ISSN: 2711-3760
DOI: https://doi.org/10.47185/27113760.v2n2.62

Transformada Cuántica de Fourier

Horacio Arango Marín

Universidad Nacional de Colombia.
Profesor Emérito.

RESUMEN

La Transformada Cuántica de Fourier (TCF) es la generalización de la transformada clásica de Fourier en la cual se usan conceptos de la mecánica cuántica. Se presentan dos algoritmos y sus circuitos cuánticos para calcular la TCF. Con ella se puede factorizar un número entero, en sus factores primos.

Palabras clave: Cubit. Puerta cuántica. Producto tensorial. Superposición.

The Quantum Fourier Transform

ABSTRACT

The Quantum Fourier Transform (TCF) is the generalization of the classical Fourier transform in which concepts from quantum mechanics are used. Two algorithms and their quantum circuits are presented to calculate TCF. With it you can factor a whole number into its prime factors.

Keywords: Qubit. Quantum gate. Tensor product. Superposition.

Recibido: 26/10/2021 Aceptado: 17/12/2021
Correspondencia: (*) harangom@une.net.co

ISSN: 2711-3760
DOI: https://doi.org/10.47185/27113760.v2n2.62

1. INTRODUCCIÓN

La mecánica cuántica ha creado nuevos conceptos (Miller, 2008) algunos de los cuales son útiles en el diseño de algoritmos cuánticos:

A. Superposición. Los sistemas cuánticos, como los electrones (carga, momento angular, velocidad, energía y spin) en superposición, pueden estar, en un momento dado, en dos o más estados. simultáneamente. El spin es una propiedad intrínseca del electrón de dos estados que cuando se mide solo toma un valor.

B. El Entrelazamiento es la capacidad para formar un sistema de cubits, (la unidad de información para los computadores cuánticos), de tal manera que al medir uno de ellos se obtiene información sobre el estado de los otros. El entrelazamiento correlaciona los resultados de la medición de los cubits del sistema.

C. Interferencia. Los cubits en superposición tienen un comportamiento análogo al de las ondas y presentan interferencia constructiva que aumenta la probabilidad de un estado, al colapsar la superposición en el proceso de medida.

1.1. El Cubit.

Se definen dos estados básicos mediante los vectores:

$$|0> = \begin{pmatrix}1\\0\end{pmatrix}, |1> = \begin{pmatrix}0\\1\end{pmatrix}, \qquad (1)$$

denominados cubits, representados con la notación bra, ket: | > , < | de Dirac.
Con ellos se define la superposición del estado $|\psi> \in \mathbb{C}^2$, como la combinación lineal de los estados |0 > y |1 >,

$$|\psi> = \alpha|0> + \beta|1> =$$

$$\alpha\begin{pmatrix}1\\0\end{pmatrix} + \beta\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}\alpha\\\beta\end{pmatrix}.$$

Los números complejos α y β satisfacen la condición $\alpha^2 + \beta^2 = 1$. El cubit $|\psi>$ y los dos estados básicos se representan por puntos en la superficie de la esfera de Bloch de radio 1.

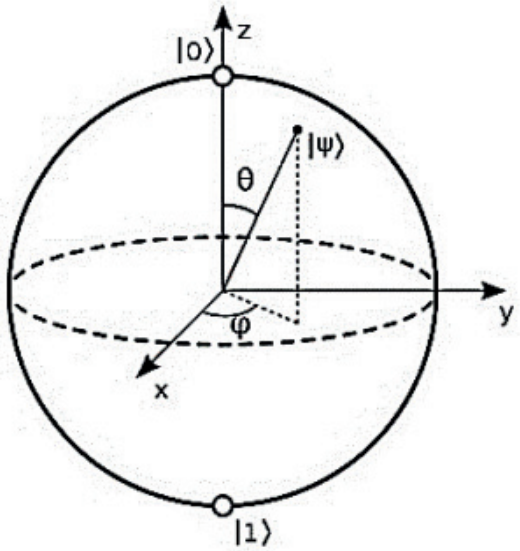


Figura 1. Esfera de Bloch.

La acción de medir a $|\psi>$ produce el colapso del estado de superposición (decoherencia) en uno de los dos estados.

El resultado de la medición es el estado |0 > con probabilidad α^2 ó el estado |1 > con probabilidad β^2.

Si se realizan 1.000 medidas del estado $|\psi>$ y si $\alpha^2 = 0.63$ entonces en 630 medidas, el estado $|\psi>$ colapsa en el estado |0 > o en el estado |1 > en 370 medidas.

La superposición de estados termina cuando se realiza una medida.

Por esta razón el estado $|\psi>$ no puede ser copiado.

En la computación cuántica, el bit actual se reemplaza por el cubit como nueva unidad de información y con la superposición se incrementa la capacidad de cálculo y se evita su copia.

El cubit modela una “partícula elemental” en superposición y se materializa con las trampas iónicas: Circuitos magnéticos que suspenden iones en un tubo de iones al vacío a bajas temperaturas.

