PEDECIBA Informática
Instituto de Computación – Facultad de Ingeniería
Universidad de la República
Montevideo, Uruguay

Reporte Técnico RT 04-15

Criptografía cuántica

Sergio Nesmachnow

Noviembre de 2004

Criptografía cuántica
Nesmachnow, Sergio

ISSN 0797-6410
Reporte Técnico RT 04-15
PEDECIBA
Instituto de Computación – Facultad de Ingeniería
Universidad de la República

Montevideo, Uruguay, Noviembre de 2004

Criptografía cuántica

Sergio Nesmachnow
Centro de Cálculo, Instituto de Computación
Facultad de Ingeniería, Universidad de la República
Uruguay

Noviembre, 2004

Resumen

Este trabajo presenta los conceptos generales sobre las técnicas criptográficas basadas en los principios de la informática cuántica. Presenta en detalle los protocolos cuánticos de distribución de claves más difundidos y los aspectos relacionados con la seguridad del protocolo BB84, el cual exige los menores requerimientos de hardware cuántico. En particular, se examina la prueba presentada por parte de Shor y Preskill sobre la seguridad del mecanismo de distribución.

1 Introducción

El desarrollo de la computación cuántica presenta un complejo problema a las propuestas actualmente existentes para comunicar de manera segura a dos interlocutores. La computación cuántica tiene la potencialidad de aprovechar el paralelismo implícito en los estados cuánticos, siendo capaz de realizar en tiempos reducidos las complejas operaciones sobre las que se basan los sistemas criptográficos más populares en la actualidad.

Compensando el efecto negativo anteriormente mencionado, la informática cuántica ha permitido el desarrollo de técnicas criptográficas en las cuales la seguridad de una comunicación queda garantizada por los propios postulados de la física y no depende de conjeturas matemáticas o de la imposibilidad de disponer de la enorme potencia de cómputo requerida para descifrar mensajes encriptados por las técnicas tradicionales.

Este trabajo presenta de manera resumida los conceptos relacionados con la criptografía cuántica, describe los protocolos de distribución cuántica de claves y se concentra en explicar los detalles de una prueba que garantiza la seguridad del protocolo BB84, el primer protocolo cuántico para distribución de claves propuesto y uno de los más importantes desde el punto de vista práctico, ya que es el protocolo que exige los menores requerimientos de hardware cuántico para su implementación.

El artículo se organiza del modo que se describe a continuación. Comienza con una sección introductoria que presenta un breve resumen de conceptos relacionados con las técnicas criptográficas tradicionales y la presentación de las técnicas de criptografía cuántica. La Sección 3 ofrece una reseña histórica sobre los trabajos que plantearon el uso de la computación cuántica con el objetivo de implementar mecanismos de comunicación segura, y describe de modo genérico los protocolos de distribución cuántica de claves propuestos. A continuación, la Sección 4 introduce conceptos de teoría cuántica de la información, que serán relevantes en el análisis de los protocolos y en la prueba de seguridad presentada. La Sección 5 presenta en detalle los mecanismos de distribución cuántica de claves, explicando en forma concreta el primer protocolo propuesto, el protocolo BB84. La Sección 6 constituye la parte principal del trabajo y presenta detalladamente la prueba de seguridad original de Shor y Preskill, derivando la seguridad del protocolo BB84 a partir de una implementación de un protocolo cuántico seguro por construcción. Por último, unos breves comentarios resumen la importancia del tema y sirven como conclusión del trabajo.

Este trabajo fue desarrollado en el marco del curso *Computación Cuántica*, dictado en el Instituto de Física de la Facultad de Ingeniería, Universidad de la República, Uruguay, durante el segundo semestre del año 2004.

2 Introducción a las técnicas criptográficas

El objetivo de las técnicas criptográficas, también conocidas como técnicas de encriptado, consiste en posibilitar la comunicación segura entre dos interlocutores, utilizando un canal público de modo que un eventual espía no sea capaz de conocer la información contenida en los mensajes enviados. A los efectos prácticos, se requiere que el conocimiento que pueda adquirir el espía sobre la información transmitida esté limitado.

A lo largo de la historia, diversos mecanismos de encriptado conocidos como *técnicas de criptografía simétrica* o *de clave privada* fueron presentados para posibilitar la transmisión segura de información. En la criptografía simétrica se utiliza la misma clave para encriptar y para desencriptar la información. Este mecanismo involucra un inconveniente a la hora de transmitir datos, ya que el remitente debe enviar previamente la clave al destinatario para que éste pueda desencriptar la información, y el envío de la clave debe hacerse por un conducto seguro. De este modo, se necesita de un canal seguro como requisito previo para garantizar la seguridad de los mensajes transmitidos por el canal público. La criptografía clásica no ofrece una solución exacta para el problema de distribución de claves, y esta limitación hizo parecer a las técnicas criptográficas fuera del alcance de usuarios que no dispusieran de complejas técnicas de distribución que permitieran intercambiar claves con sus posibles interlocutores.

Este escenario pesimista cambió con la introducción de las técnicas de *criptografía asimétrica o de clave pública* en 1976. La criptografía de clave pública se basa en que cada interlocutor escoge aleatoriamente un par de transformaciones inversas –una transformación utilizable para el encriptado de datos y otra para el desencriptado– generando un par de claves. Cada usuario presenta las instrucciones para encriptar datos (publicando su *clave pública*) pero mantiene en secreto el mecanismo de desencriptado (y su *clave privada*). De este modo, cualquier posible interlocutor puede utilizar la información disponible para codificar mensajes con una clave pública de un modo tal que solo podrán ser desencriptados utilizando la clave privada correspondiente. Este esquema no presenta el problema distribución de claves, que deja de ser necesario, ya que la clave pública se distribuye sin restricciones y la clave privada permanece en poder de su creador. El propio mecanismo de generación de claves utilizado garantiza que ningún espía es capaz de derivar la clave privada de un usuario con la información disponible en su clave pública. Desafortunadamente, la seguridad del mecanismo de generación de claves, y con él toda la criptografía de clave pública, se basa en suposiciones matemáticas no probadas, como la dificultad de factorizar números enteros grandes. En la práctica, se exigen criterios de seguridad que posibiliten que la factorización de los números involucrados sea una tarea inabordable en un tiempo razonable utilizando las técnicas y los recursos computacionales disponibles en la actualidad.

El esfuerzo computacional requerido por el mecanismo de desencriptado utilizado en las técnicas criptográficas de clave pública es considerablemente superior que el requerido en los esquemas de clave privada. Este inconveniente fue superado por la introducción de un protocolo de *acuerdo de clave* diseñado por Diffie y Hellman [12], que permite a dos usuarios intercambiar una clave secreta a través de un medio inseguro, sin requerir de información secreta previa.

El protocolo de Diffie y Hellman se basa en dos parámetros públicos: un número primo p y un entero g, denominado *generador* que verifican que $g < p$ y que para cada número natural n entre 1 y $p-1$ inclusive, existe un exponente k tal que $n = g^k \bmod p$. Para acordar un clave privada entre dos interlocutores (Alicia y Bob) utilizando el protocolo Diffie–Hellman, Alicia debe generar un número entero aleatorio a y Bob un número entero aleatorio b. Luego deben derivar valores públicos utilizando los parámetros del protocolo, $g^a \bmod p$ para Alicia y $g^b \bmod p$ para Bob, los cuales son intercambiados. Por último, Alicia calcula $g^{ab} = (g^b)^a \bmod p$ y Bob calcula $g^{ba} = (g^a)^b \bmod p$. El valor $g^{ab} = g^{ba} = K$ constituye la clave secreta. La seguridad del protocolo depende de la complejidad de invertir las operaciones realizadas por Alicia y Bob, que impide a un espía (Eva) calcular el valor de K a partir de los valores públicos $g^a \bmod p$ y $g^b \bmod p$ cuando el número primo p es suficientemente grande. Maurer [20] mostró que romper el protocolo de Diffie–Hellman es equivalente a calcular la función logaritmo discreto bajo ciertas hipótesis.

En la actualidad, son popularmente utilizados tanto los mecanismos de encriptado de clave pública (en general para la comunicación de volúmenes de información reducidos), como los mecanismos de encriptado con clave privada acordada mediante el protocolo de Diffie–Hellman. Si se utilizan claves de longitud adecuada, los actuales sistemas que combinan clave pública y clave privada son lo suficientemente seguros para el estado actual de la tecnología computacional.

Sin embargo, el desarrollo de la computación cuántica presenta un complejo problema a los actuales sistemas de seguridad. Con su capacidad de aprovechar el paralelismo implícito en los estados cuánticos, una computadora cuántica es capaz de factorizar enteros grandes en tiempos notoriamente inferiores que los que necesitaría una computadora clásica. Esto implica que la seguridad de los esquemas criptográficos de clave pública se ve seriamente amenazada. A modo de ejemplo, descifrar un mensaje encriptado con el sistema RSA utilizando una clave de 2048 bits, sin conocer la clave privada, involucra estrategias de ataque que demandarían miles de años con un gran número de supercomputadoras de la actual tecnología, inclusive trabajando en forma simultánea con varios elementos de procesamiento interconectados en paralelo. Este mismo mensaje se descifraría en cuestión de segundos en caso de contar con la capacidad de cómputo con que dispone una computadora cuántica.

Pero la rueda ha seguido girando, y el desarrollo de la informática cuántica ha permitido el desarrollo de nuevas técnicas criptográficas. Estas técnicas, conocidas como *técnicas de criptografía cuántica*, garantizan la seguridad de la transmisión de información basándose en los postulados de la física cuántica, evitando los problemas que padecen los sistemas de criptografía clásica.

Los esquemas propuestos para criptografía cuántica se basan en protocolos de *distribución de claves*. Un protocolo de distribución cuántica de claves consiste en un procedimiento que propone el intercambio de información de modo probabilísticamente seguro, a través de un canal público, con el objetivo de derivar una clave compartida segura para utilizar en un sistema clásico de encriptado de clave privada. Los detalles de los protocolos cuánticos de distribución de claves se presentan en la Sección 5

En la actualidad, la criptografía cuántica está en una etapa de desarrollo más avanzada que las computadoras cuánticas: ya existen varios prototipos funcionales de sistemas basados en criptografía cuántica, cuando todavía existen limitaciones significativas para la realización de una computadora cuántica capaz de realizar operaciones complejas.

Para tener una idea de la velocidad con la cual se está desarrollando la criptografía cuántica, pueden mencionarse los siguientes eventos en orden cronológico. En 1989, Bennett y Brassard llevaron a cabo uno de los primeros experimentos orientados a probar la viabilidad de la distribución cuántica de claves. En 1991 se construyó un prototipo que podía operar con una distancia máxima de 32 centímetros entre el emisor y el receptor. Desde ese momento a los 23 kilómetros de distancia que Zbinden comunicó por debajo del lago Génova [31] mediante estados de polarización de fotones pasaron sólo seis años. A mediados del 2003, la distancia máxima sobre la que era capaz de operar un dispositivo cuántico de distribución de claves ya era de 100 kilómetros. En la actualidad todavía subsisten algunos problemas tecnológicos para la implementación práctica de sistemas de comunicación basados en criptografía cuántica para uso masivo, pero se prevé que serán resueltos paulatinamente en el correr de los próximos años y de hecho existen empresas orientadas a comercializar dispositivos de criptografía cuántica.

La importancia de las técnicas criptográficas basadas en la mecánica cuántica podría resumirse en un breve párrafo: para romper los sistemas actuales de encriptación solamente se requiere la potencia de computación necesaria para resolver complejos problemas matemáticos, mientras que para romper un mensaje encriptado con criptografía cuántica requeriría una alteración de la formulación actual de las leyes naturales de la física.

