Criptografía Cuántica y Post Cuántica en Guatemala

Marzo, 2026

Introducción:

La **criptografía cuántica** utiliza principios físicos (mecánica cuántica) para asegurar la comunicación, requiriendo hardware especial. En cambio, la **criptografía post-cuántica (PQC)** emplea algoritmos matemáticos complejos que se ejecutan en computadoras clásicas actuales, diseñados para ser resistentes a los futuros ataques de ordenadores cuánticos.

Este video explica los conceptos básicos de la criptografía post-cuántica: https://youtu.be/sjXIqEzHAMA

Diferencias clave:

Fundamento: La cuántica se basa en la física (fotónica); la post-cuántica se basa en problemas matemáticos difíciles.

Implementación: La cuántica necesita hardware específico; la post-cuántica funciona en computadoras actuales.

Funcionalidad: La cuántica se centra en la distribución de claves; la post-cuántica es más versátil (cifrado, firma, etc.).

Resistencia: Ambas buscan proteger contra ordenadores cuánticos, pero la PQC es más práctica y escalable hoy.

Criptografía Cuántica y Post-Cuántica: Su Relación con la Inteligencia Artificial

Presentación: https://www.genspark.ai/slides?project_id=5ac27bc5-67f6-4e38-817a-1b53cbee7beb&export_dialog=true

La intersección entre la criptografía cuántica, la criptografía post-cuántica y la inteligencia artificial (IA) representa uno de los campos más fascinantes y estratégicos de la ciberseguridad moderna. Permíteme explorar estos conceptos y sus conexiones.

Mas detalle:

Criptografía Cuántica

La **criptografía cuántica** aprovecha las propiedades de la mecánica cuántica para garantizar la seguridad de las comunicaciones. Su pilar fundamental es la **distribución cuántica de claves (QKD - Quantum Key Distribution)**.

Principios Fundamentales

Principio	Descripción	Implicación para la Seguridad
Superposición	Los qubits pueden existir en múltiples estados simultáneamente	Permite codificación densa de información
Entrelazamiento	Partículas correlacionadas instantáneamente	Detección de intrusos en comunicaciones
No-clonación	Imposibilidad de copiar estados cuánticos desconocidos	Garantiza detección de espionaje

Aplicaciones Prácticas

- **QKD (Quantum Key Distribution)**: Protocolos como BB84 permiten intercambiar claves criptográficas con seguridad teórica absoluta
- **Teletransportación cuántica**: Transferencia de estados cuánticos entre ubicaciones distantes
- **Generación de números aleatorios verdaderos**: Esenciales para criptografía de alta seguridad

Criptografía Post-Cuántica (PQC)

La **criptografía post-cuántica** se refiere a algoritmos criptográficos resistentes a ataques tanto de computadoras clásicas como cuánticas. A diferencia de la criptografía cuántica, no requiere hardware cuántico y puede ejecutarse en dispositivos convencionales.

Amenaza de los Ordenadores Cuánticos

Los algoritmos cuánticos, particularmente el **algoritmo de Shor**, pueden factorizar números enteros y resolver logaritmos discretos en tiempo polinomial, rompiendo:

- RSA
- DSA
- Curvas elípticas (ECC)
- Diffie-Hellman

Algoritmos Post-Cuánticos Estándar (NIST 2024)

El NIST ha estandarizado los primeros algoritmos PQC:

Algoritmo	**Tipo**	**Basado en**	**Uso Principal**
ML-KEM (Kyber)	Cifrado asimétrico	Retículos (Lattices)	Encapsulación de claves
ML-DSA (Dilithium)	Firma digital	Retículos	Autenticación e integridad
SLH-DSA (SPHINCS+)	Firma digital	Hash	Firmas de respaldo conservadoras
FN-DSA (FALCON)	Firma digital	Retículos	Firmas compactas

Intersección con Inteligencia Artificial

La relación entre estos campos y la IA es bidireccional y profunda:

1. IA para Criptografía

Optimización de Algoritmos Criptográficos

- **Búsqueda de parámetros óptimos**: Algoritmos de aprendizaje por refuerzo para encontrar configuraciones seguras y eficientes
- **Análisis de seguridad**: Redes neuronales para detectar patrones de vulnerabilidad en implementaciones criptográficas
- **Generación de pruebas de seguridad**: IA para crear casos de prueba exhaustivos

Detección de Ataques

- Sistemas de IA para identificar intentos de interceptación en canales cuánticos
- Análisis de anomalías en redes QKD

2. Criptografía para IA

Privacidad Preservante en Machine Learning

- **Aprendizaje federado con cifrado homomórfico**: Entrenamiento de modelos sin exponer datos
- **MPC (Multi-Party Computation)**: Entrenamiento colaborativo seguro
- **Zero-Knowledge Proofs**: Verificación de integridad de modelos sin revelar parámetros

