El Paradigma de la Computación Cuántica: Estrategias de Desarrollo, Seguridad y Formación ante la Próxima Revolución Tecnológica

Leonardo Corbalán, Pablo Thomas, {corbalan, pthomas}@lidi.info.unlp.edu.ar
Juan Fernández Sosa, Luciano Marrero, {jfernandez, lmarrero}@lidi.info.unlp.edu.ar
Verena Olsowy, Fernando Tesone, Patricia Pesado. {volsowy, ftesone, ppesado}@lidi.info.unlp.edu.ar

Contexto

Esta línea de Investigación forma parte del Proyecto “Diseño, desarrollo y evaluación de sistemas en escenarios híbridos para áreas clave de la sociedad actual: educación, ciudades inteligentes y gobernanza digital” del Instituto de Investigación en Informática LIDI de la Facultad de Informática, acreditado por el Ministerio de Educación de la Nación. Hay cooperación con Universidades de Argentina y se está trabajando con Universidades de Europa y Latinoamérica.

Líneas de Investigación y Desarrollo

Ingeniería de Software Cuántico (QSE): Metodologías para el ciclo de vida, técnicas de *testing/debugging* y optimización de circuitos en entornos de simulación.

Seguridad y Criptografía Post-Cuántica: Impacto en Blockchain y sistemas distribuidos. Desarrollo de marcos conceptuales y arquitecturas para la transición criptográfica.

Educación en Computación Cuántica: Evaluación de estrategias pedagógicas y materiales interactivos para optimizar la curva de aprendizaje de la programación cuántica en carreras de informática.

Algoritmos Híbridos Clásicos-Cuánticos: Orquestación de sistemas CPU/GPU con unidades cuánticas (QPU) simuladas. Investigación en algoritmos variacionales.

Arquitecturas para Laboratorios Cuánticos Remotos: Diseño de software y middleware para la gestión de cuántica como servicio (QaaS).

Mitigación de Errores (NISQ): Experimentación en procesadores RMN para implementar códigos de corrección (bit-flip) y técnicas de reducción de ruido.

Resultados Obtenidos y Esperados

Se realizó un relevamiento taxonómico de lenguajes, SDKs y simuladores para educación.

Se presentó un modelo conceptual de tres fases para la migración a criptografía post-cuántica y cuántica.

Se espera consolidar un núcleo de investigación y docencia en el área. Se prevé la creación de una suite de Jupyter Notebooks y guías interactivas para la enseñanza de algoritmos cuánticos fundamentales.

Se plantea avanzar en la verificación y validación de software cuántico mediante el uso de aserciones y pruebas metamórficas en simuladores.

Se pretende alcanzar conclusiones relevantes sobre el rendimiento de criptografía post-cuántica (PQC) a través de la medición de latencia y rendimiento de firmas digitales PQC en redes distribuidas emuladas.

Se plantea simular protocolos de comunicación segura, analizando el protocolo BB84 bajo condiciones de ruido con el fin de establecer umbrales de seguridad en la distribución de claves cuánticas (QKD).

Se prevé experimentar en procesadores de RMN con el objetivo de caracterizar el ruido físico y la decoherencia en dispositivos de escala intermedia (NISQ), con miras a optimizar la fidelidad de los resultados.

Formación de Recursos Humanos

Los integrantes de esta línea de investigación dirigen Tesinas de Grado y Tesis de Postgrado en la Facultad de Informática, y Becarios III-LIDI en temas relacionados con este proyecto. Además, participan en el dictado de asignaturas/cursos de grado y postgrado de la Facultad de Informática de la UNLP.