

Distribución cuántica de claves

ALGORITMOS Y APLICACIONES 

Calificación: 98

DANIEL VICENTE GARCÍA FRANCO

IGNACIO GARCÍA-ESCRIBANO MARTÍN

ISMER DAVID DORADO SABOGAL

CRISTIAN FERNÁNDEZ PARDO

MARCOS GARCÍA FERNÁNDEZ

JUAN PABLO DOMÍNGUEZ MAYO

La QKD (distribución de claves cuántica) es una nueva forma de generación y transmisión de claves a través de un canal cuántico (inseguro) y un canal clásico (no necesariamente privado) autenticado. Una vez se ha hecho la distribución de claves, estas se pueden usar para mandar mensajes cifrados vía un canal clásico (inseguro) usando la criptografía simétrica ya conocida ([1] y [2]).

La pieza fundamental de este método de distribución de claves reside en las propiedades cuánticas en las que se apoya, a saber, el entrelazamiento cuántico y el principio de incertidumbre de Heisenberg. Estas garantizan (en condiciones ideales) seguridad matemáticamente probada contra cualquier tipo de ataque, tanto clásico como cuántico. Otra ventaja es que permite al emisor y al receptor detectar cualquier intento de espionaje en el proceso de distribución ([1] y [3]).

Cabe destacar que otro punto importante de la QKD son los generadores de números aleatorios. Para garantizar seguridad incondicional, se usan efectos cuánticos para la generación de números aleatorios verdaderos (TRNG). Este tipo de generadores consisten en dispositivos que generan números aleatorios a partir de procesos físicos, en vez de mediante algoritmos ([4]).

Sin embargo, la QKD del mundo real dista mucho de ser perfecta y, por tanto, cualquier protocolo que se quiera usar ha de ser estudiado con cuidado previamente. Algunos de los problemas que plantea la QKD son los siguientes: ratio y rango de transmisión limitados, protocolos punto a punto en vez de por paquetes (que son los que se usan en Internet), hardware costoso y difícil de mantener, la autenticación e integridad no están cubiertas por la QKD y deben tratarse de manera clásica ([3]).

En cuanto a los protocolos que se han desarrollado los hay de distintos tipos: BB84 y variantes (basados en la medición de la polarización de fotones), E91 (llamado así por Ekert, se basa en el entrelazamiento cuántico) y QKD de variable continua ([1] y [3]).

Algunos de los posibles ataques a este tipo de protocolos pueden ser: interceptación-reenvío, ataques de tiempo, ataque troyano, ataques de canal lateral ([3]).

[PROTOCOLO E91](#)

Este protocolo criptográfico fue propuesto por Artur Ekert en 1991 y está basado en el Teorema de Bell. Establece su seguridad en el uso de pares de un estado cuántico de 2 qubits entrelazados. Este protocolo utiliza un enfoque diferente a la QKD, además su utilización permite una mayor probabilidad en la detección de espías o intrusos durante la comunicación a diferencia de los otros protocolos ([5] y [6]).

El esquema de comunicación del protocolo E91 es parecido a BB84. Sin embargo, con E91 se requiere una fuente que produzca una serie de pares de qubits entrelazados, dicha fuente puede estar en manos del emisor o del receptor o de algún tercero, lo más importante es que de cada par de qubits entrelazados producido, un qubit llegue al emisor y el otro al receptor ([7]).

Cuando dos qubits quedan entrelazados y hagamos la comparación de los mismos, ambos qubits deben tener el mismo valor, con esto quiere decir que cualquiera de los dos puede utilizar esta cadena secreta.

El procedimiento básicamente consta de 3 pasos ([7]):

- 1: Se origina una secuencia de qubits entrelazadas para Emisor y Receptor.
- 2: Tanto Emisor y Receptor eligen de manera independiente una secuencia de bases para medir la serie.
- 3: Emisor y Receptor comparan sus secuencias y mantienen únicamente los bits coincidentes en la misma base.

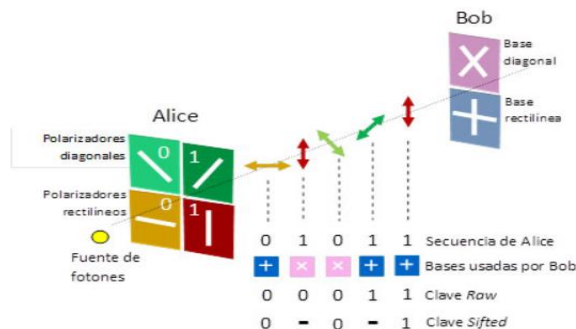
EL PROTOCOLO BB84

Es un algoritmo de distribución de clave cuántica que complementa a otros métodos de cifrado, como puede ser el cifrado de Vernam. Se considera el primer protocolo de distribución de claves cuánticas y es el más sencillo. Fue ideado por Charles Bennett y Gilles Brassard en 1984, por eso se le conoce como BB84 ([8]).

