Itineraris per la Física Quotidiana (i 3)

Caos i sincronització: un còctel per a comunicar-se de forma segura

Pere Colet

Index

- Motivació
- Transmissió de missatges. La radio.
- Informació en forma digital.
- Sistemes de comunicacions òptiques. Fibres, làsers
- Criptografia.
- Caos.
- Sincronització.
- Sincronització de sistemes caótics.
- Comunicacions codificades mitjançant làsers caótics.
- Resumen.

Motivació

Seguritat y privacitat son assumptes molt importants en xarxes de comunicacions:

- Compres per internet.
- Transaccions comercials.
- Accés “on-line” a comptes bancaris. Transferències bancàries.
- Televisió codificada.
- Declaració de renta (IRPF). Firma digital.

Típicament la informació privada es codificada abans de ser transmesa. Per això s’empren algorismes matemàtics implementats mitjançant software.

Objectiu: Millorar la seguretat emprant una codificació addicional a nivell de dispositius físics (hardware) fent servir portadors caòtics.

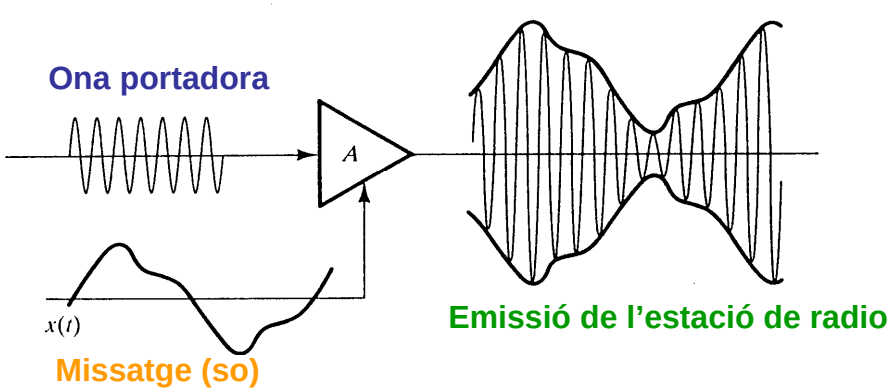
I això ho farem fent un passeig per la vida quotidiana i per la història on veurem relacions insospitades entre coses (aparentment) diverses.

Transmissió de missatges. La radio

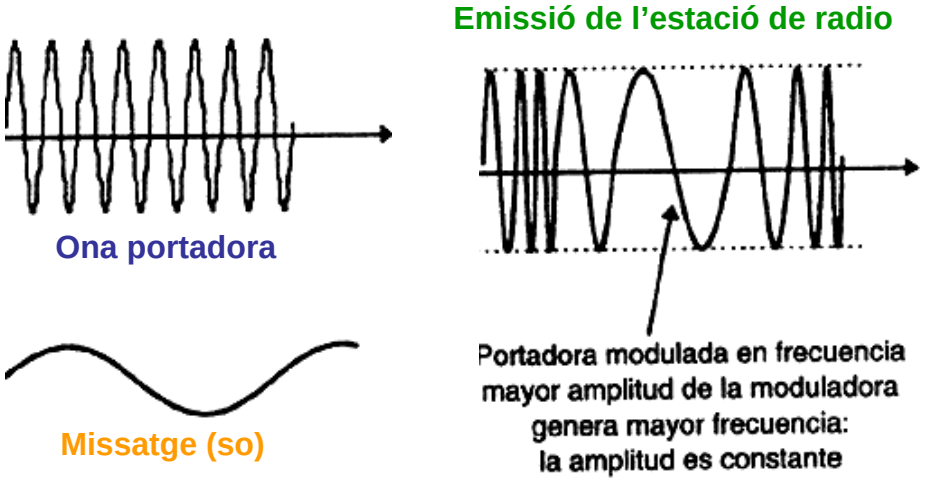
Una forma habitual de transmetre informació es modulant una “ona portadora”.

Exemples

Radio AM (amplitud modulada):
El so (missatge) es transmet modulant l’amplitud de una ona electromagnètica.



Radio FM (freqüència modulada):
El so es transmet modulant la freqüència de la onda portadora.



Informació digital

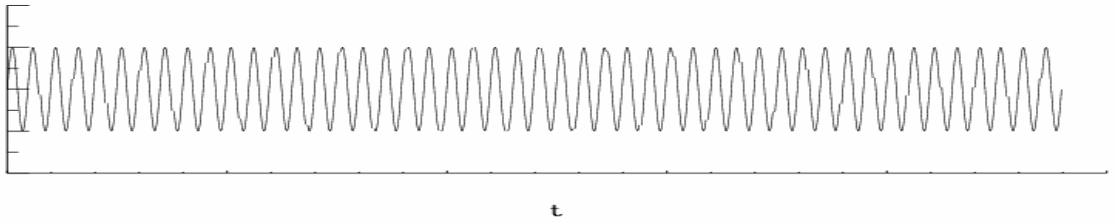
Usualment la informació s'emmagatzema i es transmet en forma digital:

Una llarga seqüència de “1” y “0”.

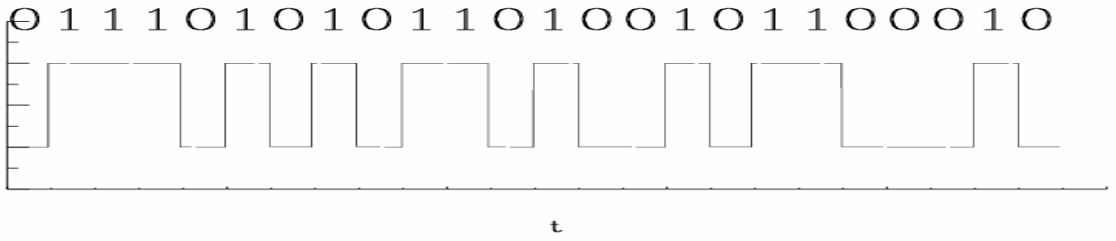
Exemple, el codi ascii:

a	01100001
b	01100010
c	01100011

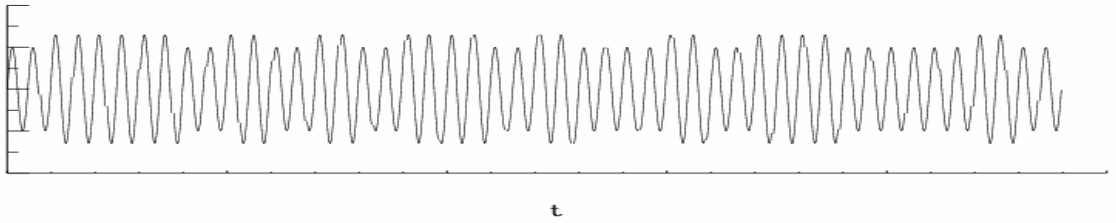
Ona portadora



Missatge: “uib”

