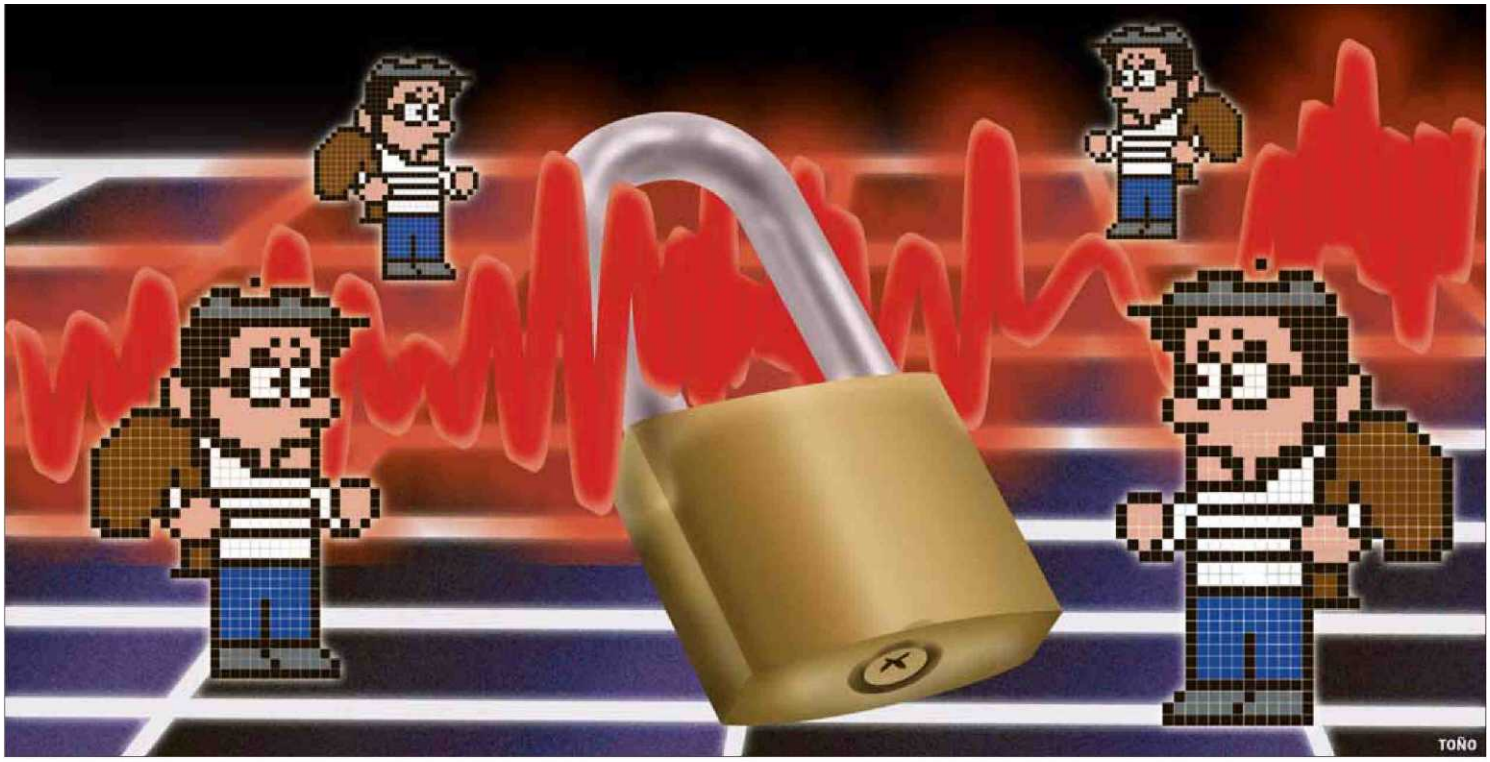
EL MUNDO-EL DIA DE BALEARES (B@LEÓPOLIS) 18/10/11
PALMA DE MALLORCA

Prensa: Semanal (Martes)
Tirada: 22.753 Ejemplares
Difusión: 18.646 Ejemplares

Página: 1

Sección: OTROS Valor: 1.880,00 € Área (cm2): 597,4 Ocupación: 63,72 % Documento: 1/2 Cód: 51442715



La seguridad del caos

›Física/ Un grupo de investigación mallorquín añade a las técnicas clásicas de encriptación de mensajes un segundo nivel de inaccesibilidad usando las ondas caóticas generadas por láseres semiconductores. **Elena Soto**

En siglo V a.C. los espartanos para ocultar los mensajes usaban la escítala –una cinta enrollada en un bastón sobre el que se escribía el texto en forma longitudinal–. La llave del sistema era el diámetro y la longitud de este objeto, de forma que solamente un receptor autorizado podía descifrarlo porque tenía una copia exacta del mismo bastón. La criptografía –término que procede del griego *kriptos* (ocultar) y *graphos* (escritura) es la técnica para hacer ininteligible un mensaje, y surgió sobre todo de la necesidad de esconder información privilegiada a los enemigos en época de guerra.

