Ibermática

Ibermática innova en computación cuántica para hacer frente a la nueva generación de ciberataques

La computación cuántica tendrá un impacto tan profundo en la ciberseguridad que cambiará las reglas del juego

Juan Ignacio Sanz
Director General y Consejero Delegado de Ibermática

La computación cuántica es una de las tecnologías más punteras que existen en la actualidad. Gracias a los enormes avances que se han producido durante los últimos años en hardware y software ya ha dejado de ser pura teoría, convirtiéndose en algo real. Es muy prometedora en muchos sectores, como el financiero, salud, cadena de suministros, sector logístico en su ámbito de aplicación en investigación médica, la inteligencia artificial, el pronóstico del tiempo, etc. Pero también representa una amenaza significativa para la ciberseguridad, que requiere un cambio en la forma en que ciframos nuestros datos.

A pesar de que las computadoras cuánticas técnicamente no tienen, todavía, el poder de romper la mayoría de nuestras formas actuales de cifrado, debemos adelantarnos a la amenaza y encontrar soluciones a prueba de computación cuántica ahora. Si esperamos hasta que esas poderosas computadoras cuánticas comiencen a romper nuestro cifrado, será demasiado tarde.

Otra razón para actuar ahora es la amenaza del robo de datos, independientemente de cuándo las computadoras cuánticas estén disponibles comercialmente, porque los actores nefastos que roban y comercializan con datos están ya sustrayendo información y aferrándose a ella hasta que puedan tener en sus manos una computadora cuántica para descifrarla. En ese momento, los datos ya se habrán visto comprometidos. La única forma de garantizar la seguridad de la información, en particular la información que debe permanecer segura en el futuro, es salvaguardarla ahora con una solución a prueba de cuánticas.

La amenaza a la ciberseguridad

Las computadoras cuánticas podrán resolver problemas que son demasiado complejos para las computadoras clásicas. Esto incluye resolver los algoritmos que hay detrás de las claves de cifrado que protegen nuestros datos y la infraestructura de Internet. Gran parte del cifrado actual se basa en fórmulas matemáticas, pero piense en dos números grandes, por ejemplo, y multiplíquelos. Es fácil encontrar el resultado, pero muy difícil comenzar con ese número grande y factorizarlo en sus dos números primos. Una computadora cuántica, sin embargo, puede factorizar fácilmente esos números y romper el código.

«Estamos investigando una nueva generación de tecnologías cuánticas que se integren en el ecosistema industrial»

El cifrado RSA es uno de los sistemas de cifrado asimétricos más exitosos de la actualidad. Utilizado para enviar datos confidenciales a través de Internet, se basa en números de 2048 bits. Los expertos estiman que una computadora cuántica necesitaría una capacidad de 70 millones de cúbits (bits cuánticos) para romper ese cifrado. Teniendo en cuenta que la computadora cuántica más grande de la actualidad es la de 53 cúbits de IBM, podría pasar mucho tiempo antes de lograrlo. Sin embargo, a medida que el ritmo de la investigación cuántica continúa acelerándose, no se puede descartar el desarrollo de una computadora de este tipo en los próximos 3-5 años.

Hay muchas preguntas que rodean a la computación cuántica y los científicos continúan trabajando para responderlas. Sin embargo, cuando se trata de su impacto en la ciberseguridad, una cosa es innegable: representará una amenaza contra nuestras formas actuales de cifrado. Para mitigar esa amenaza, debemos cambiar la forma en que mantenemos nuestros datos seguros y comenzar a hacerlo ahora. Y para ello, hay que acercarse a la amenaza cuántica como lo hacemos con otras vulnerabilidades: mediante la implementación de un enfoque de defensa en profundidad, caracterizado por múltiples capas de protección cuántica segura.

Computación cuántica en Ibermática

Las organizaciones de seguridad avanzada entienden esta necesidad de agilidad criptográfica y están buscando soluciones para hacer que su cifrado sea cuántico seguro ahora y esté listo para las amenazas del mañana. Ibermática, a través de su Instituto de Innovación (i3B), lleva más de tres años embarcada en el desarrollo de proyectos en computación cuántica, principalmente en el ámbito industrial y en la ciberseguridad. No es casualidad. La computación cuántica tiene un enfoque práctico directo en aquellos ambientes en los que la variabilidad de escenarios es ingente, y la posibilidad de evaluar las diferentes soluciones sería un problema complejo aplicando modelos clásicos de búsqueda o incluso de inteligencia artificial.

En estos casos (proyectos de optimización, simulación y machine learning en tiempo real) la computación cuántica, gracias a sus propiedades basadas en la superposición de estados, entrelazamiento e interferencia, permite con los ordenadores cuánticos actuales una ventaja sobre los algoritmos clásicos, y es ahí donde i3B ya está desarrollando modelos que abordan la optimización de rutas productivas, la detección inmediata de anomalías en ciberseguridad y los primeros esbozos de la aplicación de redes neuronales cuánticas en entornos de aprendizaje online.

La labor de Ibermática está centrada principalmente en desarrollar una base de conocimiento en torno a las tecnologías cuánticas impulsando un ecosistema cuántico nacional, así como en investigar una nueva generación de tecnologías cuánticas que se integren en el ecosistema industrial, buscando casos de uso de aplicación en nuestros clientes y posicionar las tecnologías cuánticas y sus aplicaciones en las agendas y programas de I+D+i.

Estamos convencidos de que en los próximos tres años la computación cuántica va a cambiar el mundo de la ingeniería informática y de la inteligencia artificial, tal y como la conocemos, y nos vemos en la obligación de estar preparados e ir también preparando a nuestros clientes para esta disrupción tecnológica, tanto a nivel algorítmico como metodológico y generador de talento. Por eso ya estamos trabajando en la confección de una estrategia nacional en computación cuántica, dentro de grupos de trabajo a nivel estatal, como el grupo cuántico de Ametic, entre otros, y por otro lado, a través de los laboratorios de innovación propios, comenzando a implantar casos de uso sobre tecnología cuántica en nuestros clientes más importantes.

Al alcance de las empresas

La computación cuántica es una tecnología que se acerca rápidamente al ámbito de la ciberseguridad. Las empresas deben entrar en acción de inmediato y analizar las diferentes formas de implementar la cuántica para mejorar la seguridad y evitar que los intrusos roben datos confidenciales. Las empresas deben comenzar a pensar estratégicamente sobre los riesgos a largo plazo y los beneficios de la tecnología de computación cuántica y participar de manera seria para implementar las mejores prácticas de ciberseguridad. Algunas tecnologías cuánticas están ya disponibles para su implementación industrial (principalmente seguridad, optimización y comunicaciones). Las compañías que den un paso adelante, innovando y preparándose para esta revolución en la computación cuántica, podrán capitalizar las oportunidades que esta tecnología traerá al mercado.