UNIVERSIDAD SIMÓN BOLÍVAR
DPTO. DE ELECTRÓNICA Y CIRCUITOS
DISTRIBUCIÓN DE LLAVES CUÁNTICAS

Proyecto:

Quantum Secret Direct Comunication (QSDC) with authentication

Autor:

Ángel Álvarez

16-10031

Abril, 2022

Introducción

La noción de Quantic Secret Communication acaba de desarrollarse; es un tipo de comunicación cuántica en la que se pueden enviar mensajes secretos a través de un canal cuántico con o sin comunicaciones clásicas complementarias. Una comunicación cuántica directa segura (QSDC) envía mensajes secretos directamente entre las partes que se comunican, del remitente al receptor, sin el uso de protocolos de comunicación convencionales adicionales que no sean los necesarios para chequear intrusos.

En otras palabras, en QSDC, el proceso de distribución de clave cuántica (QKD) y la comunicación de texto cifrado clásico se combinan en un único mecanismo de comunicación cuántica. La noción de transmisión directa de comunicaciones secretas tiene dos significados en QSDC: por un lado, se entregan mensajes secretos en lugar de claves sin procesar; por otro lado, el receptor no requiere ninguna comunicación clásica adicional del emisor para decodificar los mensajes secretos.

Para este tema solo se escogieron los papers de Farouk et al. ya que son bastante densos en contenido y además que resumen muy bien todo el proceso de comunicación con autenticación, además de tener un enfoque empresarial aplicado. El primero se usa unicamente por ser un protocolo de autenticación de identidad robusto que se utiliza previa a la comunicación y el segundo engloba todo el sistema de comunicación.

1. A generalized architecture of quantum secure direct communication for N disjointed users with authentication by Farouk, Zakaria, Megahed and Omara (2015)

En este paper, se generaliza el proceso de QSDC entre N usuarios con parcial y completa cooperación del quantum server (QS). Así, $N-1$ usuarios disjuntos $u_1, u_2, ..., u_{N-1}$ pueden transmitir un mensaje secreto de bits clásicos a un usuario remoto u_N utilizando la propiedad de *dense coding* y las transformaciones de Pauli.

1.1. Fase de autenticación basada en 'Robust general N user authentication scheme in a centralized quantum communication network via generalized GHZ states by Farouk et al.

- **A.1**: El QS y los N usuarios, $u_1, u_2, ..., u_i, ..., u_N$, comparten una llave de autenticación J_k previa a cualquier comunicación, definida como:

$$J_k = \{J_1, J_2, ..., J_{N+1}\}. \tag{1}$$

- **A.2**: Si u_i quiere enviar un mensaje a u_j, u_i le informa a u_j y al QS. Cuando el QS recibe la solicitud, el genera una secuencia de estados GHZ de $N+1$ partículas, se define a continuación:

$$S = \left\{ \left|\Psi_1^+\right\rangle, \left|\Psi_2^+\right\rangle, ..., \left|\Psi_{N+1}^+\right\rangle \right\}, \tag{2}$$

donde cada estado GHZ es:

$$\left|\Psi_k^+\right\rangle = \frac{1}{\sqrt{2}}(|000\cdots0\rangle + |111\cdots1\rangle)_{S12\cdots N}. \tag{3}$$

Luego, el QS conserva la partícula S y le transmite a cada u_i la partícula i, respectivamente.

- **A.3**: Una vez los usuarios reciben sus partículas, cada uno de ellos genera una partícula propia resultado de la encriptación de su llave de autenticación y una operación binaria en particular. Estos estados son:

$$|\phi_{n_i}\rangle = \begin{cases} |J_i \otimes J_k\rangle, & i < k, \\ |J_{i+1} \otimes J_k\rangle, & i \geq k. \end{cases} \tag{4}$$

donde $\otimes$ denota la operación en particular previamente acordada por los usuarios y el QS.

- **A.4**: Luego, cada u_i realiza una operación $C_{OP}^{i\to n_i}$ en su partícula i del GHZ y n. El estado producido p será:

$$|\phi_{p_i}\rangle = C_{OP}^{i\to n_i}(|\Psi_k^+\rangle \otimes |\phi_{n_i}\rangle), \tag{5}$$

donde $C_{OP} = C_0$ si $J_{N+1} = 0$ y $C_{OP} = C_1$ si $J_{N+1} = 1$. C_0 y C_1 se definen como:

$$C_0 = |0\rangle_i \langle 0|_i \otimes I_{n_i} + |1\rangle_i \langle 1|_i \otimes X_{n_i}, \tag{6}$$

$$C_1 = |+\rangle_i \langle +|_i \otimes I_{n_i} + |-\rangle_i \langle -|_i \otimes X_{n_i}. \tag{7}$$

- **A.5**: Cada u_i preserva la partícula i del GHZ y le envía n_i al QS.

- **A.6**: Cuando QS recibe cada n_i empieza a desencriptar realizando una operación $C_{OP}^{S\to n_i}$ en cada n_i, obteniendo:

$$|\phi'_{p_i}\rangle = C_{OP}^{S\to n_i} |\phi_{p_i}\rangle . \tag{8}$$

- **A.7**: El QS empieza a verificar midiendo $|\phi\rangle_{n_i}$ en las bases de Z. La medida debería arrojar $J_i \otimes J_{N+1}$ si el usuario u_i tiene la llave correcta. En caso de ser diferente, entonces existe un impostor o hay intrusos interceptando las partículas y se debe repetir la fase completa.

2. Comunicación entre dos usuarios disjuntos con cooperación parcial y completa del server cuántico

En este esquema, cuando el servidor cuántico recibe una solicitud de comunicación de un usuario con otro usuario, el servidor cuántico distribuye estados GHZ entre los usuarios involucrados en el proceso de comunicación. La distribución se establece después de completar con éxito la autenticación antes del inicio del proceso de comunicación. El servidor cuántico distribuye a todos los usuarios partículas generadas pero tiene una para sí mismo. Como consecuencia, el servidor cuántico y los usuarios se entrelazan debido a la presencia de una sola partícula por usuario para un estado GHZ distribuido. Además, la medición de GHZ es utilizada por el receptor o el servidor cuántico, según el tipo de cooperación utilizada durante la comunicación entre usuarios. En el caso de cooperación parcial del QS, es el usuario receptor encargado de descifrar el mensaje y realizar la medida GHZ. Para la cooperación completa del QS, el usuario receptor solo debe esperar por la medida GHZ del QS y descifrar el mensaje con su medida en X.

Durante los diferentes modos de comunicación se utilizan 8 pares GHZ de 3 partículas, definidos como:

$$\left|\psi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}(|000\rangle \pm |111\rangle), \tag{9}$$

$$\left|\gamma^{\pm}\right\rangle = \frac{1}{\sqrt{2}}(|011\rangle \pm |100\rangle), \tag{10}$$

$$\left|\phi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}(|010\rangle \pm |101\rangle), \tag{11}$$

$$\left|\varphi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}(|001\rangle \pm |110\rangle). \tag{12}$$

Y además los 4 pares de Bell de costumbre:

$$\left|\Phi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), \tag{13}$$

$$\left|\Psi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle). \tag{14}$$

Aquí se usa la propiedad de la codificación densa para codificar y transmitir una serie de mensajes clásicos entre dos usuarios disjuntos con soporte parcial del servidor cuántico. En otras palabras, el mensaje se transmite de acuerdo con la publicación del servidor cuántico y la medida del usuario receptor. En este escenario, u_i forma al servidor cuántico sobre su solicitud de transmitir un mensaje a u_j distante.

