REVISTA
UPM
UNIVERSIDAD POLITÉCNICA DE MADRID
JULIO 2010 Nº 17

Exposición "*Yusur*-Puentes"

El libro electrónico

Obladibeer gana el concurso *Beertual Challenge*

Sistemas para prevenir incendios e inundaciones

Inauguración de la sede del CeDInt y del CeSVIMa

JULIO 2010 - nº 17
UNIVERSIDAD POLITÉCNICA DE MADRID

SUMARIO

UPM

POLITÉCNICA

REVISTA UPM (NUEVA ÉPOCA) Nº 17

CONSEJO EDITORIAL:
EU DE INFORMÁTICA Francisca López Hernández
EUIT AGRÍCOLA Tomás Ramón Herrero Tejedor
ETSI DE MONTES Fernando Blasco
ETS DE ARQUITECTURA Guillermo Cabeza
EU DE ARQUITECTURA TÉCNICA Agustín Rodríguez
RECTORADO Adolfo Cazorla
EUIT FORESTAL Juan Martínez
ETSI TOPOGRAFÍA Julián Aguirre
ETSI AERONÁUTICOS Vanesa García
GABINETE DEL RECTOR Victoria Ferreiro
ETSI AGRÓNOMOS Cristina Velilla
ETSI INDUSTRIALES Ángeles Soler
ETSI NAVALES Miguel Ángel Herreros
CENTRO SUPERIOR DE DISEÑO DE MODA –CENTRO ADSCRITO– Mercedes Jamart
INEF Javier Pérez Tejero
EUIT INDUSTRIAL Julián Pecharromán
ETSI DE TELECOMUNICACIÓN Alberto Almendra
ETSI DE TELECOMUNICACIÓN Alberto Hernández
ETSI DE MINAS Alberto Ramos
FACULTAD DE INFORMÁTICA Xavier Ferré
RECTORADO Cristina Pérez
RECTORADO Antonio Pérez Yuste
EUIT DE TELECOMUNICACIÓN Rafael Herradón
EUIT DE AERONÁUTICA Ángel Antonio Rodríguez
ETSI DE CAMINOS, CANALES Y PUERTOS Javier Valero
EUIT DE OBRAS PÚBLICAS Rafael Soler

CONSEJO DE REDACCIÓN (CR):
Gabinete de Comunicación UPM

FOTOGRAFÍA:
Lucía CASTILLO
Banco de imágenes Fotolia
La tinta electrónica, ilustración página 8 - E Ink Corporation, 2002
Sistemas de alerta para prevenir inundaciones e incendios, página 12 superior – T-mote Sky
Conferencia sobre el Futuro del Espacio, página 29 - ESA/C. Carreau
Una ciudad llamada España, páginas 40 y 41 - Cemal Emden

DISEÑO GRÁFICO:
Servicio de Programas Especiales y Diseño Gráfico.
Unidad de Diseño Gráfico

MAQUETACIÓN Y SERVICIOS EDITORIALES:
Cyan, Proyectos Editoriales, S.A.

PUBLICIDAD
Ángel José Gutiérrez
Tel.: 91 336 61 25

ISSN: 1699-8162

DEPÓSITO LEGAL: M-51754-2004

www.upm.es

Impreso en papel reciclado.

La revista UPM respeta las opiniones expresadas en las colaboraciones firmadas, aunque no se hace necesariamente solidaria con las mismas.

QUITEMAD: nuevas fronteras de la tecnología cuántica

La UPM, a través del Grupo de Investigación en Información y Computación Cuántica y del Centro de Supercomputación y Visualización de Madrid, forma parte del equipo científico que desarrolla el proyecto QUITEMAD. Este consorcio científico está constituido por cinco grupos de investigación y un laboratorio, que trabajan con tecnología de vanguardia en el campo de la Información Cuántica.

QUITEMAD (Quantum Information Technologies Madrid) tiene cinco objetivos científicos concretos: criptografía cuántica, computación cuántica, control cuántico y tomografía, correlaciones cuánticas y simulación cuántica. Estas líneas de investigación tienen aplicaciones científicas y tecnológicas relevantes, que van desde la implementación de criptografía cuántica para el sector industrial hasta el desarrollo y la puesta en funcionamiento de nuevas técnicas de computación e información cuánticas, incluyendo su realización experimental en colaboración con laboratorios nacionales e internacionales.

Además de sus objetivos científicos, el proyecto contempla otros de carácter estratégico como formar en las tecnologías de la información cuántica a nuevos equipos que puedan abordar con éxito los retos futuros de universidades y empresas, con la finalidad de dotar a Madrid de un estatus de excelencia y vanguardia en el ámbito europeo y mundial.

