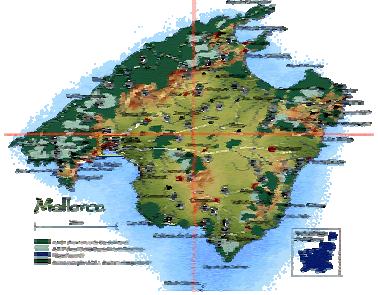
Palma de Mallorca
Spain



Communicating with Chaotic Light

Claudio R. Mirasso

Departament de Física, Universitat de les Illes Baleares

http://nova.uib.es/project/occult

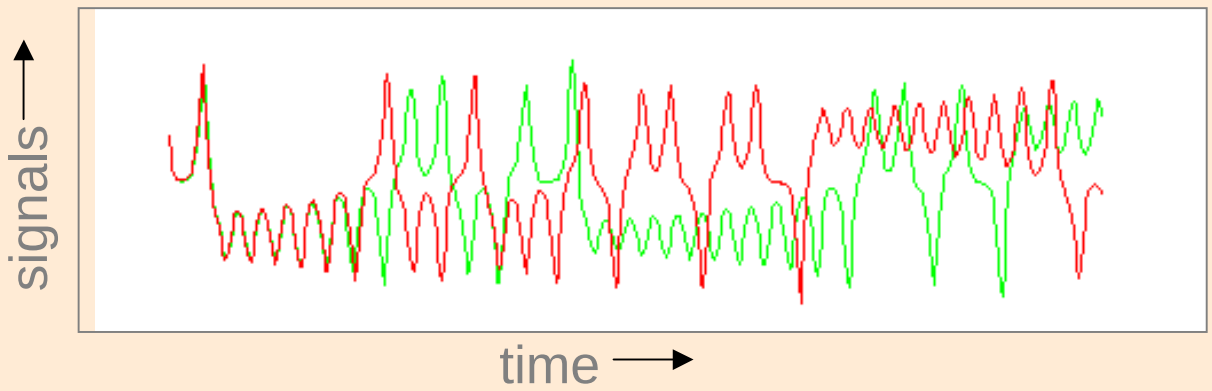
IST FET
Open Domain
2001-2004

Outline

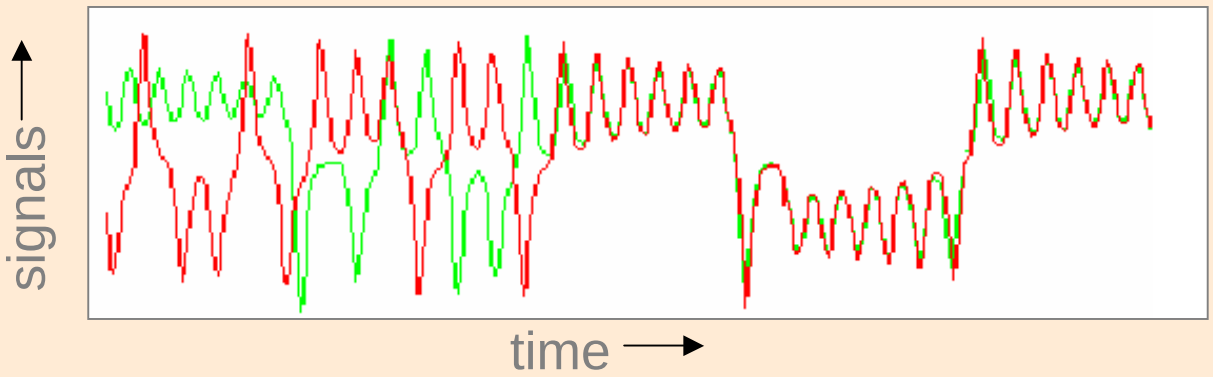
- Synchronization of Chaotic Systems
- Encryption Techniques
  - Software Cryptography
  - Quantum Cryptography
- Optical Chaos Cryptography
- Chaos Generators / Receptors
- Eavesdropper attacks
- Information Encryption
- Conclusions and challenges for the future

Synchronization of Chaotic Systems

- A system operates in a chaotic regime when its output fluctuates erratically in time
- The outputs of two identical systems started at nearly the same initial conditions quickly become uncorrelated



- **Two systems synchronize when the trajectory of one of the systems converge to the one of the other and both trajectories remain close to each other in time.**



- **The synchronization appears to be structurally robust.**

Software Encryption

- Privacy and security are major issues in communication services networks.
- Up to now, these issues have been covered by using key cryptosystems.

- Nowadays, all widespread encryption methods are based on software implementation where a message is completely scrambled before its transmission according to a given key
- Data Encryption Standard uses a single key for both encryption and decryption.