3 Reseña histórica

Los argumentos pioneros sobre criptografía cuántica fueron propuestos por Wiesner en la década de 1970, pero sus ideas no fueron aceptadas por la comunidad científica y permanecieron no publicadas hasta 1983 [29]. Wiesner propuso un mecanismo de dinero cuántico basado en la autenticación de cheques y una idea de multiplexación de canales de transmisión, pero no presentó un protocolo de distribución de claves en el marco del enfoque de criptografía comentado.

La primer propuesta de un algoritmo cuántico para distribución de claves fue realizada por Bennett y Brassard en 1984 [2]. El protocolo, denominado BB84, se basa en la utilización de cuatro estados cuánticos para codificar valores de bit y utiliza mecanismos clásicos que permiten derivar una clave secreta compartida entre dos interlocutores. El protocolo BB84 garantiza que la información que pueda adquirir un posible espía esté acotada convenientemente de acuerdo a los resultados de una prueba de verificación realizada muestreando aleatoriamente parte de la información transmitida. El protocolo BB84 se presenta en detalle en la Sección 5.1 y una prueba de la seguridad del mecanismo de distribución se presenta en la Sección 6.

En 1991, Eckert presentó un protocolo de distribución cuántica de claves basado en la utilización de estados cuánticos enredados, trabajando con pares correlacionados de partículas para compartir la información que permite derivar una clave secreta compartida [13]. El protocolo se basa en la conocida versión de Bohm del *gedankenexperiment* Einstein–Podolski–Rosen (EPR) y utiliza las desigualdades de Bell para verificar la intervención de espías. Como consecuencia, la seguridad del protocolo depende exclusivamente de la completitud de las leyes físicas de la mecánica cuántica. Desde el punto de vista teórico, la propuesta constituye una extensión de la idea original de Bennet y Brassard, mientras que desde el punto de vista práctico provee una implementación que utiliza elementos y dispositivos característicos de la computación cuántica. Eckert conjeturó que su protocolo sería robusto aún frente a sofisticadas estrategias de ataque que involucraran el reemplazo de la fuente de pares EPR por una fuente falsa diseñada para imitar el comportamiento de la original. El protocolo de distribución cuántica de claves fue asociado con el nombre de su autor, pero más comúnmente se lo suele denominar como protocolo EPR. La sección 5.3 presenta en detalle la propuesta de Eckert.

En forma casi inmediata, Bennnett et al. [3] presentaron en 1992 un protocolo de distribución cuántica de claves para probar que ni las partículas correlacionadas en estados EPR ni los mecanismos de verificación basados en las desigualdades de Bell son parte esencial en el proceso de generación y certificación de claves secretas. El protocolo constituye una versión simplificada del propuesto por Eckert, donde los interlocutores no necesitan realizar mediciones en la base de Bell, sino que pueden utilizar aleatoriamente ejes

ortogonales para realizar las mediciones. Los autores presentaron una prueba de que esta versión del protocolo no se ve comprometida ante ataques que involucren el reemplazo de la fuente de pares EPR por una fuente falsa y probaron la equivalencia del esquema propuesto al esquema de distribución cuántica de clave del protocolo BB84 original.

El mismo año, Bennett presentó una variante simplificada del protocolo BB84 original que utiliza solamente un par de estados para la codificación de información, que fue denominado protocolo B92 [4]. Más allá de su simplicidad, la propuesta no reúne características de interés específicas que no se encontraran presentes en el protocolo BB84 original. Los detalles del protocolo B92 se presentan en la sección 5.2.

Numerosas variantes de los protocolos previamente comentados han sido presentadas para resolver problemas específicos, mejorar la seguridad de la comunicación o responder a eventuales estrategias de ataque por parte de espías. Los protocolos mencionados constituyen los más tradicionales dentro de la criptografía cuántica y sus descripciones detalladas se presentarán en la Sección 5.

4 Conceptos útiles de teoría cuántica de la información

Esta sección presenta una revisión de conceptos de teoría cuántica de la información que serán utilizados en la descripción de los protocolos cuánticos de distribución de claves y en la prueba de seguridad del protocolo BB84.

4.1 Teoría cuántica de la información

A continuación se resumen conceptos básicos de teoría cuántica de la información y se comparan con sus resultados análogos en la teoría de la información clásica.

4.1.1 Entropía cuántica

En teoría de la información clásica, la entropía viene dada por la fórmula de Shannon [26]

$$H(X) = -\sum_x p(x).\log(p(x))$$

donde $p(x)$ indica la probabilidad de existencia de un dato x en la serie X, mientras que en teoría de la información cuántica, se utiliza la denominada entropía de Von Neumann, que para un estado cuántico ρ queda definida por

$$S(\rho) = -\mathrm{tr}(\rho \log \rho)$$

Para la cantidad de información distinguible o accesible, en información clásica vale la igualdad $N = |X|$, mientras que en información cuántica se usa el resultado conocido como cota de Holevo.

4.1.2 Cota de Holevo

De modo general, puede indicarse que la información clásica codificable (o accesible) en un sistema cuántico está acotada por la entropía del estado cuántico, que puede interpretarse como el número de qubits necesarios para representar fielmente una fuente de información cuántica descrita por el estado.

La cota de Holevo presenta un resultado más preciso, que indica que el máximo de información clásica accesible cuando se intenta distinguir entre estados cuánticos ρ_x enviados con probabilidades de distribución p_x está determinada por

$$H(X:Y) \leq \chi = S(\sum_x p_x \rho_x)) - \sum_x p_x S(\rho_x)$$

Este resultado fue conjeturado por Gordon en 1964 [14] y su enunciado concreto y demostración fue presentado por Holevo en 1973 [17].

4.1.3 Teorema de no clonación

Un resultado muy importante para los mecanismos de distribución cuántica de claves es presentado por el teorema que indica la imposibilidad de copiar un estado cuántico. El teorema enuncia que ningún dispositivo cúantico puede tener como salida $|\psi_i\rangle\langle\psi_i|$, dado el estado $|\psi_i\rangle$ como entrada, para un $|\psi_i\rangle$ cualquiera. Este resultado fue presentado por Dieks [11] y Wootters y Zurek [30] en 1982, se relaciona directamente con el postulado de medida en mecánica cuántica, y si bien es muy útil en el ámbito de la criptografía cuántica, constituye una de las principales dificultades para la construcción física de un computador cuántico. En su forma más simple, el teorema indica que es imposible clonar un estado cuántico desconocido, ya que al intentar adquirir conocimiento mediante una operación de medida, se modifica el propio estado cuántico.

4.2 Códigos cuánticos

Un código cuántico corrector de errores es un subespacio de un espacio de Hilbert C^{2^n} que está "protegido"de errores en un número reducido de qubits, los cuales pueden medirse y corregirse *sin perturbar el estado codificado.*

Un código cuántico CSS (Calderbank-Shor-Steane) de n bits Q se deriva de dos códigos binarios de n bits C_1 y C_2, uno de ellos contenidos en el otro: $0 \subset C_2 \subset C_1 \subset F_2^n$, siendo F_2^n el espacio de vectores binarios de n bits.

Un conjunto de estados base para el subespacio de códigos CSS, denominados *codificaciones* o *palabras de código*, se obtiene a partir de vectores $v \in C_1$ del siguiente modo:

$$v \rightarrow \frac{1}{|C_2|^{1/2}} \sum_{w \in C_2} |v + w\rangle$$

Si $v_1 - v_2 \in C_2$, entonces las codificaciones correspondientes a v_1 y v_2 son idénticas y corresponden a cosets de C_2 en C_1. Este tipo de códigos protege a un espacio de Hilbert de dimensión $2^{dimC_1 - dimC_2}$.

Un código cuántico como el presentado anteriormente tiene un código dual equivalente Q^*, que se obtiene a partir de dos códigos binarios que cumplen $0 \subset {C_2}^{\perp} \subset C_1^{\perp} \subset F_2^n$,

Esta equivalencia puede demostrarse de modo sencillo, aplicando la transformación de Hadamard para codificar cada qubit. La transformación de Hadamard, que se presenta en la Figura 4.2 intercambia la base computacional (definida por $\{|0\rangle, |1\rangle\}$) con la base compuesta por los estados $\{|+\rangle$ y $|-\rangle\}$ definidos por:

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad\qquad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

Asimismo, la transformación de Hadamard intercambia los subespacios correspondientes a los códigos Q y Q^*, (aunque las palabras de código no son intercambiadas).

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Figura 1: Transformación de Hadamard

Los cuatro estados con enredo máximo:

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \qquad\qquad |\beta_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

$$|\beta_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \qquad\qquad |\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

forman una base ortogonal del espacio de estados cuánticos de dos bits denominada *base de Bell*. La base de Bell tiene un rol importante en los mecanismos de los códigos correctores de errores, porque permite definir los proyectores para realizar las medidas que detectan los cambios de valor de bit y cambios de fase en qubits.

4.3 Reconciliación de información y amplificación de privacidad

El proceso de *reconciliación de información* involucra operaciones y comunicaciones a través de un canal público de modo de eliminar posibles discrepancias entre la información que contienen dos interlocutores luego de una transmisión. Las diferencias pueden surgir esencialmente debido al uso de un mecanismo o canal imperfecto de transmisión o por manipulación expresa de un tercero que intenta espiar la comunicación. El objetivo del procedimiento de reconciliación de información consiste en acceder a un string único compartido, con información que permita derivar una clave privada.

En la práctica, la reconciliación de información se implementa como un mecanismo de corrección de errores que se realiza mediante comunicaciones sobre un canal público, que permite obtener el string único compartido divulgando la menor cantidad de información posible a un eventual espía.

Un mecanismo de *amplificación de privacidad* permite derivar una clave suficientemente segura (de acuerdo a criterios predefinidos) a partir de información común disponible luego de aplicado un proceso de reconciliación de información. Aplicando operaciones conjuntas sobre la información común, se trata de reducir el posible conocimiento de un espía hasta un nivel mínimo que garantice la seguridad de la clave derivada.

Un modo usual de llevar a cabo la amplificación de privacidad consiste en utilizar *funciones de hash universales* $\mathcal{G}$, que permiten mapear el conjunto de strings de n bits $\mathcal{A}$ con el conjunto de strings de m bits $\mathcal{B}$, siendo $m < n$. El mapeo se realiza de modo tal que para dos palabras $a_1, a_2 \in \mathcal{A}$, al elegir g aleatoriamente de modo uniforme en G, la probabilidad de que $g(a_1) = g(a_2)$ sea a lo sumo $1/|\mathcal{B}|$. Seleccionando públicamente una función $g \in \mathcal{G}$, los interlocutores pueden obtener a partir de un string W un nuevo string K que oficiará como clave secreta compartida. Si la incertidumbre de un espía sobre el string original W está acotada por un valor d, la teoría de la información clásica indica que la incertidumbre sobre la clave K será mayor que $m - 2^{m-d}$. Este resultado implica que m puede elegirse lo suficientemente pequeño para garantizar que el conocimiento de un espía sobre la clave final sea próximo a m, maximizando la incertidumbre y produciendo una clave confiable.

El mecanismo de reconciliación de información reduce el número de bits que Alicia y Bob pueden obtener, ya que hace necesario el envío de mensajes para garantizar la corrección de los errores, y Eva puede utilizar esta información para obtener conocimiento adicional sobre la clave. De todos modos, aún en este escenario existe un resultado de teoría de la información clásica que acota que el conocimiento adquirido por parte de un espía: suponiendo que los mensajes de reconciliación de información son de u bits, es posible incorporar un *parámetro de seguridad* s que garantice que luego de aplicado el procedimiento de amplificación de privacidad, el conocimiento adquirido por un espía sea menor que 2^{m-d+2s} con probabilidad mayor que $1 - 2^{-s}$.

En el ámbito clásico, la reconciliación de información se encuentra estrechamente ligada a los procedimientos de corrección de errores utilizados en teoría de códigos. Esta relación se mantiene en el ámbito cuántico, donde los protocolos de intercambio de claves utilizan códigos con capacidad de corregir errores para llevar a cabo la reconciliación de información y la amplificación de privacidad con el objetivo de derivar una clave secreta común.

