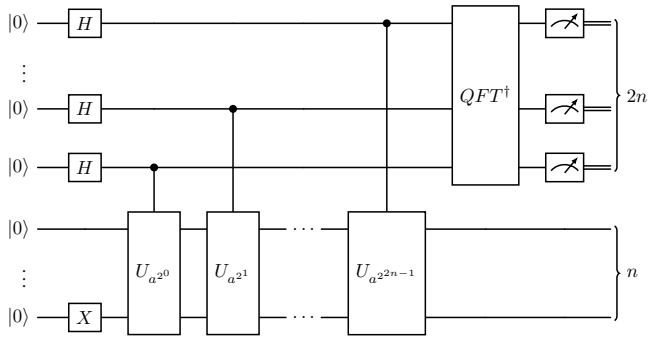


Figura 9: Circuito de la estimación de fase

$$(I^{\otimes n} \otimes M^{\otimes 2n})(I^{\otimes n} \otimes QFT^{\dagger}) \left(\prod_{i=0}^{2n-1} (CU_{a^{2n-1-i}} \otimes I^{\otimes 2n-1}) \right) (X \otimes I^{\otimes n-1} \otimes H^{\otimes 2n}) \left|0\right\rangle^{\otimes 3n}$$

Figura 10: Notación tradicional de la estimación de fase

$$\left|0\right\rangle^{\otimes 3n} H_{1:2n} X_{3n} \prod_{i=0}^{2n-1} (U_{a^{2^i}})^{2n-i}_{2n+1:3n} (QFT^{\dagger})_{1:2n} M_{1:2n}$$

Figura 11: Notación optimizada de la estimación de fase

En el ejemplo de la estimación de fase se pueden observar los mismos problemas que los mencionados en el circuito de la teleportación cuántica mostrado en la figura 6. Además, en este ejemplo se observa también lo complicada y confusa que se puede volver la notación tradicional y la gran cantidad de espacio que puede llegar a consumir. En cambio, la notación optimizada consume menos espacio.

V. Resultados

En esta sección se introducen algunas propiedades y relaciones entre algunas puertas cuánticas y ciertos estados de cúbits. Se utiliza la notación $(j)_2$ para expresar la notación binaria de j.

Se comienza con un resultado que caracteriza el efecto que tiene el aplicar una puerta H a todos los cúbits de un estado cualquiera $|x_1 \dots x_n\rangle$.

Proposición 5.1:

$$\left|x_1 \dots x_n\right\rangle H_{1:n} = \frac{1}{\sqrt{2^n}} \sum_{y=1}^{2^n-1} (-1)^{x \cdot y} \left|(y)_2\right\rangle \tag{8}$$

donde $x \cdot y$ representa el producto módulo 2 de x e y bit a bit, es decir, $x \cdot y = x_1 y_1 + \ldots + x_n y_n$, siendo $(y)_2 = y_1 y_2 \dots y_n$ con $y_r, x_r \in \{0,1\} \ \wedge \ r \in \{1, \dots, n\}$.

Proof:

$$\begin{aligned} \left|x_1 \dots x_n\right\rangle H_{1:n} &= (H \left|x_1\right\rangle) \otimes \ldots \otimes (H \left|x_n\right\rangle) \\ &= \left(\frac{1}{\sqrt{2}} \sum_{y_1 \in \{0,1\}} (-1)^{x_1 y_1} \left|y_1\right\rangle \right) \otimes \cdots \\ &\quad \otimes \left(\frac{1}{\sqrt{2}} \sum_{y_n \in \{0,1\}} (-1)^{x_n y_n} \left|y_n\right\rangle \right) \\ &= \frac{1}{\sqrt{2^n}} \sum_{y_1 \dots y_n \in \{0,1\}^n} (-1)^{x_1 y_1 + \ldots + x_n y_n} \left|y_1 \dots y_n\right\rangle \\ &= \frac{1}{\sqrt{2^n}} \sum_{y=1}^{2^n-1} (-1)^{x \cdot y} \left|(y)_2\right\rangle \end{aligned}$$

■

A continuación, se demuestra una caracterización del efecto que tiene el aplicar una puerta H a todos los cúbits del estado $|1\rangle^{\otimes n}$.