¿Qué es la criptografía cuántica?

La criptografía cuántica es un nuevo método para transferir información de manera segura. Su seguridad se basa en las mismas leyes de la naturaleza y no depende de suposiciones no demostradas sobre la complejidad de ciertos procesos matemáticos, que es la base de los métodos usados en la actualidad en muchas de las transacciones realizadas en Internet. Desde el punto de vista estrictamente matemático, permite obtener una seguridad absoluta: nadie podría descifrar nuestros mensajes, ni aun contando con toda la potencia de cálculo imaginable. Ni siquiera con un ordenador cuántico, al contrario de lo que ocurriría con los métodos usados hoy en día. En la práctica, no obstante, la implementación de un sistema de criptografía cuántica descansa sobre dispositivos físicos que no necesariamente implementan la abstracción matemática en la que se basa la afirmación de "seguridad absoluta". El campo de la seguridad en las comunicaciones es un tema delicado, donde los usuarios no pueden confiar ciegamente en lo que un determinado fabricante afirme de sus productos. Necesitan de un conjunto de pruebas y definiciones que puedan ser comprobadas por ellos mismos o por terceras partes confiables. Éste es un campo activo de trabajo en el que, dada la novedad de la criptografía cuántica, hay todavía que definir estándares, hacer pruebas y certificaciones que cierren la brecha entre el laboratorio y la utilización práctica, para que estos dispositivos puedan ser usados industrialmente. En estas áreas el grupo de investigación GIICC está involucrado como grupo fundador y líder de varias tareas del *Industry Specification Group on Quantum Cryptography,* dentro del *European Telecommunications Standards Group,* una de las tres organizaciones europeas con capacidad legal para crear estándares.

Información codificada

En la criptografía cuántica se codifica la información en qubits, el análogo cuántico

del bit clásico, que tiene nuevas propiedades. Para esto se puede usar un fotón, por ejemplo.

Las leyes de la mecánica cuántica permiten descubrir si alguien ha leído la información codificada en el qubit. Por tanto, entre "emisor" y "receptor" se establece un canal de comunicaciones especial, caracterizado por que si otra persona escucha el canal el sistema es capaz de detectarlo.

Por este canal de comunicaciones nosotros no introducimos información directamente, sino que lo usamos para acordar una clave entre los extremos del canal cuántico. En aquellas partes en las que sabemos que la clave ha sido escuchada, la desechamos y no la utilizamos. Sólo empleamos la clave que sabemos que exclusivamente nosotros conocemos, y con ella podemos transmitir información de manera segura.

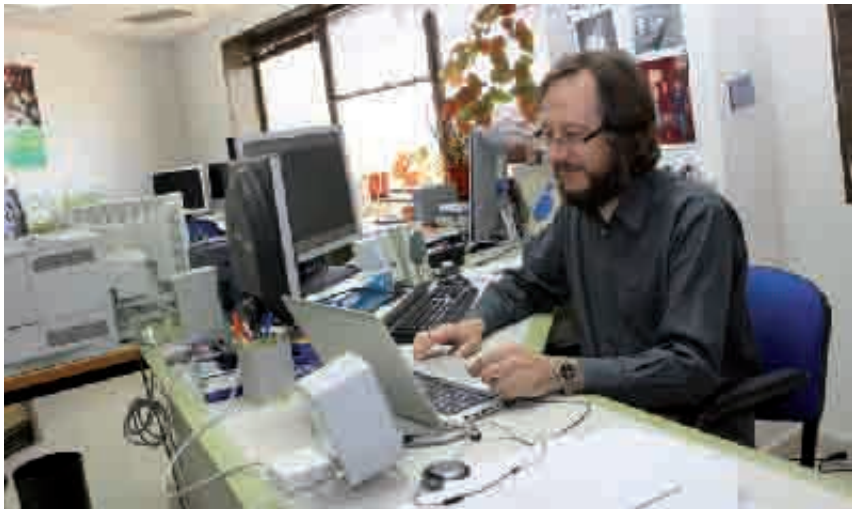
¿En qué consiste la computación cuántica?

La computación cuántica se ocupa de procesar información almacenada en los qubits. Se podría decir que los qubits almacenan más información y que esta información también puede ser procesada de maneras nuevas. Cuando leemos un qubit sólo podemos leer "cero" o "uno", al igual que un bit, pero en realidad el qubit tiene una infinidad de estados internos que, además, pueden estar relacionados con los estados de otro qubit y éstos con los de otro, etcétera.

