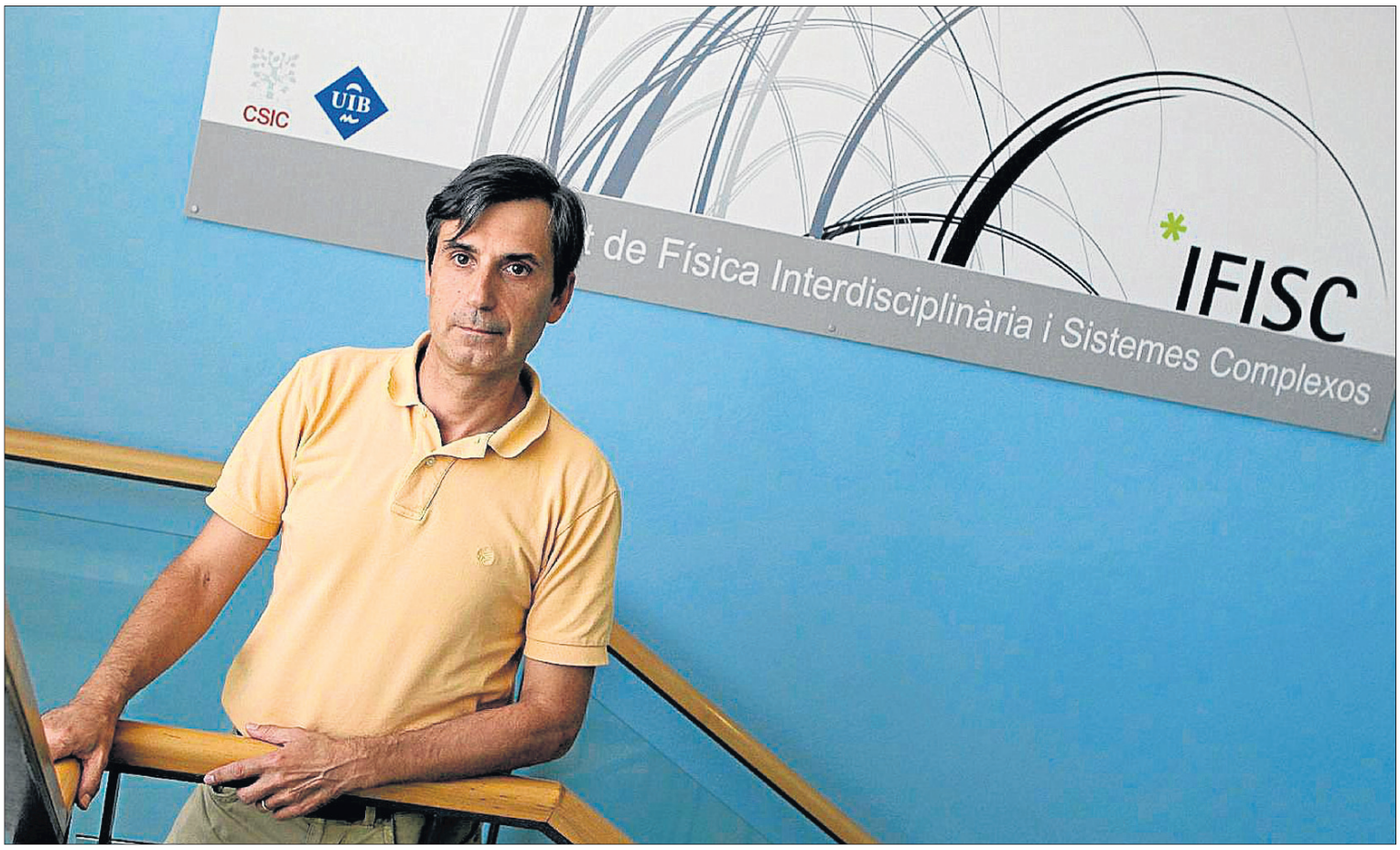

Pere Colet, investigador del IFISC-Instituto de Física Interdisciplinar y Sistemas Complejos (CSIC-UIB). / CATI CLADERA

VIENE DE **PORTADA** Y esta es precisamente una de las líneas de investigación realizadas por el Instituto de Física Interdisciplinaria y Sistemas Complejos (IFISC), que consiste en superponer a las técnicas clásicas de encriptación de mensajes (*software*) un segundo nivel o capa de inaccesibilidad incorporando dichos mensajes en ondas caóticas generadas por láseres semiconductores.

El cifrado mediante algoritmos matemáticos, aunque siga siendo seguro, presenta riesgos evidentes puesto que la existencia de ordenadores cada vez más potentes facilita que, con tiempo suficiente, se puedan llegar a romper las claves de seguridad. El sistema investigado por el grupo del IFISC introduce en el campo de la seguridad y privacidad de las comunicaciones esa segunda capa de protección. Ya que cuando la información viaje sobre fibra óptica, a la encriptación algorítmica del mensaje se añade un elemento nuevo: la utilización de una onda lumínica caótica como portadora.

«La portadora es una señal periódica, explica Pere Colet, físico del IFISC e investigador de este método, la idea es utilizar un láser de semiconductor que opere en un régimen caótico y que genere una portadora caótica –que varíe de forma irregular en el tiempo– y sobre ella pongo el mensaje».