ISSN: 2711-3760
DOI: https://doi.org/10.47185/27113760.v2n2.62

1.2. Producto Tensorial.

El estado producto tensorial (⊗) de dos cubit $\psi = \begin{pmatrix}\alpha\\ \beta\end{pmatrix}$ y $\varphi = \begin{pmatrix}\gamma\\ \delta\end{pmatrix}$ se define como:

$$\psi \otimes \varphi = \begin{pmatrix}\alpha \times \begin{pmatrix}\gamma\\ \delta\end{pmatrix}\\ \beta \times \begin{pmatrix}\gamma\\ \delta\end{pmatrix}\end{pmatrix} = \begin{pmatrix}\alpha\gamma\\ \alpha\delta\\ \beta\gamma\\ \beta\delta\end{pmatrix} \quad (2)$$

Y produce un vector de 4 × 1. Con los productos:
$|0>\otimes|0> = |00>$, $|0>\otimes|1> = |01>$,
$|1>\otimes|0> = |10>$ y
$|1>\otimes|1> = |11>$ se define un nuevo estado en superposición mediante la combinación lineal:
$\alpha|0>\otimes|0> + \beta|0>\otimes|1> +$
$\gamma|1>\otimes|0> + \delta|1>\otimes|1>$.
El producto tensorial de n bits es
$|x> = |xn_{-1}\otimes xn_{-2}\otimes \ldots . \otimes x_2 \otimes x_1 \otimes x_0>$ de acuerdo con (2) es un vector de $2^n \times 1$.

2. PUERTAS CUÁNTICAS

Las puertas cuánticas son operadores que actúan sobre los cubits modificando sus estados y las probabilidades asociadas. Las matrices que multiplicadas por su transpuesta dan la identidad se llaman unitarias y se usan para representar y operar con las puertas cuánticas.

Los circuitos cuánticos son diagramas formados por líneas horizontales que representan la evolución de cubits cuando sobre ellos operan las diferentes puertas cuánticas colocadas en esas líneas.

El circuito tiene, a la izquierda del diagrama la entrada de los cubits definidos por el problema a resolver y a la derecha tiene como salida los estados o los bits correspondientes a la medida de los cubits obtenidos como solución del problema dado.

Los Algoritmos Cuánticos son procesos formados por circuitos cuánticos que para un problema dado tienen una inicialización de cubits y una evolución definida por las puertas cuánticas que producen, después de la medida, una salida de estados o bits como solución del problema (Benjumea, 2018).

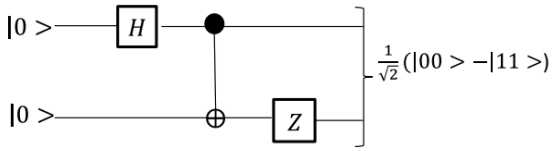


Figura 2. Circuito Cuántico.

2.1. La Puerta H de Hadamard.

Es una puerta que opera sobre un cubit mediante la matriz unitaria $H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$ y su inversa es también la matriz H.
Produce los estados en superposición del cubit $|0>$ ó $|1>$ con probabilidades de 0.5.

$$H(|0>) = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}1\\ 0\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\ 1\end{bmatrix} = \frac{1}{\sqrt{2}}(|0> + |1>) = |+>,\ H(|+>) = |0>$$

$$H(|1>) = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}0\\ 1\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\ -1\end{bmatrix} = \frac{1}{\sqrt{2}}(|0> - |1>) = |->,\ H(|->) = |1>$$

En resumen:

$H(x) = \frac{1}{\sqrt{2}}(|0> + (-1)^x|1>)$, para $x = 0, 1$ y
$H\left(\frac{1}{\sqrt{2}}(|0> + (-1)^x|1>)\right) = |x>$.

2.2. La Puerta $CNOT$.

La puerta $CNOT$ (⊕) se representa por la matriz

$$\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix}$$

y ella realiza la negación controlada de un cubit de un estado formado por 2 cubits, el primer cubit es un control sobre el segundo cubit. Si el control es 0, el segundo sigue igual y si el control es 1, el segundo es 0.

$CNOT|11> = |10>$,
$CNOT|10> = |11>$.

Esta puerta se define para las entradas $|x>$, $|y>$ como $CNOT(|xy>) = |x, y\oplus x>$ en donde ⊕ es la

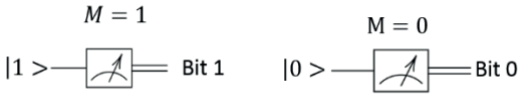
ISSN: 2711-3760
DOI: https://doi.org/10.47185/27113760.v2n2.62

suma binaria.

2.3 Operador para la Medida de Cubits.

El circuito de medida M se denota con el símbolo

Después de la medida de un cubit su estado colapsa en $|0>$, si M es 0 ó en $|1>$, si M es 1.



2.4. La Puerta R_θ de Rotación.

La rotación R_θ se define con $R_\theta(|0>) = |0>$, $R_\theta(|1>) = |1>e^{i\theta}$ y ella modifica la fase de $|1>$.

