**EMULADOR DE UN SISTEMA DE CRIPTOGRAFÍA CUÁNTICA: COMPARACIÓN DE LOS PROTOCOLOS DE DISTRIBUCIÓN DE CLAVES CUÁNTICAS BB84 Y BB84 EFICIENTE**

I. Carnoto[1], P. Fajardo[1], E. García[1], J. Cabrero[2], F. Morales[2], R. Pulido[2]. [1]Universidad Carlos III de Madrid (UC3M). Avda. Universidad 30, 28911. Leganés. (icarnoto@ing.uc3m.es), [2] Ingeniería de Sistemas para la Defensa de España (ISDEFE). Calle Beatriz de Bobadilla, 3. 28040. Madrid.

**Introducción:** En este trabajo se han comparado dos protocolos de distribución de claves cuánticas, el BB84 y BB84 eficiente, y se ha desarrollado un emulador de un sistema de criptografía cuántica para implementar aquel que brinda las mejores prestaciones en términos de eficiencia y capacidad de detección de un espía.

**Bases Teóricas:** La criptografía cuántica aprovecha las características de la mecánica cuántica para generar mensajes teóricamente indescifrables. Estos son: la verdadera aleatoriedad, el teorema de no-clonación y la capacidad de detección de espías. Es posible generar secuencias de bits completamente aleatorias, por ejemplo, haciendo incidir un fotón polarizado diagonalmente sobre un divisor de haz, este será transmitido o reflejado con un 50% de probabilidad. El teorema de no-clonación afirma que es imposible crear una copia exacta de un estado cuántico aleatorio desconocido. Por último, la monitorización pasiva de señales desconocidas se encuentra prohibida, un espía que intenta robar información sobre estados cuánticos causará casi siempre alteraciones detectables.

El emulador desarrollado simula ambos protocolos. En el protocolo BB84 se codifica la información de un bit en la polarización de un fotón usando dos bases, la "+" y la "×". Estas son equiprobables.

*Figura 1. Bases de polarización.*

Alice transmitirá una secuencia de bits codificada según una secuencia aleatoria de bases y Bob usará otra cadena arbitraria de bases para medir cada fotón. Cuando las bases coinciden, la medida realizada es correcta, mientras que cuando no sean iguales Bob obtendrá como resultado '0' o '1' aleatoriamente. Alice y Bob se intercambian la secuencia de bases usada y descartan todos los bits donde las bases no coinciden. De la secuencia restante intercambian algunos bits como prueba, si existen diferencias en estos concluyen que ha habido un espía en la comunicación.

El protocolo BB84 eficiente funciona igual que el original, pero con algunos cambios. Las bases ahora no son equiprobables, siendo la base "+" la mayoritaria. Al comparar las bases se descartan los bits de bases no coincidentes, la clave se forma con los bits donde coincide la base "+" y en los que coincide la base "×" se usan para detectar al espía.

Teóricamente, el protocolo BB84 tiene una eficiencia menor al 50%, debido a que solo el 50% de los bits coincidirán en bases y además, se descarta otro porcentaje en pruebas. En el BB84 eficiente la eficiencia viene dada por la probabilidad de la base "+" al cuadrado y teóricamente, puede llegar casi al 100% aumentando la longitud de la clave.

**Resultados y discusión:** Se realizaron simulaciones de ambos protocolos bajo condiciones ideales para ver la capacidad de detección frente a la eficiencia. En la figura 2, vemos el resultado para una clave de 320 bits establecida con el BB84.

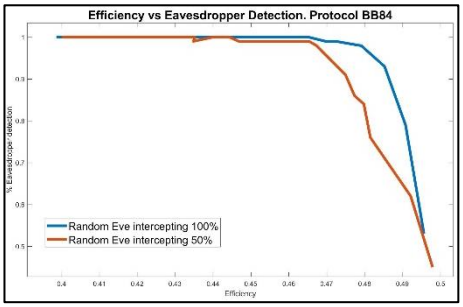


*Figura 2. BB84 con 320 bits de clave.*

Se observa como la eficiencia es siempre menor al 50%. Se realizaron las mismas simulaciones con el protocolo BB84 eficiente, pero con 10.000 bits de clave y se obtuvo el gráfico de la figura 3.

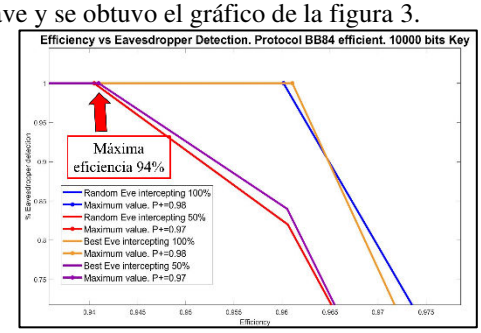


*Figura 3. BB84 eficiente con 10.000 bits de clave.*

Se ve como la eficiencia aumenta hasta un 94% manteniendo una capacidad de detección del 100%.

Por último, se repitió la última simulación añadiendo distorsión por ruido térmico (hasta $0\,^{\circ}C$) y distancia (fibra óptica de 10 km) y se obtuvo que se mantienen las mismas prestaciones.

**Conclusiones:** Tras comparar ambos protocolos se concluye que el BB84 eficiente ofrece mejores prestaciones logrando una eficiencia de 94% con capacidad de detección del 100% para 10.000 bits de clave, aun bajo condiciones no ideales. Si se aumentase la cantidad de bits, esta eficiencia seguiría creciendo mientras que, en el BB84, no importa cuantos bits se utilicen, la eficiencia no superará el 50%.

**Referencias:** [1] Carnoto, I. (2021) *Criptografía Cuántica*. Universidad Carlos III de Madrid.