Protección de Modelos de IA

- Firmas post-cuánticas para autenticar modelos y prevenir envenenamiento
- Cifrado de modelos propietarios contra extracción

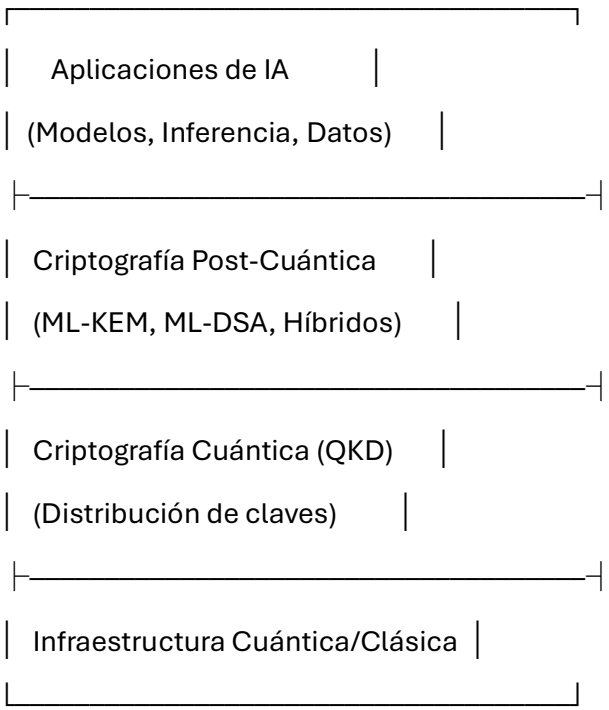
3. Amenazas Cuánticas a la IA

Vulnerabilidad	Descripción	Mitigación
Descifrado de datos de entrenamiento	Datos históricos cifrados con RSA/ECC vulnerables	Migración inmediata a PQC

Vulnerabilidad	Descripción	Mitigación
Manipulación de modelos	Firma de modelos con algoritmos rotos	Adopción de ML-DSA
Ataques a infraestructura	Compromiso de sistemas de IA mediante claves rotas	Arquitectura híbrida clásica-cuántica

Sistemas Híbridos: El Futuro Cercano

La estrategia de seguridad óptima combina múltiples capas:



Casos de Uso Emergentes

1. **Centros de Datos Cuánticos**: Protección de entrenamiento de IA a gran escala
2. **IoT Cuántico-Seguro**: Dispositivos edge con capacidades PQC limitadas
3. **Blockchain Resistente a Cuántica**: Contratos inteligentes con firmas post-cuánticas
4. **Comunicaciones Gubernamentales**: Redes QKD para inteligencia de alto nivel

Línea de Tiempo y Preparación

Año	Hitos Esperados
2024-2025	Estándares NIST PQC publicados, migración inicial
2026-2028	Despliegue masivo de QKD en infraestructura crítica
2029-2035	Ordenadores cuánticos cryptographically relevant
2035+	Ecosistema completamente post-cuántico

Conclusión

La convergencia de criptografía cuántica, post-cuántica e inteligencia artificial está redefiniendo la seguridad digital. Mientras la **criptografía cuántica** ofrece seguridad física basada en leyes naturales, la **criptografía post-cuántica** proporciona soluciones prácticas e inmediatas. La **IA** actúa tanto como beneficiaria (protección de modelos y datos) como habilitadora (optimización y detección de amenazas) de estos sistemas.

La transición hacia un mundo post-cuántico no es opcional: es una necesidad estratégica para proteger tanto la información actual como la futura generada por sistemas inteligentes.

Videos y presentación:

https://www.dailymotion.com/video/x975c7q

https://youtu.be/-jAcNVoJ8nM?si=1sZY6h_ZQLwGmSD_ post-Quantum

Cryptography: Standards and Progress https://share.google/Yexic5SMRhzqiQh4e

Presentación: https://notebooklm.google.com/notebook/b8b2f705-cfcf-4187-9b40-33149ec7fe77

Google: Google Cloud ofrece soluciones proactivas de **criptografía poscuántica (PQC)** para proteger datos contra futuras amenazas de computadoras cuánticas. Sus servicios incluyen la integración de algoritmos resistentes a cuántica en TLS (Chrome), el uso de implementaciones híbridas para mayor seguridad, y el soporte en Cloud KMS. Google también ha desarrollado el procesador cuántico ***Willow***. Aquí se detallan los servicios y enfoque de Google en esta área:

- **Criptografía Poscuántica (PQC) en Google Cloud:**
    - **Seguridad en el transporte (TLS):** Google Chrome ya implementa el intercambio de claves resistente a la computación cuántica (algoritmos híbridos como X25519Kyber768) para proteger el tráfico de usuario.
    - **Cloud KMS (Key Management Service):** Google trabaja para que su servicio de administración de claves sea "seguro para la computación cuántica" (quantum-safe), apoyando la migración de algoritmos de los clientes.
    - **Implementaciones Híbridas:** Google combina algoritmos clásicos (como ECDH) con algoritmos post cuánticos para asegurar que la seguridad no disminuya durante la transición.
    - **Algoritmos Verificados:** Colaboran para verificar formalmente los algoritmos PQC aprobados por el NIST.
- **Infraestructura y Hardware Cuántico:**
    - **Chip Willow:** Presentado como su chip cuántico de última generación (105 cúbits) con capacidades mejoradas de corrección de errores, fundamental para la investigación en seguridad.
    - **Cloud HSM:** Módulos de seguridad de hardware certificados (FIPS 140-2 Nivel 3) para alojar claves de encriptado.
- **Enfoque de Seguridad:**
    - **Protección de datos:** Los servicios de seguridad de Google buscan proteger la información confidencial, tanto en reposo como en tránsito, contra futuros ataques de descifrado por computadoras cuánticas.
    - **Asesoramiento:** Google proporciona pautas y recursos para ayudar a las organizaciones a migrar sus sistemas a la nueva generación de criptografía.

IBM (GBM):

IBM ofrece servicios de PQC en Guatemala:

Criptografía Post-Cuántica (PQC) bajo el ecosistema de **IBM Quantum Safe** para ayudar a las organizaciones en Guatemala a migrar sus sistemas y proteger sus datos ante la futura amenaza de la computación cuántica.

Servicios y Herramientas Disponibles

- **IBM Quantum Safe Transformation Services:** Servicios de consultoría guiada por expertos para diseñar una hoja de ruta de migración a algoritmos resistentes a ataques cuánticos.
- **IBM Quantum Safe Advisor:** Una herramienta que permite visualizar el inventario criptográfico de la empresa, identificar vulnerabilidades y priorizar riesgos en entornos híbridos.
- **Sistemas con PQC Nativa:** Hardware como el **IBM z16** e **IBM LinuxONE** ya integran algoritmos estándar por el NIST (como ML-KEM) para proteger transacciones y firmas digitales desde el nivel de infraestructura.
- **Automatización de Migración:** Uso de plataformas como el *Quantum Safe Migration Orchestrator (QSMO)* para automatizar la actualización de protocolos en toda la organización.
- **IBM Cloud Support:** Para temas técnicos sobre la IBM Quantum Platform, los casos se gestionan a través del centro de soporte de IBM Cloud seleccionando el tópico "Qiskit Runtime".

Temas adicionales:

Acceso a Computador Cuántico en Barcelona para Guatemala: https://www.facebook.com/watch/?v=2400997996932345 o https://www.youtube.com/watch?v=fe8TD9V-e6s

Agradecimiento:

Este documento fue posible gracias a la colaboración de miembros de los grupos de trabajo de colaboradores del Observatorio de Tecnología de Guatemala.

Se trata de un ejercicio de redacción colectivo. Se define como “crowdsourcing” que es el acto de recopilar servicios, ideas o contenido a través de las contribuciones de un gran grupo de personas. Se trata de una nueva forma de conectarse con personas dispuestas a colaborar y en muchos casos se usa consultas a inteligencia artificial pero debidamente revisadas y adecuadas al contexto del evento.

Especial agradecimiento al **Ing. Luis Felipe Figueroa de ABBA Cyberdata** por los escenarios básicos acá presentados y que fueron revisados por el grupo de trabajo del evento que agrego, reviso y sugirió contenido que incluye a:

Empresas y expertos de IA y Ciberseguridad, Mindef, Comisión de seguridad del Congreso, SIT/MICIVI, Mingob, Gobierno electrónico, 3 Bigtechs internacionales, 3 organismos internacionales que están viendo el tema, Senacyt, 2 cámaras empresariales privadas, sector financiero y el Observatorio de Tecnología

Observatorio de Tecnologia:

· Que es el observatorio de tecnología: Es una plataforma de apoyo a la transferencia de tecnología, la innovación y el emprendimiento desde la vigilancia tecnológica

· Qué entendemos por observatorio de tecnología: Un observatorio de tecnología es una plataforma de apoyo a la transferencia de tecnología, la innovación y el emprendimiento desde la vigilancia tecnológica

· Qué entendemos por vigilancia tecnológica: Vigilancia tecnológica: Identificación, evaluación y uso de señales débiles para reconocer y advertir en una fase temprana, tecnologías emergentes, discontinuidades tecnológicas (innovaciones disruptivas o rupturistas), oportunidades y amenazas.

· Qué entendemos por tecnología: La tecnología es el conjunto de saberes, conocimientos, experiencias, habilidades y técnicas a través de las cuales nosotros los seres humanos cambiamos, transformamos y utilizamos nuestro entorno con el objetivo de crear herramientas, máquinas, productos y servicios que satisfagan nuestras necesidades y deseos.

Para cualquier consulta o comentario adicional, le invitamos a visitar los foros del Observatorio de Tecnología de Guatemala: https://observatorioca.tech/ o escribir a maria@zaghi.co