2.1. Cooperación parcial

- **P.2.1**: El QS genera una secuencia de estados GHZ:

$$S = \left\{ \left|\psi_1^+\right\rangle, \left|\psi_2^+\right\rangle, ..., \left|\psi_N^+\right\rangle \right\}, \tag{15}$$

donde,

$$\left|\psi_k^+\right\rangle_{iqj} = \frac{1}{\sqrt{2}}(|000\rangle_{iqj} + |111\rangle_{iqj}). \tag{16}$$

Teniendo las bases de Z en función de las bases de X:

$$|0\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle), \tag{17}$$

$$|1\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle), \tag{18}$$

y además:

$$|00\rangle = \frac{1}{\sqrt{2}}\Big(\left|\Phi^+\right\rangle + \left|\Phi^-\right\rangle \Big), \tag{19}$$

$$|11\rangle = \frac{1}{\sqrt{2}}\Big(\left|\Phi^+\right\rangle - \left|\Phi^-\right\rangle \Big). \tag{20}$$

Usando las ecuaciones (19-20) en las partícula ij de la ecuación (16) y las ecuaciones (17-18) en la partícula q de la misma ecuación (16):

$$\begin{aligned}
\left|\psi^+\right\rangle_{iqj} &= \frac{1}{\sqrt{2}}(|000\rangle_{iqj} + |111\rangle_{iqj}), \\
&= \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}\Big(\left|\Phi^+\right\rangle + \left|\Phi^-\right\rangle \Big)_{ij} \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle)_q + \right. \\
&+ \left. \frac{1}{\sqrt{2}}\Big(\left|\Phi^+\right\rangle - \left|\Phi^-\right\rangle \Big)_{ij} \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle)_q \right), \\
&= \frac{1}{2\sqrt{2}}\Big(\left|\Phi^+\right\rangle|+\rangle + \left|\Phi^+\right\rangle|-\rangle + \left|\Phi^-\right\rangle|+\rangle + \left|\Phi^-\right\rangle|-\rangle + \\
&+ \left|\Phi^+\right\rangle|+\rangle - \left|\Phi^+\right\rangle|-\rangle - \left|\Phi^-\right\rangle|+\rangle + \left|\Phi^-\right\rangle|-\rangle \Big)_{ijq}, \\
&= \frac{1}{2\sqrt{2}}\Big(2\left|\Phi^+\right\rangle_{ij}|+\rangle_q + 2\left|\Phi^-\right\rangle_{ij}|-\rangle_q \Big), \\
&= \frac{1}{\sqrt{2}}\Big(\left|\Phi^+\right\rangle_{ij}|+\rangle_q + \left|\Phi^-\right\rangle_{ij}|-\rangle_q \Big)
\end{aligned} \tag{21}$$

Con la secuencia generada, el QS la reparte entre u_i, u_j y el mismo. Los subíndices, i, q y j representan a quién le pertenece cada partícula respectivamente.

- **P.2.2**: El usuario disjunto u_i escoge al azar un subconjunto de la secuencia S, llamado S_{u_i}, y la mantiene confidencial.

- **P.2.3**: u_i genera una secuencia de bits, $b_i \in \{00, 01, 10, 11\}$, esta es el mensaje a transmitir. De acuerdo a dicha cadena, aplica una de las siguientes operaciones a su partícula en la secuencia codificando el mensaje b_i:

b_i	U_{b_i}
00	$U_{00} = I$
01	$U_{01} = X$
10	$U_{10} = Y$
11	$U_{11} = Z$

Cuadro 1: Codificación de mensaje.

- **P.2.4**: La conversión se divide en cuatro posibles casos:

  - $b_i = 00$:

$$(I \otimes I \otimes I)\left|\psi^{+}\right\rangle_{iqj} = \frac{1}{\sqrt{2}}\Big(\left|\Phi^{+}\right\rangle_{ij}\left|+\right\rangle_{q} + \left|\Phi^{-}\right\rangle_{ij}\left|-\right\rangle_{q}\Big) \tag{22}$$

- $b_i = 01$:

$$\begin{aligned}(X \otimes I \otimes I)\left|\psi\right\rangle_{ijq} &= (X \otimes I \otimes I)\frac{1}{\sqrt{2}}\Big(\left|\Phi^{+}\right\rangle_{ij}\left|+\right\rangle_{q} + \left|\Phi^{-}\right\rangle_{ij}\left|-\right\rangle_{q}\Big),\\ &= (X \otimes I \otimes I)\frac{1}{\sqrt{2}}\Big(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{ij}\left|+\right\rangle_{q} +\\ &+ \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)_{ij}\left|-\right\rangle_{q}\Big),\\ &= \frac{1}{\sqrt{2}}\Big(\frac{1}{\sqrt{2}}(|10\rangle + |01\rangle)_{ij}\left|+\right\rangle_{q} + \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle)_{ij}\left|-\right\rangle_{q}\Big),\\ &= \frac{1}{\sqrt{2}}\Big(\left|\Psi^{+}\right\rangle_{ij}\left|+\right\rangle_{q} + \left|\Psi^{-}\right\rangle_{ij}\left|-\right\rangle_{q}\Big),\end{aligned} \tag{23}$$

- $b_i = 10$:

$$\begin{aligned}(Y \otimes I \otimes I)\left|\psi^{+}\right\rangle_{iqj} &= (Y \otimes I \otimes I)\frac{1}{\sqrt{2}}\Big(\left|\Phi^{+}\right\rangle_{ij}\left|+\right\rangle_{q} + \left|\Phi^{-}\right\rangle_{ij}\left|-\right\rangle_{q}\Big),\\ &= (Y \otimes I \otimes I)\frac{1}{\sqrt{2}}\Big(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{ij}\left|+\right\rangle_{q} +\\ &+ \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)_{ij}\left|-\right\rangle_{q}\Big),\\ &= \frac{1}{\sqrt{2}}\Big(\frac{1}{\sqrt{2}}(-|10\rangle + |01\rangle)_{ij}\left|+\right\rangle_{q} + \frac{1}{\sqrt{2}}(-|10\rangle - |01\rangle)_{ij}\left|-\right\rangle_{q}\Big),\\ &= \frac{1}{\sqrt{2}}\Big(\left|\Psi^{-}\right\rangle_{ij}\left|+\right\rangle_{q} - \left|\Psi^{+}\right\rangle_{ij}\left|-\right\rangle_{q}\Big),\end{aligned} \tag{24}$$

- $b_i = 11$:

$$\begin{aligned}(Z \otimes I \otimes I)\left|\psi^{+}\right\rangle_{iqj} &= (Z \otimes I \otimes I)\frac{1}{\sqrt{2}}\Big(\left|\Phi^{+}\right\rangle_{ij}\left|+\right\rangle_{q} + \left|\Phi^{-}\right\rangle_{ij}\left|-\right\rangle_{q}\Big),\\ &= (Z \otimes I \otimes I)\frac{1}{\sqrt{2}}\Big(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{ij}\left|+\right\rangle_{q} +\\ &+ \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)_{ij}\left|-\right\rangle_{q}\Big),\\ &= \frac{1}{\sqrt{2}}\Big(\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)_{ij}\left|+\right\rangle_{q} + \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{ij}\left|-\right\rangle_{q}\Big),\\ &= \frac{1}{\sqrt{2}}\Big(\left|\Phi^{-}\right\rangle_{ij}\left|+\right\rangle_{q} + \left|\Phi^{+}\right\rangle_{ij}\left|-\right\rangle_{q}\Big),\end{aligned} \tag{25}$$

- **P.2.5**: Luego, u_i le transmite el estado codificado al usuario disjunto u_j.

- **P.2.6**: u_j ejecuta una medida de Bell en su partícula y en la de u_i. Al mismo tiempo, el QS calcula el estatus de su partícula de acuerdo a las bases de X, y anuncia el resultado de su medida.

- **P.2.7**: u_j usa el resultado de su medida y la publicación del QS para retribuir el mensaje original b_i, de acuerdo a los resultados en las ecuaciones (22-25) se puede construir el Cuadro 1.

Medida del u_j	Medida del QS	Operación de u_i	b_i
$\|\Phi^+\rangle_{ij}$	$\|+\rangle_q$	I	00
$\|\Phi^+\rangle_{ij}$	$\|-\rangle_q$	Z	11
$\|\Psi^+\rangle_{ij}$	$\|+\rangle_q$	X	01
$\|\Psi^+\rangle_{ij}$	$\|-\rangle_q$	Y	10
$\|\Phi^-\rangle_{ij}$	$\|+\rangle_q$	Z	11
$\|\Phi^-\rangle_{ij}$	$\|-\rangle_q$	I	00
$\|\Psi^-\rangle_{ij}$	$\|+\rangle_q$	X	10
$\|\Psi^-\rangle_{ij}$	$\|-\rangle_q$	Y	01

Cuadro 2: Decodificación según medidas para el caso de cooperación completa.