Entre la escítala espartana y los complejos algoritmos o la encriptación cuántica de la actualidad han transcurrido miles de años pero todos estos métodos persiguen básicamente el mismo objetivo: proporcionar comunicaciones seguras y secretas. Y si en la antigüedad con los mensajes cifrados se buscaba la victoria en la guerra del Peloponeso, por poner un ejemplo, hoy en día las batallas se llevan a cabo en Internet y buscan, entre otras cosas, la victoria de sectores como el del comercio electrónico defendiendo los datos de las transacciones financieras que viajan por las redes.

Lo más común es que cualquier información de carácter privado sea cifrada antes de ser transmitida. Para codificarla se emplean algoritmos matemáticos implementados mediante *software*. Cuando realizamos cualquier transacción comercial en la Red y damos el número de nuestra tarjeta de crédito entran en juego complejas técnicas de cifrado que están íntimamente ligadas al cálculo computacional y que se encargan de dar un alto grado de seguridad al mensaje transmitido a través de canales de comunicación a los que pueden acceder millones de usuarios.

La criptografía moderna se divide en dos grandes bloques: la simétrica, en la que el emisor y el receptor de un mensaje cifrado comparten la misma clave que lo descifra; y la asimétrica, en la que cada usuario dispone de una clave distinta: el emisor de una clave pública y el receptor de una clave privada asociada a la del emisor. De forma que la clave pública permite codificar el mensaje, pero sólo la clave privada permite descifrarlo. El éxito del cifrado consiste en establecer un sistema computacional tan complicado que sea casi imposible deducir la clave privada.

En ambos casos, la encriptación de los datos está basada en el *software*, pero en los últimos años se están estudiando nuevas formas que permitan enmascarar la información y se ha experimentado con el *hardware* como nuevo elemento para camuflar el mensaje, permitiendo aumentar los niveles de seguridad y privacidad.

SIGUE EN **PÁGINA 2**

EL MUNDO-EL DIA DE BALEARES (B@LEÓPOLIS) 18/10/11
PALMA DE MALLORCA
Prensa: Semanal (Martes)
Tirada: 22.753 Ejemplares
Difusión: 18.646 Ejemplares
Página: 2
Sección: OTROS Valor: 2.087,00 € Área (cm2): 663,3 Ocupación: 70,75 % Documento: 2/2 Cód: 51442715

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.

DIARIO DE MALLORCA (UNIVERSITAT)
PALMA DE MALLORCA
13/10/11
Prensa: Otra
Tirada: 23.557 Ejemplares
Difusión: 20.618 Ejemplares
Página: 4
Sección: OTROS Valor: 296,00 € Área (cm2): 104,2 Ocupación: 9,54 % Documento: 1/1 Cód: 51297437

UIB

R. Modeste Nguimbo i P. Colet.

RECERCA

Nova proposta per millorar la seguretat en les comunicacions

Els investigadors Romain Modeste Nguimdo i el doctor Pere Colet, tots dos membres de l'Institut de Física Interdisciplinària i Sistemes Complexos (IFISC) proposen un nou sistema per augmentar la seguretat en les comunicacions. Tradicionalment en aquests sistemes el missatge es codifica mitjançant un dispositiu optoelectrònic. La seva proposta és un nou esquema que integra una clau digital en el dispositiu optoelectrònic que genera llum caòtica.

Aquesta combinació, que utilitza dos bucles de retard, permet que la clau digital "oculti" el temps de retard al mateix temps que el caos emmascara la mateixa clau. Conceptualment, aquest esquema constitueix un primer pont entre la criptografia algorísmica tradicional i la basada en caos. Des d'un punt de vista aplicat, el disseny proposat permet comunicacions segures a molt alta velocitat (10 Gbit/s), és altament flexible i permet la reconfiguració instantània dels receptors autoritzats per a cada missatge.

D'aquesta investigació, se n'ha fet ressò la revista *Physical Review Letters*, una de les publicacions més prestigioses en l'àmbit de la física. La recerca ha comptat amb la col·laboració del doctor Laurent Larger, de l'Institut FEMTO-ST (CNRS-Universitat del Franc Comtat) i el doctor Luis Pesquera, de l'Institut de Física de Cantàbria (CSIC-Universitat de Cantàbria).