Computación Cuántica y Ataque a la Criptografía Clásica de Clave Pública

Harold Alejandro Villanueva Borda

Objetivo

- Romper sistemas criptográficos clásicos:
  - simétricos
  - asimétricos
- Dar a conocer algoritmos cuánticos.
- Estudios Post-Quantum.

Algoritmo Grover

- Algoritmo de búsqueda
- También usado en la factorización.
- Número de pasos cuadráticos.
- Requiere de una QC a gran escala.

Algoritmo Shor

- Factorización de números primos.
- Logaritmos discretos.
- Problema difícil de resolver.
- Tiempo polinomial.
- Requiere de una QC a gran escala.

Transformada cuántica de Fourier

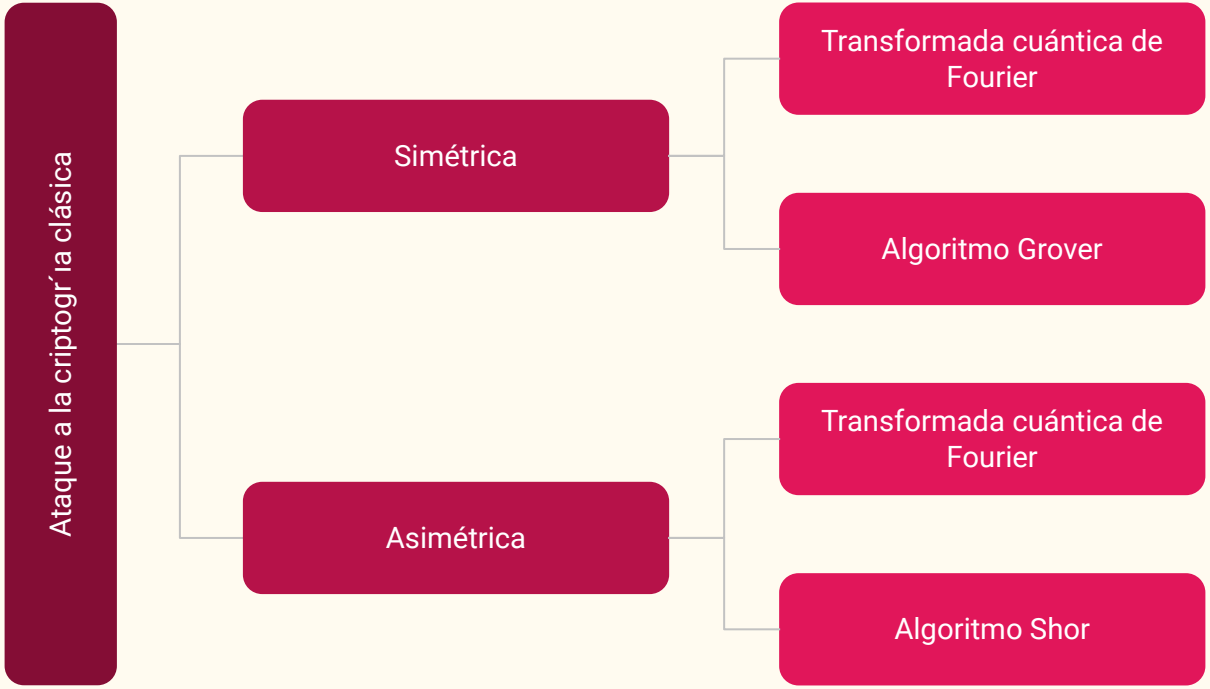
- Analiza funciones en el espacio de frecuencia.
- Búsqueda cuántica
- Factorización de números.
- Simulación de sistemas cuánticos.

Problema de escalabilidad

.

- Lograr realizar operaciones cuanticas complejas.
- Es un gran desafío
- Requiere precisión y control.
- Aumento de ruido y pérdida de coherencia.
- Disminuye la precisión.

Taxonomía


Ataque a la criptogr´ıa clásica
Simétrica
Asimétrica
Transformada cuántica de Fourier
Algoritmo Grover
Transformada cuántica de Fourier
Algoritmo Shor

Análisis

- Ventaja cuántica.
- Coherencia cuántica.
- Errores ambientales.

Ataque a la criptografía asimétrica:

- Resueltos por una QC.
- Factorización de primos.
- Logaritmos discretos.
- Algoritmo Shor.
- Nuevos modelos matemáticos.

Ataque a la criptografía simétrica:

- Algoritmo Grover.
- Duplicar el tamaño de la clave.

Limitaciones de una Quantum Computer:

- Problemas de coherencia.
- Conectividad limitada entre qubits.

Conclusión

- Campo en desarrollo.
- Inversión en la seguridad postunática.
- Resuelve el problema en tiempo polinomial.
- limitantes como:

  - Cantidad de qubits.

  - Ruido

  - Coherencia

Trabajos futuros:

- Cantidad reducida de qubits.

  Para mejorar este problema, investigaré sobre las técnicas de compresión de datos, y así reducir la cantidad de información necesaria para representar un número grande, lo que permite trabajar con él, utilizando un número reducido de qubits

- El ruido.

  Para mejorar este problema, investigaré los diferentes enfoques como la corrección de errores y la utilización de técnicas de reducción de ruido en los circuitos cuánticos.