Bajo los auspicios de *IMDEA Networks*, expertos en Computación y Redes Cuánticas de todo el mundo se reunieron en Madrid el 17 y 18 de junio de 2009 en el *International Seminar on Quantum Networking* para debatir el estatus, la visión y las metas en la investigación de esta área tan prometedora e innovadora. IMDEA Networks es un instituto de investigación internacional ubicado en la U. Carlos III de Madrid y centrado en el desarrollo de avances científicos y tecnológicos fundamentales en redes de comunicaciones.

REDES CUÁNTICAS CIBER-SEGURAS PARA LA INTERNET DE NUEVA GENERACIÓN

¿Hacia una Internet cuántica?

Redacción *Antena*

La teoría cuántica explora el mundo de lo muy pequeño y lo muy inesperado. Desde su inicio a principios del pasado siglo, el estudio del comportamiento discontinuo (cuántico) de los átomos y moléculas ha puesto a prueba la capacidad de comprensión de la mente humana. Partículas atómicas y subatómicas se comportan de manera diferente que la materia microscópica, y hay modos de crear tecnologías noveles que utilizan esta noción para nuestro beneficio. La Criptografía cuántica representa tal ejemplo, ya que subyace tras la tecnología de las redes cuánticas de comunicaciones, proporcionando niveles de seguridad sin precedentes a flujos de tráfico de Internet tales como la navegación Web, el e-commerce (comercio electrónico), o el streaming de vídeo.

Bajo los auspicios de *IMDEA Networks*, expertos en Computación y Redes Cuánticas se reunieron en Madrid el 17 y 18 de junio de 2009 en el *International Seminar on Quantum Networking* para debatir el estatus, la visión y las metas en la investigación de esta área tan prometedora e innovadora, además de sus aplicaciones a redes de comunicaciones. El estudio emergente de las redes cuánticas es

Varios de los participantes en el International Seminar on Quantum Networking: (de izquierda a derecha) José Félix Kukielka (IMDEA Networks), Nicolas Georganas (Univ. of Ottawa, Canadá), Jon Crowcroft (Univ. of Cambridge, Reino Unido), Ioannis Stavrakis (NKUA, Grecia), Gonzalo Camarillo (Ericsson Labs, Finlandia), Michele Mosca (Inst. of Quantum Computing, Canadá), Werner Steinhoegl (Comisión Europea), Marco Ajmone Marsan (Politecnico di Torino, Italia & IMDEA Networks, España), Emina Soljanin (Bell Labs, EE.UU.), Arturo Azcorra (IMDEA Networks, España), Chip Elliott (BBN Technologies, EE.UU), Matthieu Legré (id Quantique, Suiza), Ralf Steinmetz (TU Darmstadt, Alemania), Enrique Diaz (Telefonica R+D, España), Paolo Villoresi (Univ. of Padova, Italia), Nick Maxemchuk (Columbia University, EE.UU. & IMDEA.

un ejemplo de investigación interdisciplinar, que reunió en esta ocasión a expertos en computación, ingeniería, matemáticas y ciencias físicas –incluyendo investigadores tras la primera red distribuida de clave cuántica (QKD– Quantum Key Distributed): «DARPA Quantum network», creada en 2003.

Estos visionarios exploran lo que es, en esencia, un método revolucionario, extremadamente seguro y muy robusto, para la transmisión de comunicaciones, que unido a los últimos avances hacia la computadora cuántica, aspira a ofrecer al mundo las abrumadoras posibilidades de la casi-instantánea resolución de problemas y la transmisión de datos perfectamente segura.

Los expertos participantes analizaron las perspectivas futuras para la planificación a largo plazo y analizaron el diseño de un programa de investigación que asegure la financiación destinada a la investigación fundamental en función de las necesidades de futuras aplicaciones y, en particular, enfocada a la producción de dispositivos de comunicación prácticos: el diseño y el desarrollo de nuevo hardware, software y protocolos de red que faciliten que las Redes Cuánticas sean operativas a gran escala. Este Seminario ha sido el primero de una iniciativa de IMDEA Networks, un Instituto de investigación respaldado por el Gobierno de la Comunidad de Madrid y por la Unión Europea, para establecer colaboraciones efectivas para el desarrollo de investigación conjunta con sus participantes.