- **Public key encryption:** Bob and Alice, wishing to exchange messages in a secure way, use pair of keys; one is published while the other is kept secret.
- A file encrypted with one key can be decrypted by the other of the same pair, but not with the key by which it was encrypted.
- This technique is more secure but slower.
- Most of the algorithms contain keys of length between 250 – 512 bits.

Quantum Cryptography

- It is proposed as a method to exchange a key, by the interaction of sender and receiver; the key will be later used with a standard software algorithm for encryption.
- The method can reveal if the key is intercepted by an eavesdropper during transmission.
- In this case that portion of the key is simply discarded and the key construction procedure is continued.
- Quantum cryptography is based on the fact that when making a measure on a particle (photon) its properties (polarization) are altered.

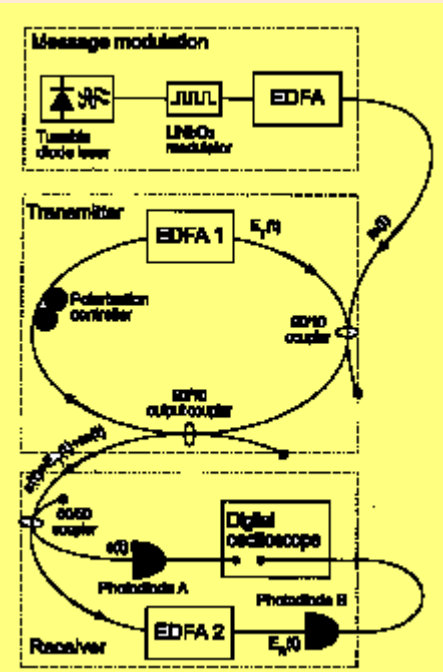
Chaos Communications

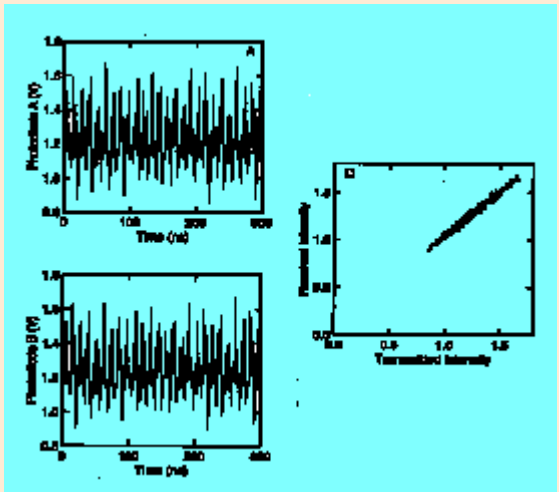
- Started with the ideas of Thomas & Carrol, Hayes & coworkers that at beginning of 90th studied the synchronization properties of chaotic systems.
- It was postulated that chaos could be used to encode information
- Cuomo and Openheim (Phys. Rev. Lett. 71, p. 65, 1993) demonstrated, using chaotic electronic circuits, that it was possible to encode and decode a message in such a system.
- Electronic circuits have low bandwidth (few tens of KHz) and are in general low dimensional systems => *easy to break the code*
- These limitations can be overcome by using high dimensional chaos generated by non-linear electro-optical devices

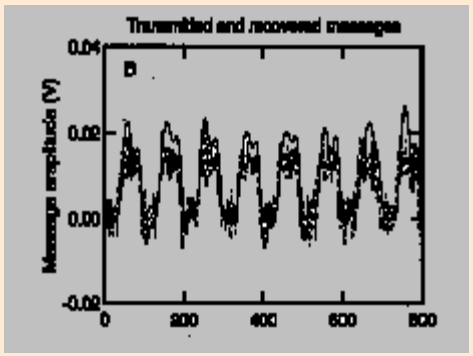
Optical Chaos Communications

- An alternative way to improve security is by additionally encoding at device level (hardware encryption) using chaotic carriers generated by components operating in the non-linear regime.

G.D. VanWiggeren and R. Roy, Science vol. 279, p. 1198 (1998).