Proposición 5.2:

$$\left|0\right\rangle^{\otimes n} X_{1:n} H_{1:n} = \left|-\right\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{j=1}^{2^n-1} (-1)^{w((j)_2)} \left|(j)_2\right\rangle \tag{9}$$

donde el Peso de Hamming de $(j)_2$ se denota como:

$$w((j)_2) = \sum_{r=0}^{n-1} j_r$$

Proof:

$$\left|0\right\rangle^{\otimes n} X_{1:n} H_{1:n} = \left|1\right\rangle^{\otimes n} H_{1:n}$$

Aplicando *Proposición 5.1* para:

$$(x)_2 = (2^n - 1)_2 = \underbrace{1 \dots 1}_{n}$$

y sabiendo que:

$$\left|1\right\rangle^{\otimes n} H_{1:n} = \left|-\right\rangle^{\otimes n}$$

se obtiene lo siguiente:

$$\begin{aligned} \left|-\right\rangle^{\otimes n} &= \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} (-1)^{\sum_{r=0}^{n-1} j_r} \left|(j)_2\right\rangle \\ &= \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} (-1)^{w((j)_2)} \left|(j)_2\right\rangle \end{aligned}$$

■

Como consecuencia del resultado anterior se obtiene el siguiente resultado que caracteriza el efecto que tiene el aplicar una puerta H a todos los cúbits del estado $|0\rangle^{\otimes n}$.

Proposición 5.3:

$$|0\rangle^{\otimes n} H_{1:n} = |+\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} |(j)_2\rangle \tag{10}$$

Proof:

$$\begin{aligned} |0\rangle^{\otimes n} H_{1:n} &= |+\rangle^{\otimes n} \\ &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \ldots \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ &= \frac{1}{\sqrt{2^n}}(|0\rangle + |1\rangle) \otimes \ldots \otimes (|0\rangle + |1\rangle) \\ &= \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} |(j)_2\rangle \end{aligned}$$

■

El siguiente resultado describe el efecto que tiene el aplicar una puerta cuántica A_R sobre un autovector con autovalor asociado λ_i.

Proposición 5.4: Sea A una puerta cuántica y $|a\rangle$ un estado de n cúbits tal que:

$$|a\rangle A_i = \lambda_i |a\rangle, \ \forall i \in \{1, \ldots, n\}$$

es decir, que $|a\rangle$ sea un autovector de A_i con autovalor asociado λ_i para todo $i \in \{1, \ldots, n\}$. Entonces si $R \subseteq \{1, \ldots, n\}$:

$$|a\rangle A_R = \left(\prod_{i \in R} \lambda_i \right) |a\rangle \tag{11}$$

Proof:

$$\begin{aligned} |a\rangle A_R &= |a\rangle \prod_{i \in R} A_i \\ &= \prod_{i \in R} |a\rangle A_i \\ &= \left(\prod_{i \in R} \lambda_i \right) |a\rangle \end{aligned}$$

■

Como consecuencia directa de la proposición anterior, se demuestra un resultado que explica el comportamiento de una puerta con respecto a un autovector cuando su autovalor asociado es -1.

Proposición 5.5: Sea A una puerta cuántica y $|a\rangle$ un estado de n cúbits tal que:

$$|a\rangle A_i = -|a\rangle, \ \forall i \in \{1, \ldots, n\}$$

es decir, que $|a\rangle$ sea un autovector de A_i con autovalor asociado -1 para todo $i \in \{1, \ldots, n\}$. Entonces si $R, S \subseteq \{1, \ldots, n\}$:

$$|a\rangle A_R = (-1)^{|R|-|S|} |a\rangle A_S \tag{12}$$

donde $|R|$ y $|S|$ representan el cardinal de R y S respectivamente.