La Figura 1 esquematiza el protocolo para el caso de la cooperación parcial del QS.

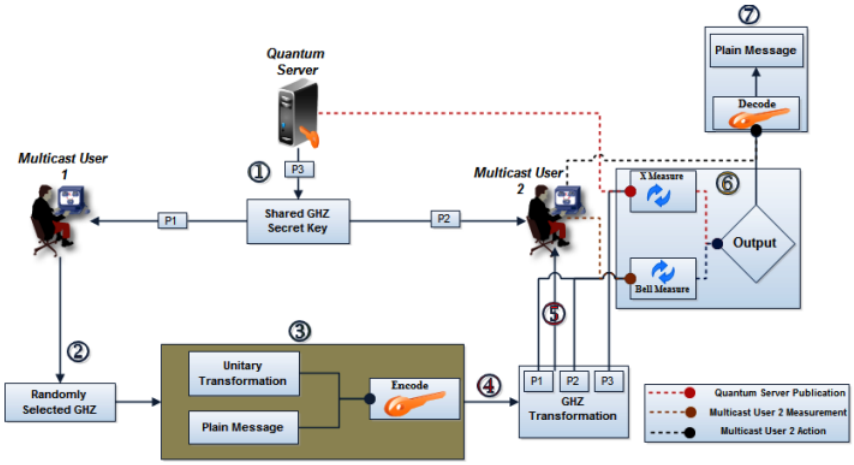

Figura 1: Proceso de comunicación entre dos usuarios disjuntos usando el soporte parcial del QS.

2.2. Cooperación completa

Este proceso consta de los pasos necesarios para la transmisión de un mensaje clásico entre dos usuarios disjuntos con soporte completo del servidor cuántico. En otras palabras, el servidor cuántico funciona como un centro de paso de mensajes entre los usuarios disjuntos comunicados.

Hay que tener en cuenta que para este paso los cambios de base de la ecuación (16) a las bases de Bell ocurren sobre las partículas iq, y el cambio a las bases de X sobre j, los cálculos de transformaciones siguen la misma lógica y resultados. Ahora, repitiendo los pasos P.2.1-P.2.4 con esta consideración, retomamos el protocolo de la siguiente forma:

- **C.2.5**: Luego de aplicar la transformación de GHZ correcta, u_i transmite el mensaje codificado al QS.
- **C.2.6**: El QS realiza la medida de Bell en su partícula y la de u_i. u_j calcula el estatus de su partícula de acuerdo a las bases de X y anuncia el resultado de su medida.
- **C.2.7**: u_j emplea la medida del QS y su publicación para retribuir el mensaje original según el Cuadro 2.

Medida del QS	Publicación de u_j	Operación de u_i	b_i
$\|\Phi^+\rangle_{iq}$	$\|+\rangle_j$	I	00
$\|\Phi^+\rangle_{iq}$	$\|-\rangle_j$	Z	11
$\|\Psi^+\rangle_{iq}$	$\|+\rangle_j$	X	01
$\|\Psi^+\rangle_{iq}$	$\|-\rangle_j$	Y	10
$\|\Phi^-\rangle_{iq}$	$\|+\rangle_j$	Z	11
$\|\Phi^-\rangle_{iq}$	$\|-\rangle_j$	I	00
$\|\Psi^-\rangle_{iq}$	$\|+\rangle_j$	X	10
$\|\Psi^-\rangle_{iq}$	$\|-\rangle_j$	Y	01

Cuadro 3: Decodificación según medidas para el caso de cooperación completa.

La Figura 2 esquematiza el protocolo para el caso de la cooperación completa del QS.

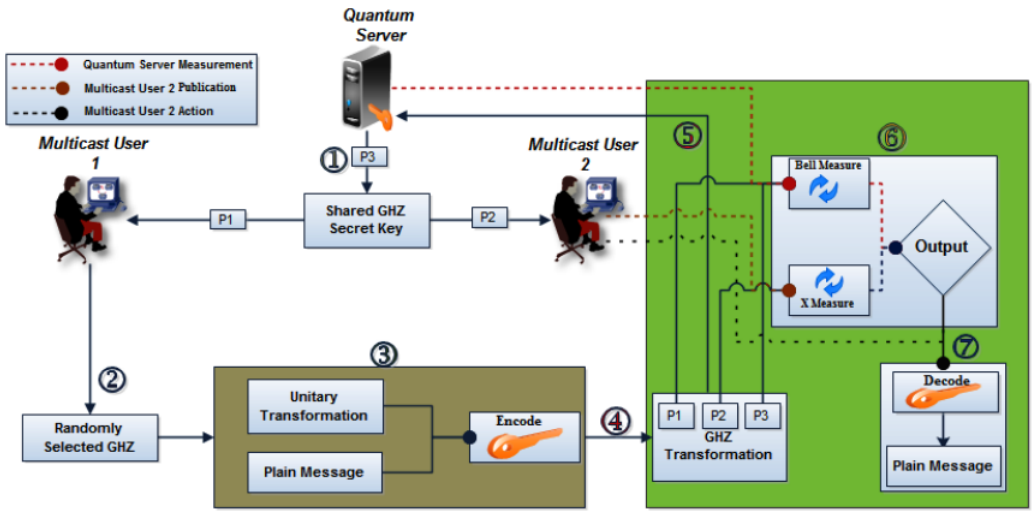

Figura 2: Proceso de comunicación entre dos usuarios disjuntos usando el soporte completo del QS.

3. Comunicación entre tres usuarios disjuntos con cooperación parcial y completa del server cuántico

3.1. Cooperación parcial

- **P.3.1**: El QS genera una secuencia de estados GHZ:

$$S = \left\{ |\Psi_1\rangle, |\Psi_2\rangle, ..., |\Psi_{N+1}\rangle \right\}, \tag{26}$$

donde,

$$|\Psi_k\rangle = \frac{1}{\sqrt{2}} \left(|0000\rangle_{ijql} + |1111\rangle_{ijql} \right). \tag{27}$$

De la ecuación (8):

$$\left|\psi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}(|000\rangle \pm |111\rangle) \tag{28}$$

sumando estos estados obtenemos:

$$|000\rangle = \frac{1}{\sqrt{2}} \left(\left|\psi^{+}\right\rangle + \left|\psi^{-}\right\rangle \right), \tag{29}$$

$$|111\rangle = \frac{1}{\sqrt{2}} \left(\left|\psi^{+}\right\rangle - \left|\psi^{-}\right\rangle \right). \tag{30}$$

Usando las ecuaciones (29-30) sobre ijl de la ecuación (27) y además las ecuaciones (17-18) sobre la partícula q en la misma ecuación (27), tenemos:

$$\begin{aligned}
|\Psi_k\rangle &= \frac{1}{\sqrt{2}} \left(\frac{1}{\sqrt{2}} \left(\left|\psi^{+}\right\rangle + \left|\psi^{-}\right\rangle \right)_{ijl} |0\rangle_q + \frac{1}{\sqrt{2}} \left(\left|\psi^{+}\right\rangle - \left|\psi^{-}\right\rangle \right)_{ijl} |1\rangle_q \right), \\
&= \frac{1}{2\sqrt{2}} \left(\left(\left|\psi^{+}\right\rangle + \left|\psi^{-}\right\rangle \right)_{ijl} (|+\rangle + |-\rangle)_q + \left(\left|\psi^{+}\right\rangle - \left|\psi^{-}\right\rangle \right)_{ijl} (|+\rangle - |-\rangle)_q \right), \\
&= \frac{1}{2\sqrt{2}} \Big(\left|\psi^{+}\right\rangle_{ijl} |+\rangle_q + \left|\psi^{+}\right\rangle_{ijl} |-\rangle_q + \left|\psi^{-}\right\rangle_{ijl} |+\rangle_q + \left|\psi^{-}\right\rangle_{ijl} |-\rangle_q + \\
&+ \left|\psi^{+}\right\rangle_{ijl} |+\rangle_q - \left|\psi^{+}\right\rangle_{ijl} |-\rangle_q - \left|\psi^{-}\right\rangle_{ijl} |+\rangle_q + \left|\psi^{-}\right\rangle_{ijl} |-\rangle_q \Big), \\
&= \frac{1}{2\sqrt{2}} \left(2 \left|\psi^{+}\right\rangle_{ijl} |+\rangle_q + 2 \left|\psi^{-}\right\rangle_{ijl} |-\rangle_q \right), \\
&= \frac{1}{\sqrt{2}} \left(\left|\psi^{+}\right\rangle_{ijl} |+\rangle_q + \left|\psi^{-}\right\rangle_{ijl} |-\rangle_q \right).
\end{aligned} \tag{31}$$

Luego, el QS reparte las partículas ijl entre los usuarios u_i, u_j y u_l respectivamente, conservando él la partícula q.