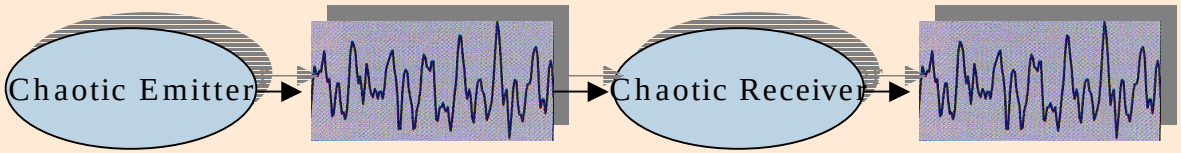
Up to hundred Mbit/s and transmission distances of ~ 100 Km

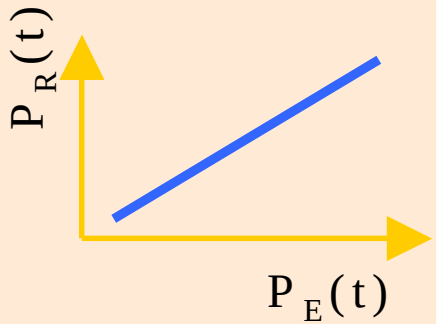
Not very non-linear → *"easy" to break*

- **Semiconductor lasers can very well overcome the limitations of fibre lasers and are ideal candidates to for these non-linear optical emitter / receiver systems due to many reasons:**
  - **Easily exhibit high-dimensional and complex chaotic behavior with large bandwidth (~ tens of GHz)**
  - **Reliable, compact and low cost sources**
  - **Their dynamics is well understood**
  - **Fully compatible with optical fiber networks**
- **Theoretically proposed and numerically verified in 1996 by two independent groups**
  - **C. Mirasso et al., Phot. Tech. Lett 8, p. 299, 1996**
  - **V. Annovazzi-Lodi et al., J. Q. E. 32, p. 953, 1996.**
- **Experimentally demonstrated by J.P. Goedgebuer et al., Phys. Rev. Lett. 80, p. 2249, 1998**

How does the encoding / decoding process work?

- Two spatially separated chaotic lasers can synchronise to each other when a small amount of the output of one laser is injected into the other. Consequently the irregular time evolution of the emitter laser light is well reproduced by the receiver laser.



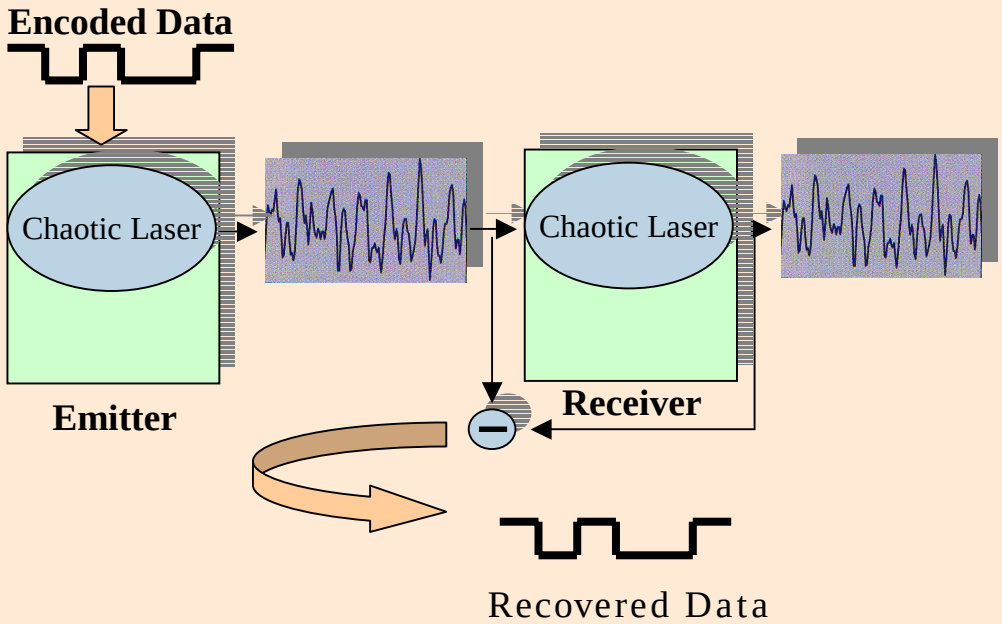


- Synchronization can be only achieved when using very similar components for both chaotic systems, with close matching parameters and operation conditions (within ~ 2 %).

- Once the two lasers have been synchronized, the chaotic output of the emitter can be used as the carrier on which the message is encoded.

- The other laser, in the receiver system, allows the message to be extracted.

- It turns out that the receiver synchronizes to the chaotic oscillations of the emitter (the carrier) suppressing the encoded message (a very small perturbation of the carrier). By comparing the input (carrier + message) and output (carrier only) of the receiver, the message can be extracted.