Si Alicia envía un string de bits v a Bob sobre un canal de comunicación del cual se conoce que la tasa esperada de errores (incluyendo errores de transmisión y posibles errores ocasionados por espías) está acotada por un valor t, para asegurar la reconciliación de información puede utilizarse un código corrector de t bits. De este modo, el string que recibe Bob corresponde a $w = v + \varepsilon$ y el error ε puede ser depurado para obtener un string w' idéntico al originalmente enviado por Alicia (v). Además, si se utiliza un código CSS(C_1,C_2), es posible reducir la posible información adquirida por un espía calculando el coset de $w + C_2$ en C_1. De este modo se realiza la amplificación de privacidad, ya que las propiedades de los códigos CSS garantizan la obtención de un string de m bits suficientemente seguro, que puede ser utilizado como clave compartida.

4.4 Corrección de errores en códigos cuánticos CSS

Las matrices de Pauli, presentadas en la Figura 2, tienen una relación directa con los mecanismos de corrección de errores utilizados en los códigos cuánticos. Recordemos que la operación hermítica **X** asociada a la matriz de Pauli σ_x corresponde a un intercambio de valor de bit (correspondiente a un *bit flip error* en el contexto de códigos correctores de errores), mientras que la operación hermítica **Z** asociada a la matriz de Pauli σ_z corresponde a un cambio de fase (correspondiente a un *phase flip error* en el contexto de códigos correctores de errores).

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Figura 2: Matrices de Pauli

Cuando se trabaja sobre un código CSS, se nota $\sigma_{a(k)}$ a la aplicación de la matriz de Pauli σ_a sobre el k-ésimo bit del código, indicando a una de las tres transformaciones posibles, $a \in \{x, y, z\}$. De este modo, para un vector binario s se tendrá que

$$\sigma_a^{[s]} = \sigma_{a(1)}^{s_1} \otimes \sigma_{a(2)}^{s_2} \otimes \sigma_{a(3)}^{s_3} \otimes \cdots \otimes \sigma_{a(n)}^{s_n}$$

siendo σ_a^0 la matriz identidad y s_i el i-ésimo bit de s. Las matrices $\sigma_x^{[s]}$ y $\sigma_z^{[s]}$ tienen como valores propios a $+1$ y -1.

Un código clásico C detecta y corrige los errores midiendo el *síndrome* mediante el uso de una *matriz de verificación de paridad* P, que define una base del espacio dual del espacio vectorial $C^{\perp}$. Cuando el emisor envía un string codificado v que se transmite con errores, de modo que el receptor recibe $w = v + \varepsilon$, la k-ésima fila de la matriz de verificación de paridad determina el k-ésimo bit del síndrome para w, correspondiente a $r_k.w \pmod 2$. El síndrome completo se calcula mediante el producto $P.w$, y permite discriminar dos casos: si el síndrome es 0, entonces no ocurrieron errores durante la transmisión y el string recibido $w \in C$. Por el contrario, si el síndrome es no nulo, el valor más probable de ε puede calcularse a partir del valor del síndrome, coorigiéndose el error ocurrido.

En un código cuántico CSS deben corregirse tanto los errores de cambio de bit como los errores de cambio de fase. Esto puede hacerse considerando dos matrices de verificación de paridad, P_1 asociada al código C_1 y P_2 asociada al código C_2 y las transformaciones de Pauli presentadas anteriormente.

Para calcular el síndrome para los errores de cambio de bit se halla el valor propio de σ_z^r para cada fila $r \in P_1$, correspondiendo los valores propios -1 y 1 a los valores 1 y 0 del síndrome respectivamente. De modo similar, para calcular el síndrome para los errores de cambio de fase, debe hallarse el valor propio de σ_x^r para cada fila $r \in P_2$. Este procedimiento permite corregir tanto los errores de cambio de bit como los errores de cambio de fase. Un código capaz de corregir t de estos errores será capaz de corregir arbitrariamente errores en hasta t qubits a lo sumo.

Una importante propiedad de los códigos cuánticos CSS consise en que la etapa de corrección de errores de cambio de bits se encuentra *desacoplada* de la etapa de corrección de errores de cambio de fase. Esta propiedad es de suma utilidad para probar la seguridad de los protocolos de distribución cuántica de claves, ya que permite incorporar a los códigos CSS como mecanismos de reconciliación de información y amplificación de privacidad sin requerir de computadores cuánticos. Otros códigos estabilizadores cuánticos pueden incorporarse a protocolos de distribución de claves, pero al parecer todos necesitarían disponer de computadoras cuánticas para su implementación.

Si se requiere que el código CSS corrija *todos* los errores en al menos $t = \delta n$ qubits, pueden utilizarse los mejores códigos CSS existentes, que satisfacen la versión cuántica de la cota de Gilbert–Varshamov: a medida que el largo del bloque de qubits n crece, los códigos tienden asintóticamente a proteger hasta δn errores de bit y δn errores de fase.

En la práctica es más útil requerir solamente que errores aleatorios sean corregidos con probabilidad alta. En este caso existen códigos que permiten detectar y corregir hasta δn errores aleatorios de bit y δn errores aleatorios de fase.

4.5 Códigos cuánticos parametrizados

Existe una clase de códigos correctores de errores equivalentes a los códigos cuánticos CSS, parametrizados por dos vectores de n bits x y z.

Suponiendo que un código cuántico CSS Q queda determinado por los códigos C_1 y C_2, entonces $Q_{x,z}$ tiene una base compuesta por vectores indexados por los cosets de C_2 en C_1. Para un vector $v \in C_1$, la palabra de código correspondiente está dada por

$$v \to \frac{1}{\sqrt{|C_2|}} \sum_{w \in C_2} (-1)^{z.w} |x + v + w\rangle$$

Los códigos cuánticos correctores de errores están íntimamente relacionados con los mecanismos de *purificación del enredo cuántico*. Suponiendo que dos interlocutores distantes, Alicia y Bob, comparten N pares de qubits en un estado cercano al de máxima correlación un proceso de purificación del enredo cuántico permite derivar (suele utilizarse el término *destilar*) un número $k < N$ de pares de qubits de *alta fidelidad*. Un protocolo de purificación del enredo cuántico correspondiente a un código CSS Q se describe a continuación.

Asumiendo que los códigos C_1 y $C_2^{\perp}$ corrigen hasta t errores y que Q codifica n qubits en m qubits. Si dos interlocutores (Alicia y Bob) comparten n pares de qubits en un estado cercano a $|\beta_{00}\rangle^{\otimes n}$, pueden purificar el enredo cuántico midiendo separadamente los valores propios de $\sigma_z^{[r]}$ para cada fila $r \in P_1$ y $\sigma_x^{[r']}$ para cada fila $r' \in P_2$. Las medidas pueden realizarse simultáneamente porque $\sigma_z^{[r]}$ y $\sigma_x^{[r']}$ conmutan, al ser ortogonales los espacios $C_1^{\perp}$ y C_2.

Si Alicia y Bob comienzan con n pares EPR perfectos, al medir $\sigma_z^{[r]}$ para cada fila $r \in P_1$ y $\sigma_x^{[r']}$ para cada fila $r' \in P_2$, proyectan sus espacios sobre el subespacio de códigos $Q_{x,z}$, siendo x y z vectores binarios tales que $P_1.x$ y $P_2.z$ corresponden a los síndromes de errores de valores de bit y de cambio de fase respectivamente. Luego de la proyección, el estado resultante es $|\beta_{00}\rangle^{\otimes n}$ codificado de acuerdo a $Q_{x,z}$.

Un caso diferente se da cuando Alicia y Bob comienzan con n pares EPR en un estado imperfecto (cercano, pero no idéntico a $|\beta_{00}\rangle^{\otimes n}$) donde todos los pares EPR se encuentran en la base de Bell, salvo t o menos para los cuales existen errores de cambio de valor de bit y t o menos para los cuales existen errores de cambio de fase. Cuando Alicia y Bob comparan sus mediciones realizadas según $\sigma_z^{[r]}$ y $\sigma_x^{[r']}$ las filas r para las cuales las medidas no concuerdan indican a los bits en los cuales existieron errores de cambio de valor de bit o de cambio de fase respectivamente. A partir de estos síndromes, Alicia y Bob pueden calcular las posiciones de los errores, corregirlos y decodificar utilizando $Q_{x,z}$ para obtener m pares EPR perfectos.

5 Distribución cuántica de claves

Un protocolo de distribución cuántica de claves permite el intercambio de información de modo probabilísticamente seguro, utilizando un canal público. La información comunicada puede utilizarse para derivar una clave compartida segura para utilizar en un sistema clásico de encriptado de clave privada. Los protocolos cuánticos de distribución de claves requieren la posibilidad de comunicación de qubits con una tasa de error menor que una cota determinada, de modo que la seguridad de la clave resultante queda garantizada por propiedades de la teoría cuántica de la información.

La idea básica detrás de los protocolos cuánticos de distribución de claves consiste en la imposibilidad de que un espía pueda ganar información de los qubits transmitidos entre los interlocutores Alicia y Bob, sin modificar el estado del sistema. Por una parte, el teorema de no clonación garantiza que Eva no pueda clonar los qubits de Alicia, para analizarlos y adquirir información sobre la clave. Por otra parte, un importante resultado, relevante para garantizar la seguridad de los protocolos, indica que en un intento de diferenciar entre dos estados cuánticos *no ortogonales*, solo es posible obtener información *modificando el estado del sistema*.

Utilizando los postulados presentados anteriormente, los mecanismos de distribución cuántica de claves basan su funcionamiento en transmitir qubits en estados no ortogonales, de modo que Alicia y Bob sean capaces de establecer una cota superior para cualquier interferencia, debida a ruido en el canal de comunicación o a la posible acción de un espía. Un conjunto de qubits de *control* o de *verificación* se intercalan aleatoriamente entre los qubits de datos, para permitir detectar las intromisiones de un eventual espía. Analizando la tasa de errores en los qubits de control es posible obtener una cota superior que permita determinar la fiabilidad de los qubits de datos.

Luego de determinar si se dispone de un conjunto de datos comunes seguros, Alicia y Bob pueden llevar a cabo los mecanismos de reconciliación de información y de amplificación de privacidad para derivar una clave privada compartida. La cota que especifica la máxima tasa de error tolerable por el protocolo de distribución de claves queda determinada por la eficacia del mejor de los protocolos utilizados para la reconciliación de información y para la amplificación de privacidad.

Las subsecciones siguientes presentan en detalle los protocolos de distribución cuántica de claves más conocidos: el protocolo BB84, el protocolo B92 y el protocolo EPR.

5.1 El protocolo BB84 (Bennett y Brassard, 1984)

El primer protocolo de distribución cuántica de claves fue presentado en 1984 por Bennett y Brassard [2]. Utilizando los conceptos básicos mencionados con anterioridad, los interlocutores pueden derivar una clave probabilísticamente segura mediante la transferencia de qubits (mediante un canal cuántico) y el intercambio de mensajes (utilizando un canal clásico) que posibilitan llevar a cabo los mecanismos de reconciliación de información y de amplificación de privacidad. Los detalles del protocolo se presentan a continuación.

Para que sea posible derivar una clave probabilísticamente segura de m bits es necesario disponer de un número n ($n > m$) de bits fiables sobre los cuales aplicar mecanismos de reconciliación de información y de amplificación de privacidad. Por otra parte, se requerirán de al menos n bits de control para aplicar un mecanismo de verificación por muestreo aleatorio basado en comunicaciones a través del canal clásico, para detectar la posible intromisión de un espía.

