NOTA DE PRENSA

LAS TECNOLOGÍAS CUÁNTICAS PUEDEN APLICARSE EN UNA RED ESTÁNDAR DE TELECOMUNICACIONES

Desarrollada con éxito en España una experiencia piloto de criptografía cuántica que combina la transmisión de datos y de claves cuánticas sobre la misma fibra

13.09.2018. España ha experimentado con éxito, por primera vez, una red de criptografía cuántica en redes ópticas comerciales a través de tecnologías basadas en SDN (*Software Defined Networking*), que facilitan la implementación de servicios de red de una manera flexible, dinámica y escalable.

La red usa una infraestructura de fibra proporcionada por Telefónica de España, que conecta tres de sus centrales situadas en el área metropolitana de Madrid. La experiencia se está desarrollando desde el pasado mes de Mayo.

La red integra asimismo equipos de distribución cuántica de claves (CV-QKD) desarrollados por los Laboratorios de Investigación de Huawei en Munich, con la colaboración del Centro de Simulación Computacional (CCS) de la Universidad Politécnica de Madrid, a través del Grupo de Investigación en Información y Computación Cuántica de la Escuela Técnica Superior de Ingenieros Informáticos.

Los módulos de gestión de la red basados en SDN han sido desarrollados por el equipo de Innovación en Tecnologías de Red del GCTIO de Telefónica, y los mecanismos de integración de la criptografía cuántica han sido desarrollados por el CCS con tecnologías SDN y NFV (*Network Function Virtualization*).

La integración de todos estos elementos ha permitido demostrar que las técnicas QKD se pueden aplicar en un entorno de producción real, combinando la transmisión de datos y de claves cuánticas sobre la misma fibra.

También ha comprobado que es posible llevar a cabo la gestión de estos servicios y su uso a través de diferentes aplicaciones. Que toda la experiencia se haya desarrollado sobre una infraestructura en producción y usando los sistemas de comunicaciones desplegados en redes ópticas estándar destaca a su vez la madurez de esta tecnología, que admite conmutación con enlaces de hasta 60Km cada uno.

Esta tecnología es capaz asimismo de más de 20 canales compartiendo la misma fibra y en la misma banda óptica que usa el canal cuántico, lo que le permite transmitir más de 2 Tbps de

datos usando tecnología de comunicaciones estándar de 100 Gbps en redes de área metropolitana.

Solución cuántica de seguridad avanzada

Todas las comunicaciones seguras se basan en el uso de la criptografía, de manera que la información se cifra utilizando una clave que permite que sólo los participantes que la conocen sean capaces de descifrar los mensajes intercambiados entre ellos. Las técnicas actuales de criptografía están basadas en problemas matemáticos que son complejos de resolver. A medida que la capacidad de computación crece, el tiempo de resolución de estos problemas, y por tanto la seguridad de las claves, disminuye.

El tamaño de las claves y la complejidad de los algoritmos de encriptación han tenido que aumentar a medida que la capacidad de cálculo ha ido creciendo. Y estas técnicas pueden quedar completamente obsoletas con la aparición de los ordenadores cuánticos, capaces de aplicar los principios de la Mecánica Cuántica para la resolución de problemas actualmente insolubles, incluyendo el romper las claves generadas por los métodos actuales de criptografía, haciendo inútiles la mayoría de las infraestructuras de seguridad en las comunicaciones.

Las tecnologías cuánticas ofrecen, sin embargo, una solución a la vulnerabilidad de los métodos actuales. Con estas tecnologías es posible aplicar principios cuánticos para intercambiar una clave entre los extremos de un canal de comunicaciones, de manera que esa clave sea segura frente a cualquier ataque, incluyendo los de un ordenador cuántico. La tecnología cuántica hace posible incluso que cualquier intento de ataque sea inmediatamente detectado.

Tecnologías cuánticas

La Distribución Cuántica de Claves es una de estas tecnologías: no sólo soluciona el problema de la amenaza que supone la computación cuántica para los algoritmos criptográficos en uso, sino que además puede proporcionar un nivel de seguridad mucho más alto a cualquier intercambio de datos. QKD requiere de una infraestructura física de fibra óptica de alta calidad, provista por Telefónica de España conectando sus centrales de comunicaciones usadas en el piloto.

La viabilidad de QKD ha sido demostrada hasta ahora en laboratorios y en pruebas de campo controladas (como la que Telefónica y el Grupo de Investigación en Información y Computación Cuántica realizaron en 2009, intercambiando claves a través de un anillo metropolitano de fibra), pero siempre ha habido problemas para poder desplegarla sobre infraestructuras comerciales y para su integración con los mecanismos de operación de estas infraestructuras. Con esta experiencia se ha mostrado como es posible superar estos obstáculos.

En la red se ha utilizado además una nueva tecnología para la distribución cuántica de claves basada en “variables continuas” (CV-QKD), más compatibles con tecnologías clásicas que las

existentes. La combinación de estas tecnologías ha posibilitado una red completa integrada de comunicaciones clásicas y cuánticas.

El despliegue sobre una infraestructura de comunicaciones en producción y usando sistemas de telecomunicaciones estándar que se ha realizado en esta experiencia, es la primera de su clase, demostrando la capacidad de la tecnología para su uso en el mundo real.