Entre los representantes que han acudido a este evento se encontraban miembros de uno de los originadores de las redes cuánticas *(idQuantique)*, el cual realizó un primer experimento en teleportación cuántica; *BBN Technologies* como coautores de la red DARPA; el Institute for Quantum Computing; Telefonica I+D; la *Comisión Europea* y representantes de las principales universidades internacionales, tales como *Universidad Carlos III de Madrid* y *University of Cambridge, University of Ottawa* y *Columbia University in the City of New York*, entre otras.

Este catedrático de la Universidad Carlos III de Madrid es el responsable de IMDEA Networks, un instituto de investigación internacional que centra su actividad en el desarrollo de avances científicos y tecnológicos fundamentales en redes de comunicaciones. En esta entrevista, Arturo Azcorra desvela la importancia que cobrará en el futuro la teoría cuántica en Internet.

ENTREVISTA A ARTURO AZCORRA, DIRECTOR DE IMDEA NETWORKS

«En una o dos décadas, las comunicaciones cuánticas podrían impregnar nuestra vida diaria»

Fernando Cohnen

—¿Qué ofrece la teoría cuántica a Internet?

La Física cuántica proporciona fundamentos científicos dramáticamente diferentes tanto para la computación como para las comunicaciones. Los algoritmos específicos de los computadores cuánticos tienen potencial para resolver rápidamente problemas que se consideran computacionalmente inviables para los sistemas de computación actuales. Las tecnologías cuánticas también prometen hacer los protocolos de comunicación más eficientes y seguros: por ejemplo, las técnicas de distribución cuánticas de claves están emergiendo como elementos de gran valor para redes que requieran un alto nivel de seguridad.

—¿Habría seguridad absoluta en las comunicaciones y en el tráfico de datos que circula por Internet?

En general no existe tal cosa como la seguridad absoluta. La seguridad es

un problema de doble filo ya que los errores humanos del defensor y la inteligencia del atacante presentarán siempre oportunidades para vulnerar cualquier sistema de seguridad. No obstante, la criptografía cuántica presenta una ventaja fundamental sobre la criptografía clásica con respecto al espionaje. Puesto que la lectura de un mensaje cuántico transforma inevitablemente dicho mensaje, tanto el emisor como el receptor pueden detectar si su mensaje ha sido interceptado por un espía. Por consiguiente, las comunicaciones cuánticas permiten la distribución segura de claves que pueden ser empleadas para el cifrado de sesión, utilizando algoritmos convencionales.

—¿Podría comentar qué metas persiguen los investigadores que trabajan en este campo?

Aunque este campo permanece inexplorado en su mayor parte, se están llevando a cabo prometedoras investigaciones en varias direcciones. La distribución cuántica de claves citada anteriormente es uno de los focos de intensa atención. La construcción de computadoras cuánticas que sean viables en coste busca hacer realidad los beneficios teóricos de la computación cuántica. Los satélites están probando ser componentes de éxito de las redes cuánticas de comunicación: la investigación en repetidores cuánticos se esfuerza por ampliar las comunicaciones cuánticas desde el espectro actual de unos 50 Km sobre fibra oscura a distancias mucho mayores, sobre medio aeréo. El avance de enlaces cuánticos de última generación a las redes cuánticas es de particular interés.

—¿Cuándo podríamos tener en funcionamiento redes cuánticas para Internet?

Es difícil predecir el futuro de la tecnología con precisión pero al menos una o dos décadas han de transcurrir antes de que las comunicaciones cuánticas impregnen nuestra vida diaria. En este punto, no sabemos cuáles de las tecnologías cuánticas emergerán como dominantes o incluso qué propiedades teóricas específicamente cuánticas utilizarán aquellas. Sin embargo, todo parece apuntar que la combinación de computación y transmisión cuántica puede alterar de forma dramática Internet, tal y como la conocemos hoy en día.