R^θ define un giro antihorario de θ radianes en el plano xy de la esfera de Bloch, a partir del estado $|+> = H(|0>)$.

2.5. La Puerta Z.

La puerta Z se representa por la matriz $\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$ y su acción sobre el cubit $|x>$ está definida por $Z(|x>) = (-1)\,x\,|x>$ para $x = 0, 1$.
$Z(\alpha|0> + \beta|1>) = \alpha|0> - \beta|1>$

2.6. La Puerta S de Intercambio de Cubits.

En las líneas de un circuito cuántico correspondientes a x_i y x_j, la puerta S definida por $S\{x_i\,|x_j\} = S\{x_j\,|x_i\}$ permite que los cubits se intercambian (Garcia, 2016).

3. DISEÑO DE ALGORITMOS PARA CALCULAR LA TCF

3.1. Bases Ortogonales y Definición de la TCF.

Dados n cubits:
$|x_{n-1}>, |x_{n-2}>, |x_{n-1}>, \dots, |x_2>, |x_1>, |x_0>$
su producto tensorial se calcula como:

$$|x_{n-1}\otimes x_{n-2}\otimes \dots . \otimes x_2\otimes x_1\otimes x_0> = |x_{n-1}x_{n-2} \dots . x_2x_0> = |x>$$

$|x>$ es un número en base 2 o computacional, ya que $x_i = 0$ ó 1, $i = 0, 1, . . , n - 1$. Con la expresión $\sum_{k=0}^{n-1} x_k 2^k$ este producto es también un número en base 10. Con los n cubits se representan los números desde 0 hasta $M - 1$, siendo $M=2^n$. El cubit $|1101>$ en base 2 es $|11>$ en base 10.
El conjunto de estados $\{|0>, |1>, |2>, |3>, \dots \dots, |M - 1>\}$ forman una base ortonormal para el espacio $\mathbb{C}^{2^n}$ y se llama base de Fourier.

La transformada cuántica de Fourier es una aplicación lineal de $\mathbb{C}^{2^n}$ en $\mathbb{C}^{2^n}$ que transforma un estado $|x>$ de la base computacional en una combinación lineal $|\hat{x}>$ de estados de la base de Fourier (Preskill, 2020).

La TCF se define en forma análoga a la transformada discreta de Fourier con la expresión:

$$TCF(|x>) = |\hat{x}> = \frac{1}{\sqrt{M}}\sum_{y=0}^{M-1} e^{\frac{2\pi i x y}{M}}|y> \qquad (3)$$

3.2. Matriz de Fourier.

Con $w = e^{\frac{2\pi i}{M}}$ y $M = 2^n$ se construye la matriz de Fourier F_M de orden $M \times M$. Ella tiene la siguiente expresión:

$$\begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & w & w^2 & \dots & w^{M-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & w^{M-2} & w^{2(M-2)} & \dots & w^{(M-2)(M-2)} \\ 1 & w^{M-1} & w^{2(M-1)} & \dots & W^{((M-1)(M-1)} \end{bmatrix}$$

Como $|x> = |x_{n-1}x_{n-2} \dots . x_2x_2x_0>$, es un vector de $2^n \times 1$ componentes y la TCF se calcula con la matriz F_M, como el producto $F_M \times |x> =$ TCF $(|x>)$

Existen algoritmos más eficientes para calcular la *TCF* que los realizados con la expresión (3) o con la

ISSN: 2711-3760
DOI: https://doi.org/10.47185/27113760.v2n2.62

matriz de Fourier (Garcia, 2016).

3.3. Proposición.

Para diseñar un nuevo algoritmo se requiere la siguiente proposición:

$$TCF(|x>) = \frac{1}{\sqrt{M}}\sum_{y=0}^{M-1} e^{\frac{2\pi i x y}{M}} |y> = \frac{1}{\sqrt{2^n}} \bigotimes_{l=1}^{n} (|0> + e^{\frac{2\pi i x}{2^l}} |1>). \quad (4)$$

Su demostración se consigue expandiendo el producto tensorial, multiplicando los cubits y agrupando los términos usando la igualdad (4) y luego la base de Fourier.

El factor $\frac{x}{2^l}$ del producto o tensorial se escribe en base 2 como

$$\frac{x}{2^l} = \frac{x_{n-1}\times 2^{n-1} + .. + x_l \times 2^l + .. + x_0 \times 2^0}{2^l}$$

$$= x_{n-1} \times 2^{n-1-l} + x_{n-2} \times 2^{n-2-l} + x_l + \frac{x_{l-1}}{2} + \frac{x_{l-2}}{2^2} + + \cdots \frac{x_1}{2^{l-1}} + \frac{x_0}{2^l}.$$

En la anterior expresión, si $l = n$, se obtiene

$$\frac{x}{2^n} = 0.\, x_{n\text{-}1}\, x_{n\text{-}2}\, x_{n\text{-}3} .. x_2\, x_1\, x_0.$$