En el protocolo BB84, Alicia comienza construyendo dos strings aleatorios (clásicos) a y b, cada uno de $(4+\delta)n$ bits. Cada string se codifica como un bloque de $(4+\delta)n$ qubits, que queda definido por el estado:

$$|\psi\rangle = \bigotimes_{k=1}^{(4+\delta)n} |\psi_{a_k b_k}\rangle$$

donde a_k es el k-ésimo bit de a y b_k es el k-ésimo bit de b, y cada qubit corresponde a uno de cuatro estados:

$$|\psi_{00}\rangle = |0\rangle \qquad |\psi_{01}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$|\psi_{10}\rangle = |1\rangle \qquad |\psi_{11}\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Este procedimiento permite codificar a en una de las bases $\{|0\rangle, |1\rangle\}$ o $\{|+\rangle, |-\rangle\}$, de acuerdo a los valores de los bits de b. Como los cuatro estados que componen la base $\{\psi_{i,j}\}$ no son mutualmente ortogonales, un espía no será capaz de realizar una medida para distinguirlos con certeza sin modificar el estado codificado. Alicia envía el estado codificado ψ a Bob utilizando su canal público de comunicación cuántico.

Bob recibe el resultado combinado del efecto del canal y la posible acción del espía y comunica a Alicia la recepción. Luego de la comunicación, tanto Alicia, como Bob, como un eventual espía Eva disponen de sus propios estados que quedan descritos por matrices de densidad diferentes. Dado que Alicia no ha revelado el string b que determina la codificación, Eva no tiene conocimiento sobre en qué base debería medir para espiar la comunicación sin alterar el estado recibido por Bob.

En este punto del proceso, Bob no es capaz de obtener información del mensaje recibido, ya que desconoce el string b que determinó la base en la cual Alicia realizó la codificación. Sin embargo, Bob puede proceder a medir cada qubit en una de las bases $\{|0\rangle, |1\rangle\}$ o $\{|+\rangle, |-\rangle\}$, de acuerdo a los bits de un string b', de largo $(4+\delta)n$, que él mismo genera aleatoriamente. Como resultado de la medición, Bob obtiene un string a'.

Luego de que Bob realiza su medición, Alicia anuncia su string b, haciendo públicos los estados utilizados para la codificación. Interactuando mediante un canal público, los interlocutores descartan todos los bits en a y a', excepto aquellos las bases utilizadas para codificar y medir coincidan (es decir, aquellos para los cuales los bits correspondientes de b y b' sean iguales). Para cada uno de los bits restantes se verifica que a_k'$=a_k$, ya que para estos bits Bob midió en la misma base en que Alicia los preparó. El proceso de reconciliación a aplicar requiere que como resultado de la fase de medición, Alicia y Bob mantengan al menos $2n$ bits iguales. Este hecho puede garantizarse con alta probabilidad seleccionando adecuadamente para el parámetro δ valores suficientemente grandes, ya que el mecanismo llevará a descartar en promedio la mitad de los bits enviados.

A continuación, Alicia y Bob deben realizar las verificaciones para determinar los niveles de ruido en el canal y la posibilidad de que un espía haya interferido la comunicación. Alicia selecciona aleatoriamente n bits de su conjunto de $2n$ bits y anuncia la selección a Bob, quien publica los valores de sus correspondientes n bits de chequeo. Comparando estos valores, es posible detectar la intervención de un espía. Si más de t bits toman valores diferentes, existen indicios de la intromisión de un espía o de existencia de ruido en el canal de comunicación, de modo que se aborta el proceso de distribución de la clave y el protocolo se reinicia desde el comienzo. El valor del parámetro t es elegido tal que si el proceso de verificación es exitoso, Alicia y Bob puedan aplicar mecanismos de reconciliación de información y de amplificación de privacidad para obtener una clave aceptablemente segura compuesta por m de los restantes n bits no utilizados en la verificación.

Un esquema del protocolo BB84 se presenta en la Figura 5.1, donde se han diferenciado las cuatro etapas del protocolo: la preparación de qubits (codificación) por parte de Alicia y su transmisión, la fase de medición de Bob, la etapa de verificación para detectar la posible intromisión de un espía y la fase final de derivación de la clave secreta.

Fase de preparación de Alicia.

1: Alicia crea aleatoriamente un string a de largo $(4+\delta)n$ bits.
2: Alicia crea un string aleatorio b de largo $(4+\delta)n$ bits.
3: PARA cada bit a_k en a, b_k en b // *Codificar a en qubits*
SI ($b_k = 0$)
4: Alicia codifica a_k en la base computacional $\{|0\rangle, |1\rangle\}$.
SINO // $b_k = 1$
5: Alicia codifica a_k en la base $\{|+\rangle, |-\rangle\}$.
6: Alicia envía los qubits resultantes a Bob.

Fase de medición de Bob.

7: Bob recibe los $(4+\delta)n$ qubits, y los mide aleatoriamente en la base $\{|0\rangle, |1\rangle\}$ o en la base $\{|+\rangle, |-\rangle\}$

Fase de verificación.

8: Alicia anuncia su string aleatorio b.
9: Alicia y Bob descartan aquellos bits para los que las bases utilizadas no coincidan. Con probabilidad alta existirán al menos $2n$ bits restantes (en caso contrario, se aborta el protocolo).
10: Alicia selecciona un subconjunto de n *bits de control* y los anuncia públicamente.
11: Alicia y Bob comparan los valores de los n bits de control.

Fase de derivación de la clave.

SI (más de un número t de bits de control difieren)
12: Abortar el protocolo. // *Posible acción de espía detectada.*
SINO
13: Aplicar reconciliación de información y amplificación de privacidad para derivar una clave secreta común.

Figura 3: Seudocódigo del protocolo BB84.

5.2 El protocolo B92 (Brassard, 1992)

El protocolo BB84 puede generalizarse para trabajar con otros estados y bases de codificación, manteniendo sus características. En particular, un protocolo simple que utiliza solamente dos estados para codificar en qubits fue propuesto por Brassard en 1992 y es conocido como protocolo B92. A continuación se describe el funcionamiento del protocolo, que sigue las líneas generales del esquema del protocolo BB84, salvo en los procesos de codificación y verificación. Por simplicidad, es suficiente con analizar lo que ocurre al codificar y transmitir un único bit, generalizándose el procedimiento para trabajar con bloques de bits.

En el protocolo B92, Alicia considera un bit aleatorio a y de acuerdo a su valor lo codifica en uno de los dos estados $|\psi\rangle$ definidos por:

$$|\psi\rangle = \begin{cases} |0\rangle & si \;\; a = 0 \\ \frac{1}{\sqrt{2}}.(|0\rangle + |1\rangle) & si \;\; a = 1 \end{cases}$$

Luego, Alicia envía a a Bob el qubit resultado de la codificación. Dependiendo del valor de un bit aleatorio a' que él mismo genera, Bob mide el qubit recibido en la base computacional $\{|0\rangle, |1\rangle\}$ (si $a' = 0$) o en la base $\{|+\rangle, |-\rangle\}$ (si $a' = 1$).

Bob obtiene un resultado b de su medición y lo comunica a Alicia, manteniendo oculto su bit aleatorio a'. Posteriormente, Alicia y Bob se comunican para conservar solamente aquellos pares a, a' para los cuales b=1. Cuando a=a' ocurre que b=0, y solamente cuando a'=1-a Bob obtiene b=1, y estos dos eventos ocurren con probabilidad 1/2. En el caso simplificado de un bit, la clave final es a para Alicia y $1 - a'$ para Bob. Cuando se trabaja con bloques de bits, el mismo procedimiento se aplica para derivar la clave compartida concatenando los valores de bit secretos.

Basado en la imposibilidad de obtener información por parte de un espía sin modificar la correlación entre los bits que Alicia y Bob finalmente conservan, este protocolo (al igual que el protocolo BB84) permite crear una clave compartida y especificar una cota superior para las perturbaciones debidas a ruido en el canal y acciones de eventuales espías durante la comunicación. Luego, los interlocutores pueden aplicar los mecanismos de reconciliación de la información y de amplificación de la privacidad para extraer bits secretos de sus strings aleatorios correlacionados.

5.3 El protocolo EPR (Eckert, 1991)

En los protocolos BB84 y B92, las claves parecen haber sido generadas unilateralmente por Alicia, ya que es ella quien lleva la iniciativa al momento de la creación de los bits y la codificación de los qubits involucrados. Sin embargo, la clave puede obtenerse de un proceso aleatorio que involucra propiedades del enredo cuántico, tal como propone el protocolo presentado por Eckert [13], también conocido como protocolo EPR. Supongamos que Alicia y Bob comparten un conjunto de *pares EPR*, es decir n pares de qubits en el estado de máximo enredo

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Alicia y Bob seleccionan un subconjunto aleatorio de pares EPR y comprueban si violan la desigualdad de Bell o realizan algún otro chequeo de fidelidad que permita confirmar que los estados cuánticos seleccionados se encuentran puramente enredados, definiendo una cota inferior para la fidelidad de los restantes pares EPR (y por tanto para el ruido o la interacción de un espía). Cuando Alicia y Bob miden los pares EPR no utilizados en la verificación utilizando bases aleatorias determinadas conjuntamente, obtienen strings correlacionados a partir de los cuales pueden obtener una clave secreta del modo presentado para el protocolo BB84. Tomando como fundamento la cota de Holevo, la fidelidad de los pares EPR puede utilizarse para establecer una cota superior a la información accesible por parte un espía. En el protocolo EPR la clave es generada aleatoriamente, mediante un proceso simétrico, ya que tanto Alicia como Bob realizan las mismas operaciones sobre sus qubits.

Este mismo procedimiento puede aplicarse para el protocolo BB84, que es un caso particular del protocolo EPR. Supongamos que Alicia genera un bit aleatorio b y de acuerdo a su valor mide la mitad de sus pares EPR en una de las dos bases posibles $\{|0\rangle, |1\rangle\}$ o $\{|+\rangle, |-\rangle\}$ obteniendo a. Bob mide en su base (aleatoriamente elegida) b' y obtiene a'. Comunicando b y b' a través del canal público, Alicia y Bob pueden conservar como clave aquellos pares a, a' para los cuales se cumpla que $b = b$'. Siguiendo este mecanismo, la clave se encuentra *indeterminada* hasta que los interlocutores realizan las medidas sobre sus pares EPR.

El funcionamiento descrito justifica que los protocolos de criptografía cuántica sean usualmente catalogados como protocolos de *generación* de claves secretas en lugar de protocolos de *transmisión* de claves, ya que en general los interlocutores no son capaces de conocer a priori la clave que proporcionará finalmente el protocolo.

6 Seguridad del mecanismo cuántico de distribución de claves: desde EPR hasta BB84

Un resultado importante relaciona la seguridad de la clave obtenida luego de aplicadas las fases de reconciliación de la información y amplificación de privacidad en un protocolo de distribución cuántica de claves con la tasa máxima de transmisión obtenible para códigos CSS sobre canales con ruido. La idea genérica se presenta a continuación.

Los protocolos BB84, B92 y EPR son "seguros"si Eva solamente puede atacar la transmisión de a un qubit a la vez. El problema surge cuando se realiza un ataque colectivo, en el cual Eva puede manipular y posiblemente almacenar largos bloques de qubits transmitidos. En este caso, un mecanismo de seguridad puede derivarse bajo la suposición que Eva solamente es capaz de introducir a lo sumo t errores en qubits por bloque transmitido. En este caso, Alicia puede codificar sus qubits en un código corrector de t qubits, de modo que las modificaciones introducidas por Eva puedan ser removidas por Bob aplicando la decodificación correspondiente. Para establecer una cota superior para el valor de t, debe utilizarse un mecanismo de muestreo del canal apropiado para tal fin. Desafortunadamente, un protocolo con estas características exigiría una computadora cuántica tolerante a fallas, capaz de codificar y decodificar qubits de modo robusto. Para hacer práctico el esquema, es necesario utilizar una estrategia de codificado cuántico de modo que los procesos de codificación, decodificación y medición puedan ser llevado a cabo sin requerir cómputo o almacenamiento de información cuántica. En este punto los códigos CSS pueden ser utilizados, conjuntamente con algunas simplificaciones, para obtener el código BB84 garantizando la propiedad de *seguridad*.