Proof:
Aplicando la *Proposición* (5.4) para $\lambda_i = -1, \ \forall \lambda_i$

$$|a\rangle A_S = |a\rangle \prod_{k \in S} A_k = (-1)^{|S|} |a\rangle$$

$$\implies |a\rangle = (-1)^{-|S|} |a\rangle A_S$$

Además:

$$\begin{aligned} |a\rangle A_R =& (-1)^{|R|} |a\rangle \\ \implies & |a\rangle A_R = (-1)^{|R|} \cdot (-1)^{-|S|} |a\rangle A_S \\ \implies & |a\rangle A_R = (-1)^{|R|-|S|} |a\rangle A_S \end{aligned}$$

■

A continuación, se demuestra que el resultado anterior se puede aplicar a la puerta X.

Proposición 5.6: Sean $R, S \subseteq \{1, \ldots, n\}$, entonces:

$$|-\rangle^{\otimes n} X_R = (-1)^{|R|-|S|} |-\rangle^{\otimes n} X_S \tag{13}$$

Proof: La demostración de este resultado se basa en demostrar lo siguiente:

$$|-\rangle^{\otimes n} X_i = -|-\rangle^{\otimes n}, \ \forall i \in \{1, \ldots, n\}$$

Para ello demostraremos que $|-\rangle X = -|-\rangle$:

$$\begin{aligned} |-\rangle X &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) X \\ &= \frac{1}{\sqrt{2}}(|1\rangle - |0\rangle) X \\ &= -|-\rangle \end{aligned}$$

Una vez obtenido esto se consigue:

$$\begin{aligned} |-\rangle^{\otimes n} X_i &= |-\rangle^{\otimes i-1} \otimes X |-\rangle \otimes |-\rangle^{\otimes n-i} \\ &= |-\rangle^{\otimes i-1} \otimes -|-\rangle \otimes |-\rangle^{\otimes n-i} \\ &= -|-\rangle^{\otimes n} \end{aligned}$$

Aquí se está suponiendo que $i \neq 1$ y $i \neq n$. Estos casos se demuestran de manera análoga:

- $|-\rangle^{\otimes n} X_1 = -|-\rangle \otimes |-\rangle^{\otimes n-1} = -|-\rangle^{\otimes n}$
- $|-\rangle^{\otimes n} X_n = |-\rangle^{\otimes n-1} \otimes -|-\rangle = -|-\rangle^{\otimes n}$

Ahora basta aplicar la *Proposición* (5.5) para $A = X$ y $|a\rangle = |-\rangle^{\otimes n}$:

$$\implies |-\rangle^{\otimes n} X_R = (-1)^{|R|-|S|} |-\rangle^{\otimes n} X_S$$

■

De manera análoga, se demuestra el siguiente resultado.

Proposición 5.7:

$$|+\rangle^{\otimes n} X_R = |+\rangle^{\otimes n}; \ \forall R \subseteq \{1, \ldots, n\} \tag{14}$$

Proof: La demostración resulta trivial teniendo en cuenta que:

$$\begin{aligned} |+\rangle X &= \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) X \\ &= \frac{1}{\sqrt{2}}\left(|1\rangle + |0\rangle\right) \\ &= |+\rangle \end{aligned}$$

pues aplicando las ideas desarrolladas en la demostración de la *Proposición* (5.6) y la *Proposición* (5.4) para $\lambda_i = 1,\ \forall i$ se obtiene la prueba del resultado. ■