Como $TCF(|x>) =$

$$TCF(x_{n-1} \otimes x_{n-2} \otimes \ldots \otimes x_2 \otimes x_1 \otimes x_0) =$$
$$TCF(|x_{n-1}>) \otimes TCF(|x_{n-2}>) \otimes$$
$$\ldots \otimes TCF(|x_1>) \otimes TCF(|x_0>).$$

En (4) tenemos que

$$TCF(|x>) = \frac{1}{2\sqrt{2}}((|0> + e^{\frac{2\pi i x}{2}} |1>) \otimes (|0> + e^{\frac{2\pi i x}{4}} |1>) \otimes \ldots .. \otimes (|0> + e^{\frac{2\pi i x}{2^n}} |1>)) \quad (5)$$

Para cada factor de (5) se tienen las siguientes igualdades:

$$TCF(|x_{n-1}>) = \frac{1}{\sqrt{2}}(|0> + e^{2\pi i \left(\frac{x}{2}\right)} |1>) = \frac{1}{\sqrt{2}}(|0> + e^{2\pi i\, (0.x_0)} |1>)$$

$$\vdots$$

$$TCF(|x_1>) = \frac{1}{\sqrt{2}}(|0> + e^{2\pi i \left(\frac{x}{2^{n-1}}\right)} |1>) = \frac{1}{\sqrt{2}}(|0> + e^{2\pi i\, (0.x_{n-2} \ldots\ x_1 x_0)} |1>)$$

$$TCF(|x_0>) = \frac{1}{\sqrt{2}}(|0> + e^{2\pi i \left(\frac{x}{2^n}\right)} |1>) = \frac{1}{\sqrt{2}}(|0> + e^{2\pi i\, (0.x_{n-1} x_{n-2} \ldots x_1 x_0)} |1>)$$

El producto tensorial (4) es entonces igual a:

$$TCF\ (|x>$$

$$TCF\ (|x> = \frac{1}{\sqrt{2^n}}((|0> + e^{\frac{2\pi i x}{2}} |1> \otimes (|0> + e^{\frac{2\pi i x}{4}} |1>) \otimes \ldots .. \otimes \left(|0> + e^{\frac{2\pi i x}{2^n}} |1>\right) =$$

$$\frac{1}{\sqrt{2^n}}((|0> + e^{2\pi i\, (0.x_0)} |1>) \otimes (|0> + e^{2\pi i 0.x_1 x_0} |1>) \otimes \ldots .. \otimes \left(|0> + e^{2\pi i\, (0.x_{n-1} \ldots x_1 x_0)} |1>\right) \quad (6)$$

4. ALGORITMOS PARA CALCULAR LA TCF

4.1. Primer Algoritmo Cuántico.

El primer algoritmo cuántico se construye con el cálculo del ángulo de giro de la fase de $|1>$ en cada uno de los factores del producto tensorial (5) (Ulises, 2019). Para ello:

La puerta de Hadamard se ha definido por $H(|x_k>) = (|0> + e^{\pi i x_k} |1>)$ con $x_k = 0$ ó 1. $e^{\pi i x_k}$ es la fase de $|1>$.

En el producto tensorial (4) la fase de $|1>$ es $e^{\frac{i2\pi x}{2^l}}$ y el ángulo de giro en el plano xy es

$\theta_l = \frac{2\pi x}{2^l}$, para $l = 1, 2, \ldots n$.

ISSN: 2711-3760
DOI: https://doi.org/10.47185/27113760.v2n2.62

Si $l = n$, el ángulo de giro de la fase $e^{\frac{i2\pi x}{2^n}}$ en $TCF(|x_0>)$ es $\theta_n = \frac{2\pi x}{2^n}$ Y $\varphi_k = \theta_n \times 2^k$, es el ángulo de giro para la fase de $|1>$ en $TCF(|x_k>)$.
Con $k = 0,1,2, \ldots n-1$.

Entonces para calcular TCF $(|x>)$ realizamos el siguiente proceso:

1: Dado el estado $|x>$ y el número de cubits n, se calcula el ángulo de giro de la fase de $|1>$ en TCF $(|x_0>)$ con $\varphi_0 = \frac{2\pi\,(2^0)x}{2^n} = \frac{2\pi\,x}{2^n}$, Luego

TCF $(|x_0>) = \frac{1}{\sqrt{2}}\,(|0> + e^{\frac{i2\pi x}{2^n}}|1>)$.

2: Con φ_0, se calcula $\varphi_1 = 2 \times \varphi_0$ y, por tanto

TCF $(|x_1>) = \frac{1}{\sqrt{2}}\,(|0> + e^{i\varphi_1}|1>)$.

3: Se halla $\varphi_2 = 4 \times \varphi_0$ y

TCF $(|x2>) = \frac{1}{\sqrt{2}}\,(|0> + e^{i\theta_2}|1>)$ y así sucesivamente hasta n: Se determina $\varphi_{n-1} = 2^{n-1}\,\varphi_0$ y

TCF $(|x_{n-1}>) = \frac{1}{\sqrt{2}}\,(|0> + e^{i\varphi_{n-1}}|1>)$.