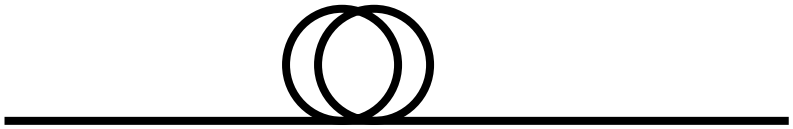


Senyal transmesa

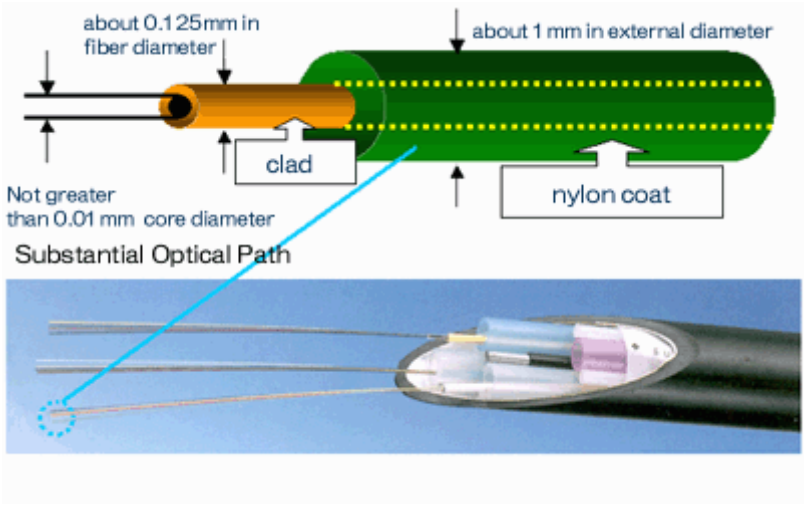


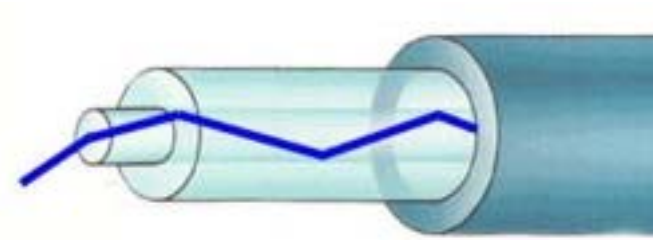
Sistemes de comunicacions òptiques

La gran majoria de les comunicacions es fan emprant sistemes de fibra òptica



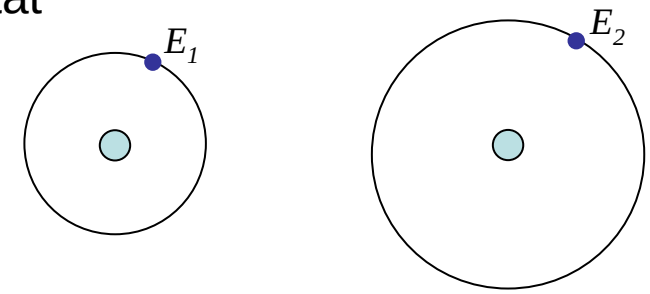
Fibra òptica

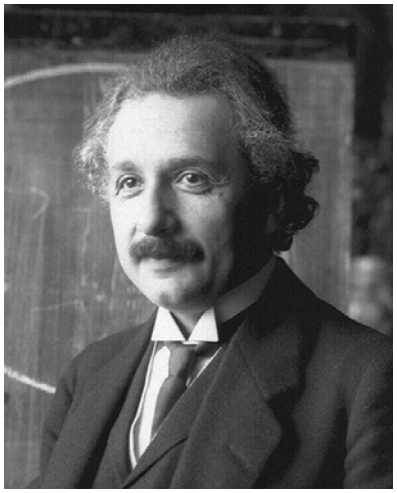




L'emissió de llum

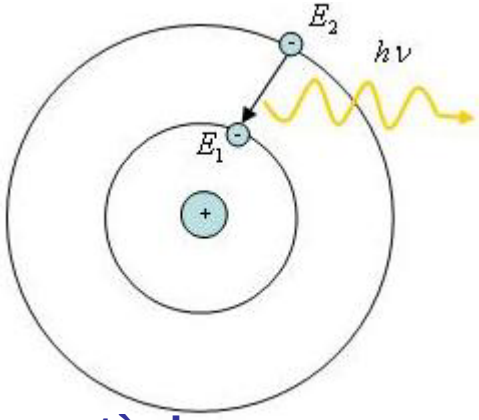
Si donem energia a un àtom un electró pot passar del seu nivell d'energia a un nivell excitat





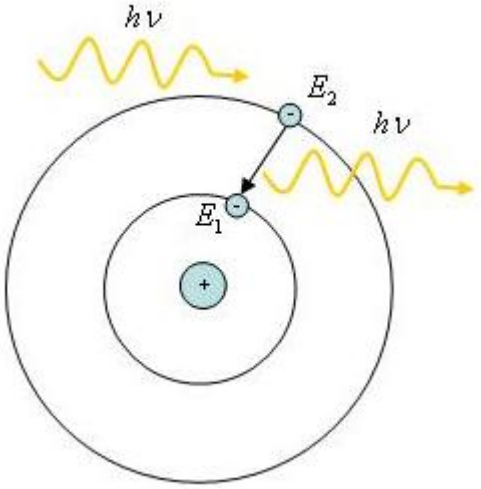
Albert Einstein (1879-1955)

Al cap d'una mica l'electró torna al nivell d'energia fonamental. La diferencia d'energia es emesa en forma de llum (fotó)



Emissió espontània.
Cada fotó s'emet en una direcció diferent

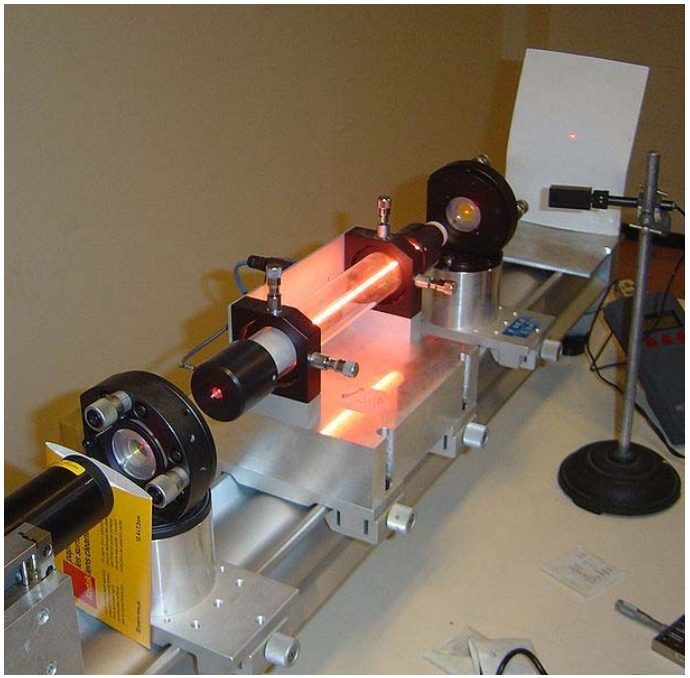
Emissió estimulada (1917). Si pasa un fotó per allà l'electró excitat decau immediatament emetent un fotó **idèntic i en la mateixa direcció.**