Chaos Generator / Receptor

	Physical	Technical
PERFORMANCE	good signal/carrier discrimination	robust
	broad bandwidth	compact design
	well-controllable system parameters	well-controllable system
	small signal / carrier modulation	low-cost design
SECURITY	broad bandwidth	
	white rf-spectrum	
	strong nonlinearity	
	rapidly decreasing correlation	
	high-dimensional dynamics	
	secure encoding methods	

- **Three main types of optical chaos generators:**
  - **Non-linear electro optical feedback; linear laser**
  - **Linear electro-optical feedback; non-linear laser**
  - **Linear all-optical feedback; non-linear laser**

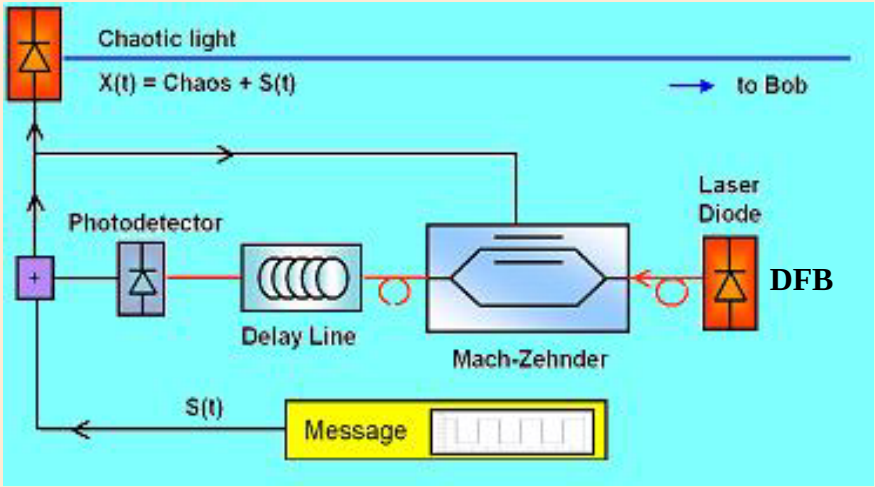
- **Non-linear electro-optical feedback: followed by Jean Pierre Goedgebuer group, Besançon and Metz, France.**

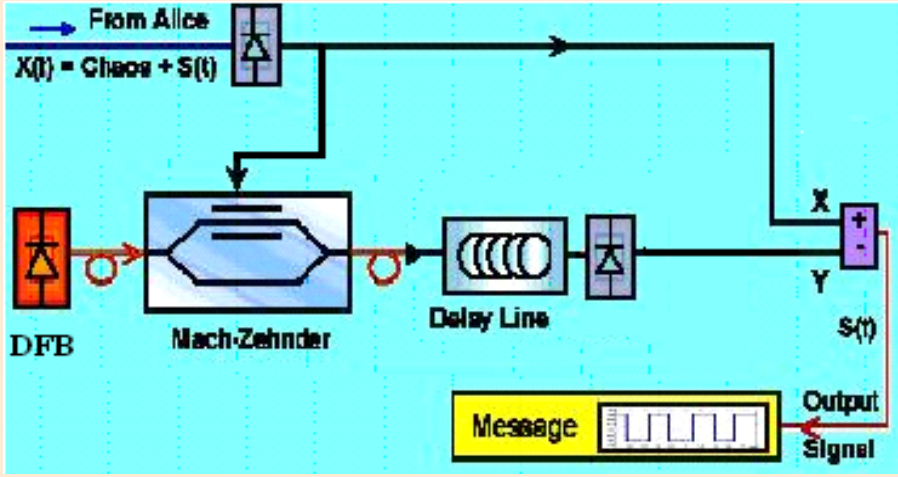
- **Linear electro-optical feedback: followed by Jia-Ming Liu group, University of California, Los Angeles.**

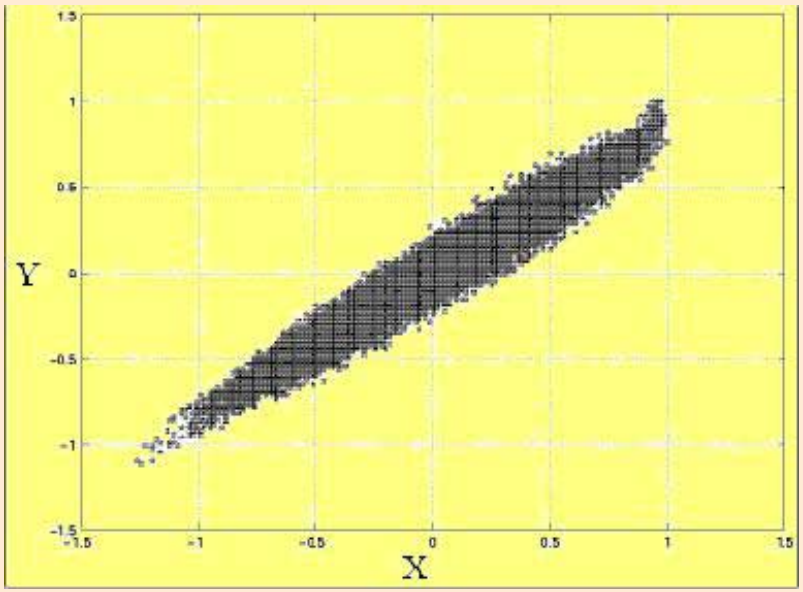
- **Linear all-optical feedback: followed by different groups: I. Fischer, Technical University of Darmstadt, Germany, K. A. Shore, Bangor, Wales, J. Ohtsubo, Shizuoka University, Japan, Y. Liu and P. Davis, ATR Japan, P. Colet and C. Mirasso, Mallorca, Spain**