Aplicando una serie de "puertas cuánticas", que es el análogo cuántico de las operaciones que hace el procesador de un ordenador normal, podemos usar estos grados de libertad internos y así tener acceso a una potencia de cálculo mucho mayor. Esta potencia de cálculo es la que nos permitiría, por ejemplo, descifrar los esquemas de criptografía más extendidos en la actualidad.

La criptografía cuántica y el proyecto QUITEMAD

De las nuevas tecnologías de información y computación cuánticas, la criptografía cuántica es la más próxima al mercado. Está saliendo ya de los laboratorios y existen dispositivos comerciales que se han usado en la práctica. Tal vez el más conocido sea la aplicación de esta tecnología en las recientes elecciones suizas. En aquella ocasión se transmitió toda la información desde el centro de recuento al



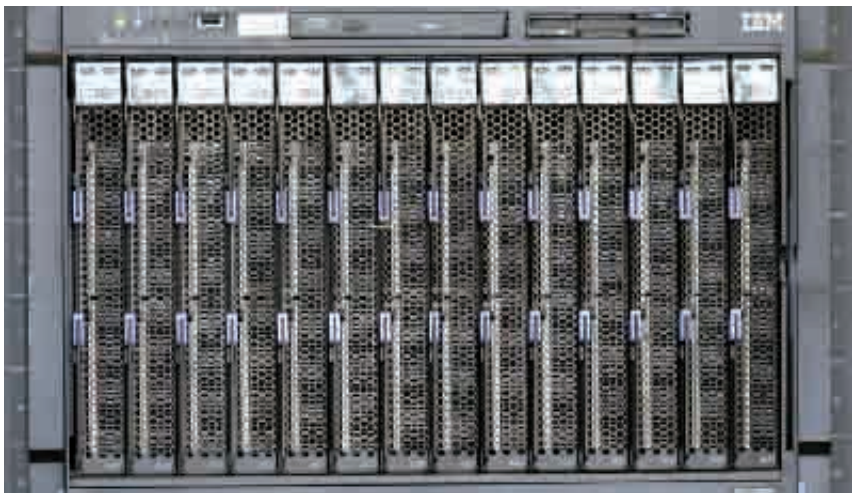
El profesor Vicente Martín es el coordinador del Grupo de Investigación y Computación Cuántica de la Facultad de Informática de la UPM.

de proceso de datos. Se recibían todas las papeletas en urnas selladas y se procedía a contarlas. A medida que iban obteniendo los resultados, esta información se pasaba a un centro de datos en las afueras de Ginebra donde se procesaba. En este caso lo importante era asegurarse no del secreto de la transmisión sino de que ésta no era modificada de ninguna manera. Esa línea de comunicaciones era el eslabón más débil si alguien quería alterar los resultados de manera inadvertida.

En España, la UPM, a través del Grupo de Investigación en Información y Computación Cuántica (GIICC) coordinado por Vicente Martín, profesor de la Facultad de Informática, conjuntamente con Telefónica Investigación y Desarrollo, está construyendo un prototipo de red metropolitana de criptografía cuántica. Su objetivo es cerrar la brecha que hay entre lo que es una tecnología de laboratorio extremadamente delicada y el uso comercial de la misma. Esta red es única ya que tiene una estructura diseñada para dar servicio a multitud de usuarios, en contraste con los sistemas actuales, que usan conexiones "punto a punto" con conexiones que no son reconfigurables. Su línea de trabajo básica consiste en integrar los sistemas de criptografía cuántica en redes de comunicación ópticas convencionales.

La infraestructura de comunicaciones que ahora transporta nuestros datos está principalmente basada en fibra óptica. Estas infraestructuras son tremendamente caras, por lo que es impensable construir una específica para criptografía cuántica. No obstante, las redes existentes tienen ya la capacidad de transmitir los

El supercomputador Magerit es el ordenador más grande del Centro de Supercomputación y Visualización de Madrid. En la actualidad está compuesto por un elevado número de procesadores, y es el segundo más potente de España.



El ordenador Magerit está formado por cerca de 2.800 CPU. Para lograr conectar un número tan elevado de procesadores, éstos se organizan en "blades" o cuchillas.
El bloque de 14 cuchillas de la imagen contiene 28 procesadores.

qubits necesarios para la criptografía cuántica. Sin embargo, incluso las señales más pequeñas que se transmiten en las comunicaciones habituales están compuestas por cientos de millones de fotones entre los cuales habría que distinguir aquellos en los que hay un qubit codificado, además de lograr que los qubits pasen por sistemas diseñados con objetivos muy distintos. Ésta es una tarea extremadamente difícil, pero hacer que se pueda usar la misma infraestructura es fundamental para lograr que la criptografía cuántica se abarate y generalice y no quede tan sólo como una tecnología nicho, al alcance de aquellos usuarios capaces de pagar un coste de entrada muy alto.

