CSIC
Consejo Superior de Investigaciones Científicas

Nota de prensa

CSIC comunicación
Tel.: 91 568 14 77
g.prensa@csic.es
www.csic.es

Madrid, martes 28 de abril de 2015

Un nuevo sistema permite el intercambio seguro de claves secretas a larga distancia

- **El método, demostrado por un equipo con participación del CSIC, recurre a las propiedades físicas de los láseres ultralargos de fibra óptica**

- **La investigación aporta un nuevo sistema de intercambio de claves "extremadamente seguro" basado en la criptografía**

Un equipo internacional con participación de investigadores del Consejo Superior de Investigaciones Científicas (CSIC) ha demostrado la viabilidad de un nuevo método criptográfico para el intercambio seguro de claves secretas a decenas de kilómetros de distancia. El sistema se basa en aprovechar las propiedades físicas de los láseres ultralargos de fibra óptica. La investigación aparece publicada en el último número de la revista *Light: Science & Applications*, del grupo *Nature*.

Los investigadores han aprovechado las variaciones de longitud en las cavidades de un láser ultralargo de fibra. Este tipo de láser utiliza como medio activo una fibra óptica de gran longitud (de unos cinco kilómetros a varios cientos de kilómetros), de modo que se puede emplear su interior como medio de transmisión. El concepto de láser ultralargo fue propuesto en 2004 por Juan Diego Ania, investigador del CSIC en el Instituto de Óptica, para amplificar señales en sistemas de comunicación a larga distancia de gran capacidad con muy poco ruido. Actualmente se aplican, por ejemplo, en comunicaciones, en el desarrollo de sensores de fibra o en el diseño de fuentes de luz de amplio espectro.

"En este nuevo trabajo demostramos que variaciones fijas en la longitud del láser, controladas desde ambos extremos por los usuarios, pueden ser utilizadas para transmitir claves de forma segura. La seguridad está asegurada por la indistiguibilidad, para un potencial espía, de los estados del láser cuando sólo uno de los dos usuarios decide variar su longitud", señala Ania.

La investigación aporta un nuevo sistema de intercambio de claves criptográficas "extremadamente seguro". La criptografía es la única forma de garantizar la privacidad de los datos bancarios y personales cuando se transmiten a través de las redes de comunicación. "A pesar de que sabíamos que era teóricamente posible transmitir

claves de forma segura mediante este procedimiento, hay muchos elementos que pueden influir en el resultado final en un sistema de comunicaciones. El desafío estaba en demostrar la seguridad ante un potencial espía externo en una situación realista", detalla el científico.

Se trata de un estudio inicial y los investigadores seguirán trabajando en la mejora del sistema y en hacerlo más rápido y seguro. "Esta solución tiene como ventajas principales una menor complejidad y coste que otras soluciones existentes como las basadas en transmisión cuántica de claves. Más aún, el sistema puede montarse con componentes disponibles comercialmente, y es especialmente atractivo en situaciones en las que las claves deban enviarse a grandes distancias y con gran rapidez", agrega el investigador del CSIC.

La investigación es resultado de una colaboración entre científicos de la Universitè de Limoges, en Francia, el Instituto de Óptica del CSIC, y la Aston University, en Reino Unido.

Alessandro Tonello, Alain Barthélémy, Katarzyna Krupa, Vincent Kermène, Agnés Desfarges-Berthelemot, Badr Mohamed Shalaby, Sonia Boscolo, Sergei K Turitsyn y Juan Diego Ania-Castañón. **Secret key exchange in ultralong lasers by radiofrequency spectrum coding**. *Light: Science & Applications*. DOI: 10.1038/lsa.2015.49.