Esta sección comienza ofreciendo una breve reseña histórica de las pruebas de seguridad propuestas por los investigadores. Luego se presenta un criterio de seguridad para un protocolo de distribución cuántica de claves genérico. A continuación se enuncia una condición para garantizar la seguridad de un protocolo de distribución basado en el uso de pares EPR y se presenta cómo es posible acotar el conocimiento adquirido por parte de un espía mediante muestreos aleatorios. Por último, la parte principal de la sección esquematiza el proceso de derivar el código BB84 a partir de un código seguro basado en el uso de pares EPR. Este proceso aplica propuestas para resolver los inconvenientes previamente mencionados para un protocolo EPR genérico, evitando el cómputo y el almacenamiento de información cuántica. La prueba sigue los lineamientos generales propuestos por Shor y Preskill en su trabajo de 2000 [27].

6.1 Pruebas de seguridad: reseña histórica

Desde la primer propuesta de un algoritmo cuántico para distribución de claves realizada por Bennett y Brassard en 1984, los investigadores concentraron sus esfuerzos en presentar pruebas formales de la correctitud del mecanismo de distribución y de su seguridad.

En general, las pruebas de seguridad de los protocolos cuánticos de distribución de claves ante los tipos de ataques genéricos permitidos por la mecánica cuántica han demostrado ser muy complejas.

La primer prueba de seguridad incondicional para el protocolo BB84 fue presentada por Mayers [21]. La prueba de Mayers considera una variante práctica del protocolo BB84 en la que se considera la transmisión de información sobre un canal cuántico imperfecto, donde los fotones utilizados pueden perderse como consecuencia del ruido en el canal. Asimismo, considera que la fuente emisora de fotones es perfecta, y no impone restricciones sobre la capacidad del detector utilizado para la recepción de fotones, salvo que la detección sea independiente de la base utilizada para la medición del sistema. Para tratar con el problema del canal imperfecto, que impone más limitaciones para establecer una cota inferior en los errores, Mayer utiliza conceptos basados en el *principio de complementariedad*. Este principio indica que si un operador de medida es capaz de proporcionar mucha información sobre un conjunto de qubits cuando se utilizan bases conjugadas (definidas a partir de bases originales determinadas), el mismo operador proveerá muy poca información cuando se utilicen las bases originales. El resultado de Mayers es importante, y aún hoy en día constituye uno de los resultados más fuertes sobre la seguridad de los mecanismos de distribución cuántica de claves, pero su prueba es compleja, estrictamente formal y relativamente extensa.

Lo y Chau [18] siguieron un enfoque diferente, basado en trabajos previos de Deustch et al. [10] y Bennett et al. [1], trabajando sobre el concepto de purificación del enredo cuántico. Recordemos que, suponiendo que dos interlocutores distantes, Alicia y Bob, comparten n pares EPR *imperfectos* (en el sentido que algunos pares pueden no estar exactamente correlacionados), un proceso de purificación del enredo cuántico permite derivar un número $k < n$ de pares EPR de *alta fidelidad*, aplicando operaciones locales y comunicaciones de información clásica. Ha sido probado que los protocolos basados en la purificación del enredo cuántico que involucran comunicaciones clásicas de una vía entre los interlocutores son equivalentes a los protocolos cuánticos de codificación para corrección de errores, permitiendo la comunicación (y el almacenamiento) de información cuántica. Por otra parte, los protocolos basados en la purificación del enredo cuántico que involucran comunicaciones clásicas de doble vía entre los interlocutores son capaces de tolerar mayores niveles de interferencia y ruido que aquellos que involucran solamente comunicaciones de una vía, permitiendo la comunicación eficiente de información cuántica, pero no su almacenamiento.

Una clave (para nada trivial) en la prueba de Lo y Chau consiste en un *argumento de reducción* de un modelo cuántico a uno clásico, que permite asignar, de modo consistente, probabilidades *clásicas* a los $2n$ estados de la base de Bell utilizados en el procedimiento de verificación. Como se comprueba en la famosa *paradoja EPR* (Einstein–Podolski–Rosen), generalmente es inconsistente (e ingenuo) asignar probabilidades clásicas a estados cuánticos. Pero en el argumento de Lo y Chau, la estrategia se justifica por el hecho conocido como "conmutación de los observables".

La parte compleja en la prueba de Lo y Chau consiste en la construcción de los observables relevantes para llevar a cabo la purificación del enredo cuántico, de modo que conmuten entre si. La prueba es conceptualmente más simple que la propuesta por Mayers, pero tiene la complejidad práctica de que la implementación del protocolo examinado requiere de computadores cuánticos y mecanismos de almacenamiento de estados cuánticos.

Biham et al. [7, 8] presentaron una prueba de seguridad de los mecanismos cuánticos de distribución de claves ante las estrategias de ataques más genéricas que pueden aplicarse por parte de un espía que tiene acceso al canal de comunicación, capacidad tecnológica ilimitada (poder de cómputo, dispositivos de almacenamiento cuántico, etc.) y todas las capacidades no limitadas por las leyes (clásicas y cuánticas) de la física.

Para probar la seguridad de la distribución cuántica de claves aún ante un espía ilimitadamente poderoso, los autores desarrollan varios resultados técnicos obteniendo resultados sobre información y entropía que resaltan el poder de la teoría cuántica de la información. Trabajando sobre el protocolo BB84, los autores argumentan y prueban que la potencia del mecanismo de distribución cuántica de claves queda determinada por la aleatoriedad de elección de las bases utilizadas para las mediciones y la capacidad de selección aleatoria de los bits de verificación. Los resultados obtenidos por los autores pueden considerarse equivalentes a los de Mayers, en el sentido que prueban la seguridad de un protocolo realista, de implementación práctica factible, ante estrategias genéricas de un espía no limitado, presentando cotas explícitas para la cantidad de información obtenida por el espía. Bajo las hipótesis estándar del protocolo BB84, el resultado presentado por Biham et al. prueba la seguridad incondicional del protocolo contra cualquier tipo de ataque permitido por las leyes físicas. Complementariamente, los autores prueban la seguridad asintótica del protocolo aún en escenarios con canales de comunicación imperfectos donde la tasa de error de transmisión es inferior a un 7.56%. Resultados adicionales indican que la cota de error de transmisión puede ser incrementada significativamente introduciendo pequeñas modificaciones al protocolo, de modo de obtener resultados de seguridad de aplicación práctica.

En el año 2000, Shor y Preskill presentaron una prueba simple de la seguridad del protocolo BB84 utilizando el enfoque de purificación del enredo cuántico. La prueba es muy importante porque elimina el requerimiento de computadores cuánticos para llevar a cabo la distribución de claves. La clave del argumento de Shor y Preskill consiste en que para garantizar la seguridad del protocolo es suficiente con mostrar que los interlocutores *podrían haber realizado* un mecanismo de purificación del enredo cuántico, si dispusieran de computadores cuánticos, pero que no es necesario realizarlo efectivamente.

La demostración de Shor y Preskill hace uso de los códigos CSS, una clase específica de códigos cuánticos correctores de errores que tienen la característica de que el procedimiento de corrección puede *desacoplarse* en una etapa de corrección de errores de bit y otra etapa de corrección de errores de fase. Como los errores de fase no afectan el valor de la clave final, no es necesario que los interlocutores anuncien el síndrome de errores de fase. Por este motivo, Alicia y Bob pueden llevar a cabo el mecanismo cuántico de distribución de claves, sin disponer de computadores cuánticos. La prueba de Shor y Preskill es importante por su sencillez, y porque muestra que el mecanismo de purificación del enredo cuántico puede utilizarse efectivamente en un protocolo de implementación práctica como lo es el BB84. La prueba garantiza la efectividad del protocolo en escenarios donde los errores de bits pueden alcanzar hasta un 11%. Un exposición detallada de la prueba de Shor y Preskill se presenta en las Secciones 6.3.1–6.3.3.

Recientemente, Gottesman y Lo [16] generalizaron el resultado de Shor y Preskill para probar la seguridad del protocolo BB84 hasta una tasa de errores del 19%, requiriendo comunicaciones bidireccionales de información clásica entre los interlocutores para llevar a cabo la purificación del enredo cuántico. Adicionalmente, probaron que un esquema que utilice seis estados cuánticos para la codificación de la información puede hacerse incondicionalmente seguro en escenarios que tengan hasta aproximadamente una tasa de error de bits del 27%. Dado que la versión estándar del protocolo BB84 ha sido probada como insegura cuando la tasa de errores de bits es del orden del 25% (siendo posible atacarla mediante una estrategia basada de intercepción y reenvío), los autores probaron que el protocolo de seis estados tolera una tasa de errores mayores que el protocolo BB84.

El mecanismo de purificación del enredo cuántico se ha manifestado como muy útil en la investigación de la seguridad de los protocolos cuánticos de distribución de claves. Su uso ha permitido probar la existencia de protocolos incondicionalmente seguros en un espacio de escenarios más amplio que los previamente conocidos.

6.2 Criterio de seguridad para un protocolo de distribución cuántica de claves

Un criterio para la seguridad del mecanismo cuántico de distribución de claves debe explicitar una cota para el conocimiento obtenido por parte de un espía de la clave derivada por los interlocutores. El criterio que se ofrece en la Figura 4 es presentado por Nielsen y Chuang [24] como *aceptable*.

Un protocolo de distribución cuántica de claves se define como *seguro* si genera strings aleatorios y para cualquier elección de dos *parámetros de seguridad* $l, s > 0$ elegidos por Alicia y Bob, y para cualquier estrategia de ataque del espía Eva, el protocolo aborta o finaliza exitosamente con una probabilidad de al menos 1-$O(2^{-s})$, y garantiza que la información conocida por Eva sobre la clave final es menor que 2^{-l}.

Figura 4: Criterio para la seguridad de un protocolo de distribución cuántica de claves.

6.2.1 Requerimientos de seguridad para un protocolo de distribución cuántica de claves basado en pares EPR

Consideremos que Alicia y Bob disponen de n pares de qubits enredados, cada uno en el estado

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

definiendo un estado conjunto $|\beta_{00}\rangle^{\otimes n}$.

Cuando Alicia transmite la mitad de cada par a Bob, el estado resultante puede resultar impuro debido a ruido presente en el canal de comunicación o a la interferencia de un espía; este estado resultante puede describirse por medio de una matriz de densidad ρ. Luego, Alicia y Bob llevan a cabo sus mediciones locales descritas previamente, para obtener la clave compartida. La fidelidad de ρ con respecto al estado $|\beta_{00}\rangle^{\otimes n}$ constituye una cota superior para la información de la clave adquirida por parte del espía, de acuerdo al resultado original de Lo y Chau [18] que se presenta en la Figura 6.2.1, donde F indica la fidelidad de los pares de qubits y S denota a la entropía, que representa al conocimiento adquirido por el espía.

Si $F(\rho, |\beta_{00}\rangle^{\otimes n})^2 > 1 - 2^{-s}$, entonces $S(\rho) < (2n + s + 1/\ln 2)2^{-s} + O(2^{-2s})$.

Figura 5: Alta fidelidad implica baja entropía

6.2.2 Muestreo aleatorio para limitar la información adquirida por un espía

Para asegurar la fidelidad en los pares EPR de Alicia y Bob, puede utilizarse el muestreo aleatorio introducido al presentar el protocolo BB84. Los argumentos basados en probabilidades clásicas no son necesariamente aplicables cuando se trabaja con resultados de mediciones cuánticas (tal como lo refleja la desigualdad de Bell). Sin embargo, los experimentos cuánticos admiten interpretaciones clásicas cuando consideran mediciones de observables referidas solamente en una base, y precisamente éste es el caso aplicado para acotar la fidelidad de los pares EPR utilizados por Alicia y Bob.

La transmisión de un qubit a través de un canal cuántico ruidoso puede describirse como una operación que modifica el qubit mediante una de cuatro operaciones: la identidad ($\mathbf{I}$), un cambio de bit ($\mathbf{X}$), un cambio de fase ($\mathbf{Z}$) o un cambio de bit y fase combinados ($\mathbf{Y}$). Las bases de Bell permiten definir los proyectores para realizar las medidas que detectan los cambios de valor de bit y cambios de fase.

