UNIVERSIDAD NACIONAL DE SAN AGUSTÍN DE AREQUIPA

FACULTAD DE PRODUCCIÓN Y SERVICIOS
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

SEGURIDAD INFORMATICA

INVESTIGACION FORMATIVA 2.1

INTEGRANTES:

- Cozco Mauri Yoset

DOCENTE: LUCY ANGELA DELGADO BARRA

AREQUIPA – PERÚ
2023

Los procesadores cuánticos y su uso en la criptografía

I. Procesadores Cuánticos:

Los procesadores cuánticos son dispositivos que utilizan qubits para realizar cálculos y procesar información de manera más eficiente que los computadores clásicos, que utilizan bits. Los qubits son partículas subatómicas que pueden existir en múltiples estados simultáneamente, gracias al fenómeno de superposición cuántica, lo que permite realizar cálculos de manera paralela y resolver problemas complejos de forma más rápida.

Los procesadores cuánticos se implementan mediante diferentes enfoques, como los basados en superconductores, trampas de iones, fotones y topología.

II. Modelos de Procesadores Cuánticos:

Algunos modelos de procesadores cuánticos incluyen el modelo de circuitos cuánticos, el modelo adiabático y el modelo de computación cuántica topológica. Cada modelo tiene características y aplicaciones específicas, y se encuentran en diferentes etapas de desarrollo y madurez tecnológica.

Ejemplos de procesadores cuánticos son:

1. Modelo de circuitos cuánticos: IBM Q System One
   - Utiliza qubits para realizar operaciones.
2. Modelo adiabático: D-Wave 2000Q
   - Utiliza un enfoque diferente al modelo de circuitos cuánticos y se basa en la ley de conservación de la energía.
3. Modelo de computación cuántica topológica: Microsoft's Station Q
   - Utiliza qubits topológicos para realizar operaciones.

Cada uno de estos modelos tiene sus propias características y enfoques específicos para la implementación de procesadores cuánticos. Estos ejemplos representan algunos de los avances más destacados en el campo de los procesadores cuánticos, demostrando la diversidad de enfoques en la construcción de estas tecnologías.

III. Empresas Influyentes en Procesadores Cuánticos:

IBM, Google, Microsoft, Intel, D-Wave Systems y Rigetti Computing son algunas de las empresas líderes en la investigación y desarrollo de procesadores cuánticos. Cada empresa ha logrado avances significativos en la construcción de procesadores cuánticos de mayor escala y menor error cuántico, aunque todavía se encuentran en una fase experimental y no están disponibles comercialmente a gran escala.

IV. Aplicación de Procesadores Cuánticos en Criptografía:

1. Factorización de números enteros:

Los procesadores cuánticos pueden factorizar grandes números en tiempo polinómico utilizando el algoritmo de Shor, lo que amenaza los sistemas criptográficos basados en la factorización, como RSA.

2. Búsqueda en bases de datos:

Los algoritmos cuánticos, como el algoritmo de Grover, pueden realizar búsquedas en bases de datos no estructuradas de manera más eficiente que los algoritmos clásicos, lo que compromete la seguridad de ciertos sistemas de encriptación basados en la dificultad de la búsqueda.

3. Criptoanálisis de clave pública:

Los procesadores cuánticos pueden descomponer rápidamente algoritmos de clave pública, como el algoritmo de Shor mencionado anteriormente, lo que pone en riesgo sistemas como el cifrado de curva elíptica y el cifrado de retícula.

4. Generación de claves seguras:

Los procesadores cuánticos pueden generar claves criptográficas seguras mediante el uso de generadores de números aleatorios cuánticos, basados en propiedades intrínsecas de la mecánica cuántica, como el entrelazamiento cuántico.

5. Protocolos cuánticos seguros:

Los procesadores cuánticos permiten la implementación de protocolos de comunicación seguros basados en criptografía cuántica, como la distribución cuántica de claves (QKD, por sus siglas en inglés) y la teletransportación cuántica, que garantizan la seguridad incluso frente a ataques de computadoras cuánticas.

En resumen, los procesadores cuánticos representan una tecnología prometedora con implicaciones significativas en el campo de la criptografía, tanto en términos de fortalecer la seguridad como de romper algoritmos criptográficos existentes. Es fundamental seguir investigando y desarrollando tecnologías y criptografía post-cuánticas para garantizar la seguridad de la información en el futuro.

La ciberseguridad basada en Inteligencia artificial

1. Plataformas: IBM Watson for Cybersecurity, Darktrace y Cylance utilizan inteligencia artificial para abordar amenazas cibernéticas, con enfoques distintos en análisis de datos, sistema inmunológico humano y aprendizaje profundo.

2. Casos de estudio: Estas soluciones han demostrado éxito en casos reales, previniendo ataques de phishing, ransomware y exploits desconocidos.

3. Desafíos y limitaciones: A pesar de los avances, existen dificultades en la detección de ataques sofisticados y la necesidad de análisis adicionales.

4. Tendencias y avances: Las tendencias actuales incluyen técnicas de análisis de comportamiento avanzadas y la integración con tecnologías emergentes como big data e IoT.

5. Consideraciones éticas y legales: El uso de inteligencia artificial en ciberseguridad plantea consideraciones éticas y legales, como la privacidad de datos y la responsabilidad en su uso.

Bibliografia

[1] A. Sajjad, K. R. Choo y A. Shrestha, "A comprehensive survey of cybersecurity and machine learning," Computers & Security, vol. 88, p. 101632, 2020.

[2] S. Sheng, S. Versteeg y Z. Wang, "Cybersecurity meets artificial intelligence: A review," IEEE Access, vol. 6, pp. 28812-28823, 2018.