Germán Granados
geragran@espol.edu.ec
FIEC

Washintong Velasquez
wavelasq@espol.edu.ec
FIEC

Ricardo Cajo
rcajo@espol.edu.ec
FIEC

María Alvarez
aalvare@espol.edu.ec
FIEC

Quantum Key Distribution in Multiple Fiber Networks and Its Application in Urban Communications: A Comprehensive Review

PROBLEMA

- Los sistemas criptográficos clásicos (RSA, AES) son vulnerables a computación cuántica (Shor, Grover).
- Aumento del 300 % en ciberataques a infraestructura urbana (2020–2024).
- Necesidad urgente de soluciones informacionalmente seguras, no solo computacionalmente resistentes.

OBJETIVO GENERAL

Evaluar la viabilidad técnica y operativa de la QKD en redes urbanas reales, integrando protocolos avanzados (BB84, TF-QKD, DI-QKD) en infraestructura existente (fibra multicore, coexistencia con señales clásicas).

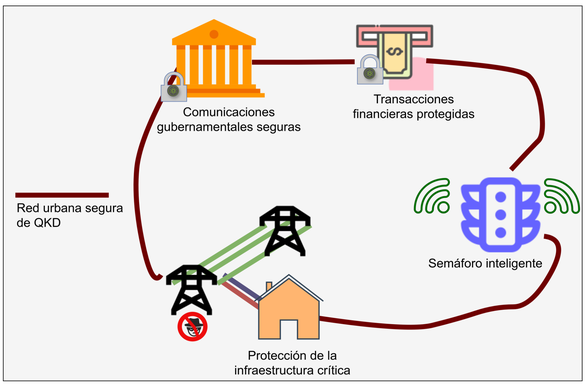

Figura 4. Aplicaciones de la QKD en las comunicaciones urbanas y las ciudades inteligentes

PROPUESTA

Enfoque mixto:

- Revisión sistemática (PRISMA) de 120+ estudios.
- Análisis comparativo de protocolos y medios (MCF, fibra estándar, espacio libre).
- Evaluación en redes reales: Red de 46 nodos (Hefei) y Cambridge Quantum Network.

RESULTADOS

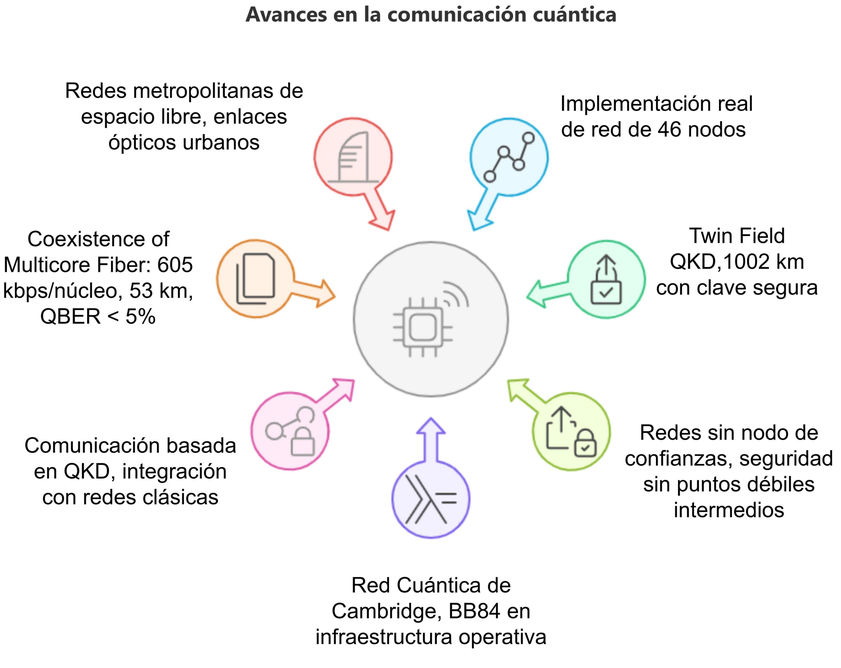

Figura 2. Avances en la distribución cuántica de claves (QKD).

CONCLUSIONES

- QKD ofrece seguridad basada en física, no en complejidad computacional.
- BB84 + MCF es viable hoy para redes metropolitanas densas.
- TF-QKD permite enlaces inter-ciudad sin repetidores confiables.
- DI-QKD es prometedor para infraestructura crítica, aunque con tasas bajas.
- Enfoque híbrido (QKD + PQC) es la estrategia más realista para ciudades inteligentes.

🔗 **Artículo completo disponible en IEEE Xplore**