El protocolo es demostrablemente seguro, confiando en la propiedad cuántica de que la ganancia de información solo es posible a expensas de alterar la señal si los dos estados que se intentan distinguir no son ortogonales (ver teorema de no clonación) y un público autenticado canal clásico. Por lo general, se explica como un método para comunicar de manera segura una clave privada de una parte a otra para usarla en el cifrado de una sola vez ([9]).

El protocolo BB84 se basa en el hecho de que se puede medir o preparar un estado en la base $\{|0\rangle, |1\rangle\}$ o en la base $\{|0'\rangle, |1'\rangle\}$ (considerándose estas bases ortonormales).

- 1- Alice elige de manera aleatoria un estado particular entre los cuatro elementos de las dos bases y envía una serie de fotones con distintos estados a Bob.
- 2- Bob elige de manera aleatoria sobre qué base hacer mediciones para cada uno de esos fotones. Si escoge el mismo conjunto en cual se encontraba el estado enviado por Alice, Bob obtendrá el resultado correcto. Si elige un conjunto diferente hay una probabilidad 1/2 de que equivoque el resultado.
- 3- Por un canal clásico, como el teléfono, Alice y Bob intercambian información sobre en qué base fueron codificados los 0s y 1s. No se mencionan los resultados específicos solo se intercambia información sobre las bases de codificación. Si las bases de codificación son diferentes el resultado se descarta. Ambos se quedan con los resultados que han coincidido para formar la clave secreta.
- 4- Tras esto, se realiza una prueba en abierto, sin importar que alguien pueda estar escuchando la comunicación, utilizando parte de la clave para confirmar que la clave que están utilizando es la misma. No utilizan el 100% de la longitud de la clave puesto que sino luego no la podrán utilizar para cifrar.



Protocolo de distribución cuántica de clave BB84

Figura 1: Protocolo BB84 ([10])

Posibles problemas ([11]):

Man-in-the-middle attack: puede haber un tercer ente en la comunicación que intercepte los fotones enviados desde Emisor a Receptor pero, una vez interceptado el fotón, tal y como explica el ‘teorema de no clonación’ el fotón cambiará su valor original al copiarse por un atacante externo.

Photon number splitting attack: En el protocolo original se usan estados mono-fotónicos. En la práctica se tienen que usar pulsos láser muy débiles.

Pérdidas debido al ruido en el canal: el Fotón que viaja entre las dos partes interactúa con el medio y aparece una probabilidad de que cambie espontáneamente su polarización. Estos cambios son equivalentes a la interceptación por un espía.

PROTOCOLO B92

El protocolo B92 [2], propuesto por Bennet en 1992, es una generalización muy simple del BB84, que utiliza solamente dos estados no ortogonales ([12]).

Protocolo B92

- Alicia genera una cadena aleatoria a de 0's y 1's.
- Alicia envía a Bob cada bit de la cadena a , codificado del siguiente modo:
Un 0 lo codifica con $|0\rangle$ y un 1 con $|+\rangle$
- Bob genera una cadena a' de 0's y 1's y mide cada estado recibido usando B_1 si en la posición correspondiente $a=0$ y B_x , cuando $a=1$.
- A partir de esta medición Bob obtiene una cadena b de 0's y 1's, del siguiente modo:
Si ha usado B_1 y obtiene $|0\rangle$ pone $b=0$ y si obtiene $|1\rangle$, pone $b=1$.
Si ha usado B_x y obtiene $|+\rangle$ pone $b=0$ y si obtiene $|-\rangle$, pone $b=1$
- Bob publica las posiciones en que $b=1$ y, sólo con estas posiciones, las claves son a para Alicia y $1-a'$ para Bob.

Las claves coinciden (salvo ruidos o espías) con probabilidad 1.
La longitud de la clave es $\frac{1}{2}$ de la de la cadena original


 CIEMATIC
Centro de Innovación Matemática
e-2016-2017

Figura 2: Protocolo B92 ([12])

REFERENCIAS:

- [1] <https://www.quantiki.org/wiki/quantum-key-distribution>
- [2] <https://www.quintessencelabs.com/wp-content/uploads/2016/08/QKD-What-is-Quantum-Key-Distribution-whitepaper.pdf>
- [3] <https://arxiv.org/pdf/1504.05471.pdf>
- [4] https://en.wikipedia.org/wiki/Hardware_random_number_generator
- [5] https://en.wikipedia.org/wiki/Quantum_key_distribution
- [6] https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-33052015000200009
- [7] https://es.wikipedia.org/wiki/Criptograf%C3%ADa_cu%C3%A1ntica#Protocolo_E91
- [8] <https://www.gaussianos.com/criptografia-protocolo-de-distribucion-de-clave-bb84/>
- [9] <https://en.wikipedia.org/wiki/BB84>
- [10] <http://www.itefi.csic.es/en/content/semana-de-la-ciencia-2016/computacion-cuantica-vs-criptografia-cuantica>
- [11] <http://aici.uta.cl/aci/images/stories/clase21.pdf>
- [12] <http://www.criptored.upm.es/crypt4you/temas/cuantica/leccion2/leccion02.html>