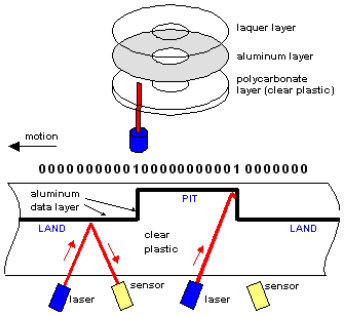


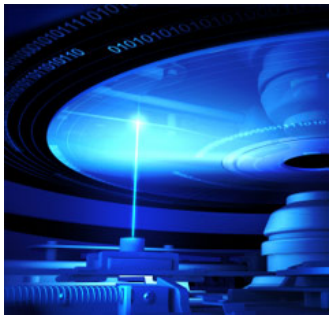
IFISC

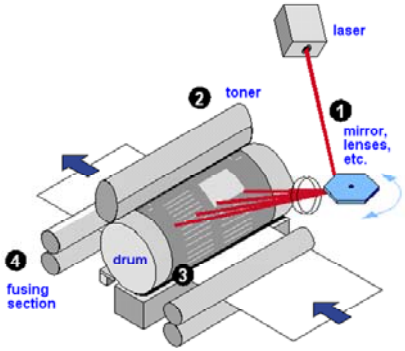
L.A.S.E.R.: Light Amplification by Stimulated Emission of Radiation

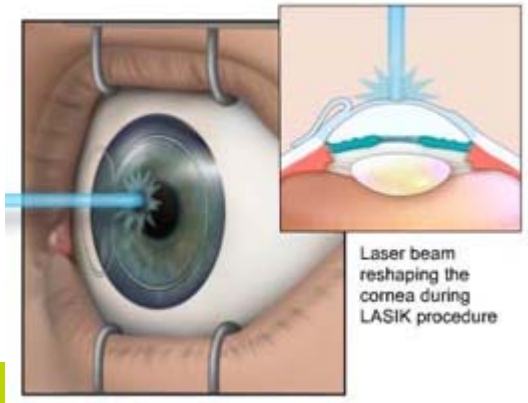
Amplificació de llum per emissió estimulada de radiació

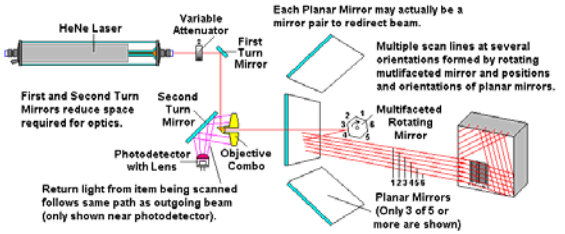




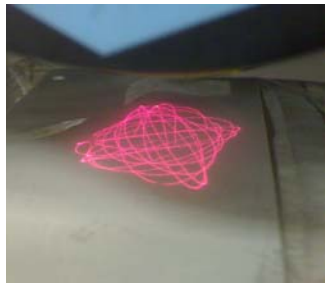




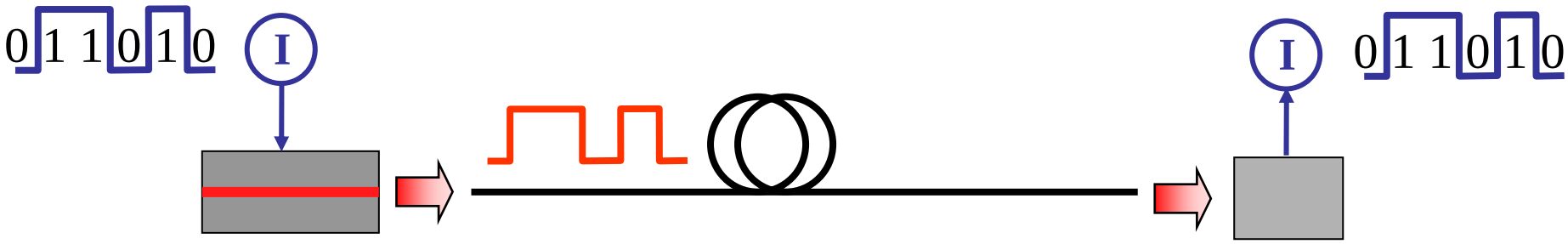




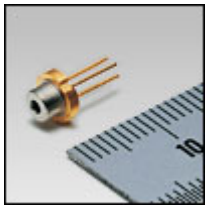
Optical Path of Typical Supermarket Checkout Barcode Scanner

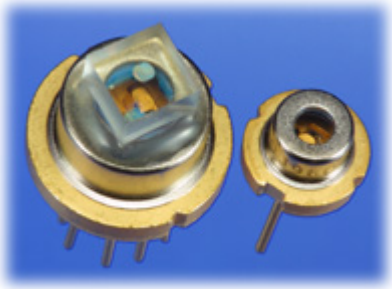


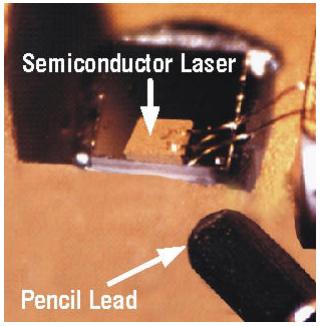
Sistemes de comunicacions òptiques



Làser de semiconductor **Fibra òptica** **Fotodiode**







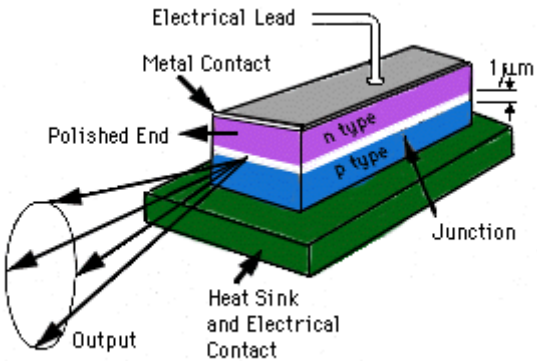
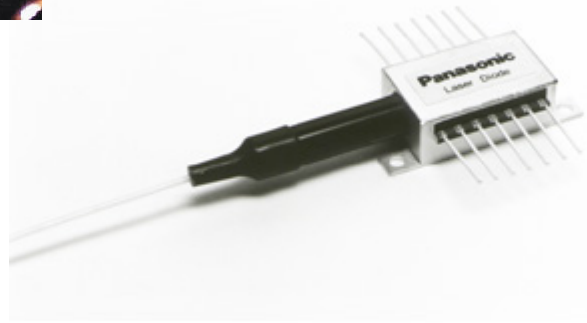


Diagram of Semiconductor Laser



High power DFB Semiconductor Laser for Optical Communication
Semiconductor Company, Matsushita Electronics Corporation
September 2000

El missatge es completament distorsionat abans de la transmissió emprant un algorisme i una clau específica.

