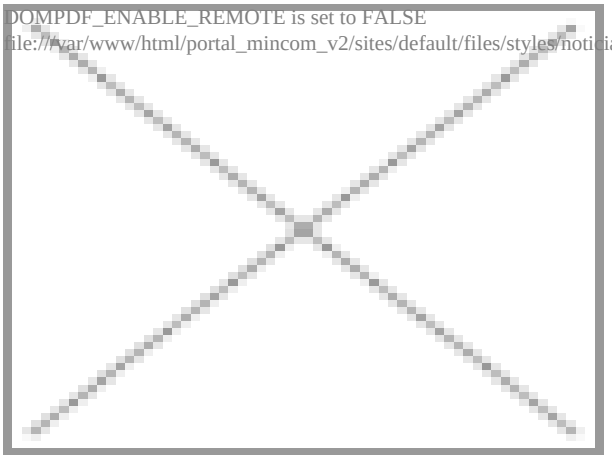
DOMPDF_ENABLE_REMOTE is set to FALSE
file:///var/www/html/portal_mincom_v2/sites/all/themes/mincom/logo.png

DOMPDF_ENABLE_REMOTE is set to FALSE
file:///var/www/html/portal_mincom_v2/sites/default/files/styles/noticias/public/computacion-cuantica_2.jpg


Fuente:
computerworld

Una nueva investigación ha revelado la plena viabilidad de una novedosa red de distribución de claves cuánticas (QKD) para áreas metropolitanas que es resistente a los ataques de la computación cuántica.

Según JPMorgan Chase, Toshiba y Ciena, la red QKD recién desarrollada admite un cifrado de 800 Gbps en condiciones ambientales reales y puede detectar y defenderse al instante de las amenazas de tipo cuántico. En una supuesta primicia en el sector, la red también ha demostrado ser capaz de proteger una aplicación de blockchain de misión crítica, según han afirmado las empresas.

La red de distribución de claves cuánticas es "la primera de su clase"

Bajo la dirección del Future Lab for Applied Research and Engineering (FLARE) de JPMorgan Chase y de los equipos de infraestructura de red global, los investigadores de las tres organizaciones colaboraron para lograr los siguientes resultados:

Se multiplexó por primera vez un canal QKD en la misma fibra que los canales ópticos de 800 Gbps de ancho de banda ultra alto y se utilizó para proporcionar claves para el cifrado del flujo de datos.

Se demostró la coexistencia del canal cuántico con dos canales de 800 Gbps y ocho de 100 Gbps para una fibra de 70 km, con una tasa de claves suficiente para soportar hasta 258 canales encriptados AES-256 a una tasa de actualización de claves de 1 clave/seg.

Se demostró el funcionamiento de QKD y de los diez canales de gran ancho de banda para distancias de hasta 100 km.

La infraestructura de red de la prueba de concepto se basó en el sistema QKD multiplexado de Toshiba, fabricado por Toshiba Europe en su sede de Cambridge, Reino Unido, y en la plataforma Waveserver 5 de Ciena, equipada con encriptación de capa óptica de 800 Gbps y API abiertas que se ejecutan sobre la solución fotónica 6500 de Ciena.

La tecnología QKD, un cifrado robusto, la clave para asegurar el futuro de la computación cuántica

A medida que se acerca la era de la computación cuántica, QKD es la única solución que se ha probado matemáticamente para defenderse de un potencial ataque basado en la computación cuántica con garantías de seguridad basadas en las leyes de la física cuántica, dijeron JPMorgan Chase, Toshiba y Ciena.

"Este trabajo llega en un momento importante, ya que seguimos preparándonos para la introducción de ordenadores cuánticos de calidad de producción, que cambiarán el panorama de la seguridad de tecnologías como el blockchain y la criptomoneda en un futuro próximo", comentó Marco Pistoia, distinguido ingeniero y jefe del grupo de investigación FLARE.

En declaraciones a CSO, Pistoia añade: "El éxito de este prototipo demuestra que ahora tenemos un método probado y comprobado para defender la confidencialidad de aplicaciones como el blockchain contra futuros fisgones equipados con tecnología cuántica". Con la tecnología QKD, las organizaciones pueden prepararse para las necesidades de seguridad del futuro y estarán mejor preparadas para asegurar sus aplicaciones contra los riesgos que puedan surgir cuando se alcance la supremacía cuántica, afirma.

Dado que cada día se distribuye más información sensible a través de las redes de fibra óptica, un cifrado robusto es de vital importancia, afirma el CTO de Ciena, Steve Alexander. "A medida que se acerca la era de la computación cuántica, los avances en investigación y desarrollo seguirán garantizando la confidencialidad de los datos críticos mientras viajan por la red".

Disponible en:

https://cso.computerworld.es/tendencias/nueva-red-de-distribucion-de-cla... [1]

Links
[1] https://cso.computerworld.es/tendencias/nueva-red-de-distribucion-de-claves-resistente-a-ataques-cuanticos