La computación cuántica y el DNS

Oficina del Director de Tecnologías de la ICANN

Paul Hoffman
OCTO-031
11 de febrero de 2022

ICANN

ÍNDICE

Este documento forma parte de la serie de documentos de la Oficina del Director de Tecnologías (OCTO) de la ICANN. Consulte la página de publicaciones de la OCTO para ver la lista de documentos que integran la serie. Si tiene preguntas o sugerencias sobre cualquiera de estos documentos, puede enviarlas a octo@icann.org.

Este documento respalda el objetivo estratégico de la ICANN de mejorar la responsabilidad común de preservar la seguridad y estabilidad del Sistema de Nombres de Dominio (DNS) mediante el fortalecimiento de la coordinación de este sistema en asociación con partes interesadas relevantes. Forma parte del objetivo estratégico de la ICANN de fortalecer la seguridad del DNS y del Sistema de Servidores Raíz (RSS) del DNS.

Resumen ejecutivo

En los últimos años, las computadoras cuánticas han atraído la atención del sector de la seguridad debido a la posibilidad de que sean capaces de debilitar los algoritmos criptográficos que se utilizan en la actualidad. Hoy en día no existen computadoras cuánticas lo suficientemente potentes como para hacerlo, pero a medida que la tecnología mejore poco a poco, puede llegar un día en que este nuevo tipo de computadoras pueda quebrantar sin dificultad algunos de los algoritmos que se utilizan actualmente. Sin embargo, como la tecnología de la computación cuántica es todavía nueva, y la construcción y el funcionamiento de las computadoras cuánticas son increíblemente costosos, es difícil predecir en qué momento del futuro cercano podría llegar ese día.

Actualmente, se están estandarizando nuevos algoritmos que se suponen impermeables a las computadoras cuánticas. Este artículo examina trabajos realizados recientemente, en los cuales se presentan estimaciones más aproximadas sobre el momento en que la comunidad del Sistema de Nombres de Dominio (DNS) necesita considerar el cambio de los algoritmos criptográficos actuales a otros nuevos.

1 Introducción

Algunos algoritmos de la criptografía moderna dependen de la dificultad de ciertos problemas matemáticos cuya resolución requiere enormes cantidades de tiempo. Las computadoras cuánticas podrían ser capaces de resolver estos problemas mucho más rápido, lo cual debilitaría las garantías que ofrecen esos algoritmos. Las computadoras basadas en principios cuánticos son fundamentalmente diferentes de las computadoras que se han utilizado ampliamente en los últimos 70 años. El procesamiento de datos en las computadoras cuánticas se basa en bits cuánticos, denominados *cúbits*, en lugar de los bits binarios que utilizan todas las computadoras hoy en día.

Si se pudieran construir computadoras cuánticas a gran escala, podrían resolver algunos problemas que son imposibles con la tecnología informática actual porque las computadoras cuánticas pueden gestionar muchos procesos complejos al mismo tiempo. Aunque las computadoras de la actualidad, denominadas *computadoras clásicas*, pueden manejar procesos paralelos, las computadoras cuánticas pueden hacerlo utilizando conexiones más estrechas entre las partes de los datos que se analizan.

Los conceptos en los que se basan las computadoras cuánticas se han teorizado durante casi 50 años, pero es extraordinariamente difícil construir incluso computadoras cuánticas muy pequeñas. La información de los cúbits es bastante frágil, por lo que deben estar completamente aisladas del entorno externo y a temperaturas cercanas a los cero grados Kelvin durante los cálculos. Para ello se necesita mucha maquinaria y espacio físico. Sin embargo, los cúbits también son muy propensos a errores durante el procesamiento. Una computadora cuántica necesita cientos o miles de cúbits refrigerados adicionales para corregir los errores de cada cúbit en el cálculo, y construir una computadora cuántica con millones de cúbits puede ser imposible debido a los requisitos de refrigeración y comunicación.