Exemple: Algorisme de Vernam

US Pattent 1310719, 22 de Juliol de 1919

La porta lògica xor:

entrada 1	0	0	1	1
entrada 2	0	1	0	1
sortida xor	**0**	**1**	**1**	**0**

Xifrat:

Missatge: "uib"	01110101 01101001 01100010
Clau: nombre aleatori d'igual longitud	00100001 00100000 00000011
Text xifrat	01010100 01001001 01000001

Desxifrat:

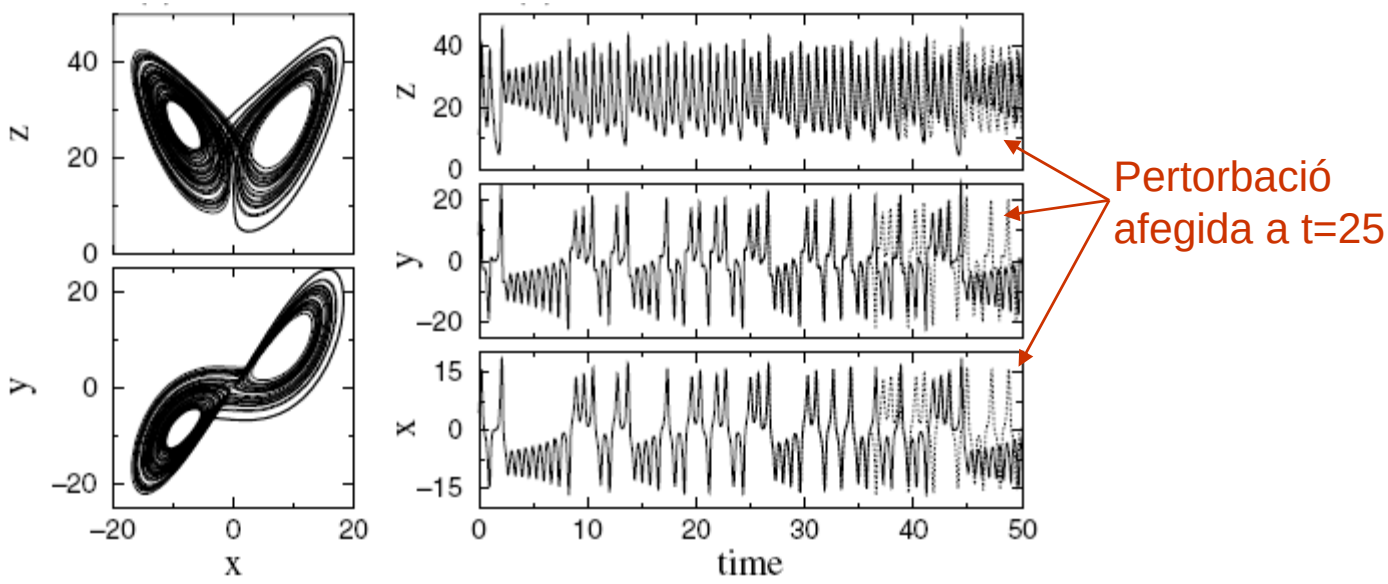
Text xifrat	01010100 01001001 01000001
Clau	00100001 00100000 00000011
Desxifrat: xor (text xifrat i clau)	01110101 01101001 01100010

Els sistemes amb comportament caòtic es caracteritzen por la gran sensibilitat a petites variacions de les condicions inicials.

La separació entre dues trajectòries que comencin en punts propers creix exponencialment amb el temps.

Els exponents de Lyapunov mesuren aquest creixement

Exemple:
Modelo de Lorenz



Idea: Emprar com portadora una senyal caòtica en la que podem ocultar el missatge.

Problema: ¿Com pot extreure el missatge el receptor autoritzat?

Determinació de la posició en alta mar

Navegació al segles XVI i XVII.
A alta mar es fàcil determinar la latitud mesurant la inclinació del sol al migdia i coneixent el dia de l'any.

El problema latent es la determinació de la longitud.

Solució: Rellotge al vaixell posat en hora al port de sortida. Per cada hora de diferencia entre el rellotge i l'hora local (posició sol) la longitud ha canviat en 15 graus.

PERÒ: Els rellotges son de pèndul i després de dies de navegació acostumen a endarrerir-se o avançar-se uns quants minuts.
I un error de 5 minuts equival a 140 Km!

⇨ **Es necessiten rellotges mes precisos.**

Huygens

Christiaan Huygens desenvolupava rellotges d'alta precisió per a la marina holandesa.

Extrait d'unne Lettre eferite de la Haye, le 26 Fevrier 1666

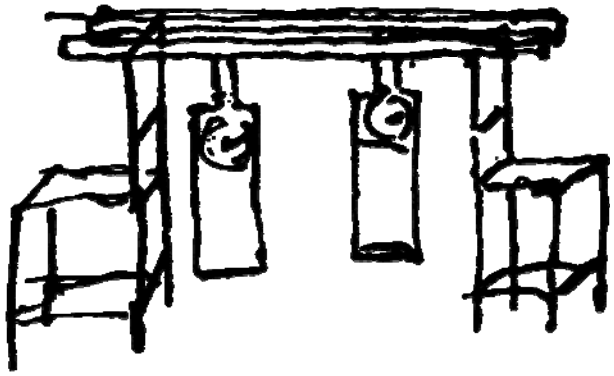
Ayant efté abligé de garder la Chambre pedant quelques jours, mefmes occupé à faire des obfervations fur mes deux Horloges de la nouvelle fabrique, j'en ay remarqué un effet admirable, auquel perfonne n'auroit jamais pu penfer. C'eft que ces deux Horloges eltant fufpendües l'une à cofté de l'autre, à la diftance d'un ou deux pieds, gardent entr'elles une jufteffe fi exacfe, que les deux Pendules battent toufiours enfemble, fans jamais varier. Ce qu'ayant fort admiré quelque temps; j'ay enfin trouvé que cela arrivoit par une efpece de fympathie: en forte que failant battre les pendules par des coups entremeflez; j'ay trouvé que dans une demie heure de temps, elles fe remettoient toufiours à la confonance, la gardoient par apres conftamment, auffi long-temps que je les laiffois aller.