«Los sistemas con comportamiento caótico se caracterizan por la sensibilidad a pequeñas variaciones de las condiciones iniciales, añade. La trayectoria que sigue una piedra de un determinado tamaño cuando cae no es muy diferente de la otra piedra similar, aunque la lanzásemos desde una altura mayor. En cambio si repetimos el experimento con dos folios de papel idénticos la trayectoria que seguirían sería distinta y difícilmente predecible. No habría dos que cayeran exactamente en el mismo sitio, y eso se debe a que existen gran cantidad de factores aleatorios. La idea es que, dadas dos condiciones iniciales muy cercanas, éstas conducen a la evolución en formas completamente diferentes en la salida. Los sistemas caóticos se comportan de manera similar y es, precisamente, esta propiedad la que resulta útil para enmascarar el mensaje, ya que reproducir el mismo caos sería prácticamente imposible».

El diseño propuesto por este grupo permite comunicaciones seguras a muy alta velocidad

En principio, los láseres de semiconductor están diseñados para tener un comportamiento estable, pero se les puede perturbar para convertirlos en un sistema caótico que camufle la información. «Se puede hacer de varias formas», explica Colet, «una de las más simples es colocarle un espejo externo semitransparente, que lo que hace, en definitiva, es crear un sistema con retraso, clave para generar la luz caótica».

La otra parte es ¿cómo puedo recuperar el mensaje? y según este investigador esto es posible gracias a la sincronización.»A pesar de que dos sistemas sean caóticos se puede conseguir que hagan lo mismo y esta particularidad es la que permite rescatar la información. Necesito un sistema que genere exactamente la misma portadora caótica».

La seguridad se basa a mantener ocultas las características del sistema. Para ello uno de los parámetros relevantes es el tiempo de retraso, y éste se puede detectar empleando las técnicas estadísticas apropiadas. Aunque su identificación no implica que se pueda descifrar el mensaje –se necesitarían conocer otros parámetros– sí que puede ser la llave para abrir las puertas a ataques posteriores.

La siguiente parte de esta investigación busca subsanar esta laguna construyendo un sistema más complejo, y este trabajo acaba de ser publicado en la revista *Physical Review Letters*. Para incrementar la seguridad, los científicos proponen un nuevo esquema que integra una clave digital en el dispositivo optoelectrónico que genera luz caótica. Esta combinación, que utiliza dos bucles de retraso, permite que la clave digital 'oculte' el tiempo de retraso y que el caos enmascare a la clave digital para que no sea posible detectarla.

Conceptualmente, este esquema constituye un primer puente entre la criptografía algorítmica tradicional y la basada en el caos. Desde un punto de vista aplicado, el diseño propuesto permite comunicaciones seguras a muy alta velocidad (10 Gbit/s), es altamente flexible y permite la reconfiguración instantánea de los receptores autorizados para cada mensaje.

EL ARTE DE OCULTAR EL MENSAJE

● **La escitala.** Palo o bastón en el que se enrollaba en espiral una tira de cuero. Sobre ella se escribía el mensaje en columnas paralelas al eje del palo. Cuando se desenrollaba mostraba un texto sin relación aparente con el inicial, pero que podía leerse volviéndola a liar sobre un bastón del mismo diámetro y longitud que el primero.

● **Enigma.** Esta máquina fue la encriptadora oficial de las fuerzas militares de Alemania desde 1930 y se usó durante la II Guerra Mundial. Disponía de un mecanismo de cifrado rotatorio, donde se permutaban las letras tecleadas. Así, una letra «X» era cambiada en un cilindro por otra distinta, que a su vez era cambiada por otra letra en el siguiente cilindro y así sucesivamente.

● **Cuántica.** Esta criptografía utiliza fotones para crear y transmitir dígitos binarios. Cualquier intento de interceptar los fotones que componen el mensaje modifica su polarización y el cambio es detectado por el receptor.

>PROYECTOS CON FUTURO

La Semana de la Ciencia celebra el año Internacional de la Química

Por **Elena Soto**

Arqueología, Química, Física Interdisciplinaria y catas científicas son los cuatro bloques en los que se divide el programa de actividades organizadas desde el Vicerrectorado de Investigación de la UIB para la Semana de la Ciencia y la Tecnología 2011, que se clausurará el próximo 30 de noviembre.

El Grupo de investigación Arqueobalear lleva a cabo diferentes actividades para acercar el mundo, de la Arqueología a todos los que sientan curiosidad por saber más sobre la prehistoria en Baleares. Así, entre los actos organizados, están las visitas a yacimientos arqueológicos como el del Puig de Morisca o els Closos de Can Gaià.

Con el lema 'Química: nuestra vida, nuestro futuro', la ONU ha declarado 2011 el Año Internacional de la Química, y a esta disciplina está dedicado el segundo grupo de actividades. Además el año 2011 coincide con el centenario de la concesión del Nobel de Química a Marie Curie, y es una excelente oportunidad para reconocer la contribución de las mujeres a la ciencia.

Otro de los apartados es el del ciclo de catas científicas de productos de las Baleares. El objetivo de esta actividad es introducir la vertiente científica en estas experiencias. En ellas participan los estudiosos de la UIB que han realizado trabajos de investigación sobre los productos que se degustarán.

Acto de presentación de la Semana de la Ciencia en la UIB. /UIB