Aquí es donde se aplica la idea clave presentada por Lo y Chau: la construcción de proyectores que conmuten con las bases de Bell permite garantizar que sus salidas respetan los argumentos de probabilidad clásicos. Los proyectores en cuestión corresponden a $\Pi_{bf} = |\beta_{01}\rangle\langle\beta_{01}| + |\beta_{11}\rangle\langle\beta_{11}|$ e $I - \Pi_{bf}$ para detectar los cambios de valor de bit y a $\Pi_{pf} = |\beta_{10}\rangle\langle|\beta_{10}| + |\beta_{11}\rangle\langle\beta_{11}|$ e $I - \Pi_{pf}$ para detectar los cambios de fase

De este modo, muestreando aleatoriamente un subconjunto de los $2n$ pares EPR transmitidos, Alicia y Bob pueden acotar la fidelidad de los restantes pares. Alicia envía $2n$ mitades de pares EPR a Bob, y luego ambos proceden a muestrear aleatoriamente n de ellos, utilizándolos como qubits de verificación, midiendo en forma conjunta utilizando aleatoriamente Π_{bf} o Π_{pf}. Un argumento de probabilidades clásicas indica que si se detectan δn errores de cambio de bit o de fase, entonces existirá una certeza exponencial de que los restantes n pares EPR tengan el mismo número de errores si se los mide en la base de Bell. Los estados de Bell son no locales, y por tanto las mediciones en la base de Bell involucran costosas operaciones no locales. Sin embargo, estas complejas mediciones no son requeridas en el esquema propuesto, ya que $\Pi_{bf} = (\mathbf{I}\otimes\mathbf{I} - \mathbf{Z}\otimes\mathbf{Z})/2$ y $\Pi_{pf} = (\mathbf{I}\otimes\mathbf{I} - \mathbf{X}\otimes\mathbf{X})/2$, y tanto Alicia como Bob pueden realizar las verificaciones utilizando operadores de Pauli locales, midiendo ambos con los proyectores asociados a $\mathbf{Z}$ o a $\mathbf{X}$.

6.3 Prueba de seguridad de BB84

A continuación se presenta la prueba de seguridad del protocolo BB84, obtenida a partir de modificaciones realizadas a un protocolo EPR seguro por construcción.

6.3.1 El protocolo de Lo–Chau

El protocolo EPR basa su funcionamiento en el hecho que Alicia y Bob pueden obtener pares correlacionados ρ con fidelidad conocida respecto al estado ideal $|\beta_{00}\rangle^{\otimes n}$ muestreando aleatoriamente en la base de Bell. Para que ρ sea útil para la generación de una clave secreta, debe reducirse la información que sobre el estado final pueda adquirir un espía. Este objetivo puede lograrse mediante un mecanismo clásico de amplificación de privacidad, pero también puede realizarse mediante un mecanismo cuántico. Alicia y Bob pueden desenredar ρ para obtener ρ' muy cercano a $|\beta_{00}\rangle^{\otimes m}$ para algún $m < n$, y luego medir sobre el estado final.

El protocolo de Lo-Chau, cuyo seudocódigo se presenta en la Figura 6, es una variante del protocolo EPR que propone aplicar un mecanismo de purificación del enredo cuántico utilizando una corrección de errores cuántica. Dado que ρ tiene una probabilidad exponencialmente alta a tener menos de δn errores, es posible eliminar por completo los errores cometidos durante la transmisión utilizando un código capaz de corregir δn errores para codificar los qubits. Si se utiliza un código estabilizador $[n, m]$ las etapas de codificado, de medición y de corrección de errores pueden realizarse mediante los operadores de Pauli definidos por las columnas de la matriz de verificación del código. Alicia y Bob miden los síndromes y corrigen los errores en sus respectivas mitades de ρ, obteniendo un estado de m qubits con errores corregidos cuya fidelidad relativa respecto al estado $|\beta_{00}\rangle^{\otimes m}$ es del orden de 1 menos la probabilidad de que hayan ocurrido más de δn errores. Por construcción, las mediciones de los síndromes conmutan con la base de Bell, ya que las operaciones realizadas por Alicia y Bob son idénticas.

Fase de preparación de Alicia.

1: Alicia crea $2n$ pares EPR en el estado $|\beta_{00}\rangle^{\otimes n}$, y selecciona aleatoriamente n para ser utilizados como pares de control.
2: Alicia crea aleatoriamente un string b de largo $2n$ bits.
3: PARA cada par EPR generado, b_k en b
SI ($b_k = 1$)
4: Alicia aplica Hadamard en el segundo qubit del par EPR.
5: Alicia envía el segundo qubit de cada par a Bob.

Fase de recepción de Bob.

6: Bob recibe los $2n$ qubits, y anuncia la recepción.

Fase de verificación.

7: Alicia anuncia su string aleatorio b.
8: PARA cada par EPR recibido, b en B
9: SI ($b = 1$)
Bob aplica Hadamard en el segundo qubit del par EPR.
10: Alicia y Bob miden sus n qubits de control en la base $\{|0\rangle, |1\rangle\}$.

Fase de Derivación de la clave.

SI (más de t mediciones son diferentes)
11: Abortar el protocolo // *Posible acción de espía detectada.*
SINO
12: Alicia y Bob miden los n qubits restantes, de acuerdo a una matriz de verificación correspondiente a un código cuántico corrector de errores $[m, n]$, corrigiendo hasta t errores.
13: Alicia y Bob comparten los resultados, se calculan los síndromes de los errores, y se corrige su estado, obteniendo m pares EPR casi perfectos.
14: Alicia y Bob miden sus m pares EPR en la base computacional $|0\rangle$, $|1\rangle$, obteniendo una clave secreta común.

Figura 6: Seudocódigo del protocolo de Lo–Chau.

El protocolo de Lo–Chau incorpora la aplicación de transformaciones de Hadamard aleatorias por parte de Alicia (antes de enviar los qubits de los pares EPR) y de Bob (luego que Alicia hace público el string de control b), con el objetivo de crear simetría en la estrategia del espía entre la detección de información codificada en las bases $\{|0\rangle, |1\rangle\}$ y $\{|+\rangle, |-\rangle\}$ (generando errores $\mathbf{Z}$ y $\mathbf{X}$); y permite la selección aleatoria de medidas de detección de errores Π_{bf} o Π_{pf} en los qubits de control. Por último, el procedimiento de medición asociado a la matriz de un código de corrección tiene como objetivo garantizar que se cumple el criterio de seguridad sobre la clave derivada.

La validez del protocolo de Lo–Chau es demostrada por sus autores a partir de los criterios de seguridad para un protocolo EPR genérico [18]. En su trabajo de 2000, Shor y Preskill muestran que el protocolo de Lo–Chau garantiza una probabilidad exponencialmente baja de que los interlocutores acuerden una clave secreta común para la cual el espía pueda disponer más de una cantidad exponencialmente pequeña de información [27].

El argumento de Shor y Preskill se basa en calcular la probabilidad de que la fase de verificación produzca un resultado correcto pero el mecanismo de purificación del enredo falle. Para ello se consideran las medidas que proyectan cada uno de los pares EPR sobre la base de Bell.

Considerando en primer lugar los qubits de verificación para los que $b = 1$, Alicia y Bob realizan sus mediciones en la base $\{|+\rangle, |-\rangle\}$, en lugar de medir sobre la base computacional. Las relaciones existentes entre los estados de la base de Bell y las bases utilizadas en el protocolo de Lo-Chau:

$$\Pi_{bf} = |\beta_{01}\rangle\langle\beta_{01}| + |\beta_{11}\rangle\langle\beta_{11}| = |01\rangle\langle 01| + |10\rangle\langle 10|$$
$$\Pi_{pf} = |\beta_{10}\rangle\langle\beta_{10}| + |\beta_{11}\rangle\langle\beta_{11}| = |+-\rangle\langle +-| + |-+\rangle\langle -+|$$

muestran que las tasas de error de valores de bit y de cambios de fase que Alicia y Bob estiman al realizar sus medidas sobre los bits de verificación (utilizando los operadores Π_{bf} y Π_{pf}) son las mismas que habrían estimado si aplicaran las medidas utilizando las bases de Bell.

Considerando los qubits de código efectivos (aquellos que no son de verificación), es posible probar que el mecanismo de purificación del enredo cuántico aplicado por el protocolo de Lo–Chau produce un estado cercano al estado ideal codificado $|\beta_{00}\rangle^{\otimes m}$. El mecanismo de purificación funciona perfectamente al ser aplicado sobre el espacio de estados cubierto por pares de Bell que difieren del estado ideal $|\beta_{00}\rangle^{\otimes m}$ en menos de t errores de bits y en menos de t errores de fase. Denominando Π a la proyección sobre este espacio, que corresponde a la composición de Π_{bf} con Π_{pf}, es posible probar el siguiente resultado: si el mecanismo de purificación es aplicado a un operador densidad inicial ρ de n pares, el operador densidad resultado ρ' aproxima al estado $|\beta_{00}\rangle^{\otimes m}$ con una fidelidad F dada por

$$F = \langle (|\beta_{00}\rangle^{\otimes m}) \mid \rho' \mid (|\beta_{00}\rangle^{\otimes m}) \rangle \geq \mathrm{tr}(\Pi\rho)$$

Este resultado implica que la fidelidad es al menos tan grande como la probabilidad de que t o menos errores de bit y t o menos errores de fase puedan ser detectados si se realizan las mediciones en la base de Bell sobre n pares EPR.

Cuando el espía accede a los qubits, no dispone de información suficiente para determinar cuáles corresponden a qubits de control y cuáles son de código efectivo, de manera que no puede tratarlos de modo diferenciado. Los qubits de verificación que miden Alicia y Bob se comportan como si se realizara un muestreo probabilístico clásico de los qubits. De esta manera, es posible utilizar las tasas de error medidas como una estimación probabilística clásica: la probabilidad de obtener más de δn errores de bit o de fase en los bits de código y menos de $(\delta - \varepsilon)n$ errores en los bits de verificación es asintóticamente menor que $\exp[-1/4\varepsilon^2 n/(\delta - \delta^2)]$. Se concluye entonces que Alicia y Bob tienen una probabilidad mayor que un valor exponencialmente pequeño de que, si pasan el test de verificación, dispondrán de pares con una fidelidad exponencialmente cercana a 1 respecto al estado $|\beta_{00}\rangle^{\otimes m}$.

De acuerdo a los argumentos presentados, el protocolo de Lo–Chau resulta seguro, como consecuencia de su derivación de un protocolo EPR seguro genérico. La seguridad del protocolo de Lo–Chau está basada en el uso de computadores cuánticos que se asumen "perfectos" (que permiten realizar de un modo tolerante a fallos los mecanismos de reconciliación de información y amplificación de privacidad), la utilización de mecanismos de corrección de errores y el muestreo aleatorio de pares EPR.

6.3.2 Un protocolo basado en los códigos cuánticos CSS

El protocolo de Lo–Chau está basado en el uso de pares EPR y utiliza un mecanismo cuántico de corrección de errores para desenredar los estados. Pero la implementación física del protocolo no es sencilla en la situación tecnológica actual, porque el enredo es un recurso frágil y el protocolo cuántico de corrección de errores requiere disponer de un computador cuántico robusto. Para evitar estos complejos requerimientos, el protocolo puede simplificarse sistemáticamente en una serie de pasos que (probabilísticamente) no comprometen la seguridad del esquema de distribución de claves.