- **P.3.2**: Ambos, u_i y u_j, escogen aleatoriamente un subconjunto de la secuencia S y la mantienen incógnita.

- **P.3.3**: u_i genera una secuencia aleatoria de bits para transmitir el mensaje. De acuerdo a la misma codificación para el caso de dos usuarios, u_i aplica una operación U_{b_i}, donde $b_i \in \{00, 01, 10, 11\}$, sobre su partícula. Al mismo tiempo u_j aplica una operación U_{b_j}, donde $b_i \in \{0, 1\}$, sobre su partícula de acuerdo a la siguiente tabla:

b_j	U_{b_j}
0	$U_0 = I$
1	$U_1 = X$

Cuadro 4: Codificación de u_j.

- **P.3.4**: Luego, el estado GHZ será convertido de acuerdo a los bits transmitidos según los siguientes casos, en todos ellos se ignoran las operaciones identidad sobre los qubits l y q:

  - $b_i b_j = 000$:

$$\begin{aligned}(I_i \otimes I_j)\left|\Psi_k\right\rangle &= (I_i \otimes I_j)\frac{1}{\sqrt{2}}\Big(\left|\psi^+\right\rangle_{ijl}\left|+\right\rangle_q + \left|\psi^-\right\rangle_{ijl}\left|-\right\rangle_q\Big), \\ &= \frac{1}{\sqrt{2}}\Big(\left|\psi^+\right\rangle_{ijl}\left|+\right\rangle_q + \left|\psi^-\right\rangle_{ijl}\left|-\right\rangle_q\Big).\end{aligned} \tag{32}$$

  - $b_i b_j = 001$:

$$\begin{aligned}(I_i \otimes X_j)\left|\Psi_k\right\rangle &= (I_i \otimes X_j)\frac{1}{\sqrt{2}}\Big(\left|\psi^+\right\rangle_{ijl}\left|+\right\rangle_q + \left|\psi^-\right\rangle_{ijl}\left|-\right\rangle_q\Big), \\ &= (I_i \otimes X_j)\frac{1}{\sqrt{2}}\Big(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ijl}\left|+\right\rangle_q + \\ &+ \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)_{ijl}\left|-\right\rangle_q\Big), \\ &= \frac{1}{\sqrt{2}}\Big(\frac{1}{\sqrt{2}}(|010\rangle + |101\rangle)_{ijl}\left|+\right\rangle_q + \frac{1}{\sqrt{2}}(|010\rangle - |101\rangle)_{ijl}\left|-\right\rangle_q\Big), \\ &= \frac{1}{\sqrt{2}}\Big(\left|\phi^+\right\rangle_{ijl}\left|+\right\rangle_q + \left|\phi^-\right\rangle_{ijl}\left|-\right\rangle_q\Big).\end{aligned} \tag{33}$$

- $b_i b_j = 010$:

$$\begin{aligned}(X_i \otimes I_j)\,|\Psi_k\rangle &= (I_i \otimes X_j)\frac{1}{\sqrt{2}}\Big(\,|\psi^+\rangle_{ijl}\,|+\rangle_q + |\psi^-\rangle_{ijl}\,|-\rangle_q\,\Big),\\ &= (X_i \otimes I_j)\frac{1}{\sqrt{2}}\Big(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ijl}\,|+\rangle_q\\ &+ \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)_{ijl}\,|-\rangle_q\,\Big),\\ &= \frac{1}{\sqrt{2}}\Big(\frac{1}{\sqrt{2}}(|100\rangle + |011\rangle)_{ijl}\,|+\rangle_q + \frac{1}{\sqrt{2}}(|100\rangle - |011\rangle)_{ijl}\,|-\rangle_q\,\Big),\\ &= \frac{1}{\sqrt{2}}\Big(\,|\gamma^+\rangle_{ijl}\,|+\rangle_q + |\gamma^-\rangle_{ijl}\,|-\rangle_q\,\Big).\end{aligned} \tag{34}$$

- $b_i b_j = 011$:

$$\begin{aligned}(X_i \otimes X_j)\,|\Psi_k\rangle &= (X_i \otimes X_j)\frac{1}{\sqrt{2}}\Big(\,|\psi^+\rangle_{ijl}\,|+\rangle_q + |\psi^-\rangle_{ijl}\,|-\rangle_q\,\Big),\\ &= (X_i \otimes X_j)\frac{1}{\sqrt{2}}\Big(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ijl}\,|+\rangle_q +\\ &+ \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)_{ijl}\,|-\rangle_q\,\Big),\\ &= \frac{1}{\sqrt{2}}\Big(\frac{1}{\sqrt{2}}(|110\rangle + |001\rangle)_{ijl}\,|+\rangle_q + \frac{1}{\sqrt{2}}(|110\rangle - |001\rangle)_{ijl}\,|-\rangle_q\,\Big),\\ &= \frac{1}{\sqrt{2}}\Big(\,|\varphi^+\rangle_{ijl}\,|+\rangle_q - |\varphi^-\rangle_{ijl}\,|-\rangle_q\,\Big).\end{aligned} \tag{35}$$

- $b_i b_j = 100$:

$$\begin{aligned}(Y_i \otimes I_j)\,|\Psi_k\rangle &= (Y_i \otimes I_j)\frac{1}{\sqrt{2}}\Big(\,|\psi^+\rangle_{ijl}\,|+\rangle_q + |\psi^-\rangle_{ijl}\,|-\rangle_q\,\Big),\\ &= (Y_i \otimes I_j)\frac{1}{\sqrt{2}}\Big(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ijl}\,|+\rangle_q +\\ &+ \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)_{ijl}\,|-\rangle_q\,\Big),\\ &= \frac{1}{\sqrt{2}}\Big(\frac{1}{\sqrt{2}}(-|100\rangle + |011\rangle)_{ijl}\,|+\rangle_q + \frac{1}{\sqrt{2}}(-|100\rangle - |011\rangle)_{ijl}\,|-\rangle_q\,\Big),\\ &= \frac{1}{\sqrt{2}}\Big(\,|\gamma^-\rangle_{ijl}\,|+\rangle_q - |\gamma^+\rangle_{ijl}\,|-\rangle_q\,\Big).\end{aligned} \tag{36}$$

- $b_i b_j = 101$:

$$\begin{aligned}(Y_i \otimes X_j)\,|\Psi_k\rangle &= (Y_i \otimes I_j)\frac{1}{\sqrt{2}}\Big(\,|\psi^+\rangle_{ijl}\,|+\rangle_q + |\psi^-\rangle_{ijl}\,|-\rangle_q\,\Big),\\ &= (Y_i \otimes X_j)\frac{1}{\sqrt{2}}\Big(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ijl}\,|+\rangle_q + \\ &+ \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)_{ijl}\,|-\rangle_q\,\Big),\\ &= \frac{1}{\sqrt{2}}\Big(\frac{1}{\sqrt{2}}(-|101\rangle + |010\rangle)_{ijl}\,|+\rangle_q + \frac{1}{\sqrt{2}}(-|101\rangle - |010\rangle)_{ijl}\,|-\rangle_q\,\Big),\\ &= \frac{1}{\sqrt{2}}\Big(\,|\varphi^-\rangle_{ijl}\,|+\rangle_q - |\varphi^+\rangle_{ijl}\,|-\rangle_q\,\Big).\end{aligned} \tag{37}$$