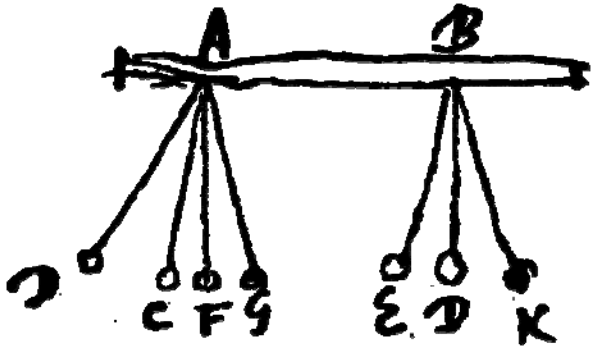
….

Leur accord n'eftoit venu auparavant que de quelcome fympathie, qui ne peut à mon advis, aovoir autre caufe, qu'ue agitation imperceptible de l'air, qui fe produit par le mouvement des Pendules.

Journal des Scavants, 16 marzo 1665

Experiments de Huygens





Observation a faire sur le dernier article du precedent Journal, où il eft parlé de la Concordance de deux Pendules fufpenduës à trois ou quatre pieds l'une de l'altre.
…
En effet, ayant examiné la chofe avec plus d'exactitude, il a reconnu que cet accord ne venoit que de ce qu'il avoit fupendu les deux pendules à un mefme bafton, qui recevoit une impreffion fecrette des pendules, enfuite leur communiquoit fon mouvement, qui leur eftant commun, les mettroit à la concordance …

Il ne fault pas qu'on trouve cette retraction eftrange: car tout le monde peut fe tromper dans fes premieres penfées. Mais il n'y a que les grands hommes qui reconnoiffent incontinenent la caufe de leur error, qui la veulent bien avoüer.
Journal des Scavants, 23 marzo 1665

Cuques de llum a Malàisia, Tailàndia i Nova Guinea

J. Buck & E. Buck, Scientific American Maig 1976.

S.H. Strogatz, I. Steward, Scientific American, Des. 1993; Investigación y Ciencia, Feb. 1994

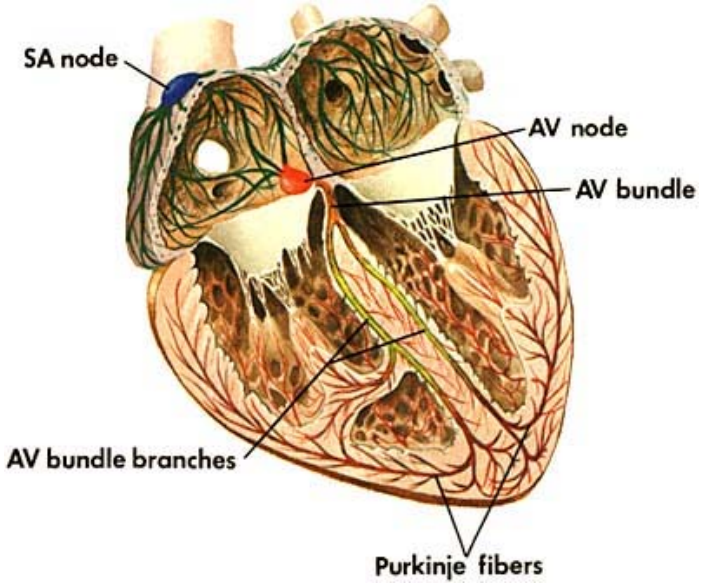
Millennium Bridge, Londres 10 juny 2000

Altres exemples de sincronització

Cor: node sinoatrial: 10000 cèl·lules sincronitzades actuant de marcapassos.

Pàncrees: cèl·lules productores d'insulina.

Cervell i Medul·la: xarxes de neurones que controlen comportaments rítmics com ara respirar, córrer, mastegar …



Ritmo de aplaudiments en un conciert. Z. Neda et. al. Nature **403**, 849 (2000).

I, ja que hi som, ¿podem sincronitzar dos sistemes caòtics?

Sincronització de sistemes caòtics

Dos sistemes es sincronitzen quan ambdós fan el mateix, es a dir, la trajectòria d'un d'ells s'aproxima a la de l'altre i romanen properes a tot temps.

En sistemes caòtics la separació entre dues trajectòries que comencin en punts propers **creix** exponencialment amb el temps.

Si tenim dos sistemes caòtics idèntics, encara que comencem amb condicions inicials pràcticament iguals, les trajectòries de seguida estaran descorrelacionades.

¿Podem sincronitzar dos sistemes caòtics?

Sí!, si els sistemes son similars i els acoblem de forma apropiada.

Pecora & Carroll, Phys. Rev. Lett. **64**, 821 (1990)

Acoblaren unidireccionalment la sortida X del Lorenz a un sistema resposta. El sistema resposta es un Lorenz modificat que fa servir el valor de X que prové del mestre.

