Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Vicepresidencia Primera del Gobierno · Ministerio de Asuntos Económicos y Transformación Digital · Secretaría de Estado de Digitalización e Inteligencia Artificial
Plan de Recuperación, Transformación y Resiliencia · España | digital 2026
incibe_ Instituto Nacional de Ciberseguridad

Daniel Guerrero Villanueva
presenta el resumen del trabajo

Infraestructuras de tecnologías cuánticas para la investigación en ciberseguridad

Natalia Costas Lago y Andrés Gomez Tato
Actas VIII JNIC, atlanTTic, 171-177, (2023).

25 de marzo de 2024

SERIE DE RESÚMENES EN ESPAÑOL

Palabras clave: Algoritmos post-cuánticos, CESGA, Ciberseguridad, Computación cuánticas, Comunicaciones cuánticas, Infraestructura cuántica, Infraestructuras de investigación, Proyectos de inversión

Introducción

las tecnologías cuánticas representan un avance con el potencial de acelerar el desarrollo económico en prácticamente todos los sectores. Estas tecnologías emergentes podrán ayudar a comprender la estructura y comportamiento de molécuals y materiales, resolver problemas de optimización, mejorar la eficiencia enerética, entre otras.

Sin embargo, las tecnologías cuánticas también plantean amenazas, especialmente en la ciberseguridad. Una vez que existan computadoras cuánticas con suficientes cúbits, podrían comprometerse los algoritmos de cifrado utilizados en los sistemas actuales.

A pesar de estas preocupaciones, las tecnologías cuánticas también ofrecen la posibilidad de mejorar la ciberseguridad de formas que antes no eran posibles, aprovechando fenómenos cuánticos establecidos.

Conscientes de esta evolución, el CESGA ha estado trabajando en el campo de las tecnologáis cuánticas durante más de 7 años y cuenta con un equipo de investigación de 8 personas. Además, está en proceso de desplegar infraestructuras basadas en tecnologías cuánticas para permitir que los investigadores exploren esta área y contribuyan a mejorar la competitividad.

1. El CESGA y su contribución

El CESGA es el centro tecnológico de Galicia que ofrece servicios avanzados de cálculo y comunicaciones para la comunidad científica y académica. Fundado en 1993 por la Xunta de Galicia y el CSIC, su misión es impulsar la investigación y la tecnología mediante recursos de computación y comunicaciones de alta calidad. Adaptándose a las necesidades cambiantes, ahora se centra en desafíos como Big Data, Industria 4.0 e Inteligencia Artificial, utilizando herramientas como la computación de alto rendimiento. Además, está explorando el campo de la computación y las comunicaciones cuánticas para seguir siendo relevante en el futuro.

2. Computación y comunicaciones cuánticas

La computación cuánticas surge en los años 80 a través de propuestas como las de R. Feynman y Y. Manin, junto con contribuciones previas como las de Paul Benioff. Estos conceptos teóricos se desarrollaron durante las décadas de los 80 y 90, dando lugar a algoritmos fundamentales como el algoritmo de factorización de Shor.

El desarrollo práctico de la computación cuántica comenzó entre 1998 y 2000, con la creación de los primeros ordenadores cuánticos experimentales con pocos cúbits. esto premitió la recreación de algunos algoritmos teórico, como el algoritmo de Deutsh o el de Grover.

En 2001, se demostró experimentalmente el algoritmo de Shor, factorizando el número 15. Esta demostración empírica marcó un importante crecimiento en la investigación en este campo.

En 2016, IBM abrió su entorno de experimentación en computación cuántica a través de la nube, proporcionando acceso a prototipos de ordenadores cuánticos a investigadores de todo el mundo. Esta iniciativa democratizó el acceso a la infraestructura cuántica y estimuló el desarrollo software en ese ámbito. Actualmente lidera en este campo con el procesador cuánti-

co más grande conocido, con 433 cúbits.

Sin embargo, los procesadores cuánticos actuales, denominados NISQ(Near Intermediate-Scale Quantum computers), tienen limitaciones importantes, como la corta vida útil de los cúbits, errores en las operaciones y errores de medida. Aunque existen propuestas técnicas para construir una Quantum Processing Unit(QPU). Se prevé que los ordenadores cuánticos serán complementarios a los clásicos, con algoritmos híbridos que combinan operaciones cuánticas y clásicas. Estos sistemas se integrarán con los superordenadores actuales, expandiendo la algoritmia hacia la programación paralela o distribuida.