- $b_i b_j = 110$:

$$\begin{aligned}(Z_i \otimes I_j)\,|\Psi_k\rangle &= (Y_i \otimes I_j)\frac{1}{\sqrt{2}}\Big(\,|\psi^+\rangle_{ijl}\,|+\rangle_q + |\psi^-\rangle_{ijl}\,|-\rangle_q\,\Big),\\ &= (Z_i \otimes I_j)\frac{1}{\sqrt{2}}\Big(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ijl}\,|+\rangle_q + \\ &+ \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)_{ijl}\,|-\rangle_q\,\Big),\\ &= \frac{1}{\sqrt{2}}\Big(\frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)_{ijl}\,|+\rangle_q + \frac{1}{\sqrt{2}}(-|000\rangle + |111\rangle)_{ijl}\,|-\rangle_q\,\Big),\\ &= \frac{1}{\sqrt{2}}\Big(\,|\psi^-\rangle_{ijl}\,|+\rangle_q - |\psi^+\rangle_{ijl}\,|-\rangle_q\,\Big).\end{aligned} \tag{38}$$

- $b_i b_j = 111$:

$$\begin{aligned}(Z_i \otimes X_j)\,|\Psi_k\rangle &= (Y_i \otimes I_j)\frac{1}{\sqrt{2}}\Big(\,|\psi^+\rangle_{ijl}\,|+\rangle_q + |\psi^-\rangle_{ijl}\,|-\rangle_q\,\Big),\\ &= (Z_i \otimes X_j)\frac{1}{\sqrt{2}}\Big(\frac{1}{\sqrt{2}}(|000\rangle) + |111\rangle)_{ijl}\,|+\rangle_q + \\ &+ \frac{1}{\sqrt{2}}(|000\rangle) - |111\rangle)_{ijl}\,|-\rangle_q\,\Big),\\ &= \frac{1}{\sqrt{2}}\Big(\frac{1}{\sqrt{2}}(|010\rangle) - |101\rangle)_{ijl}\,|+\rangle_q + \frac{1}{\sqrt{2}}(-|010\rangle + |101\rangle)_{ijl}\,|-\rangle_q\,\Big),\\ &= \frac{1}{\sqrt{2}}\Big(\,|\phi^-\rangle_{ijl}\,|+\rangle_q - |\phi^+\rangle_{ijl}\,|-\rangle_q\,\Big).\end{aligned} \tag{39}$$

- **P.3.5**: Después, ambos u_i y u_j, le transmitiendo el mensaje transformado al usuario disjunto u_l, u_l realiza una medida GHZ en las partículas ijl.
- **P.3.6**: El QS calcula el estatus de su partícula realizando una medida de su partícula en las bases de X y anuncia el resultado de su medida.
- **P.3.7** u_l utiliza su medida y la medida del QS para descifrar el mensaje $b_i b_j$, usando las ecuaciones (32-39) se construye el Cuadro 5.

Medida del u_j	Medida del QS	U_{b_i}	b_i	U_{b_j}	b_j	Mensaje $(b_i b_j)$
$\|\psi^+\rangle_{ijl}$	$\|+\rangle_q$	I	00	I	0	000
$\|\psi^-\rangle_{ijl}$	$\|-\rangle_q$	I	00	I	0	000
$\|\phi^+\rangle_{ijl}$	$\|+\rangle_q$	I	00	X	1	001
$\|\phi^-\rangle_{ijl}$	$\|-\rangle_q$	I	00	X	1	001
$\|\gamma^+\rangle_{ijl}$	$\|+\rangle_q$	X	01	I	0	010
$\|\gamma^-\rangle_{ijl}$	$\|-\rangle_q$	X	01	I	0	010
$\|\varphi^+\rangle_{ijl}$	$\|+\rangle_q$	X	01	X	1	011
$\|\varphi^-\rangle_{ijl}$	$\|-\rangle_q$	X	01	X	1	011
$\|\gamma^-\rangle_{ijl}$	$\|+\rangle_q$	Y	10	I	0	100
$\|\gamma^+\rangle_{ijl}$	$\|-\rangle_q$	Y	10	I	0	100
$\|\varphi^-\rangle_{ijl}$	$\|+\rangle_q$	Y	10	X	1	101
$\|\varphi^+\rangle_{ijl}$	$\|-\rangle_q$	Y	10	X	1	101
$\|\psi^-\rangle_{ijl}$	$\|+\rangle_q$	Z	11	I	0	110
$\|\psi^+\rangle_{ijl}$	$\|-\rangle_q$	Z	11	I	0	110
$\|\phi^-\rangle_{ijl}$	$\|+\rangle_q$	Z	11	X	1	111
$\|\phi^+\rangle_{ijl}$	$\|-\rangle_q$	Z	11	X	1	111

Cuadro 5: Decodificación según medidas para el caso de cooperación parcial con tres usuarios.

La Figura 3 esquematiza el protocolo para el caso de la cooperación parcial del QS con tres usuarios.

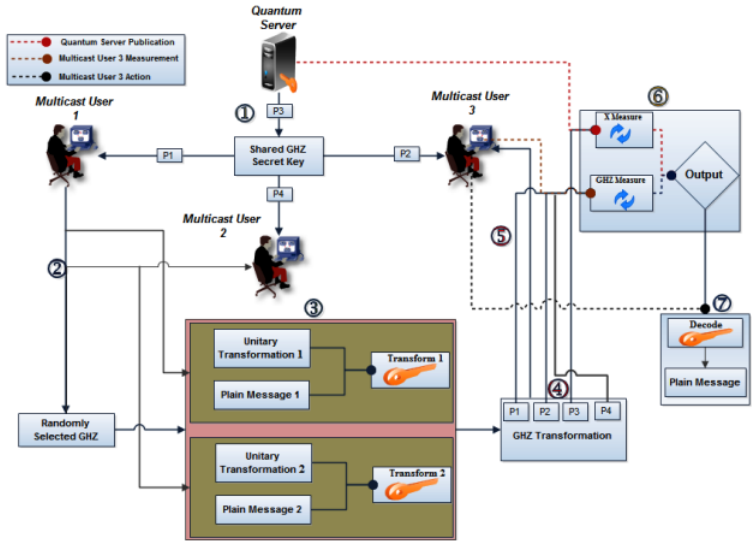

Figura 3: Proceso de comunicación entre dos usuarios disjuntos usando el soporte parcial del QS con tres usuarios.

3.2. Cooperación completa

Este proceso consta de los pasos necesarios para la transmisión de un mensaje clásico entre tres usuarios disjuntos con soporte completo del servidor cuántico. En otras palabras, el servidor cuántico funciona como un centro de paso de mensaje entre los usuarios disjuntos.

Repitiendo los pasos P.3.1-P.3.4 de la cooperación parcial, retomamos el protocolo de la siguiente forma:

- **C.3.5**: Después, ambos u_i y u_j transmiten el mensaje transformado al QS, el QS realiza una medida de GHZ sobre las partículas qij.
- **C.3.6**: u_l calcula el estatus de su partícula realizando una medida en las bases de X y anuncia su resultado.
- **C.3.7**: u_l usa su publicación y la medida del QS para retribuir el mensaje original de acuerdo al Cuadro 5.

Medida del QS	Medida del u_l	U_{b_i}	b_i	U_{b_j}	b_j	Mensaje $(b_i b_j)$
$\|\psi^+\rangle_{qij}$	$\|+\rangle_q$	I	00	I	0	000
$\|\psi^-\rangle_{qij}$	$\|-\rangle_q$	I	00	I	0	000
$\|\phi^+\rangle_{qij}$	$\|+\rangle_q$	I	00	X	1	001
$\|\phi^-\rangle_{qij}$	$\|-\rangle_q$	I	00	X	1	001
$\|\gamma^+\rangle_{qij}$	$\|+\rangle_q$	X	01	I	0	010
$\|\gamma^-\rangle_{qij}$	$\|-\rangle_q$	X	01	I	0	010
$\|\varphi^+\rangle_{qij}$	$\|+\rangle_q$	X	01	X	1	011
$\|\varphi^-\rangle_{qij}$	$\|-\rangle_q$	X	01	X	1	011
$\|\gamma^-\rangle_{qij}$	$\|+\rangle_q$	Y	10	I	0	100
$\|\gamma^+\rangle_{qij}$	$\|-\rangle_q$	Y	10	I	0	100
$\|\varphi^-\rangle_{qij}$	$\|+\rangle_q$	Y	10	X	1	101
$\|\varphi^+\rangle_{qij}$	$\|-\rangle_q$	Y	10	X	1	101
$\|\psi^-\rangle_{qij}$	$\|+\rangle_q$	Z	11	I	0	110
$\|\psi^+\rangle_{qij}$	$\|-\rangle_q$	Z	11	I	0	110
$\|\phi^-\rangle_{qij}$	$\|+\rangle_q$	Z	11	X	1	111
$\|\phi^+\rangle_{qij}$	$\|-\rangle_q$	Z	11	X	1	111

Cuadro 6: Decodificación según medidas para el caso de cooperación parcial con tres usuarios.

