

ICT Results ... Results that lead the way

Features

Creating chaos for data [security](#)



Within three years one of the most advanced data encryption systems developed to date could go into commercial use thanks to the work of OCCULT, and its gigantic strides forward in laser-based chaotic carriers to transmit data through fibre-optics.

The cutting-edge technique, which employs synchronised laser emitters and receivers to encrypt information at the hardware level, represents an important qualitative upgrade to existing security systems for protecting the transmission of data.

“Traditional systems rely on software encryption, which uses keys to code and decode information, but advances in computer processing speeds are putting data encrypted via this method at risk,” explains Claudio Mirasso, coordinator of the IST project [OCCULT](#), at the University of the Balearic Islands in Spain. “Our idea therefore is to use hardware, i.e. the emitters and receivers of the information, to carry out the encryption, which can be used in combination with software encoding to create two levels of security.”

The technique researched and evaluated by the OCCULT project relies on having two sets of semiconductor lasers that are virtually identical to send and receive information over fibre-optic cables. The light transmitted by these lasers is non-linear and chaotic so only a receiver synchronised with the emitter can decode the data, making it almost impossible for the transmission to be decrypted by someone other than the intended recipient.

“Anyone wanting to break the encryption has to know as much as the people using it and have a virtually identical device,” Mirasso notes. “We’ve demonstrated that an extremely high level of security can be achieved because cracking the system would require adjusting 200 or 300 parameters.”

For high security transmissions the lasers would have to operate with a tolerance level of just 1 or 2 per cent, something that can only be achieved if they are made with the same equipment and the same components at the same time.

“The lasers not only have to come from the same batch of semiconductors but literally be produced side-by-side because once you get further down the line the differences increase,” the project coordinator says.



Having carried out laboratory evaluations of the system, the project partners are now looking to commence field trials, possibly under a new IST project.

Their continuing work could lead to an optical chaos encryption system being commercialised “in about three years,” Mirasso says, noting that the potential market is vast. “Because the technique can be used over existing fibre-optic cables, it would be relatively cheap to employ, with the only additional components being the emitter and receiver.”

Contact:

*Claudio Mirasso
Departament de Física
Universitat de les Illes Balears
E-07122 Palma de Mallorca
Spain
Tel: +34-971-172783
Fax: + 34-971-173426
Email: claudio@galiota.uib.es*

Source: Based on information from OCCULT

INFORMATION :**DATE :** 8 Oct 2004**TECHNOLOGY AREA:** [Trust/security](#) **MARKET APPLICATION:** [Electronics/IT manuf](#) **USEFUL LINKS:** [OCCULT project](#)
[OCCULT factsheet on CORDIS](#)**RECENT ARTICLES :**

- [Small companies add value by sharing commercial information](#)
- [New software to simulate future financial crises](#)
- [Manufacturing, reinvented](#)
- [Semantic research sets world standards](#)
- [Taking the drudgery out of software development](#)

**Legal notice:**

The content is prepared by the ICT Results service and offers news and views on innovations, emerging from EU-funded Information Society Research. The views expressed in the articles have not been adopted or in any way approved by the European Commission and should not be relied upon as a statement of the Commission or the Directorate General for Information Society and Media. If errors are brought to our attention, we will try to correct them.

Reproduction of this article is authorised, provided its source "IST RESULTS" is acknowledged.