Por su parte, el Centro de Supercomputación y Visualización de Madrid (CeSViMa), también de la UPM, ofrece soporte en computación a los grupos de investigación que integran el consorcio QUITEMAD a través del supercomputador Magerit.

CeSViMa es un centro asociado a la Red Española de Supercomputación y un nodo de la Red de Laboratorios de la Comunidad de Madrid (RedLab). Magerit es su principal ordenador. Se trata de un *cluster* de más de 1.200 ordenadores, totalizando cerca de 2.800 CPU y más de 5 TB de memoria. Es el segundo ordenador más potente de España.

Aplicaciones del proyecto

El campo de la información cuántica es una de las áreas de desarrollo más prometedoras dentro de la Física y adquiere su mayor relevancia en la criptografía cuántica y la computación cuántica. Estas tecnologías prometen comunicaciones absolutamente seguras y una capacidad computacional inmensa, de forma que están llamadas a revolucionar nuestras vidas de manera comparable a como lo hicieron en su momento el láser o el ordenador personal.

Gracias a la criptografía cuántica, los mensajes que se envían a través de la red contarán con un protocolo de transmisión capaz de alcanzar las cotas más altas de seguridad, siendo absolutamente seguro desde el punto de vista matemático, sin más suposiciones que las leyes de la naturaleza que rigen nuestro mundo. Así, la Distribución Cuántica de Claves (DCC), como primera tecnología comercializable derivada de la información cuántica, permite, como hemos descrito, utilizar claves con seguridad garantizada por dos partes que comparten un canal cuántico, ya que la mecánica cuántica proporciona modos de realizar cómputos o transferir información de manera completamente distinta a los sistemas de seguridad clásicos.

La criptografía convencional basa su seguridad en la confianza de que un

EL PROYECTO QUITEMAD

Coordinado por Miguel Ángel Martín-Delgado, profesor de Física Teórica de la Complutense, QUITEMAD reúne a cinco grupos de investigación en el área de la información cuántica. Proceden de la Universidad Complutense de Madrid, la Universidad Politécnica de Madrid, la Universidad Carlos III de Madrid y el Consejo Superior de Investigaciones Científicas (CSIC). Cuenta también con un laboratorio asociado, el CeSViMa (Centro de Supercomputación y Visualización de Madrid), de la Universidad Politécnica de Madrid.

Estos equipos españoles están apoyados, además, por diez grupos de investigación y empresas internacionales y nacionales, entre los que se cuentan Toshiba Research Labs, Telefónica I+D, idQuantique, ICFO y el Instituto Max Planck de Óptica Cuántica, de Alemania.

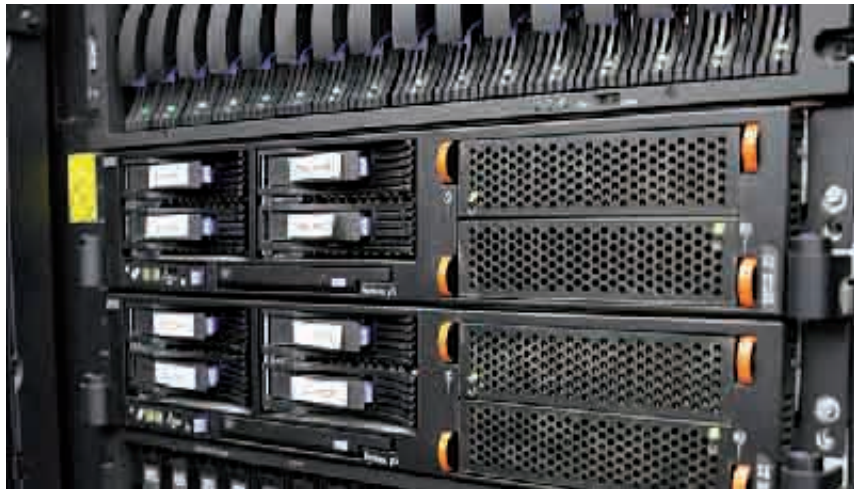
La Comunidad de Madrid financia el proyecto QUITEMAD para los próximos cuatro años, dentro de su política de apoyo a consorcios de investigación de excelencia en áreas prioritarias con un potencial de impacto elevado. El programa está cofinanciado por la Comunidad (en el Programa Regional de Innovación Científica y Tecnológica) y el Fondo Social Europeo, en una de las líneas de investigación prioritarias del Programa Marco de la Unión Europea.