Convergencia de redes

"*La capacidad de usar nuevas tecnologías como SDN, diseñadas para incrementar la flexibilidad de la red, junto con nuevas tecnologías de QKD, es lo que nos permite hacer converger las redes clásicas y cuánticas en la infraestructura de fibra óptica existente. Ahora tenemos, por primera vez, la capacidad de desplegar comunicaciones cuánticas de una manera incremental, sin grandes costes de inversión inicial y usando la misma infraestructura*", explica **Vicente Martín**, director del Centro de Simulación Computacional, responsable del equipo de la UPM que ha participado en esta experiencia, y miembro del programa de actividades I+D de la Comunidad de Madrid en Tecnología QUITEMAD+CM.

Momtchil Peev, coordinador del Proyecto de Comunicaciones Cuánticas en los Laboratorios de Huawei en Munich, añade al respecto: "*Los dispositivos de CV-QKD que usamos aquí presentan claras ventajas: no necesitan complejos detectores funcionando a temperatura ultrabaja y pueden reusar componentes de los sistemas de comunicación coherentes clásicos. En lugar de enfocarnos en conseguir nuevos record de rendimiento, nos hemos centrado en desarrollar los interfaces de control y transferencia de claves, demostrando la capacidad de una integración más transparente en las redes modernas*."

María Antonia Crespo, directora de Conectividad y Transporte IP de Telefónica de España señala asimismo: "*La red óptica de Telefónica de España, en combinación con nuestros sistemas de transmisiones ópticas de alta capacidad, ofrecen el rendimiento necesario para proveer comunicaciones seguras basadas en comunicaciones cuánticas. Este incremento en la seguridad es clave para la nueva generación de redes flexibles, virtualizadas y definidas por software*".

Diego R. Lopez, gerente de Exploración Tecnológica y Estándares de Telefónica Global CTIO, concluye: "*En Telefónica hemos estado trabajando para desarrollar una experiencia piloto que demuestra la provisión de servicios de comunicación segura basados en criptografía cuántica sobre redes ópticas comerciales gestionadas por tecnología SDN*".

Acerca del GCC

El Grupo de Investigación en Información y Computación Cuántica (GCC) de la Escuela Técnica Superior de Ingenieros Informáticos de la Universidad Politécnica de Madrid pertenece al Center for Computational Simulation, que agrupa cerca de 100 investigadores en el área de la Ciencia Computacional pertenecientes a tres universidades de Madrid: URJC, UCM y UAM. El GCC está formado por investigadores, principalmente profesores de universidad, expertos en las áreas de matemática aplicada, física cuántica, redes y ciencias de la computación, entre

otras. Tiene amplia experiencia en la distribución cuántica de claves y en la integración de comunicaciones cuánticas en redes de comunicaciones. La Escuela Técnica superior de Ingenieros Informáticos ha sido reconocida varias veces como la mejor en Estudios Informáticos del país en rankings nacionales e internacionales y atiende a más de 1700 estudiantes. La Universidad Politécnica de Madrid es la mayor Universidad Técnica de España, con dos Campus de Excelencia Internacional es una de las universidades españolas con mayor actividad investigadora y la primera en la obtención de recursos externos en proyectos competitivos. Con 38.311 estudiantes, imparte cerca de 200 titulaciones entre grados, máster y programas de doctorado.

www.gcc.fi.upm.es
www.ccs.upm.es
www.etsiinf.upm.es
www.upm.es

Acerca de Telefónica

Telefónica es una de las mayores compañías de telecomunicaciones del mundo por capitalización bursátil y número de clientes, que se apoya en una oferta integral y en la calidad de la conectividad que le proporcionan las mejores redes fijas, móviles y de banda ancha. Es una empresa en crecimiento que ofrece una experiencia diferencial, basada tanto en los valores de la propia compañía como en un posicionamiento público que defiende los intereses del cliente. Presente en 17 países y con 350 millones de accesos, Telefónica tiene una fuerte presencia en España, Europa y Latinoamérica, donde concentra la mayor parte de su estrategia de crecimiento. Telefónica es una empresa totalmente privada que cuenta con más de 1,5 millones de accionistas directos. Sus acciones cotizan en el mercado continuo de las bolsas españolas y en las bolsas de Londres, Nueva York, Lima y Buenos Aires.

http://www.telefonica.com

Sobre Huawei

Huawei es proveedor líder global de soluciones de Tecnologías de la Información y Comunicación (TIC), infraestructuras y dispositivos inteligentes. Con soluciones integradas en cuatro entornos clave: redes de telecomunicaciones, TI, dispositivos inteligentes y servicios en la nube, nos comprometemos a llevar la digitalización a cada persona, hogar y organización para lograr un mundo totalmente conectado e inteligente.

El catálogo completo de productos, soluciones y servicios de Huawei es competitivo y seguro. A través de la colaboración con los socios del ecosistema, creamos un valor añadido para nuestros clientes y trabajamos para empoderar a las personas, enriquecer la vida en los hogares e inspirar la innovación en organizaciones de todo tipo. En Huawei, la innovación se centra en las necesidades del cliente. Invertimos fuertemente en investigación, centrándonos en los avances tecnológicos que impulsan el avance del mundo. En la actualidad somos más de 180.000 empleados y operamos en más de 170 países y regiones. Fundada en 1987, Huawei es una empresa privada totalmente propiedad de sus empleados.

Huawei online.

Contacto de prensa: Eduardo Martínez press.ccs@upm.es