ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO
INSTITUTO DE POSTGRADO Y EDUCACIÓN CONTINUA
MAESTRÍA EN SEGURIDAD TELEMÁTICA
TAREA No. 2

MÓDULO: Criptografía y Encriptación
DOCENTE: Ing. Paúl Paguay
NOMBRE(s): Guillermo Valencia Petroche
FECHA: miércoles, 25 de abril de 2018

TEMA: Criptografía Cuántica

1. Introducción

Cada vez que realizamos algún tipo de transacción en línea, confías en las matemáticas, una matemática simple que es fácil de hacer en una dirección pero difícil de hacer a la inversa. Eso es lo que protege la información de posibles ladrones. Pero los sistemas pueden ser pirateados.

Un esquema de encriptación popular, por ejemplo, puede deshacerse al factorizar un gran número aleatorio, una "clave" que desbloquea información codificada, en dos números primos. Es una tarea que hoy es extraordinariamente difícil, pero no imposible. Con suficiente poder de cómputo, un gobierno espía podría romper la llave. O algún matemático inteligente podría encontrar una manera fácil de factorizar grandes números y hacerlo mañana, en teoría.

En busca de una mayor seguridad de los interruptores de código, una nueva generación de fabricantes de códigos ha pasado de las matemáticas a la física. Expertos en átomos y otras partículas, estos criptólogos quieren explotar las leyes de la mecánica cuántica para enviar mensajes que son probablemente imposibles de descifrar. Son los arquitectos de un nuevo campo llamado criptografía cuántica, que ha alcanzado la mayoría de edad en las últimas décadas.

La criptografía cuántica saca su fuerza de la rareza de la realidad a pequeña escala. Las partículas que forman nuestro universo son criaturas inherente mente inciertas, capaces de existir simultáneamente en más de un lugar o más de un estado del ser. Eligen cómo comportarse solo cuando chocan con otra cosa o cuando medimos sus propiedades. La criptografía cuántica saca su fuerza de la rareza de la realidad a pequeña escala.

La aplicación criptográfica más popular aún para este extraño comportamiento es la distribución de claves cuánticas, también conocida como QKD. Una clave cuántica codifica y envía la información necesaria para descifrar un mensaje en las propiedades difusas de las partículas, típicamente partículas claras. Los espías que intentan robar la clave deben hacer mediciones de esas partículas para hacerlo. Esas mediciones cambian el comportamiento de las partículas, introducen errores que pueden detectarse y alertan a los usuarios de que una clave se ha visto comprometida y no deberían usarse para codificar información.

2. Objetivos

2.1 Objetivo General

- Determinar el funcionamiento de la criptografía cuántica.

2.2 Objetivos Específicos

- Obtener sus características principales
- Determinar sus métodos y propiedades
- Generar el campo de acción

3. Desarrollo

La criptografía cuántica es la ciencia que permite explotar las propiedades de la mecánica cuántica para realizar tareas criptográficas. Utiliza los principios de la mecánica cuántica para encriptar y garantizar la absoluta confidencialidad de la información transmitida. La criptografía cuántica permiten crear de manera segura algoritmos, para cifrar y descifrar mensajes. La física cuántica es fundamentalmente aleatoria.

La seguridad de la criptografía cuántica descansa en las bases de la mecánica cuántica, a diferencia de la criptografía de clave pública tradicional la cual descansa en supuestos de complejidad computacional no demostrada de ciertas funciones matemáticas.

El ejemplo más conocido de criptografía cuántica es la distribución cuántica de claves que ofrece una solución teóricamente segura de la información para el problema de intercambio de claves. Excepto por la criptografía post cuántica, a partir de 2017, los encriptadores de cuántica de clave pública y los esquemas de firma (por ejemplo, criptografía de curva elíptica (ECC) y RSA) actualmente utilizados pueden romperse por adversarios cuánticos. [Stallings 2016]

La ventaja de la criptografía cuántica radica en el hecho de que permite la realización de varias tareas criptográficas que se prueban o conjeturan como imposibles utilizando solo la comunicación clásica es decir, no cuántica. Por ejemplo, es imposible copiar datos codificados en un estado cuántico y el simple hecho de leer datos codificados en un estado cuántico cambia el estado. Esto podría usarse para detectar escuchas en la distribución de claves cuánticas.

Una de las propiedades más importantes de la criptografía cuántica es que si un tercero intenta hacer eavesdropping durante la creación de la clave secreta, el proceso se altera advirtiéndose al intruso antes de que se transmita información privada. Esto es una consecuencia del principio de incertidumbre de Heisenberg, que nos dice que el proceso de medir en un sistema cuántico perturba dicho sistema.