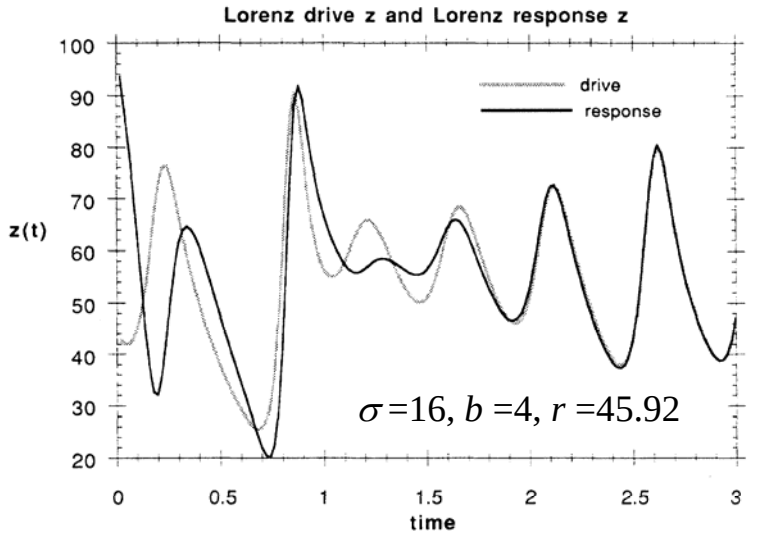
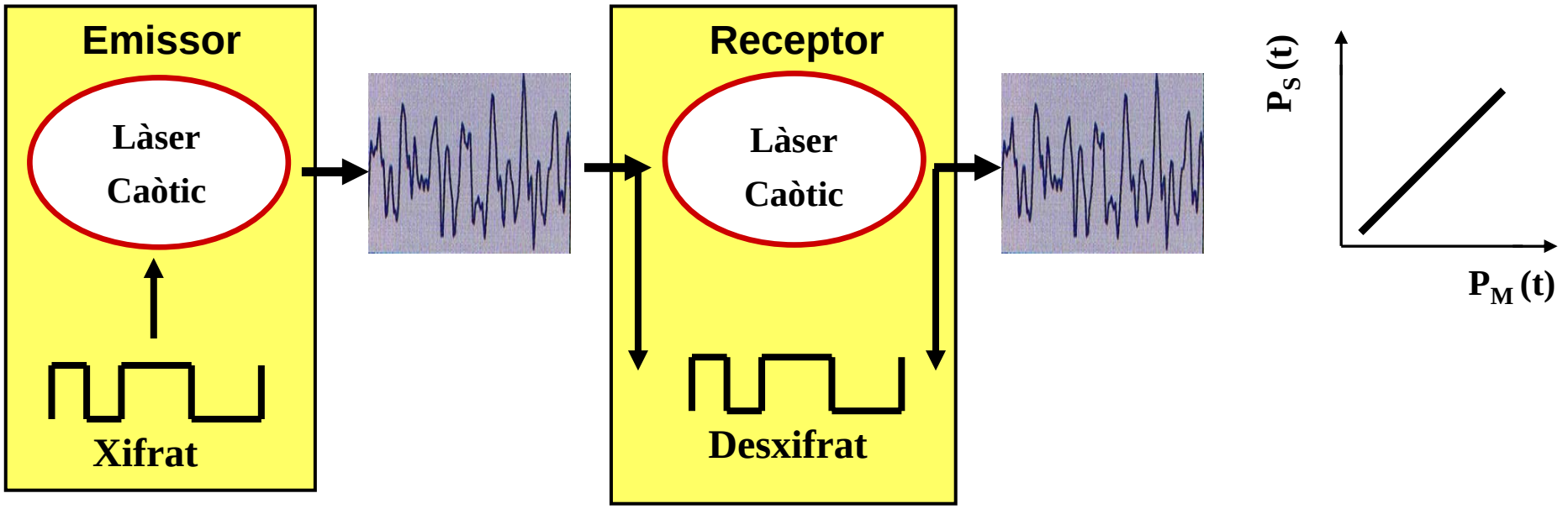


FIG. 1. Time series of the z component of the x-driven (y,z) Lorenz subsystems showing the convergence of the response $z(t)$ to the drive $z(t)$.

Comunicacions amb làsers caòtics



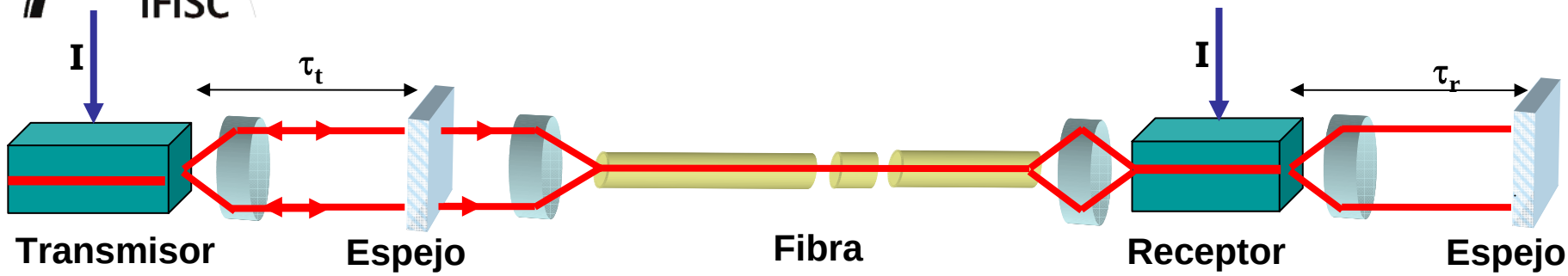
*** La sincronització només es possible si el receptor es l'adequat.**

*** Missatge d'amplitud molt menor que la portadora.**

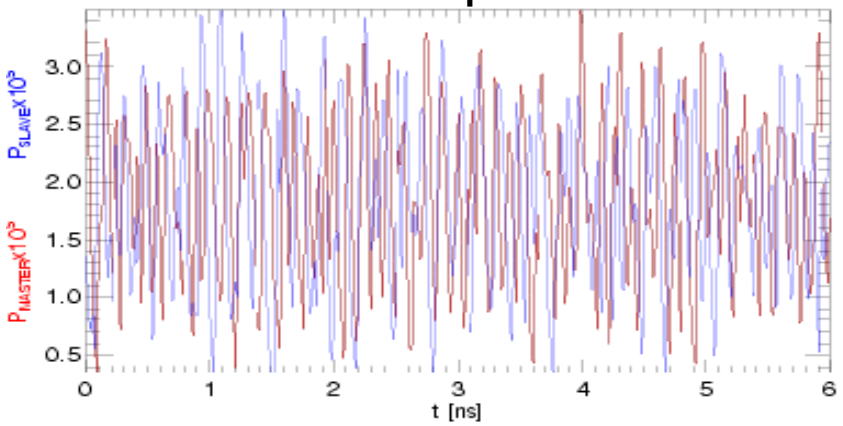
*** El làser receptor es sincronitza amb la portadora permetent desxifrar el missatge**

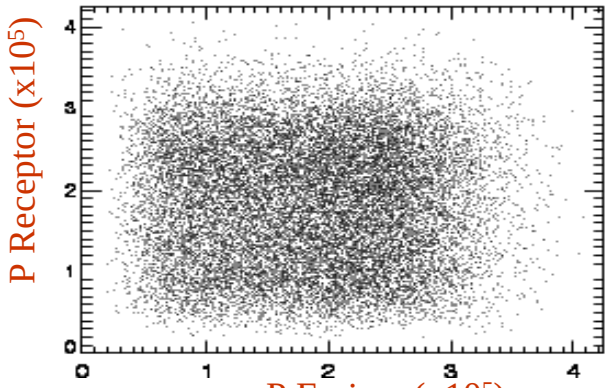
Comunicacions fent servir circuits electrònics caòtics: Cuomo & Oppenheim, PRL **71**, 64 (1993).
Comunicacions amb làsers d'estat sòlid caòtics: P. Colet & R. Roy, Opt. Lett. **19**, 24 (1994).

