Escuela Superior Politécnica del Litoral

Pares & Nones — Un break científico

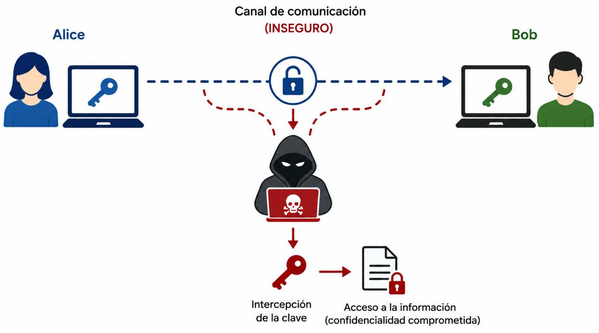
Washington Velásquez, PhD.
wavelasq@espol.edu.ec
FIEC

Manuel S. Alvarez-Alvarado, PhD.
mansalva@espol.edu.ec
FIEC

# Integrating Quantum Circuits for Enhanced Security of Symmetric Encryption Algorithms

## PROBLEMA

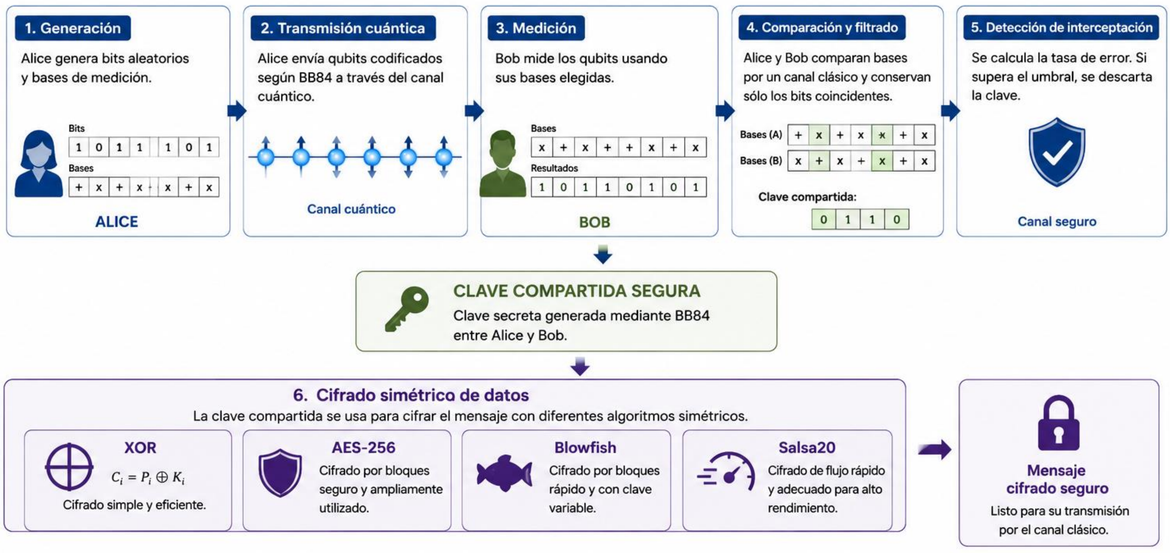
El avance de la computación cuántica representa una amenaza para los sistemas criptográficos tradicionales. Se requieren nuevos mecanismos de intercambio de claves que permitan proteger las comunicaciones y detectar intentos de interceptación durante la transmisión de información.




## OBJETIVO GENERAL

Evaluar la integración del protocolo de distribución cuántica de claves BB84 con algoritmos de cifrado simétrico (XOR, AES, Blowfish y Salsa20) para mejorar la seguridad de las comunicaciones digitales mediante el uso de circuitos cuánticos simulados.

## PROPUESTA




## RESULTADOS

### 1. IMPLEMENTACIÓN DEL PROTOCOLO BB84


- 8 qubits utilizados en la simulación.
- Se generó una clave compartida entre Alice y Bob.
- La medición de los qubits permitió detectar intentos de interceptación.

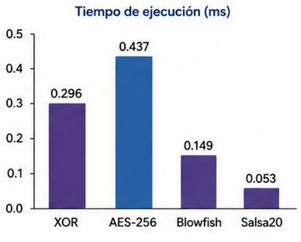
### 2. DETECCIÓN DE INTERCEPTACIÓN

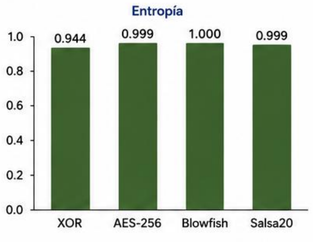
| Escenario | Tasa de error (E) | Umbral (10%) | Canal seguro |
|---|---|---|---|
| Escenario 1 | 4% | E < 10% | Sí |
| Escenario 2 | 20% | E > 10% | No |

Cuando la tasa de error supera el umbral establecido (10%), la clave generada se descarta para garantizar la seguridad de la comunicación.

### 3. DESEMPEÑO DE ALGORITMOS DE CIFRADO

| Algoritmo | Tiempo de ejecución (ms) | Entropía | Tamaño de clave |
|---|---|---|---|
| XOR | 0.296 | 0.944 | 8 bits |
| AES-256 | 0.437 | 0.999 | 256 bits |
| Blowfish | 0.149 | 1.000 | 32 – 448 bits |
| Salsa20 | 0.053 | 0.999 | 256 bits |




## CONCLUSIONES

- La integración de BB84 con algoritmos de cifrado simétrico mejora la seguridad del intercambio de claves.
- La distribución cuántica de claves permite detectar accesos no autorizados al canal de comunicación.
- Salsa20 mostró el mejor desempeño computacional, mientras que AES y Blowfish ofrecieron elevados niveles de seguridad.


- La combinación de criptografía cuántica y clásica constituye una alternativa prometedora para futuras comunicaciones seguras.