Las mediciones que Alicia realiza en su mitad de los pares EPR en la etapa de verificación del protocolo de Lo–Chau (paso **10**) tienen el efecto de colapsar los pares EPR en n qubits, de modo que en lugar de enviar los estados enredados, Alicia puede enviar solamente el resultado de la medida. Asimismo, las mediciones realizadas por Alicia en la etapa de derivación de la clave utilizando el código cuántico corrector de errores (pasos **12** y **13**) pueden realizarse al principio del esquema ya que solamente afectan a los pares EPR involucrados, sin modificar ningún otro estado. Considerando estos dos argumentos, es posible concluir que la distribución de los pares EPR no es necesaria.

La secuencia de pasos a aplicar por Alicia y Bob para obtener esta simplificación resulta:

Alicia

3: PARA cada par EPR de control
4: Alicia codifica n qubits como $|0\rangle$ o $|1\rangle$.
5: Alicia escoge aleatoriamente n posiciones para colocar los bits de control. En las restantes n posiciones coloca la mitad de cada par EPR.

Bob

13: Bob mide los n qubits de control en la base computacional $|0\rangle$, $|1\rangle$ y públicamente comparte el resultado con Alicia.

Las mediciones de los qubits de verificación equivalen a la elección aleatoria de uno de los estados $|0\rangle$ o $|1\rangle$ para codificar los qubits. Por otra parte, las mediciones que realiza Alicia en los pasos **12** y **13** hacen colapsar a los pares EPR en qubits aleatorios codificados en un código cuántico aleatorio. Una elección más conveniente es utilizar un código CSS de C_1 sobre C_2 ($\mathrm{CSS}(C_1, C_2)$), que codifica m qubits en n qubits y permite corregir hasta t errores. Para este código, P_1 y ${P_2}^{\perp}$ son las matrices de chequeo de paridad correspondientes a los códigos clásicos C_1 y $C_2^{\perp}$, en la cual cada uno de los estados de codificación es

$$\frac{1}{|C_2|^{1/2}} \sum_{w \in C_2} |v_k + w\rangle$$

donde v_k denota a un vector representante de uno de los 2^m cosets de C_2 en C_1 (el vector se encuentra determinado o "indexado"de acuerdo a un string clave k). Recordemos que existe una familia de códigos $CSS_{z,x}(C_1, C_2)$ equivalentes al elegido, con estados de codificación

$$|\xi_{v_k,z,x}\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{w \in C_2} (-1)^{z.w} |v_k + w + x\rangle$$

que forman una base ortonormal de un espacio de Hilbert de 2^n dimensiones, por lo cual el estado de los n pares EPR de Alicia puede expresarse como

$$|\beta_{00}\rangle^{\otimes n} = \sum_{j=0}^{2^n} |j\rangle|j\rangle = \sum_{v_k,z,x} |\xi_{v_k,z,x}\rangle|\xi_{v_k,z,x}\rangle$$

La expresión anterior presenta de forma separada los kets que representan a los qubits que Alicia retiene de aquellos qubits que son enviados a Bob.

En el protocolo de Lo–Chau, Alicia mide en sus qubits los síndromes $\sigma_z^{[r]}$ correspondientes a filas r de P_1 y de $P_2{}^{\perp}$ en el paso **12**, y obtiene valores aleatorios para x y z. De modo similar, su medida final de las mitades codificadas de los pares EPR en el paso **13** le proporciona un valor aleatorio de v_k. Los restantes n qubits permanecen en el estado $|\xi_{v_k,z,x}\rangle$, que corresponde a la codificación de v_k en $CSS_{z,x}(C_1, C_2)$, es decir la contraparte de un estado de 2^m qubits $|k\rangle$. De este modo, las medidas realizadas por Alicia producen qubits aleatorios codificados en un código cuántico aleatorio. Entonces, en lugar de enviar las mitades de los pares EPR, Alicia puede, de modo equivalente, elegir aleatoriamente vectores x, z y k, codificar $|k\rangle$ en el código $CSS_{z,x}(C_1, C_2)$, y enviar a Bob los n qubits codificados.

El procedimiento de preparación y codificación de Alicia y el procedimiento de recepción de Bob se modifican mediante los siguientes pasos:

Alicia

1: Alicia crea n bits de control aleatorios y de acuerdo a sus valores codifica n qubits como $|0\rangle$ o $|1\rangle$.

2: Alicia crea una clave aleatoria k de largo m bits, y dos strings aleatorios x y z de n bits cada uno, y codifica $|k\rangle$ en el código $CSS_{z,x}(C_1, C_2)$ y escoge aleatoriamente n posiciones para colocar los bits de control. En las restantes n posiciones coloca los qubits codificados.

7: Alicia anuncia b, x, z y cuáles n qubits determinan a los bits de control.

Bob

12: Bob decodifica los n qubits que no son de control de $CSS_{z,x}(C_1, C_2)$.

14: Bob mide sus n qubits para obtener la clave secreta compartida k.

El esquema resultante se conoce como el protocolo de códigos CSS, y su seudocódigo se presenta en la Figura 7.

La seguridad del protocolo basado en códigos CSS se fundamenta en su construcción a partir del protocolo de Lo–Chau y en la propiedad de que a una tasa de error suficientemente baja, un código CSS transmite la información codificada con alta fidelidad, de modo que por virtud del teorema de no clonación muy poca información puede ser ganada por un espía.

Fase de preparación de Alicia.

1: Alicia crea n bits de control aleatorios y de acuerdo a sus valores codifica n qubits como $|0\rangle$ o $|1\rangle$.

2: Alicia crea aleatoriamente una clave k de largo m bits, y tres strings b, x y z de n bits cada uno, y codifica $|k\rangle$ en el código $CSS_{z,x}(C_1, C_2)$ y escoge aleatoriamente n posiciones para colocar los bits de control.

3: PARA cada qubit generado, b_k en b

SI ($b_k = 1$)

4: Alicia aplica una transformación de Hadamard en el qubit.

5: Alicia envía los qubits resultantes a Bob.

Fase de recepción de Bob.

6: Bob recibe los $2n$ qubits, y anuncia la recepción.

Fase de verificación.

7: Alicia anuncia b, x, z y cuáles n qubits determinan a los bits de control.

8: PARA cada qubit recibido, b_k en b

SI ($b_k = 1$)

9: Bob aplica una transformación de Hadamard en el qubit.

10: Bob mide los n qubits de control en la base computacional $|0\rangle$, $|1\rangle$ y comparte sus resultados con Alicia.

Fase de Derivación de la clave.

SI (más de t mediciones son diferentes)

11: Abortar el protocolo // *Posible acción de espía detectada.*

SINO

12: Bob decodifica sus n qubits restantes, utilizando una matriz correspondiente a un código cuántico corrector de errores $CSS_{z,x}(C_1, C_2)$.

13: Bob mide sus n qubits para obtener la clave secreta compartida k.

Figura 7: Seudocódigo del protocolo basado en códigos CSS.

6.3.3 Reducción a BB84

El protocolo de distribución de claves basado en códigos CSS es más simple que el protocolo de Lo–Chau, ya que no hace uso de pares EPR. Desafortunadamente, a los efectos de implementación práctica continúa siendo insatisfactorio, porque requiere la capacidad de realizar cómputos cuánticos perfectos para codificar y decodificar qubits, y Bob necesita disponer de una memoria cuántica para almacenar qubits temporalmente mientras los recibe en la comunicación con Alicia. Pero el uso de los códigos cuánticos CSS permite eliminar estas restricciones de hardware, fundamentándose en su propiedad de desacoplar la corrección de cambios de fase de la corrección de cambios de bit. Dado que Bob mide sus qubits en la base computacional $|0\rangle$, $|1\rangle$ inmediatamente luego de la decodificación, la información que Alicia envía sobre el string aleatorio z (utilizado solamente para la corrección de fase de los qubits codificados) es innecesaria.

Entonces, cuando se utiliza un código $CSS(C_1, C_2)$, donde tanto C_1 como C_2 son códigos clásicos, en lugar de decodificar y luego medir, Bob puede medir inmediatamente luego de recibir los qubits, obteniendo un string codificado $v_k + w + x + \varepsilon$ (donde ε representa a los errores ocurridos en la transmisión, por problemas del canal de comunicación o por la acción de un espía) y luego decodificar *de modo clásico*. La decodificación clásica se realiza de modo sencillo, restando el valor de x anunciado por Alicia, y corrigiendo el resultado de acuerdo al código C_1. Si no se produjeron más errores de los que el código es capaz de corregir, el resultado será $v_k + w$. La clave final corresponde al coset de $v_k + w + C_2$ en C_1. El procedimiento de medición de Bob entonces resulta:

12: Bob mide los n qubits que no son de control, obteniendo $v_k + w + x + \varepsilon$, resta x del resultado, y corrige de acuerdo al código C_1, obteniendo $v_k + w$.
13: Bob calcula el coset de $v_k + w + C_2$ en C_1 para obtener la clave k.

Por otra parte, dado que Alicia no necesita revelar el string aleatorio z, el estado que efectivamente envía es un estado mixto, promediado sobre valores aleatorios de z, caracterizado por un operador de densidad:

$$\begin{aligned}
\rho_{v_k,x} &= \frac{1}{2^n} \sum_z |\xi_{v_k,z,x}\rangle\langle\xi_{v_k,z,x}| \\
&= \frac{1}{2^n.|C_2|} \sum_{w_1,w_2 \in C_2} (-1)^{z.(w_1+w_2)} |v_k + w + x\rangle\langle v_k + w + x| \\
&= \frac{1}{|C_2|} \sum_{w \in C_2} |v_k + w + x\rangle\langle v_k + w + x|.
\end{aligned}$$

Este estado puede crearse de modo simple: Alicia solamente necesita elegir *de modo clásico* una palabra $w \in C_2$ aleatoriamente, y construir $|v_k + w + x\rangle$ utilizando los valores de x y k determinados aleatoriamente. El procedimiento de codificación de Alicia entonces resulta:

2: Alicia crea aleatoriamente cuatro strings de largo n bits: b, x, $v_k \in C_1/C_2$ y $w \in C_2$, y codifica n qubits en el estado $|0\rangle$ o $|1\rangle$ de acuerdo a los valores de $v_k + w + x$.

Los pasos de preparación de Alicia (pasos **1** y **2**) y de medición de Bob (paso **13**) pueden simplificarse aún más, introduciendo una modificación en el paso en que Alicia anuncia el string aleatorio utilizado (paso **6**). Si Alicia elige $v_k \in C_1$, entonces el string aleatorio w es innecesario (ya que en lugar de enviar $|v_k + w + x\rangle$, Alicia puede enviar simplemente $|v_k + x\rangle$, que corresponde a un estado codificado.

Además, como $v_k + x$ es un string aleatorio, el procedimiento de codificación y decodificación es equivalente a que Alicia seleccione x aleatoriamente

y envíe el estado $|x\rangle$ que será recibido por Bob, quien lo medirá para obtener un estado modificado $x + \varepsilon$. Luego, Alicia debe enviar $x - v_k$, que será utilizado por Bob para restar y obtener $v_k + \varepsilon$. Este procedimiento muestra que no hay diferencia real entre los qubits de control y los qubits de código efectivo, por lo cual el mecanismo de codificación y decodificación resulta:

1: Alicia elige aleatoriamente un $v_k \in C_1$ y crea $2n$ qubits en el estado $|0\rangle$ o $|1\rangle$ de acuerdo a valores aleatorios de un string de largo $2n$.
2: Alicia elige aleatoriamente n posiciones y las designa como bits de control, y el resto se cataloga como $|x\rangle$.
6: Alicia anuncia b, $x - v_k$, y cuáles son los n qubits que proveen los bits de control.
12: Bob mide los restantes qubits para obtener $x + \varepsilon$, y resta $x - v_k$ del resultado, corrigiéndolo con C_1 obtiene v_k.
13: Alicia y Bob computan el coset de $v_k + C_2$ en C_1 para obtener la clave k.