atacante no tenga potencia de cálculo ni conocimientos matemáticos suficientes para descifrar las claves de una manera indetectable por los usuarios, y va perdiendo seguridad a medida que aumenta la potencia de cálculo de los sistemas. La DCC no tiene ese problema y es lo más cerca que podemos estar de la seguridad absoluta, ya que las claves estarían garantizadas contra ataques con tecnologías existentes o futuras.

Prueba del actual desarrollo de la DCC es que ya ha ido más allá del escenario teórico, para convertirse en una realidad tecnológica. De hecho, hay un número creciente de compañías que fabrican aparatos basados en la criptografía cuántica y muchas más con prototipos de laboratorio capaces de ofrecer un servicio real. La criptografía cuántica se halla ya en fase semicomercial.

Nuevos ordenadores cuánticos con ilimitadas posibilidades

El objetivo final de la computación cuántica es conseguir un ordenador cuántico, capaz de realizar cálculos numéricos inimaginables hoy en día y de hacer búsquedas en enormes bases de datos. Ese objetivo último puede estar todavía algo lejano, pero la investigación que acabará dando origen a esos ordenadores ha dejado ya importantes hallazgos, que mejoran sustancialmente la capacidad de comprender y manipular el universo cuántico.



Los servidores de discos de Magerit almacenan más de 192 TB de información en alta disponibilidad, con tolerancia a fallos y conectados con una red de alta velocidad y baja latencia.

A medida que disminuimos el tamaño de nuestros circuitos para aumentar su capacidad de procesamiento, nos acercamos ya al límite último que imponen las leyes de la física a los dispositivos actuales. Las tecnologías cuánticas suponen el próximo gran paso que representará la liberación de esas barreras y la creación de nuevos métodos, con múltiples aplicaciones tanto en ciencia básica —como la óptica cuántica, la física teórica o la mecánica cuántica— como en áreas aplicadas: fabricación de nuevos materiales y nuevos ordenadores, métodos de cálculo útiles en nanociencia, diseño de moléculas para farmacología, comunicaciones, etcétera.

Aunque todavía no se puede construir un ordenador cuántico, sí se puede fabricar ya un simulador cuántico. Miguel Ángel Martín-Delgado, profesor de Física Teórica de la UCM, coordinador de QUITEMAD, lo define como "un banco de pruebas cuánticas que no necesita corregir errores para poder funcionar". El simulador servirá para comprobar si algunas teorías cuánticas son correctas o no, algo imposible de hacer con los ordenadores tradicionales. Por otra parte, el progreso en la comprensión del entrelazamiento cuántico permite también considerar simulaciones clásicas de la mecánica cuántica mucho más eficientes de las conseguidas hasta ahora.

EL GRUPO DE INVESTIGACIÓN EN INFORMACIÓN Y COMPUTACIÓN CUÁNTICA

El Grupo de Investigación en Información y Computación Cuántica, coordinado por Vicente Martín, profesor en la Facultad de Informática de la UPM, comenzó en 2006 instalando el mismo año la primera línea experimental de criptografía cuántica en España. En 2007 se inició una colaboración con Telefónica I+D, con el objetivo de construir un prototipo de red de área metropolitana para criptografía cuántica. Este proyecto fue posteriormente financiado por el CDTI dentro del programa "CENIT Segur@: Seguridad y Confianza en las Redes de Comunicaciones". El prototipo, cuya primera fase finalizará en 2011, tiene varias características que lo hacen único en el mundo: es el primero en incluir criptografía cuántica tanto en la red troncal como en las de acceso, compatibilizando tecnologías ópticas habituales con las necesidades de la criptografía cuántica y usando nuevos protocolos avanzados de destilación de claves. El grupo desempeña también un papel destacado en el desarrollo de estándares para criptografía cuántica dentro del *European Telecommunications Standards Institute*. El objetivo final de la red es la demostración de servicios de criptografía cuántica, escalables y de coste razonable. La extensión de esta red estará financiada dentro del proyecto QUITEMAD.

Otros objetivos incluyen la corrección de errores cuánticos y la simulación de sistemas cuánticos de muchos cuerpos, donde se aplicarán técnicas derivadas de la información cuántica desarrolladas en el consorcio QUITEMAD.