Algoritmo BB84 de Distribución Cuántica de Claves

Manuel Tagle, Patricio Palacios y Lukas Wolff

28 de octubre de 2025

1. Bases de Codificación

El protocolo utiliza dos bases ortogonales mutuamente incompatibles para representar los bits:

- Base **Rectilínea (R)**: $\{|0\rangle, |1\rangle\}$, correspondiente a polarizaciones horizontal y vertical.
- Base **Diagonal (D)**: $\{|+\rangle, |-\rangle\}$, correspondiente a polarizaciones a 45° y 135°.

Un mismo bit puede codificarse en diferentes bases, y si el receptor mide en la base incorrecta, el resultado será aleatorio.

2. Parte 1: Sin intervención de Eve

2.1. Descripción del Proceso

El protocolo sin presencia de un espía se desarrolla en los siguientes pasos:

1. **Generación de secuencias por Alice:** genera N bits aleatorios (0 o 1) y N bases aleatorias (R o D). Si es R y el bit es 0, envía $|0\rangle$; si es R y el bit es 1, envía $|1\rangle$; si es D y el bit es 0, envía $|+\rangle$; si es D y el bit es 1, envía $|-\rangle$.
2. **Bob genera sus bases:** elige N bases aleatorias para medir los qubits recibidos. Ahora bien
3. **Bob mide:** compara sus bases con las de Alice. Si coinciden, conserva el bit; si no, lo descarta. Las combinaciones posibles son las siguientes:
   - Alice R, Bob R: Bob obtiene el bit correcto.
   - Alice R, Bob D: Bob obtiene un bit aleatorio (50 % de probabilidad de ser 0 o 1).
   - Alice D, Bob R: Bob obtiene un bit aleatorio (50 % de probabilidad de ser 0 o 1).
   - Alice D, Bob D: Bob obtiene el bit correcto.

- **Perdida de información:** en promedio, la mitad de los bits se descartan debido a la falta de coincidencia de bases, es decir, hay un 50 % de perdida de información, el cual tiene un 50 % de probabilidad de ser real, por lo tanto, se puede decir que hay un 25 % de perdida de información real. Aun asi, se descarta la mitad de los bits, logrando asi un Quantum Bit Error Rate (QBER) de 0 % en un canal ideal.

4. **Comparación de bases:** finalmente, Alice publica sus bases y Bob determina las coincidencias.
5. **Extracción de clave cruda:** se seleccionan los bits correspondientes a bases coincidentes.
6. **Verificación de errores:** Bob revela una pequeña fracción de la clave para comparar con Alice. Si los bits coinciden, la clave es válida.

2.2. Resultados Esperados

Si el canal es ideal (sin ruido), la tasa de error cuántica o QBER (*Quantum Bit Error Rate*) debería ser aproximadamente 0 %. La mitad de los bits se descartan debido a la falta de coincidencia de bases, resultando en una **clave cruda** de longitud cercana a $N/2$.

3. Parte 2: Con intervención de Eve

3.1. Ataque de Interceptación y Reenvío

En este escenario, un atacante (Eve) intercepta los qubits enviados por Alice, los mide en bases aleatorias y luego reenvía a Bob qubits codificados según sus propios resultados. El procedimiento es el siguiente:

1. Eve genera sus bases aleatorias.
2. Eve mide los qubits de Alice. Si su base coincide con la de Alice, obtiene el bit correcto; si no, el resultado es aleatorio.
3. Eve reenvía a Bob los bits medidos, preparados en su base.
4. Bob mide los qubits reenviados utilizando sus propias bases. Por lo cual se generan las siguientes combinaciones:
   - Alice R, Eve R, Bob R: Bob obtiene el bit correcto.
   - Alice R, Eve R, Bob D: Bob obtiene un bit aleatorio (50 % de acierto).
   - Alice R, Eve D, Bob R: Bob obtiene un bit aleatorio (50 % de acierto).
   - Alice R, Eve D, Bob D: Bob obtiene el bit correcto con 50 % de probabilidad.
   - Alice D, Eve R, Bob R: Bob obtiene el bit correcto con 50 % de probabilidad.
   - Alice D, Eve R, Bob D: Bob obtiene un bit aleatorio (50 % de acierto).
   - Alice D, Eve D, Bob R: Bob obtiene el bit correcto con 50 % de probabilidad.
   - Alice D, Eve D, Bob D: Bob obtiene el bit correcto.

3.2. Detección de la Presencia de Eve

El intento de espionaje introduce perturbaciones detectables. Si Eve mide con una base incorrecta, perturba el estado original, de modo que cuando Bob mida (incluso con la base correcta), tiene un 50 % de probabilidad de obtener el bit erróneo. El resultado es que la tasa de error esperada (**QBER**) se eleva aproximadamente a un **25 %**.