La Figura 4 esquematiza el protocolo para el caso de la cooperación parcial del QS.

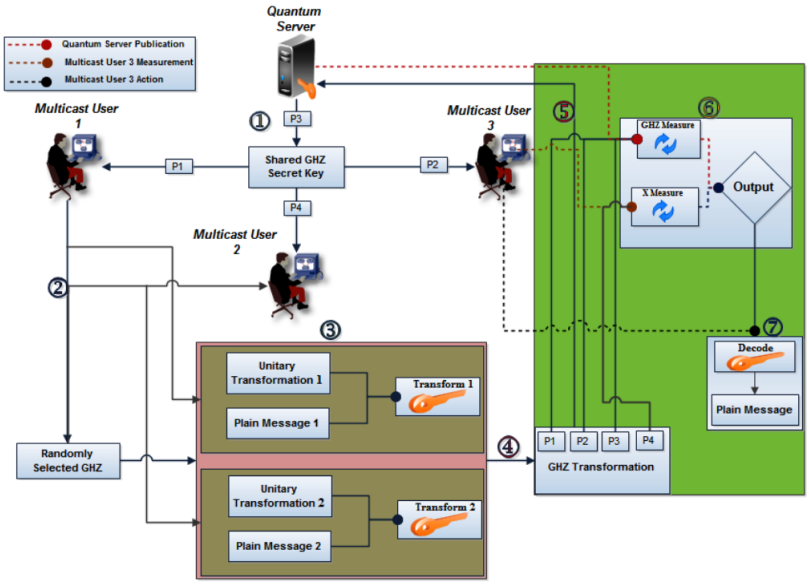

Figura 4: Proceso de comunicación entre tres usuarios disjuntos usando el soporte completo del QS.

4. Comunicación entre N usuarios disjuntos con cooperación parcial y completa del server cuántico

El proceso es esencialmente el mismo que en el de casos anteriores. En este caso, los usuarios $u_1, u_2, ..., u_{N-1}$ desean enviarle un mensaje a u_N. El QS crea un estado GHZ de $N+1$ partículas y las distribuye entre los N usuarios y él mismo. Cabe destacar que este paso se puede omitir si el proceso de comunicación continua inmediatamente después de la fase de comunicación, debido a que este último deja una repartición de estado GHZ entre los usuarios y QS exactamente igual a la necesaria. El estado es:

$$|\Psi\rangle_{q12\cdots N} = \frac{1}{\sqrt{2}}(|000\cdots0\rangle + |111\cdots1\rangle)_{q12\cdots N} \tag{40}$$

4.1. Cooperación parcial

Luego, cada uno de los usuarios $u_1, u_2, ..., u_{N-1}$ aplica una operación U_{b_i} según el mensaje que quiera enviar, la codificación sigue el estándar del Cuadro 1. Esto deja al estado GHZ en:

$$|\Psi\rangle_{q12\cdots N} = \frac{1}{\sqrt{2}}\left(\underbrace{|GHZ'\rangle}_{\substack{u_1,\ldots,u_N \\ \text{Usuarios}}}|\pm\rangle_q \pm \underbrace{|GHZ''\rangle}_{\substack{u_1,\ldots,u_N \\ \text{Usuarios}}}|\pm\rangle_q\right), \tag{41}$$

donde $|GHZ'\rangle$ y $|GHZ''\rangle$ son dos estados GHZ de longitud N que el usuario u_N para medir en la base GHZ y decodificar $b_1b_2...b_N \in \{0,1\}^N$ con la ayuda de la medida en X

de la partícula q por parte del QS.

La Figura 5 esquematiza el protocolo para el caso de la cooperación parcial del QS.

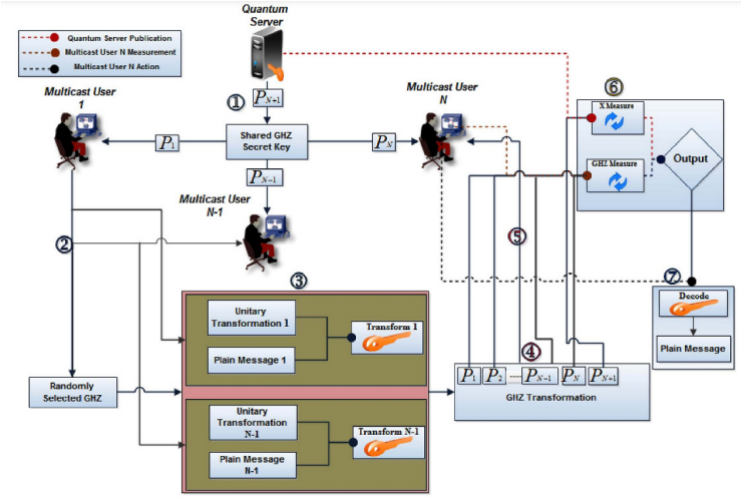

Figura 5: Proceso de comunicación entre N usuarios disjuntos usando el soporte parcial del QS.

4.2. Cooperación completa

Luego, cada uno de los usuarios $u_1, u_2, ..., u_{N-1}$ aplica una operación U_{b_i} según el mensaje que quiera enviar, la codificación sigue el estándar del Cuadro 1. Esto deja al estado GHZ en:

$$|\Psi\rangle_{q12\cdots N} = \frac{1}{\sqrt{2}}\Bigg(\underbrace{|GHZ'\rangle}_{\substack{q,u_1,\ldots,u_{N-1}\\ \text{Mensajeros+QS}}} \underbrace{|\pm\rangle_N}_{\substack{u_N\\ \text{Receptor}}} \pm \underbrace{|GHZ''\rangle}_{\substack{q,u_1,\ldots,u_{N-1}\\ \text{Mensajeros+QS}}} \underbrace{|\pm\rangle_N}_{\substack{u_N\\ \text{Receptor}}} \Bigg). \tag{42}$$

En este caso el usuario u_N descifrara el mensaje con la ayuda de la medida del QS en las bases GHZ y su medida en la base X de su partícula.

La Figura 6 esquematiza el protocolo para el caso de la cooperación completo del QS.

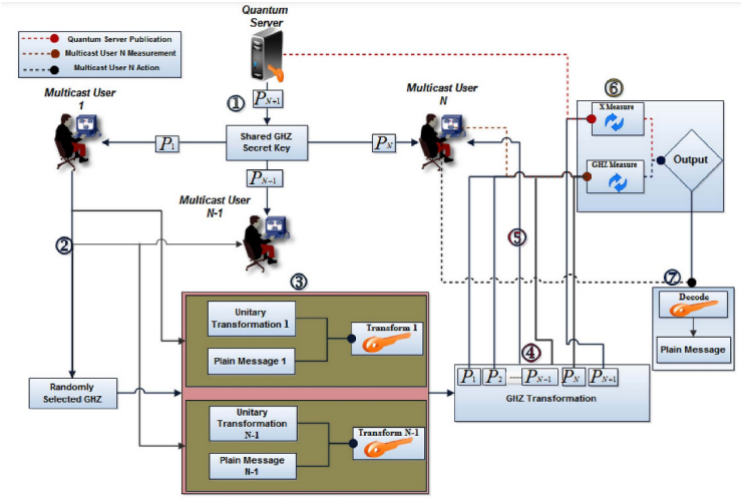

Figura 6: Proceso de comunicación entre N usuarios disjuntos usando el soporte completo del QS.