Por último, se realiza el producto tensorial de estos factores y se obtiene $TCF(|x>)$

$TCF(|x>) =$

$TCF(|x_{n-1}>) \otimes TCF(|x_{n-2}>) \otimes \ldots$

$\otimes TCF(|x_1>) \otimes TCF(|x_0>)$

Ejemplo: Consideremos tres cubits $|x_0> |x_1> |x_2>$ entonces para $n = 3$, $M = 8$.

Se tiene $|x_2 \otimes x_1 \otimes x_0> =$

$x_2 \times 2^2 + x_1 \times 2^1 + x_0 \times 2^0 = |x>$ (x_2 es el dígito binario más significativo) y x es un número en base 10 y así $\frac{x}{2^3} = 0.x_2x_1x_0$.

$$TCF\,(|x_2>) = \frac{1}{\sqrt{2}}(|0> + e^{\frac{2\pi ix}{2}}|1>)$$
$$= \frac{1}{\sqrt{2}}(|0> + e^{2\pi i\,(0.x_0)}|1>)$$

$$\text{TCF}\,(|x_1>) = \frac{1}{\sqrt{2}}(|0> + e^{\frac{2\pi ix}{4}}|1>) =$$
$$\frac{1}{\sqrt{2}}(|0> + e^{2\pi i\,(0.x_1x_0)}|1>)$$

$$\text{TCF}\,(|x_0>) = \frac{1}{\sqrt{2}}(|0> + e^{\frac{2\pi ix}{8}}|1>) =$$
$$\frac{1}{\sqrt{2}}(|0> + e^{2\pi i\,(0.x_2x_1x_0)}|1>).$$

Como el producto tensorial no es conmutativo debe realizarse según el orden definido por (5).

Si $|x_2 \otimes x_1 \otimes x_0> =$
$|x_2x_1x_0> = |100> = |4>$,

el ángulo de giro de la fase de $|1>$) en

$TCF(|x_0>)$ es

$\varphi_0 = \frac{2\pi\,(2^0)x}{2^n} = \frac{2\pi\,4}{8} = \pi$ y

$TCF(|x_0>) = \frac{1}{\sqrt{2}}\,(|0> + e^{i\pi}|1>)$.

Calculamos $\varphi_1 = 2 \times \varphi_0 = 2\pi$ y

TCF $(|x1>) = \frac{1}{\sqrt{2}}\,(|0> + e^{i2\pi}|1>)$ y

$\varphi_2 = 4 \times \varphi_0 = 4 \times \pi$.

TCF $(|x_2>) = \frac{1}{\sqrt{2}}\,(|0> + e^{i4\pi}|1>)$

y así:

TCF $(|100>) =$

$\frac{1}{\sqrt{2}}\,(|0> + e^{i4\pi}|1>) \otimes$

$\frac{1}{\sqrt{2}}\,(|0> + e^{i2\pi}|1>) \otimes$

$\frac{1}{\sqrt{2}}(|0> + e^{i\pi}|1>)$

Como $e^{i\theta} = \cos(\theta) + isen(\theta)\ y\ i = \sqrt{-1}$ tenemos

TCF $(|100>) =$

$\frac{1}{\sqrt{2}}\,(|0> + |1>) \otimes$

$\frac{1}{\sqrt{2}}\,(|0> + |1>) \otimes$

$\frac{1}{\sqrt{2}}\,(|0> - |1>)$

TCF $(|100>) =$

$\frac{1}{\sqrt{2}}\,(|0000> + |0001> +$
$|0010> + |0011> +$
$|0100> + |0101> +$
$|0110> + |0111>)$.

4.2. Segundo Algoritmo Cuántico.

El segundo Algoritmo usa el producto tensorial (6) en donde giro el ángulo de giro de la fase de $|1>$ se representa en base 2 y esto permite diseñar el circuito cuántico para el cálculo de la TCF (Preskill, 2020).

1: Graficamos las tres líneas de la evolución de los cubits en el circuito e iniciamos el circuito colocando en la parte izquierda los cubits $|x_2> |x_1> |x_0>$ de arriba hacia abajo.