—¿Qué entidades son pioneras en esta área de investigación?

Redactar una lista completa supondría un auténtico reto, no obstante, los participantes del *International Seminar on Quantum Networking* organizado por IMDEA Networks en junio de este año se encuentran claramente entre las entidades pioneras e incluyen, entre otros al *Institute for Quantum Computing* de Canadá, University of Padova de Italia, *BBN Technologies* de EE.UU., *id Quantique* de Suiza y Telefónica I+D en España.

También podemos mencionar a *Boston University* y a *Harvard University*, ambas de EE.UU. Recientemente científicos en *Northwestern University* han demostrado que es posible construir una puerta lógica cuántica –un componente fundamental de la computadora cuántica– dentro de fibra óptica. Y deberíamos también incluir al *Norman Bridge Laboratory of Physics* en Caltech, USA, responsable de algunos de los primeros experimentos en teleportación cuántica.

Las comunicaciones cuánticas permiten la distribución segura de claves que pueden ser empleadas para el cifrado de sesión, utilizando algoritmos convencionales

—¿Qué es IMDEA Networks y cuáles son sus objetivos?

IMDEA Networks es un instituto de investigación internacional ubicado en un edificio de la U. Carlos III de Madrid y centrado en el desarrollo de avances científicos y tecnológicos fundamentales en redes de comunicaciones. Estas tecnologías proporcionan la plataforma sobre la que se construirá la Futura Internet, que tendrá sin duda grandes novedades por los avances en su parte Inalámbrica, por la convergencia con los medios de comunicación de masas, y la introducción de las tecnologías cuánticas. IMDEA Networks está alcanzando una posición de excelencia y liderazgo internacional por medio de la creación de valor y conocimiento práctico, generando avances científico-técnicos en protocolos, algoritmos y sistemas de Internet con impacto en el mundo real. IMDEA Networks es un lugar de encuentro para investigadores, atrayendo a su equipo a científicos de gran prestigio internacional, que colaboran a su vez con nuestra red de socios en los sectores público y privado, potenciando así la transferencia de nuestros recursos de propiedad intelectual al mercado y generando un modelo de trabajo altamente comunicativo que estimula la innovación creativa.

Los avances hacia una Internet inalámbrica universal determinarán el progreso de las comunicaciones a nivel planetario. Por ello, nuestros investigadores buscan soluciones a la aldea global en la que 10^{12} dispositivos inalámbricos heterogéneos se interconectan a la Internet fija convencional. La Futura Internet Inalámbrica será un servicio de redes móvil, ubicuo y dominante que permita conectarse «en cualquier momento y lugar», evolucionando hacia una Internet distinta de la de naturaleza cableada generalizada hoy. IMDEA Networks existe para hacer realidad esta visión.

@ntena

General Moscardó, 33
Teléf.: 91 536 37 87 • Fax: 91 535 25 53
28020 Madrid
Gabinete de Prensa
E-mail: prensa@coitt.es

TARIFAS DE PUBLICIDAD 2009

TAMAÑO:

Sangre: 210 x 297 mm.
Mancha: 190 x 262 mm.

PERIODICIDAD:

Trimestral (4 números al año)

TIRADA:

10.000 ejemplares, de distribución entre los Técnicos, Ingenieros y empresas relacionadas con el sector electrónico y de telecomunicación

NOTAS:

- Estas tarifas estarán en vigor hasta diciembre de 2009.
- Descuento de Agencias el 15%.

TARIFAS

COLOR:

1 pág. interior	900 €
1 pág. interior durante un año*	2.705 €
1/2 página interior	600 €
1/2 pág. interior durante un año*	1.800 €
4ª de cubierta	1.140 €
4ª de cubierta durante un año*	3.425 €
2ª o 3ª de cubierta	1.050 €
2ª o 3ª de cubierta durante un año*	3.145 €

ENCARTES:

De 4 páginas	1.080 €
De 2 páginas	900 €

* 4 números al año