5. Ejemplos

5.1. Fase de autenticación

En este caso se usa un solo usuario y pasamos directamente al funcionamiento de las transformaciones C_{OP}. Asumamos que $J_A = J_1 \otimes J_2$, entonces el estado GHZ (que al ser un solo usuario es un estado de Bell) es:

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle_{SA} + |11\rangle_{SA}), \tag{43}$$

y el estado n es:

$$|\phi_n\rangle = |J_A\rangle\,. \tag{44}$$

5.1.1. Codificación del usuario

Si $J_2 = 0$:

$$C_0^{A\to n}(|\Psi\rangle \otimes |J_A\rangle_n) = C_0^{A\to n}\left(\frac{1}{\sqrt{2}}(|00\rangle_{SA} + |11\rangle_{SA}) \otimes |J_A\rangle_n\right),$$

$$C_0^{A\to n}\left(\frac{1}{\sqrt{2}}(|00\rangle_{SA}\,|J_A\rangle_n + |11\rangle_{SA}\,|J_A\rangle_n)\right) = \frac{1}{\sqrt{2}}(|00\rangle_{SA}\,|J_A\rangle_n + |11\rangle_{SA}\,|\overline{J_A}\rangle_n).$$

Si $J_2 = 1$:

$$C_1^{A\to n}(|\Psi\rangle \otimes |J_A\rangle_n) = C_1^{A\to n}\left(\frac{1}{\sqrt{2}}(|{+}{+}\rangle_{SA} + |{-}{-}\rangle_{SA}) \otimes |J_A\rangle_n\right),$$

$$C_1^{A\to n}\left(\frac{1}{\sqrt{2}}(|{+}{+}\rangle_{SA}\,|J_A\rangle_n + |{-}{-}\rangle_{SA}\,|J_A\rangle_n)\right) = \frac{1}{\sqrt{2}}(|{+}{+}\rangle_{SA}\,|J_A\rangle_n + |{-}{-}\rangle_{SA}\,|\overline{J_A}\rangle_n).$$

5.1.2. Decodificación del QS

Si $J_2 = 0$:

$$C_0^{S\to n}\left(\frac{1}{\sqrt{2}}(|00\rangle_{SA}|J_A\rangle_n + |11\rangle_{SA}|\overline{J_A}\rangle_n)\right) = \frac{1}{\sqrt{2}}(|00\rangle_{SA}|J_A\rangle_n + |11\rangle_{SA}|J_A\rangle_n),$$
$$= |\Psi\rangle_{SA}\otimes|J_A\rangle_n$$

Si $J_2 = 1$:

$$C_1^{S\to n}\left(\frac{1}{\sqrt{2}}(|{+}{+}\rangle_{SA}|J_A\rangle_n + |{-}{-}\rangle_{SA}|\overline{J_A}\rangle_n)\right) = \frac{1}{\sqrt{2}}(|{+}{+}\rangle_{SA}|J_A\rangle_n + |{-}{-}\rangle_{SA}|J_A\rangle_n),$$
$$= |\Psi\rangle_{SA}\otimes|J_A\rangle_n$$

En ambos casos si el QS mide n en las bases de Z obtendrá J_A, confirmando la identidad del usuario.

5.2. Proceso de comunicación

Supongamos una comunicación entre dos usuarios, u_a y u_b, administrada por un QS. El QS lo primero que hace preparar el estado GHZ:

$$\begin{aligned}|\psi_3^+\rangle_{abq} &= \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{abq},\\ &= \frac{1}{\sqrt{2}}\left(|\Phi^+\rangle_{ab}|{+}\rangle_q + |\Phi^-\rangle_{ab}|{-}\rangle_q\right).\end{aligned} \tag{45}$$

y lo reparte entre los usuarios, incluyéndole.

Supongamos ahora que u_a quiere enviar el mensaje $b_a = 10$ a u_b, entonces u_a aplica $U_{10} = Y$ a su partícula a dejandola en el estado de la ecuación (24):

$$Y_a|\psi_3^+\rangle_{abq} = \frac{1}{\sqrt{2}}\left(|\Psi^-\rangle_{ab}|{+}\rangle_q - |\Psi^+\rangle_{ab}|{-}\rangle_q\right). \tag{46}$$

En cooperación parcial

u_a le transmite su partícula a u_b. Luego, el QS mide su partícula q en las bases de X. Asumamos que su medida arroja $|-\rangle$. La medida proyectiva aplicada sería:

$$\begin{aligned}\hat{M}_q^-|\psi_3^+\rangle_{abq} &= (I\otimes I\otimes|{-}\rangle_q\langle{-}|_q)\frac{1}{\sqrt{2}}\left(|\Psi^-\rangle_{ab}|{+}\rangle_q - |\Psi^+\rangle_{ab}|{-}\rangle_q\right),\\ &= \frac{1}{\sqrt{2}}\left(|\Psi^-\rangle_{ab}\langle{-}|{+}\rangle_{qq}|{-}\rangle_q - |\Psi^+\rangle_{ab}\langle{-}|{-}\rangle_{qq}|{-}\rangle_q\right),\\ &= \frac{1}{\sqrt{2}}\left(-|\Psi^+\rangle_{ab}|{-}\rangle_q\right).\end{aligned} \tag{47}$$

Luego la probabilidad de encontrar ese estado:

$$
\begin{aligned}
p(-) &= \left\langle \psi_3^+ \right|_{abq} \hat{M}_q^{-\dagger} \hat{M}_q^- \left| \psi_3^+ \right\rangle_{abq}, \\
&= \frac{1}{\sqrt{2}} \left(- \left\langle \Psi^+ \right|_{ab} \langle - |_q \right) \frac{1}{\sqrt{2}} \left(- \left| \Psi^+ \right\rangle_{ab} |-\rangle_q \right), \\
&= \frac{1}{2} \left\langle \Psi^+ \middle| \Psi^+ \right\rangle_{abab} \langle - | - \rangle_{qq}, \\
&= \frac{1}{2}.
\end{aligned} \tag{48}
$$

El estado de la ecuación (46) queda en:

$$
\begin{aligned}
\left| \psi_3^+ \right\rangle'_{abq} &= \frac{\hat{M}_q^- \left| \psi_3^+ \right\rangle_{abq}}{\sqrt{p(-)}}, \\
&= \frac{1}{\sqrt{\frac{1}{2}}} \frac{1}{\sqrt{2}} \left(- \left| \Psi^+ \right\rangle_{ab} |-\rangle_q \right), \\
&= - \left| \Psi^+ \right\rangle_{ab} |-\rangle_q .
\end{aligned} \tag{49}
$$

Finalmente, u_b mide en las bases de Bell el estado $|\Psi^+\rangle_{ab}$ que junto al anuncio de la media del QS en $|-\rangle_q$ y la ayuda del Cuadro 2 descifra el mensaje $b_a = 10$.

Cooperación completa

En este caso u_a le transmite su partícula al QS. Por brevedad y sin perder generalidad, asumamos que las medidas son las mismas, pero aquí el QS mide las partículas aq en las bases de Bell obteniendo $|\Psi^+\rangle_{aq}$ y el u_b mide $|-\rangle_b$ descifrando el mismo mensaje $b_a = 10$.

6. Implementación circuital

En esta sección se detalla las posibles construcciones circuitales del protocolo detallado en las secciones anteriores, considerando que son 3 usuarios, pues la implementación de 2 usuarios será simplemente hacer los recortes pertinentes. Además se asume que $k = 4$ para usar siempre el ultimo bit de la llave compartida. Tristemente no se puede representar gráficamente el proceso de repartición de los qubits en los circuitos.

6.1. Fase de autenticación

6.1.1. Iniciacilización del GHZ

La primera parte de la fase de autenticación y comunicación es la creación de un estado GHZ. Esto se logra haciendo:

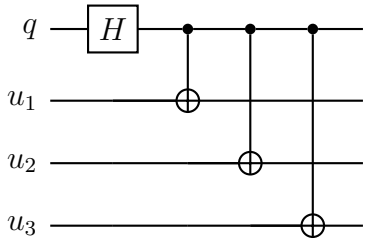

Figura 7: Iniciacilización del 4-GHZ.