ISSN: 2711-3760
DOI: https://doi.org/10.47185/27113760.v2n2.62

2: En la línea inferior $|x_0>$ se aplica a este cubit 3 puertas cuánticas primero la puerta H, luego la puerta de rotación R_θ con $\theta = \frac{\pi}{2}$ con control en $|x_1>$ y por último la puerta de rotación R_θ con $\theta = \frac{\pi}{4}$ con control en $|x_2>$. Se obtiene:

$$\frac{1}{\sqrt{2}}(|0> + e^{2\pi i\left(\frac{x_0}{2}\right)}|1> \times e^{2\pi i\left(\frac{x_1}{4}\right)} \times e^{2\pi i\left(\frac{x_2}{8}\right)}) = \frac{1}{\sqrt{2}}(|0> + e^{2\pi i\left(\frac{x_2}{8}+\frac{x_1}{4}+\frac{x_0}{2}\right)}|1>).$$

Para obtener TCF ($|x_0>$) se intercambia, en el estado anterior, x_0 por x_2.

$$TCF\,(|x_0>) = \frac{1}{\sqrt{2}}(|0> + e^{2\pi i\left(\frac{x_0}{8}+\frac{x_1}{4}+\frac{x_2}{2}\right)}|1>).$$

3: En la línea $|x_1>$ se aplica a este cubit dos puertas cuánticas primero la puerta H y luego la puerta de rotación R_θ con $\theta = \frac{\pi}{2}$ con control en $|x_2>$.

Se obtiene

$$\frac{1}{\sqrt{2}}(|0> + e^{2\pi i\left(\frac{x_1}{2}\right)}|1> \times e^{2\pi i\left(\frac{x_2}{4}\right)}) = \frac{1}{\sqrt{2}}(|0> + e^{2\pi i\left(\frac{x_2}{4}+\frac{x_1}{2}\right)}|1>).$$

Hacemos el cambio x_2 por x_0 entonces

$$TCF\,(|x_1>) = \frac{1}{\sqrt{2}}(|0> + e^{2\pi i\left(\frac{x_0}{4}+\frac{x_1}{2}\right)}|1>).$$

4: En la línea $|x_2>$ aplicamos a este cubit, la puerta H y se obtiene $\frac{1}{\sqrt{2}}(|0> + e^{2\pi i\left(\frac{x_2}{2}\right)}|1>$.

Pero para obtener TCF ($|x_2>$) se debe intercambiar en el estado anterior x_0 por x_2. Entonces. (Ver Figura 3).

$$TCF\,(|x_2>) = \frac{1}{\sqrt{2}}(|0> + e^{2\pi i\left(\frac{x_0}{2}\right)}|1>).$$

Al reemplazar $x_2 = 1$, $x_1 = 0$, $x_0 = 0$ en estas expresiones se obtiene $TCF(|x_0>)$

$$TCF\,(|x_0>) = \frac{1}{\sqrt{2}}(|0> + e^{2\pi i\left(\frac{x_0}{8}+\frac{x_1}{4}+\frac{x_2}{2}\right)}|1>) = = \frac{1}{\sqrt{2}}(|0> + e^{\pi i}|1>) = \frac{1}{\sqrt{2}}(|0> - |1>)$$

$$TCF\,(|x_1>) = \frac{1}{\sqrt{2}}(|0> + e^{2\pi i\left(\frac{x_0}{4}+\frac{x_1}{2}\right)}|1>) = \frac{1}{\sqrt{2}}(|0> + |1>)$$

$$TCF\,(|x_2>) = \frac{1}{\sqrt{2}}\left(|0> + e^{2\pi i\left(\frac{x_0}{2}\right)}|1>\right) =$$

$\frac{1}{\sqrt{2}}$ $(|0> + |1>)$.Y con el producto tensorial de estos factores se obtiene un resultado para la TCF igual al anterior.

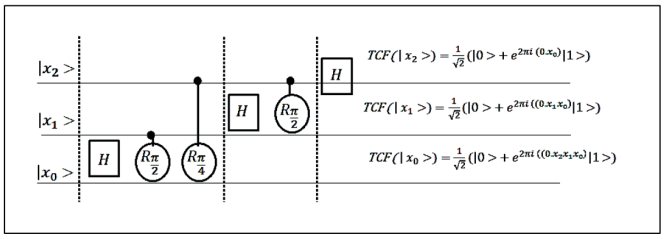


Figura 3. Circuito Cuántico TCF

5. FACTORIZACIÓN DE NÚMEROS PRIMOS CON LA TCF

En Criptografía se usa el algoritmo RSA para encriptar mensajes con clave pública y desencriptarlos con la clave privada.

Estas claves son producidas con números primos aleatorios con muchos dígitos.

El producto Q de dos números primos es entonces un número que con los algoritmos clásicos es difícil de factorizar en sus factores primos.

En 1.994, Peter W Shor creó un algoritmo cuántico para hallar el periodo r de una función periódica usando la Transformada Cuántica de Fourier y con

ISSN: 2711-3760
DOI: https://doi.org/10.47185/27113760.v2n2.62

el periodo r descompuso números grandes en sus factores primos (Shor, 1994).

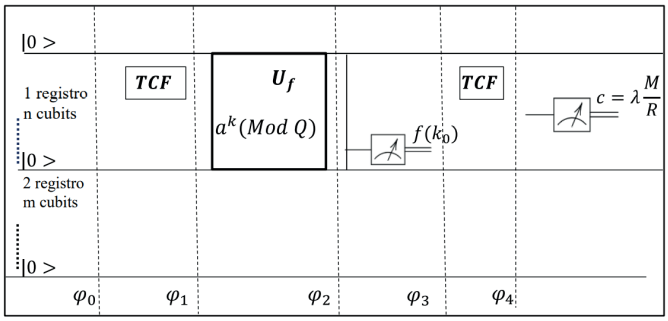


Figura 4. Circuito del algoritmo de Shor.