VI. Conclusiones

La necesidad de nuevos algoritmos criptográficos post-cuánticos para hacer frente a las amenazas de los ordenadores cuánticos, como el algoritmo de Shor, está clara. Sin embargo, la solución puede estar también en la computación cuántica. En este trabajo se propone una optimización de los algoritmos cuánticos que permite investigar con mayor facilidad e implementar con la mayor eficiencia no solo los algoritmos cuánticos que permiten romper muchos de nuestros actuales cifrados, sino también nuevos algoritmos de cifrado cuántico. Diversos ejemplos y resultados permiten demostrar que la notación optimizada introducida mejora considerablemente la notación tradicional usada en combinación con los circuitos cuánticos. Esta nueva notación algebraica no sólo hace más entendible los circuitos y elimina los diversos problemas mencionados de la notación tradicional, sino que también ayuda en gran medida a encontrar patrones entre las puertas cuánticas y los estados de los cúbits, lo que puede llevar a optimizaciones de distintos circuitos cuánticos y por tanto a la posibilidad de implementar algoritmos cuánticos en los ordenadores cuánticos actuales. Para trabajos futuros se buscará la aplicación de estos nuevos resultados a distintos circuitos para reducir el numero de puertas o cúbits necesarios, así como hallar y demostrar nuevos resultados.

Agradecimientos

Este trabajo ha sido posible gracias a las Cátedras de Ciberseguridad de la Universidad de La Laguna patrocinadas por Binter, y por INCIBE en el marco de los fondos del Plan de Recuperación, Transformación y Resiliencia, financiada por la Unión Europea (Next Generation). Además forma parte del proyecto PID2022-138933OB-I00 financiado por MCIN/AEI/ 10.13039/501100011033/FEDER, UE.

Referencias

[1] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal on Computing*, vol. 26, no. 5, p. 1484–1509, 1997.

[2] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, p. 120–126, 1978.

[3] C. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, pp. 10–12, 1984.

[4] ——, "Quantum cryptography: Public key distribution and coin tossing," *Theoretical Computer Science - TCS*, vol. 560, pp. 7–11, 2014.

[5] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Physical review letters*, vol. 67, pp. 661–663, 1991.

[6] Google-Quantum-AI, "Suppressing quantum errors by scaling a surface code logical qubit," *Nature*, vol. 614, no. 7949, pp. 676–681, 2023.

[7] IBM, "Quantum hardware," 2021, https://research.ibm.com/topics/quantum-hardware [Accessed: 17-03-2024].

[8] A. Kay, "Tutorial on the quantikz package," 2023.

[9] D. E. Deutsch and R. Penrose, "Quantum computational networks," *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, vol. 425, no. 1868, pp. 73–90, 1989.

[10] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010.

[11] D. Deutsch and R. Jozsa, "Rapid solution of problems by quantum computation," *Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences*, vol. 439, no. 1907, pp. 553–558, 1992.

[12] C. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. Wootters, "Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels," *Physical review letters*, vol. 70, pp. 1895–1899, 04 1993.

[13] A. K. Lenstra, H. W. Lenstra Jr, M. S. Manasse, and J. M. Pollard, "The number field sieve," in *Proceedings of the twenty-second annual ACM symposium on Theory of computing*, 1990, pp. 564–572.

[14] R. Crandall and C. Pomerance, *Prime Numbers: A Computational Perspective (2001)*. Springer, 2001.

[15] S. Singh and E. Sakk, "Implementation and analysis of shor's algorithm to break rsa cryptosystem security," 2024, https://www.techrxiv.org/doi/pdf/10.36227/techrxiv.170259160.05374043[Accessed: 22-03-2024].

[16] C. P. Schnorr, "Fast factoring integers by svp algorithms, corrected," Cryptology ePrint Archive, Paper 2021/933, 2021. [Online]. Available: https://eprint.iacr.org/2021/933

[17] B. Yan, Z. Tan, S. Wei, H. Jiang, W. Wang, H. Wang, L. Luo, Q. Duan, Y. Liu, W. Shi *et al.*, "Factoring integers with sublinear resources on a superconducting quantum processor," *arXiv preprint arXiv:2212.12372*, 2022.

[18] V. Marchan-Sekulic, P. Caballero-Gil, and D. Escanez-Exposito, "Implementación de los algoritmos cuánticos de simon y de shor," *Actas de las VIII Jornadas Nacionales de Investigación en Ciberseguridad*, pp. 409–414, 2023.

[19] U. Skosana and M. Tame, "Demonstration of shor's factoring algorithm for $N = 21$ on ibm quantum processors," *Scientific Reports*, vol. 11, no. 1, 2021.