Además, Alicia no necesita aplicar transformaciones de Hadamard (aunque este tipo de operación simple sobre qubits no es compleja de realizar). En su lugar puede codificar sus qubits directamente en la base computacional $|0\rangle$, $|1\rangle$ o en la base $|+\rangle$, $|-\rangle$, dependiendo de los valores de los bits del string aleatorio b. Utilizando el siguiente mecanismo de preparación por parte de Alicia se obtiene un protocolo donde la codificación y decodificación se realizan de modo "clasico":

1: Alicia crea $(4 + \delta)n$ bits aleatorios. Para cada bit, crea un qubit en la base computacional $|0\rangle$, $|1\rangle$ o en la base $|+\rangle$, $|-\rangle$, de acuerdo a los valores de un string aleatorio b.

Por último, puede eliminarse el requerimiento de una memoria cuántica por parte de Bob: no es necesario almacenar qubits si se procede a medir cada qubit inmediatamente después de recibirlo, considerando una elección aleatoria de las bases utilizadas para la codificación ($\{|0\rangle, |1\rangle\}$ o $\{|+\rangle, |-\rangle\}$). Cuando Alicia hace pública sus bases de codificación (anunciando el string aleatorio b), Bob mantiene solamente aquellos bits para los cuales las bases utilizadas coinciden. Tomando en cuenta que Bob descartará con alta probabilidad la mitad de sus bits, para finalizar con al menos el mismo número de bits que en las versiones previas del protocolo es necesario comenzar con algunos bits más (δn) del doble de bits utilizados originalmente.

Fase de preparación de Alicia.

1: Alicia crea aleatoriamente $(4+\delta)n$ bits.
2: Alicia crea un string aleatorio b de largo $(4+\delta)n$ bits.
3: PARA cada bit b_k en b // *Codificar a en qubits*
SI ($b_k = 0$)
4: Alicia codifica a_k en la base computacional $\{|0\rangle, |1\rangle\}$.
SINO // $b_k = 1$
5: Alicia codifica a_k en la base $\{|+\rangle, |-\rangle\}$
6: Alicia envía los qubits resultantes a Bob.

Fase de medición de Bob.

7: Bob recibe los $(4+\delta)n$ qubits, y los mide aleatoriamente en la base $|0\rangle$, $|1\rangle$ o en la base $|+\rangle$, $|-\rangle$

Fase de verificación.

8: Alicia anuncia su string aleatorio b.
9: Alicia y Bob descartan aquellos bits para los que las bases utilizadas no coincidan. Con probabilidad alta existirán al menos $2n$ bits restantes (en caso contrario, se aborta el protocolo).
10: Alicia selecciona un subconjunto de n *bits de control* y los anuncia públicamente.
11: Alicia y Bob comparan los valores de los n bits de control.

Fase de derivación de la clave.

SI (más de un número t de bits de control difieren)
12: Abortar el protocolo // *Posible acción de espía detectada.*
SINO
13: Alicia conocerá el string x y Bob un string $x + \varepsilon$.
14: Alicia anuncia $x - v_k$. Bob corrige con el código C_1 para obtener v_k.
13: Alicia y Bob calculan el coset de $v_k + C_2$ en C_1 para obtener la clave secreta k.

Figura 8: Seudocódigo de una variante segura del protocolo BB84.

En esta nueva versión del protocolo, Alicia debe retrasar la elección de los bits de control hasta que ambos interlocutores descartan aquellos bits para los cuales las bases utilizadas en la medición no coinciden. El protocolo resultante se presenta en la Figura 8, y corresponde al protocolo BB84 original con la pequeña diferencia que la fase de reconciliación de información se realiza utilizando un código clásico C_1 y la fase de amplificación de privacidad se lleva a cabo mediante el cómputo del coset de $v_k + C_2$ en C_1.

De este modo se prueba la seguridad del protocolo cuántico de distribución de claves BB84. Se parte de un esquema seguro que utiliza estados enredados y requiere cómputos y almacenamiento cuántico, que se reduce sistemáticamente al protocolo BB84. Dado que las modificaciones realizadas mantienen incambiado el estado cuántico de Eva (condicionado en toda la información clásica revelada), se concluye que el protocolo BB84 es seguro de acuerdo al criterio presentado en la Sección 6.2.

La prueba presentada corresponde a un caso idealizado, donde los estados enviados son "perfectos", ignorándose problemas en la generación de qubits y en su transmisión. Además, la prueba no indica cotas para el esfuerzo requerido por Alicia y Bob para llevar a cabo la decodificación (para que el sistema sea aplicable en la práctica, el código C_1 debe ser decodificable eficientemente). Por último, la demostración no indica una cota superior para el nivel de información adquirida por el espía y utiliza códigos CSS, que no son óptimos. Se estima que una tasa de errores de bit y de fase del 11% es aceptable al utilizar un protocolo del estilo de BB84, pero si se utilizan computadores cuánticos para efectuar la codificación y la decodificación, mayores tasas de error pueden ser tolerables.

7 Conclusiones

Este trabajo ha presentado los conceptos básicos de la criptografía cuántica. Se han presentado las características de los principales protocolos cuánticos de distribución de claves y se resumieron las ideas de varias pruebas de seguridad propuestas por los investigadores para demostrar la efectividad de los mecanismos de distribución.

La sección principal del trabajo explica detalladamente la prueba de seguridad original de Shor y Preskill, derivando la seguridad del protocolo BB84 a partir de una implementación segura del protocolo EPR.

La capacidad de la criptografía cuántica constituye un aspecto de importante interés, y se espera que las cuestiones fundamentales sobre las limitaciones físicas en cómputo y comunicación continúen intrigando y desafiando a los investigadores en el futuro.

Lejos de pretender realizar un aporte original y significativo, el objetivo de este trabajo ha sido modesto, presentando las reseñas mencionadas y explicando de un modo autocontenido los detalles de la prueba de seguridad de Shor y Preskill. Es deseo del autor que el contenido pueda ser útil a futuros intrépidos interesados en la materia.

8 Notas bibliográficas

Además de las referencias bibliográficas específicas citadas en el texto, el contenido del artículo se ha basado en los conceptos presentes en varios documentos disponibles que fueron utilizados de modo genérico.

La introducción a las técnicas criptográficas y la descripción de las técnicas de criptografía de clave pública están basadas en contenidos del texto de Tanenbaum [28] y del sitio web de RSA security [25]

Para la reseña de las pruebas de seguridad de los mecanismos cuánticos de distribución de claves se consultaron los artículos de Mayers [21, 22, 23], los trabajos de Lo [19], Lo y Chau [18] y Chau [9], Gottesman y Lo [16], Biham et al. [7, 8], Gottesman y Preskill [15] y Brassard y Savail [6].

La estructura de la Sección 6, que detalla la prueba de seguridad del protocolo BB84 sigue el diagrama del texto de Nielsen y Chuang [24] e incorpora contenidos del artículo de Shor y Preskill [27] y algunos breves comentarios personales.

Referencias

[1] C. Bennett, G. Brassard, J. Robert: Privacy amplification by public discussion, SIAM Journal of Computing **17**, pp. 210–229, 1988.

[2] C. Bennett, G. Brassard: Quantum cryptography: Public-key distribution and coin tossing, en *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pp. 175–179, Bangalore, India, 1984.

[3] C. Bennett, G. Brassard, N. Mermin: Quantum Cryptography without Bell's Theorem, Phys. Rev. Lett. **68**, pp. 557–559, 1992.

[4] C. Bennett: Quantum Cryptography Using any Two Nonorthogonal States, Phys. Rev. Lett. **68**, pp. 3121–3124, 1992.

[5] C. Bennett: Quantum cryptography: Uncertainty in the service of privacy, Science **257**, pp. 752-753, 1992.

[6] G. Brassard, L. Salvail. Secret-key reconciliation by public discussion, Lecture notes in computer science: Advances in Cryptology - EUROCRYPT 93, **765**, 410-423, Springer-Verlag, New York, 1994.

[7] E. Biham, T. Mor: Security of quantum cryptography against collective attacks, Phys. Rev. Lett. **78**, pp. 2256–2259, 1997.

[8] E. Biham, M. Boyer, P. Boykin, T. Mor, V. Roychowdhury: A Proof of the Security of Quantum Key Distribution, en *Proceedings of the 32nd Annual ACM Symposium on Theory of Computing*, pp. 715-724, New York, 2000.

[9] H. Chau: Practical Scheme To Share A Secret Key Through An Up To 27.6% Bit Error Rate Quantum Channel. Preprint disponible en `http://arXiv.org/abs/quant-ph/0205060`. Consultado noviembre 2004.

[10] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, A. Sanpera: Quantum privacy amplification and the security of quantum cryptography over noisy channels, Phys. Rev. Lett., **77**, pp. 2818–2821, 1996.

[11] D. Dieks. Communication by EPR devices, Phys. Lett. A **92**, 6, pp. 271-272, 1982.

[12] W. Diffie, M. Hellman: New directions in cryptography, IEEE Transactions on Information Theory **22** pp. 644–654, 1976.

[13] A. Ekert: Quantum Cryptography Based on Bell's Theorem. Phys. Rev. Lett. **67** pp. 661-663, 1991.

[14] J. Gordon: Noise at optical frequencies; information theory, en *Quantum Electronics and Coherent Light, Proceedings of the International School of Physics Enrico Fermi XXXI*, Nueva York, 1964.

[15] D. Gottesman, J. Preskill: Secure Quantum Key Distribution Using Squeezed States, Phys. Rev. A **63**, 022309, 2001.

[16] D. Gottesman, H. Lo: Proof of security of quantum key distribution with two-way classical communications, IEEE Transactions on Information Theory **49**, 2, pp. 457-475, 2003.

[17] A. Holevo. Statistical problems in quantum physics, en *Proceedings of the Second Japan-USSR Symposium on Probability Theory*, pp. 104-119, Berlin, 1973. Lecture Notes in Mathematics **330**.

[18] H.K. Lo, H. Chau: Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances, Science **283**, pp. 2050–2056, 1999.

[19] H. Lo: A Simple Proof of the Unconditional Security of Quantum Key Distribution, Technical Report HPL-1999-63, HP Laboratories Bristol, 1999. Disponible online en `http://www.hpl.hp.com/techreports/1999/HPL-1999-63.pdf`, consultado noviembre 2004.

[20] U. Maurer: Towards the equivalence of breaking the Diffie-Hellman protocol and computing discrete logarithms, en *Advances in Cryptology – Crypto '94*, pp. 271–281, 1994.

[21] D. Mayers: On the security of the quantum oblivious transfer and key distribution protocols, en *Proceedings of the 15th Annual International Cryptology Conference on Advances in Cryptology* – Lecture Notes In Computer Science, pp. 124–135, 1996.

[22] D. Mayers: Unconditional security in quantum cryptography, J. Assoc. Comp. Mach. **48**, pp. 351–406, 2001.

[23] D. Mayers: Shor and Preskill's and Mayers's security proof for the BB84 quantum key distribution protocol, Eur. Phys. J. D **18**, pp. 161–170, 2002.

[24] M. Nielsen, I. Chuang: Quantum Computation and Quantum Information, Cambridge University Press, 2000.

[25] RSA security web site, URL: `www.rsasecurity.org`. Consultado noviembre 2004.

[26] C. Shannon: The Mathematical Theory of Communication, The Univ. of Illinois Press, 1949.

[27] P. Shor, J. Preskill: Simple Proof of Security of the BB84 Quantum key Distribution Protocol, Phys. Rev. Lett. **85**, pp. 441–444, 2000.

[28] A. Tanenbaum: Redes de Computadoras, Prentice Hall Hispanoamericana, México, 1997.

[29] S. Wiesner: Conjugate coding, Sigact News **15**, 1, pp. 78–88, 1983. Manuscrito original escrito en 1970.

[30] W. Wootters, W. Zurek. A single quantum cannot be cloned, Nature **229**, pp. 802-803, 1982.

[31] H. Zbinden, A. Muller, T.Herzog, B. Huttner, W.Tittel, N. Gisin: Plug and Play systems for quantum cryptography, Applied Phys. Lett. **70**, 7, pp. 793-795, 1997.