5.1. Período de una Función Periódica.

Una función de periodo r satisface para todo x del dominio f , $f(x) = f(x + r)$. Para hallar r se usa el siguiente procedimiento del algoritmo de Shor:

1: Dados los números primos Q (grande) y a tales que $mcd\ (a, Q) = 1$, se define la función periódica modular $f(k) = a^k(Mod\ Q)$.
El algoritmo se inicia con 2 registros de cubits, el primero con $n = log_2(Q^2)$ cubits y el segundo con $m = log_2(Q)$ cubits. Ellos se usan para almacenar los valores de los números k y almacena los valores de $f(k)$. (Ver Figura 4) Inicialmente los dos registros tienen los $n + m$ cubits en el estado $|0>$.
Se escoge $M = 2^n \in \mathbb{N}$.
2: Al primer registro de n cubits $|0000 \dots 0>$ o inicialización se le aplica la TCF para obtener el estado en superposición

$$\varphi_1 = \frac{1}{\sqrt{M}} \sum_{k=0}^{M-1} |k> \oplus |0>,$$
$$k \in [0, 1, 2, ., M-1]$$

3: Se aplica el operador U_f al estado φ_1 ,

$$\varphi_2 = U_f(\varphi_1) = \frac{1}{\sqrt{M}} \sum_{k=0}^{M-1} |k> \oplus |f(k)>$$

4: Al medir en el segundo registro el cubit $|f(k)>$, este colapsa en el estado $|f(k_0)>$ y el primer registro colapsa en los números k tales que $f(k) = f(k_0)$. Como f es periódica de periodo r, los números k son:
k_0 , $k_0 + r$, $k_0 + 2r + \dots + k_0 + (\frac{M}{r} - 1)\ r$. Y se obtiene el estado en superposición

$\varphi_3 = \frac{\sqrt{r}}{\sqrt{M}} \sum_{l=0}^{\frac{M}{r}-1} (|k_0 + lr>)$. El número r debe ser un divisor de M en esta sumatoria y además ella se multiplica por $\sqrt{r}$ para que la suma de probabilidades en el estado φ_3 sea igual a 1.

5: Al aplicar la TCF a φ_3 se obtiene una TCF de periodo $\frac{M}{r}$ y una fase $\emptyset_j = e^{\frac{2\pi i k_0 j}{M}}$

$$\varphi_4 = TCF(\varphi_3) =$$
$$\frac{1}{\sqrt{M}} \sum_{j=o}^{M-1} \left(\frac{\sqrt{r}}{\sqrt{M}} \sum_{l=0}^{\frac{M}{r}-1} e^{\frac{2\pi i(k_0 + lr)j}{M}} |j>\right)$$

Esta expresión se simplifica y se obtiene

$$\varphi_4 = \frac{1}{\sqrt{r}} \sum_{\lambda=0}^{r-1} \emptyset_j \left| \frac{\lambda M}{c} \right>$$

6: Se realiza una medida en el estado φ_4 y se obtiene el número c. Entonces como $c = \frac{\lambda M}{r}$ tenemos que $\frac{c}{M} = \frac{\lambda}{r}$.
En general como λ y r no tienen factores comunes $\frac{c}{M}$ se expresa como una aproximación de $\frac{\lambda}{r}$ usando los convergentes de la fracción continua de $\frac{c}{M}$.

Si $\left|\frac{c}{M} - \frac{\lambda}{r}\right| \leq \frac{1}{2M}$, el denominador de la aproximación es un candidato para determinar el periodo r de f.

Ejemplo: para $M = 2^{14} = 16.384$, $Q = 119$, $a = 16$, $f(k) = 16^k\ (Mod\ 119)$, el primer registro tiene 14 cubits y el segundo 7.

Se mide $\left|\frac{\lambda M}{c}\right>$ en $\varphi_4 = \frac{1}{\sqrt{r}} \sum_{\lambda=0}^{r-1} \emptyset_j \left|\frac{\lambda M}{c}\right>$ y se obtiene $c = 4.256$.

La fracción continua de $\frac{4.256}{16.384} \approx 0 + \frac{1}{3 + \frac{1}{1 + \frac{1}{5}}}$. Los convergentes son $\left[0, \frac{1}{3}, \frac{1}{4}, \frac{6}{23}\right]$.

Se calcula $16^4 = 84 \neq 1\ (Mod\ 119)$ y por tanto 4 no es el período.

Repetimos el algoritmo y medimos $\left|\frac{\lambda M}{c}\right>$ y se obtiene $c = 2.660$ entonces $\frac{2.660}{16.384} \approx 0 + \frac{1}{6 + \frac{1}{6 + \frac{1}{3+1}}}$ y sus convergentes son $\left[0, \frac{1}{6}, \frac{6}{37}, \frac{25}{154}\right]$.

