MOOC: Computación y Criptografía Cuánticas

Lección 2: Criptografía Cuántica

Soluciones razonadas a los test de evaluación

1. La principal aportación de la mecánica cuántica a la criptografía es

b)La posibilidad de distribuir claves privadas de las que un espía no puede obtener información sin alterarlas.

Si se usan estados cuánticos para generar y distribuir una clave, éstos no se pueden copiar ni medir sin modificarlos irreversiblemente.

---

2. Si no ha habido espías ni interferencias en el protocolo BB84, antes de la fase de reconciliación de bases, las cadenas de bits Alicia y Bob son coincidentes aproximadamente en un

a) 75%.

Los bits serán coincidentes con probabilidad 1, cuando Alicia y Bob hayan usado la misma base, lo que ocurre para el 50% de los bits y si han usado distinta base, la probabilidad de coincidencia es del 50%. Por ello antes de la reconciliación de bases la probabilidad de coincidencia es $1 \cdot 0.5 + 0.5 \cdot 0.5 = 0.75$.

---

3. La clave bruta y la clave depurada del protocolo BB84 verifican:

c) La clave depurada es una parte de la clave bruta.

La clave depurada se obtiene de la bruta eliminando los bits utilizados para chequear la presencia de espías.

---

4. En el protocolo B92, se utiliza para codificar

b) Dos estados cuánticos no ortogonales.

Pueden ser $|0\rangle$ y $|+\rangle$, o cualquier otro par de estados no ortogonales.

---

5 ¿Cuál de los siguientes protocolos cuánticos de distribución de claves tiene más dificultades técnicas de implementación?

c) El E91

Para implementar el E91 hace falta un emisor de pares EPR, mientras que los otros dos protocolos se pueden implementar fácilmente con la tecnología actual.