Sincronización de láseres de semiconductor

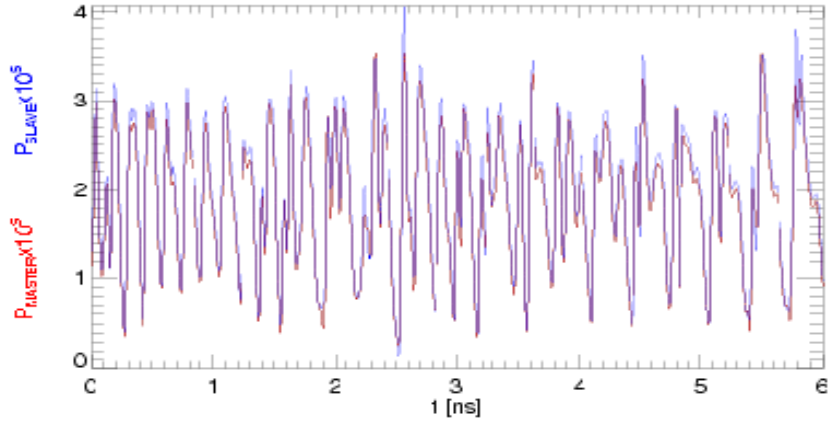


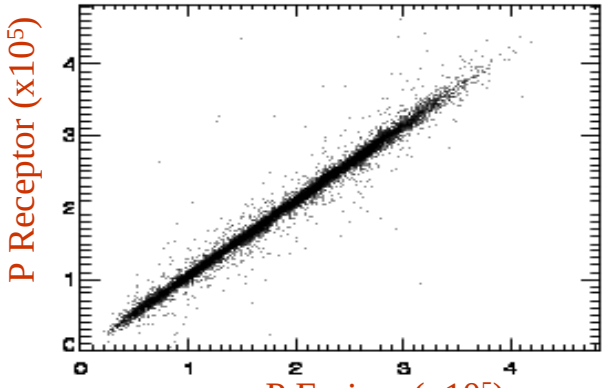
Sin acoplamiento



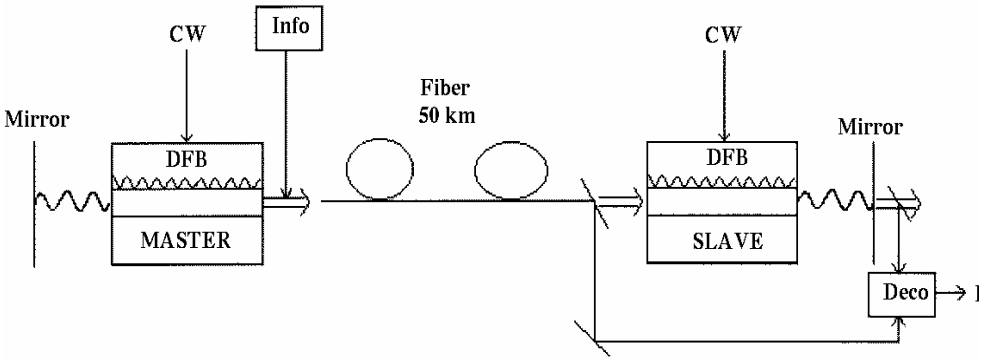


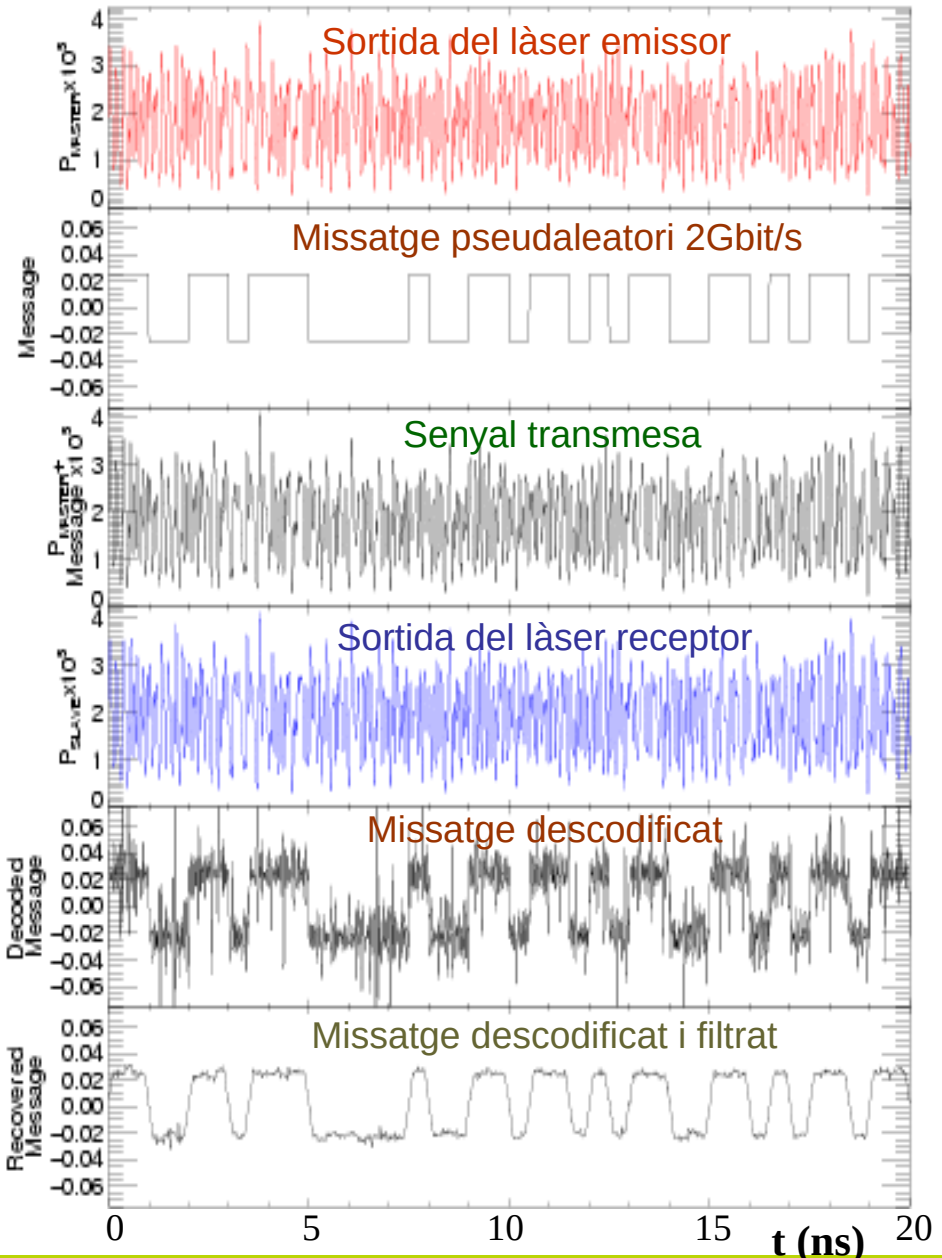
Con acoplamiento





Transmissió de missatges





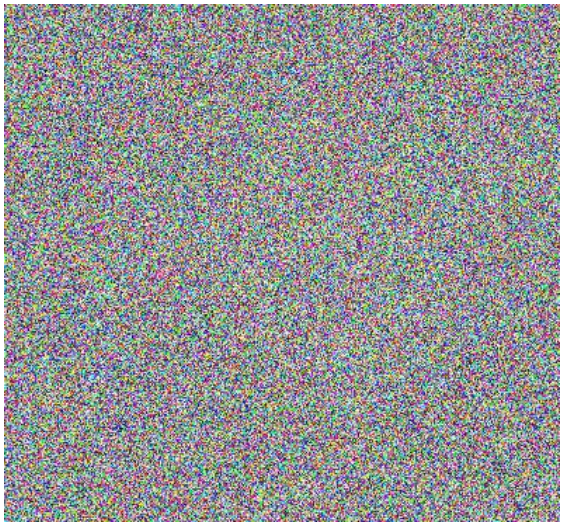
C.R. Mirasso, P. Colet & P. García-Fernàndez,
Phot. Tech. Lett. **8**, 299 (1996)

Exemple: xifrat d'una imatge

Imatge original

Imatge desxifrada

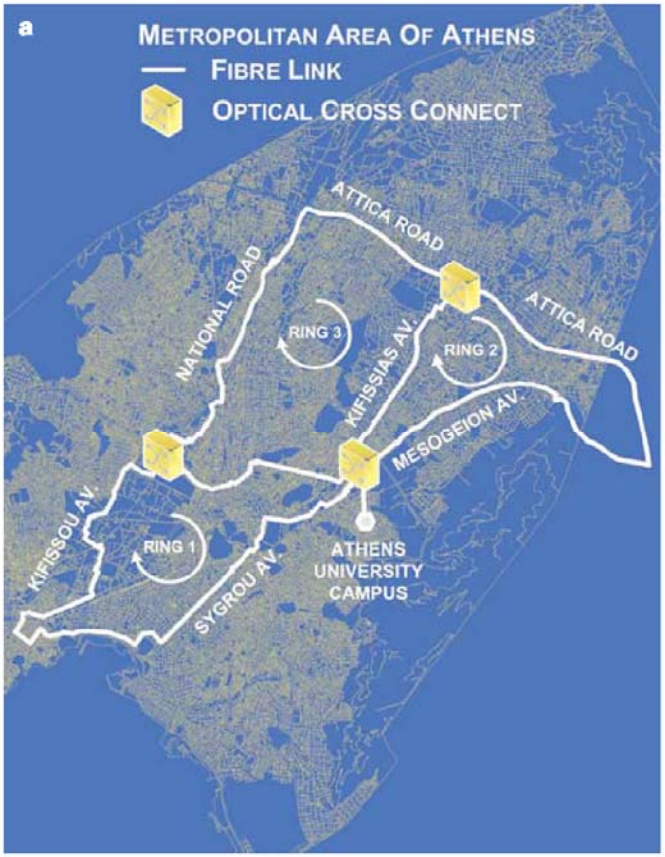
Imatge transmesa

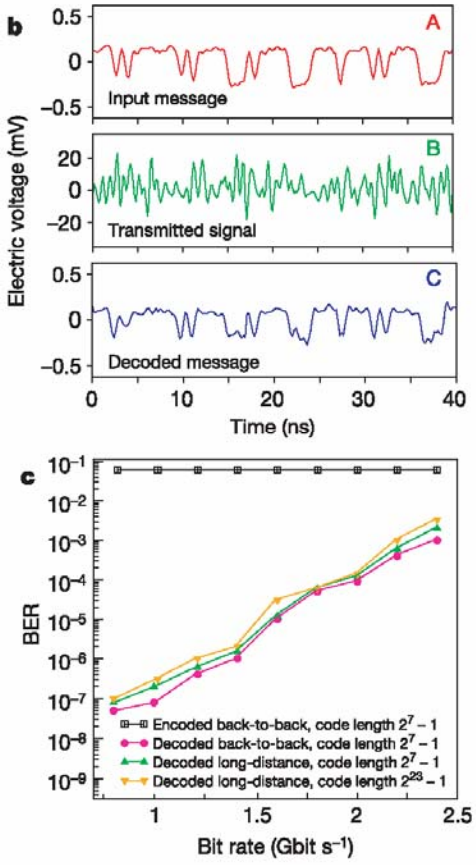


Tassa d'errors < 10^{-6}

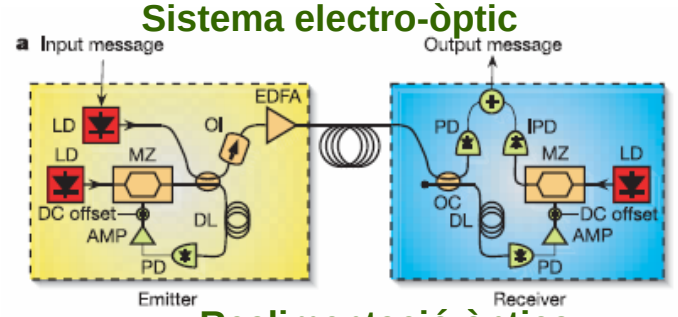
Demostració de camp

Proyecto europeo OCCULT (IST-FET Open) (2001-2004).
http://ifisc.uib-csic.es/project/occult

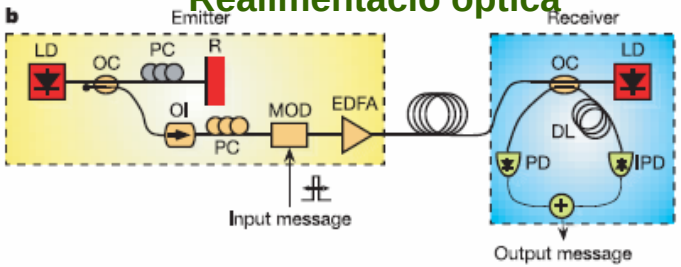




Sistema electro-òptic



Realimentació òptica



A. Argyris et al. Nature, **437**, 343 (2005)

Resumen

- Seguretat i privacitat son assumptes molt importants en xarxes de comunicacions.
- Transmissió de missatges. La radio.
- Informació en forma digital.
- Sistemes de comunicacions òptiques.
- Criptografia.
- Caos.
- Sincronització.
- Sincronització de sistemes caòtics.
- Comunicacions secretes emprant làsers caòtics.
  - Compatible con encriptació per software i proporciona seguretat addicional.
  - Missatge emmascarat en portadora caòtica generada per làser semiconductor
  - Només el receptor autoritzat es sincronitza a portadora caòtica.
  - Desxifrat: comparant entrada al receptor (caos+missatge) amb resposta del receptor.

El caos pot ser útil!