

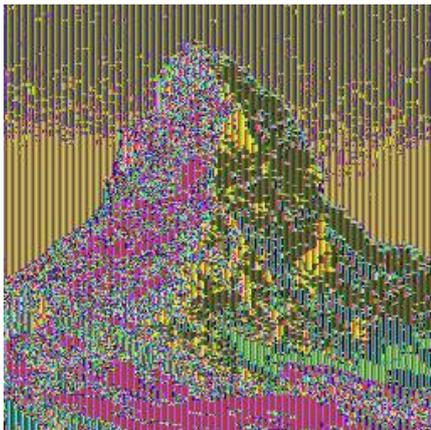
EL EXPERIMENTO SE BASA EN LAS PROPIEDADES CUÁNTICAS DE LA LUZ

Un nuevo sistema informático luchará contra el espionaje y la piratería informática

Un equipo dirigido por el Consejo Superior de Investigaciones Científicas (CSIC) ha realizado un experimento que mejorará la tecnología para luchar contra el espionaje y la piratería informática. El experimento, realizado con éxito por primera vez en España, es conocido como el efecto interferometría Hanbury-Brown-Twiss en puntos cuánticos semiconductores. El sistema permitirá fabricar dispositivos basados en criptografía cuántica que mejoren el actual sistema de transmisión de información, que es vulnerable.

CSIC

2/6/2008 12:52 CEST



Ejemplo de cifrado ECB. Foto: Dake.

El director del experimento, el investigador Benito Alén, que trabaja en el Instituto de Microelectrónica de Madrid (CSIC), señala las ventajas del sistema: "El experimento demuestra que los puntos cuánticos se comportan como átomos artificiales y son capaces de emitir fotones individuales, lo que permitirá generar códigos criptográficos inviolables. Esto ocurre porque el estado cuántico que porta el código en cada fotón emitido por la fuente queda destruido automáticamente si se intenta descifrar ilegítimamente. Así, los nuevos sistemas de transmisión de datos serían invulnerables al espionaje y la piratería informática".

El carácter cuántico del fotón individual es lo que permite detectar a un potencial espía, ya que no se puede realizar una medida sobre un estado

cuántico sin modificar sus propiedades. Si un pirata informático intentase realizar esas medidas sobre los fotones individuales para obtener la clave, introduciría unas modificaciones que serían detectadas por el emisor y receptor auténticos.

“Si se detecta al espía, el sistema, simplemente, desecha la clave y empieza otra vez con una clave nueva. Sólo cuando se completa la clave sin intromisiones se valida la clave privada para ser utilizada en las comunicaciones futuras”, señala Alén.

Una vez conseguido el experimento, el actual objetivo del equipo de investigadores es aplicar estos resultados al desarrollo de dispositivos emisores de fotones individuales basados en puntos cuánticos semiconductores. Además, estos dispositivos serán optimizados para las telecomunicaciones por fibra óptica, que acoge la mayor parte del flujo de datos mundial.

Seguridad en la transmisión de información

Los sistemas de criptografía actuales se basan en que el emisor y el receptor poseen una o varias claves que sólo ellos conocen y que utilizan para encriptar y desencriptar los mensajes. Existen diversos sistemas criptográficos, pero todos están subordinados a la integridad de la transmisión de las claves privadas. “Si se usara un sistema criptográfico cuántico, la clave podría ser enviada sin problemas. Si una persona pinchase la línea para acceder a la clave, inmediatamente se detectaría su presencia analizando el mensaje transmitido junto a la clave”, destaca el investigador del CSIC.

Los sistemas criptográficos cuánticos que se utilizan en la actualidad se basan en fuentes de luz láser muy atenuadas, en los que la misma información se codifica en más de un fotón, lo que aumenta la invulnerabilidad de la técnica. Con este sistema, un espía informático dispone de copias exactas del estado cuántico original, por lo que puede realizar sus medidas en un fotón, sin afectar a la transmisión de datos, ya que se transmite en otros fotones.

El experimento, liderado por Benito Alén y Juan Martínez Pastor, éste último

del Instituto de Ciencia de los Materiales de la Universidad de Valencia, ha contado también con la colaboración de investigadores del Instituto de Materiales Eléctricos y Magnéticos de Parma, en Italia. Este equipo está involucrado en diversos proyectos de investigación: Red SANDIE (Red Europea de Excelencia), Proyecto QOIT (Programa Consolider-Ingenio-2010), Proyecto NANIC (Acción estratégica de Nanociencia y Nanotecnología) y Proyecto NANOSELF-2 (Plan Nacional de Investigación en Tecnología Electrónica y de la Comunicaciones).

Derechos: **Creative Commons**

Creative Commons 4.0

Puedes copiar, difundir y transformar los contenidos de SINC. [Lee las condiciones de nuestra licencia](#)