Para $r = 6$, $16^6 \equiv 1\ (Mod\ 119)$ y 6 el periodo de $f(k) = 16^k\ (Mod\ 119)$.

ISSN: 2711-3760
DOI: https://doi.org/10.47185/27113760.v2n2.62

5.2. Factorización de un Número Entero.

El periodo r de $f(k)$ satisface $a^r \equiv 1$ (Mod Q). Esta expresión es lo mismo que $a^r - 1 \equiv 0$ (Mod Q), igual también $(a^{\frac{r}{2}} - 1)(a^{\frac{r}{2}} + 1) \equiv 0\ (Mod\ Q)$.
El número r deber ser par y $(a^{\frac{r}{2}}) \neq -1\ (Mod\ Q)$.
En estas condiciones $mcd\ ((a^{\frac{r}{2}} - 1), Q)$ y $mcd\ ((a^{\frac{r}{2}} + 1), Q))$ son los factores primos de Q.
Para r = 6, $16^6 \equiv 1\ (Mod\ 119)$ entonces los factores de 119 son:
$mcd(16^{3`} + 1, 119) = 17$ y
$mcd(16^{3`} - 1, 119) = 7$ y
$119 = 17 \times 7$.

6. RESULTADOS Y CONCLUSIONES

El sistema criptográfico RSA de Rivest, Shamir y Adleman desarrollado en 1.979 es un sistema de clave pública en el cual el emisor de un mensaje tiene una clave pública para encriptarlo y el receptor tiene la misma clave pública y tiene otra clave privada y secreta, para desencriptarlo.
La seguridad de la encriptación está basada en la factorización de números primos con muchos dígitos ya que esta es una tarea difícil, si se usan los algoritmos clásicos de Euclides.

El Algoritmo Cuántico de Shor hace que los algoritmos de clave publica tengan que aumentar el numero de dígitos de los números primos para poder garantizar su seguridad. Actualmente se usan primos del orden de 10^{300} con 1.024 bits. Con la construcción de Computadores Cuánticos, como el de la IBM con 127 cubits con gran capacidad de cálculo, la seguridad de los algoritmos RSA sigue en riesgo de ser vulnerada, si no se aumenta el tamaño de los números primos hasta por lo menos 2.048 bits.

En 1.985 Víctor Miller propuso el uso de las curvas elípticas en la Criptografía. Una expresión $y^2 = x^3 + ax + b$ que satisface la condición $4a^3 + 27b^2 \neq 0$ define una curva elíptica sobre el cuerpo de los números reales $\mathbb{R}$.

Se define la curva elíptica modular $y^2 = x^3 + ax + b\ (Mod\ p)$, siendo p un número primo con $x, y. a$ y $b\ \epsilon\ \mathbb{Z}_p$. $\mathbb{Z}_p$ es un Campo Finito. Los puntos de la curva modular forman un grupo finito y cíclico.

Estas curvas se usan en criptografía escogiendo un punto M de la curva modular y un número r entero y aleatorio como clave privada y se calcula $P = r * M$ como clave pública.

La dificultad de hallar r es un problema equivalente al problema del logaritmo discreto, es decir hallar z tal que $m^z = n$, para m, n conocidos y pertenecientes a un Campo Finito $\mathbb{Z}_p$ con p un número primo grande. Este es un problema de gran complejidad computacional.

Con las curvas elípticas modulares se construyen claves públicas seguras y de menor tamaño que las usadas en los algoritmos RSA. Ellas actualmente se usan para la brindar seguridad a las transacciones con criptomedas.

ISSN: 2711-3760
DOI: https://doi.org/10.47185/27113760.v2n2.62

REFERENCIAS

Benjumea, D. (2018). Elementos y conceptos de computación cuántica. Recuperado el agosto de 2021, de http://bibing.us.es/proyectos/abrepro-y/91926/fichero/TFG-1926-BENJUMEA.pdf

Garcia, J. (2016). Computación Cuántica. Universidad Politecnica de Madrid, Madrid. Recuperado el Junio de 2020, de https://docplayer.es/88529958-Computacion-cuantica-jesus-garcia- lopez-de-lacalle-francisco-garcia-mazario.html

Miller, D. (2008). Quantum Mechanics for Scientists and Engineers. Cambridge: Cambridge Univesity Press.

Preskill, J. (2020). Quantum Information. California Institute of Technology. Cambridge University Press. Obtenido de http://theory.caltech.edu/~preskill/ph219/chap6_20_6A.pdf

Shor, P. (1994). Polynomial-Time Algorithms for Prime factorization and Discrete Logarithms on a Quantum Computer. Proceedings of the 35th Annual Symposium on Foundatios of Computer Science, pp 124-134.

Ulises, D. (2019). Agoritmos Fundamentales en Computación Cuántica. Sevilla. Obtenido de https://-docplayer.es/191990088-Algoritmos-fundamentales-en-computacion-cuantica- pastor-diaz-ulises.html