Las ventajas de la computación cuántica incluyen la supremacía cuántica, la rapidez cuántica, la mejora cuántica y la eficiencia cuántica, lo que genera un gran interés en la investigación en este campo.

El avance de la computación cuántica plantea desafios para la seguridad de las comunicaciones digitales. Una vez que se desarrollen computadores cuánticos lo suficientemente grandes podrían vulnerar muchos de los sistemas criptográficos actuales.

Para garantizar la seguridad en un entorno cuántico, existen dos enfoques principales: los sistemas de distribución de clave cuántica (QKD), que utilizan principios de la cuántica para asegurar las comunicaciones y los algoritmos postcuánticos que son resistentes a los ataques desde ordenadores cuánticos y clásicos.

Los sistemas QKD permiten a las partes involucradas generar claves seguras utilizando principios cuánticos como la no clonación de la información para detectar intrusiones. Sin embargo, aunque teóricamente estos sistemas porporcionan una seguridad completa, la implementación física puede introducir vulnerabilidades.

Existen diferentes protocolos de QKD, como los de variable discreta, basados en el entrelazamiento de partículas, los protocolos independientes del dispositivo, donde la seguridad no depende de la confiabilidad de los dispositivos utilizados y los protocolos de variable continua en los que la información se condifica en la cuadratura de sus campos electromagnéticos. No obstante, el despliegue de redes QKD está limitado especialmente por la falta de repetidores cuánticos.

Para superar estas limitaciones, se están explorando arquitecturas de redes multisalto que combinen canales cuánticos y clásicos.

3. Amenazas de la computación cuántica a la ciberseguridad

Aunque es dificil prever cuándo se desarrollará un computador cuántico y amenace los sistemas criptográficos actuales,el NIST sugiere que podría ocurrir hacia 2030 y recomienda evolucionar hacia algoritmos post-cuánticos no vulnerables.

La estrategia de ciberseguridad de la UE destaca la importancia de la computación cuántica y el cifrado como tecnologías clave para desarrollar capacidades operativas para prevenir y responder ataques cibernéticos, también trabajar con socios internacionales para garantizar seguridad y estabilidad en el ciberespacio.

4. El Polo de Tecnologías Cuánticas de Galicia

El Polo de Tecnologías Cuánticas de Galicia, establecido en 2021, tiene como objetivo impulsar las tecnologías cuánticas y comunicacione. Este esfuerzo involucra a instituciones académicas e industriales, lideradas por el CESGA en computación cuántica y el VQCC en comunicaciones cuánticas.

El polo se basa en cuatro pilares: la universidad, los centros de investigación y desarrollo, las empresas y la sociedad. Se ha planificado un plan de inversiones de hasta 154 millones de euros para infraestructura de computación cuántica y comunicaciones cuánticas.Esto incluye la adquisición y despliegue de un computador cuántico, simuladores cuánticos, generadores de números aleatorios, así como laboratorios de experimentación en comunicaciones cuánticas y un enlace seguro de comunicaciones cuánticas entre Vigo y Santiago de Compostela.

El CESGA adjudicó un contrato para la adquisición de infraestructura de computación cuántica, incluyendo un computador cuántico de 32 cúbits. Además se ha adquirido un generador cuántico de números aleatorios y se están desplegando laboratorios de experimentación en comunicaciones cuánticas.

A nivel nacional se ha creado el Plan Complementario de Comunicaciones Cuánticas con el objetivo de investigar y desplegar infraestructura de comunicaciones cuánticas para conectar toda Europa.

5. Conclusiones

En este artículo se ha descrito la relevancia de las tecnologías cuánticas, por la disrupción que presentan en muchos ámbitos de conocimiento y, específicamente en el ámbito de la ciberseguridad. CESGA, bajo el amparo de los diversos programas de financiación públicos, está en proceso de despliegue de infraestructura de computación y comunicaciones cuánticas de gran relevancia para la comunidad investigadora. También cuenta con experiencia de años de trabajo en el ámbito de la investigación en tecnologías cuánticas. Las entidades públicas y empresas que deseen hacer uso de dichas infraestructuras bien sean en el ámbito gallego o nacional, podrán hacerlo mediante convenios de colaboración o bajo el paraguas de los mecanismos de acceso ya existentes.