Per a més informació contactau amb el Servei de Comunicació de la UIB

Nota informativa

Els investigadors de l'IFISC (CSIC-UIB) proposen un sistema de comunicacions caòtiques amb clau digital per millorar la seguretat en les comunicacions

La recerca dels investigadors de l'IFISC (CSIC-UIB) Romain Modeste Nguimdo i Pere Colet ha estat publicada per la revista *Physical Review Letters*

La revista *Physical Review Letters*, una de les més prestigioses en l'àmbit de la física, ha publicat al número del 15 de juliol un article dels investigadors senyor Romain Modeste Nguimdo i doctor Pere Colet, ambdós de l'Institut de Física Interdisciplinària i Sistemes Complexos (IFISC), centre de recerca mixt entre la Universitat de les Illes Balears i el Consell Superior d'Investigacions Científiques. 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).

La recerca del senyor Romain Modeste Nguimdo i del doctor Pere Colet s'emmarca en el context de les comunicacions òptiques basades en caos. Tradicionalment en aquests sistemes el missatge es codifica mitjançant un dispositiu optoelectrònic (en el nostre cas un làser de semiconductor) que emet llum caòtica i funciona com a emissor. La llum emesa pel làser retorna al mateix dispositiu un temps després, i aquest retard és crucial perquè es generi la llum caòtica. Aquesta tècnica fa que el missatge no pugui ser interceptat a menys que es disposi d'un receptor adequat, que ha de ser un sistema similar a l'emissor i que permet, mitjançant el procés de sincronització, la descodificació del missatge. La seguretat es basa a mantenir ocultes les característiques del sistema. Un dels paràmetres rellevants és el temps de retard, que es pot estimar utilitzant tècniques estadístiques apropiades. Si bé la identificació del temps de retard no implica que es pugui descodificar el missatge sí que pot obrir les portes a atacs posteriors.

Per augmentar la seguretat, els investigadors proposen 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.

Data publicació: 29/07/2011

« Torna enrere