# ExQNet (Extremadura Quantum Network): Infraestructura de comunicaciones cuánticas fiable y segura para Extremadura

**Investigadores:**

- Daniel Talaván y Juan Manuel Murillo. Fundación COMPUTAEX.

Idioma Sin definir

**Descripción:**
El proyecto ExQNet (Extremadura Quantum Network) se ha centrado en el diseño, planificación, especificación y evaluación de una red de comunicaciones cuántica para la interconexión de infraestructuras críticas para la futura prestación de conexiones fiables y seguras usando software cuántico. Buscando la sostenibilidad económica, se ha analizado y evaluado la creación de la base de la ExQNet sobre la infraestructura de la actual RCT (Red Científico Tecnológica), con las fibras ópticas necesarias que permitan dotar la infraestructura mínima para la migración de las actuales redes de conmutación de paquetes (bits) a las comunicaciones cuánticas (qubits) que sienten la base de la futura Internet cuántica. Se persigue así la posibilidad de interconectar CPDs, supercomputadores, hospitales, centros tecnológicos, institutos de investigación, universidades, empresas e infraestructuras críticas para la seguridad regional y nacional, que éstas puedan ser aprovechadas para resolver las limitaciones actuales y sus necesidades futuras.

También ha sido objeto de este proyecto investigar la posibilidad de evaluar el uso de repetidores cuánticos que permitan extender el alcance y poder abarcar una red regional de área extensa como ExQNet que, a su vez, interconecte con otras redes regionales, nacionales e internacionales, ya sea mediante repetidores cuánticos, o mediante conexiones satelitales. Se ha elaborado un testbed sobre el que investigar y experimentar todos los avances que están por venir en el ámbito de las comunicaciones cuánticas.

**Objetivos alcanzados:**
Se han publicado tres artículos, los cuales han dado lugar a una nueva línea de investigación en CénitS-COMPUTAEX con un potencial realmente significativo que ha permitido profundizar en nuevos conocimientos, impulsando la innovación y el desarrollo en el ámbito de la computación cuántica, y permitiendo, a su vez, difundir nuevos resultados en publicaciones de impacto de ámbito internacional.

Respecto a los resultados científicos, se ha conseguido desarrollar dos algoritmos clásicos para la generación automática de oráculos, uno que implementa la operación ‘menor que’ y otro la operación ‘múltiplos de’. En base a la experiencia adquirida desarrollando estos algoritmos, se han propuesto unas directrices para la construcción de oráculos cuánticos reutilizables.

En el caso del oráculo menor-que, se ha presentado un algoritmo clásico capaz de construir un circuito de oráculo de marcado de fase que realiza una operación de menor-que. Para ejemplificar su funcionalidad, se han realizado algunos experimentos tanto en simulaciones como en hardware cuántico real. Se ha realizado un estudio sobre la eficiencia, centrándose en el número de qubits y la profundidad. Se ha demostrado que no se requieren qubits ancilla. También se ha demostrado que la profundidad de esta implementación del oráculo es siempre menor que la generada por los métodos automáticos de Qiskit. Esta diferencia de profundidad es lo suficientemente significativa como para que nuestro método supere al método UnitaryGate en hardware cuántico real.

Respecto a las directrices sobre reutilización, se han propuesto dos implementaciones diferentes de un oráculo de rango de enteros construido reutilizando dos oráculos diferentes más sencillos, el oráculo de menor-que y el oráculo de suma. Esto se hace para ejemplificar la reutilización de oráculos. Se ha mostrado la funcionalidad de ambas implementaciones con el mismo ejemplo. Se ha realizado un estudio sobre la profundidad de ambas implementaciones. Se muestra claramente una mejora en la profundidad con una de las implementaciones. Además, se han presentado varias pautas para hacer oráculos reutilizables tomando como ejemplo el oráculo de rango de enteros, incluyendo las ideas que inspiran el oráculo, la función que crea el oráculo y el propio oráculo.

Finalmente, se ha presentado un método para construir un oráculo eficiente para marcar en fase múltiplos de un número dado. Se han mostrado las ideas teóricas que subyacen a esta construcción y cómo construir el circuito cuántico. Además, se ha realizado un análisis teórico de la complejidad tanto de los cálculos clásicos necesarios para construir el oráculo como del propio oráculo. El resultado de este análisis es que el método propuesto conduce a una aceleración exponencial sobre el clásico. Por último, se han explorado otras funcionalidades. Mediante ejemplos y simulaciones se ha mostrado cómo componer el oráculo ‘múltiplos de’ con otros oráculos y también cómo se pueden obtener números con otras propiedades.

**Publicaciones y congresos:**

- Sanchez-Rivero, J., Talaván, D., Garcia-Alonso, J., Ruiz-Cortés, A., & Murillo, J. M. (2023). Automatic Generation of an Efficient Less-Than Oracle for Quantum Amplitude Amplification. arXiv preprint arXiv:2303.07120.
- Sanchez-Rivero, J., Talaván, D., Garcia-Alonso, J., Ruiz-Cortés, A., & Murillo, J. M. (2023). Some Initial Guidelines for Building Reusable Quantum Oracles. arXiv preprint arXiv:2303.14959.
- Sanchez-Rivero, J., Talaván, D., Garcia-Alonso, J., Ruiz-Cortés, A., & Murillo, J. M. (2023). Operating with Quantum Integers: an Efficient'Multiples of'Oracle. arXiv preprint arXiv:2304.04440.

**Fuentes de financiación:**
Proyecto financiado por la Consejería de Educación y Empleo de la Junta de Extremadura, a través del Programa PAI (Personal

de Apoyo a la Investigación). Ayudas destinadas al fomento de la contratación de personal de apoyo a la investigación en la Comunidad Autónoma de Extremadura, correspondiente al ejercicio 2021 (Resolución de 22 de julio de 2021).




**URL del envío:**https://www.cenits.es/proyectos/exqnet-extremadura-quantum-network-infraestructura-comunicaciones-cuanticas-fiable-segura