A diferencia de las computadoras clásicas, que operan en bits que son ya sea 0 o 1, las computadoras cuánticas se basan en bits cuánticos o qubits, que puede ser 0 y 1 simultáneamente, un estado de ambigüedad llamado superposición. Los físicos descubrieron que en este mundo microscópico, las partículas tales como electrones y fotones se comportan de una manera altamente contraintuitiva antes de observar un electrón, el electrón no está en una ubicación definida en espacio, pero en varios lugares al mismo tiempo es decir, en un estado de superposición.

Quantum Bits. Los bits cuánticos (qubits), o grupos de los mismos, se caracterizan con números amplitudes llamadas, que son similares a las probabilidades, pero no son exactamente probabilidades Mientras que una probabilidad es un número entre 0 y 1, una la amplitud es un número complejo de la forma a + b × i, o simplemente a + bi, donde a y b son números reales, y yo es una unidad imaginaria. El número i se usa para formar números imaginarios, que son de la forma bi, con b una real número [Aumasson 2018]. Cuando se multiplica por un número real, obtenemos otro imaginario número, y cuando se multiplica por sí mismo da -1; eso es i 2 = -1. Los números complejos pueden verse como pertenecientes a un plano, como se muestra en la Figura 14-2. Aquí, el eje x en el la figura corresponde a a en a + bi, el eje y corresponde a b, y las líneas punteadas corresponden a la parte real e imaginaria de cada número. Por ejemplo, la línea punteada vertical que va desde el punto 3 + 2i hasta 3 es dos unidades de largo.

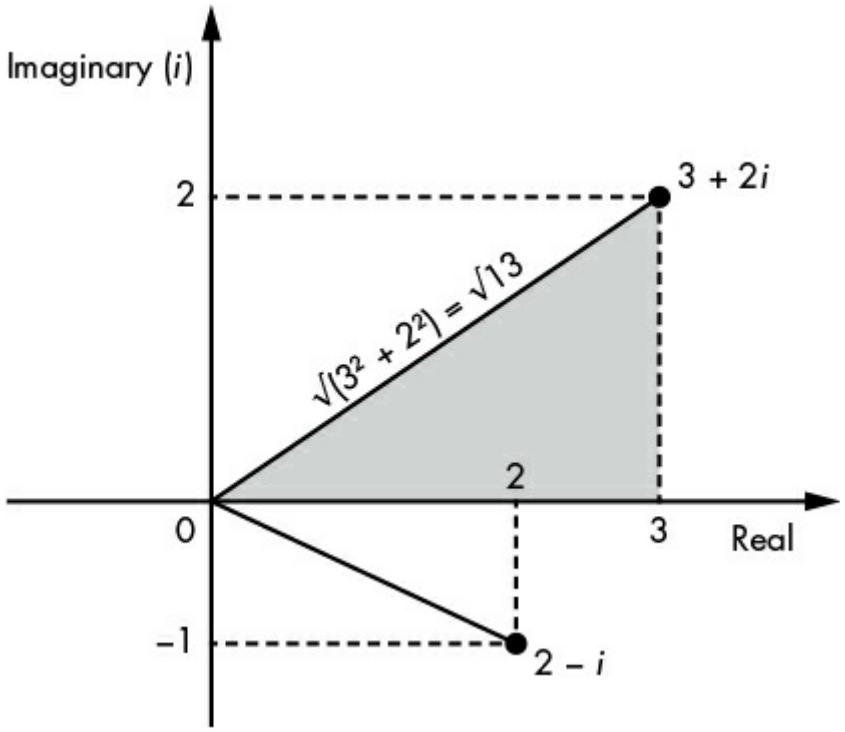


Figura 14-2: una vista de números complejos como puntos en un espacio bidimensional

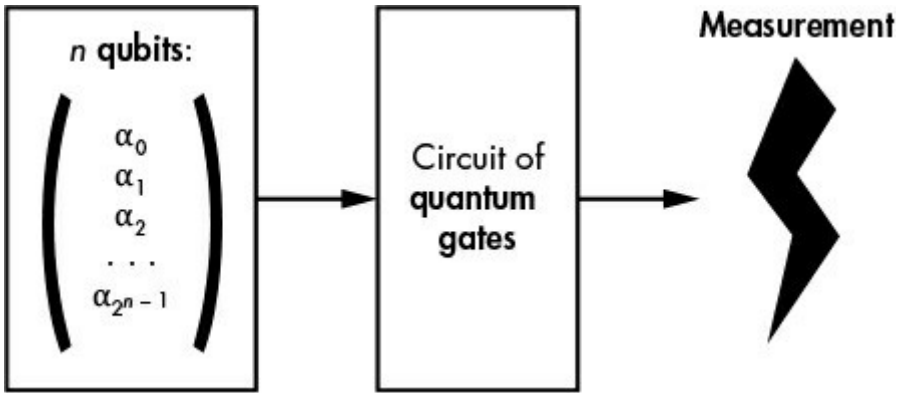
Amplitudes de un Qubit. Un solo qubit se caracteriza por dos amplitudes que llamaré α (alfa) y β (beta). Entonces podemos expresar el estado de un qubit como α | 0> + β | 1>, donde el "| > "Notación se usa para denotar vectores en un estado cuántico. Esta notación significa que cuando observe este qubit aparecerá como 0 con una probabilidad | α | 2 y 1 con una probabilidad | β | 2. Por supuesto, en orden para que estas sean probabilidades reales, | α | 2 y | β | 2 deben ser números entre 0 y 1, y | α | 2 + | β | 2 debe ser igual a 1. Por ejemplo, supongamos que tenemos el qubit (psi) con amplitudes de α = 1 / √2 y β = 1 / √2. Podemos expresar esto de la siguiente manera:

$$\Psi = \left(1 / \sqrt{2}\right)|0\rangle + \left(1 / \sqrt{2}\right)|1\rangle = \left(|0 + |1\right) / \sqrt{2}$$

Amplitudes de grupos de Qubits. Por ejemplo, un byte cuántico se puede formar con 8 qubits, cuando se pone en un estado donde los estados cuánticos de estos 8 qubits están de alguna manera conectados el uno al otro (decimos que los qubits están enredados, que es un complejo fenómeno físico). Tal byte cuántico se puede describir de la siguiente manera: donde los αs son las amplitudes asociadas con cada uno de los 256 posibles valores del grupo de 8 qubits: La criptografía cuántica está cercana a una fase de producción masiva, utilizando láseres para emitir información en el elemento constituyente de la luz, el fotón, y conduciendo esta información a través de fibras ópticas.

$$\alpha_0|00000000\rangle + \alpha_1|00000001\rangle + \alpha_2|00000010\rangle + \alpha_3|00000011\rangle + \ldots + \alpha_{255}|11111111\rangle$$

Quantum Gates. Los conceptos de amplitud y compuertas cuánticas son exclusivos de quantum informática. Mientras que una computadora clásica usa registros, memoria y una microprocesador para realizar una secuencia de instrucciones sobre datos, un cuanto computadora transforma un grupo de qubits de forma reversible mediante la aplicación de una serie de puertas cuánticas, y luego mide el valor de uno o más qubits [Aumasson 2018].



Quantum Gates como Multiplicaciones de matrices. A diferencia de las puertas booleanas de una computadora clásica (Y, XOR, y así on), una puerta cuántica actúa sobre un grupo de amplitudes justo cuando una matriz actúa cuando se multiplicó con un vector. Por ejemplo, para solicitar el simulador plest puerta cuántica, la puerta identidad, al qubit Φ, vemos I como una matriz 2 × 2 y multiplicarlo con el vector de columna que consiste en las dos amplitudes de Φ, como se muestra aquí:

$$I|\Phi\rangle = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} i/\sqrt{2} \\ -1/\sqrt{2} \end{pmatrix} = \begin{pmatrix} 1\times\frac{i}{\sqrt{2}} + 0\times\left(-\frac{1}{\sqrt{2}}\right) \\ 0\times\frac{i}{\sqrt{2}} + 1\times\left(-\frac{1}{\sqrt{2}}\right) \end{pmatrix} = \begin{pmatrix} i/\sqrt{2} \\ -1/\sqrt{2} \end{pmatrix} = \Phi\rangle$$

4. **Conclusiones y Recomendaciones**

La posibilidad de modelar el proceso cuántico y probar su aleatoriedad es esencial en dos aspectos. Primero, permite identificar los parámetros críticos, que luego se pueden monitorear en vivo para garantizar ex ante la calidad de los bits aleatorios producidos. Esta propiedad permite reducir o incluso suprimir la necesidad de realizar pruebas estadísticas en vivo de la secuencia de salida.

La segunda ventaja importante relacionada con el uso de un proceso cuántico es que sus modos de falla se pueden modelar y evaluar. Esto permite diseñar RNG que "fallan con elegancia", garantizando, por ejemplo, la inhibición del flujo de bits aleatorio en caso de fallo, en lugar de producir números aleatorios imperfectos. Dado el hecho de que la física cuántica describe el comportamiento de los bloques de construcción fundamentales (átomos, partículas, etc.) del mundo físico, uno podría argumentar que todo es cuántico y, en consecuencia, los RNG basados en la física clásica también son cuánticos.

Las computadoras cuánticas prometen más poder de computación porque con solo n qubits, pueden procesar 2n números las amplitudes de los qubits. Esta la propiedad tiene profundas implicaciones.

5. Bibliografía

Stallings, W. (2016). *Cryptography and network security: Principles and practice*. Pearson.

Aumasson, J. (2018). *Serious Cryptography: A Practical Introduction to Modern Encryption* . No Sarch press.

Bernstein, D. (2010). *Post Quantum Cryptography*. Springer.