6.1.2. Estados n

En este caso dependerá de cada $J_i \otimes J_{N+1}$. Pero si se asume que los qubits están inicializados en $|0\rangle$, entonces solo debemos aplicar una transformación X controlada por bits, esto es:

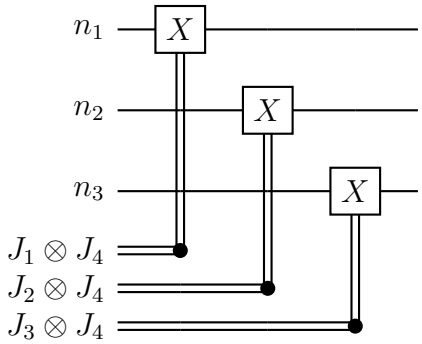

Figura 8: Estados n.

6.1.3. Transformaciones controladas C_{OP}

Recordando, C_0 corresponde a un CNOT común y C_1 a un CNOT en las bases de X, y la elección depende de J_4, para eso se propone el siguiente circuito controlado por bits:

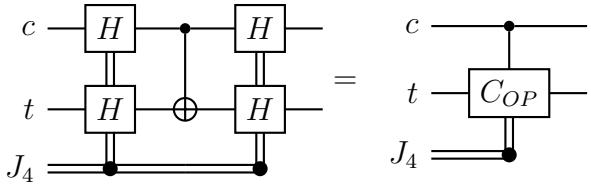

Figura 9: Transformaciones controladas C_{OP}.

Utilizando estos bloques, podemos construir el circuito de autenticación siguiente:

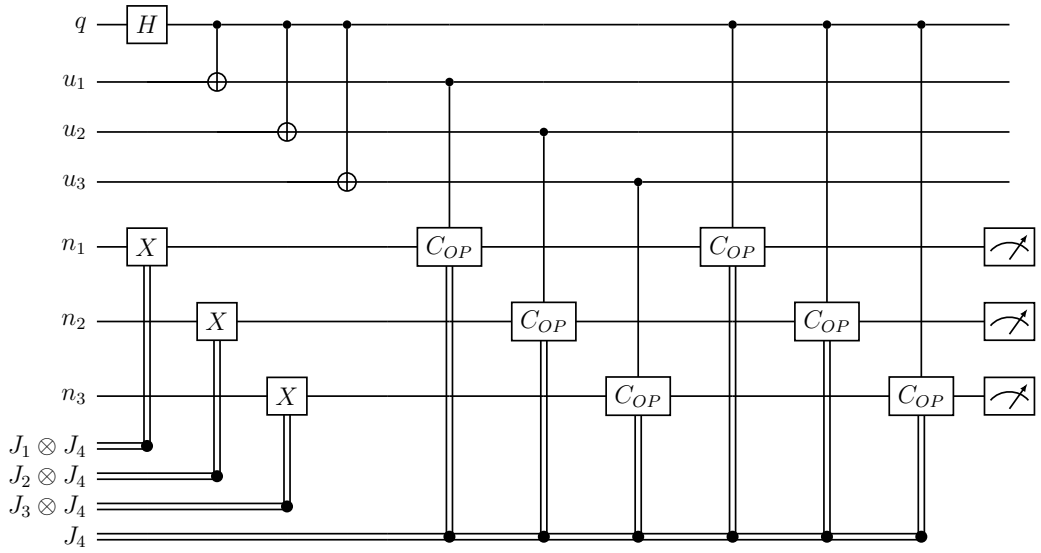

Figura 10: Circuito de autenticación para $N = 3$.

6.2. Proceso de comunicación

6.2.1. Operaciones U_{b_i} y U_{b_j}

Este caso es muy sencillo, para U_{b_i} basta simplemente hacer:

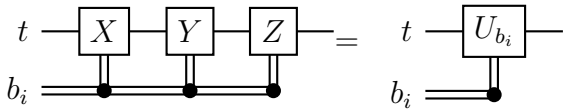

Figura 11: Transformación U_{b_i}.

Similarmente para U_{b_j}:

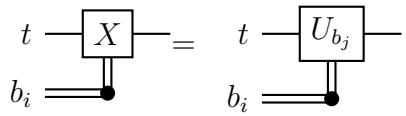

Figura 12: Transformación U_{b_j}.

6.2.2. Medida en X

Para poder medir en otras bases que no sean las de Z en un circuito, se debe asumir que el estado anterior a la medida está en estas bases que deseamos medir, aplicar una transformación que lo devuelva a las bases de Z y medir. Para la medida en X, la transformación capaz de llevar de las bases de X a la de Z es la de Hadamard. Así el circuito es:

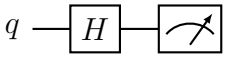

Figura 13: Medida en las bases de X.

6.2.3. Medida en GHZ

Al igual que el caso anterior, debemos hacer el cambio de GHZ a Z, para eso usamos el circuito:

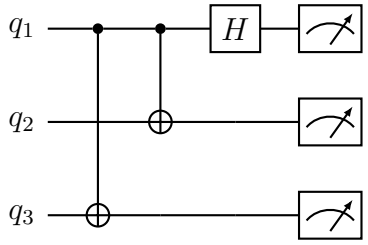

Figura 14: Medida en las bases 3-GHZ.

Finalmente, podemos uniendo todos los bloques, podemos construir los circuitos de comunicación siguientes:

Cooperación parcial

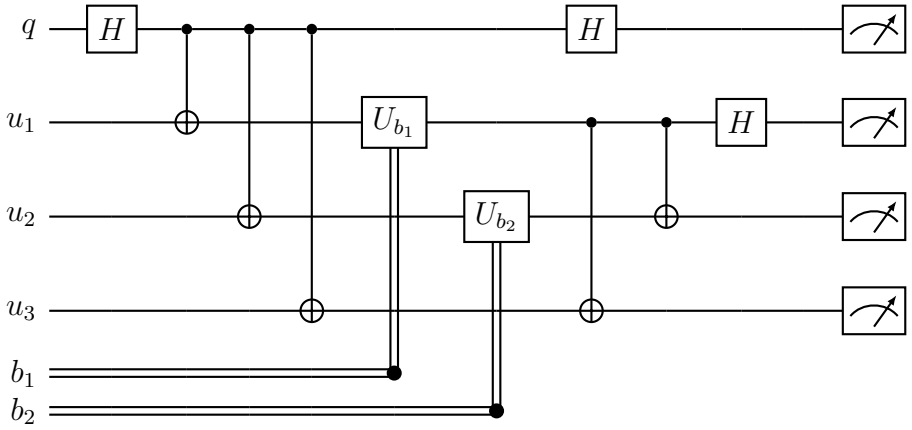

Figura 15: Circuito de comunicación para cooperación parcial.

Cooperación completa

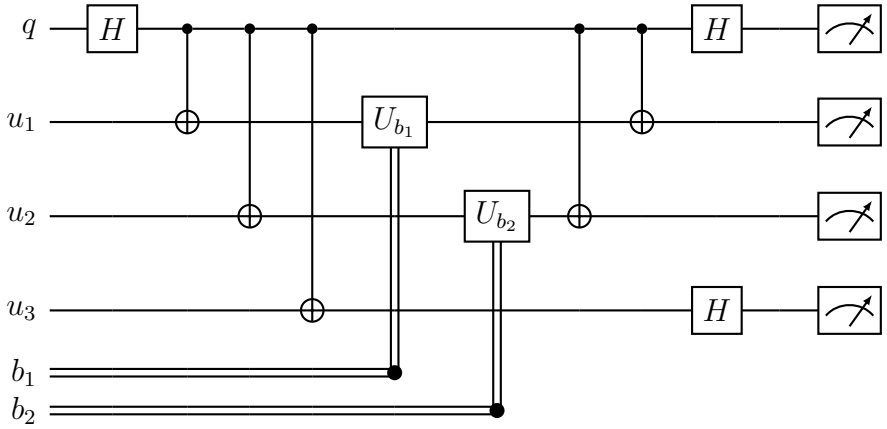

Figura 16: Circuito de comunicación para cooperación completa.

Bibliografía

1 Farouk, A. et al. A generalized architecture of quantum secure direct communication for N disjointed users with authentication. Sci. Rep. 5, 16080; doi: 10.1038/srep16080 (2015).

2 Farouk, A., Batle, J., Elhoseny, M., Naseri, M., Lone, M., Fedorov, A., Alkhambashi, M., Ahmed, S. and Abdel-Aty, M., 2017. Robust general N user authentication scheme in a centralized quantum communication network via generalized GHZ states. Frontiers of Physics, 13(2).