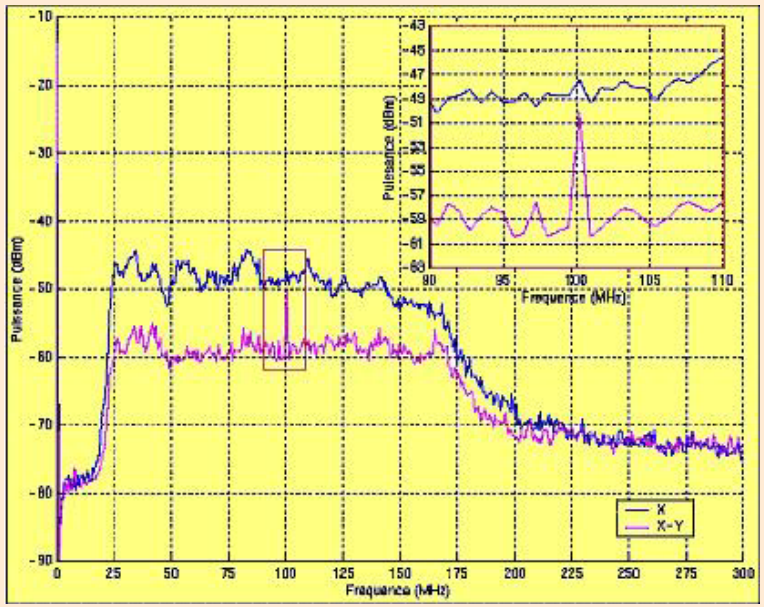
Chaos Generator / Receptor
Electro-optical Feedback

J.P. Goedgebuer Group
France (Experimental)



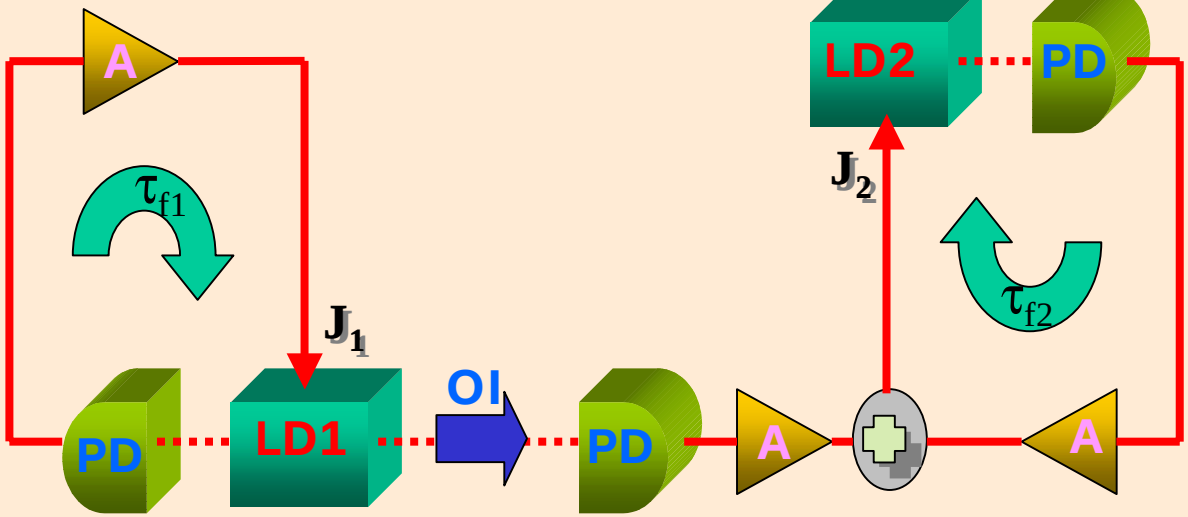


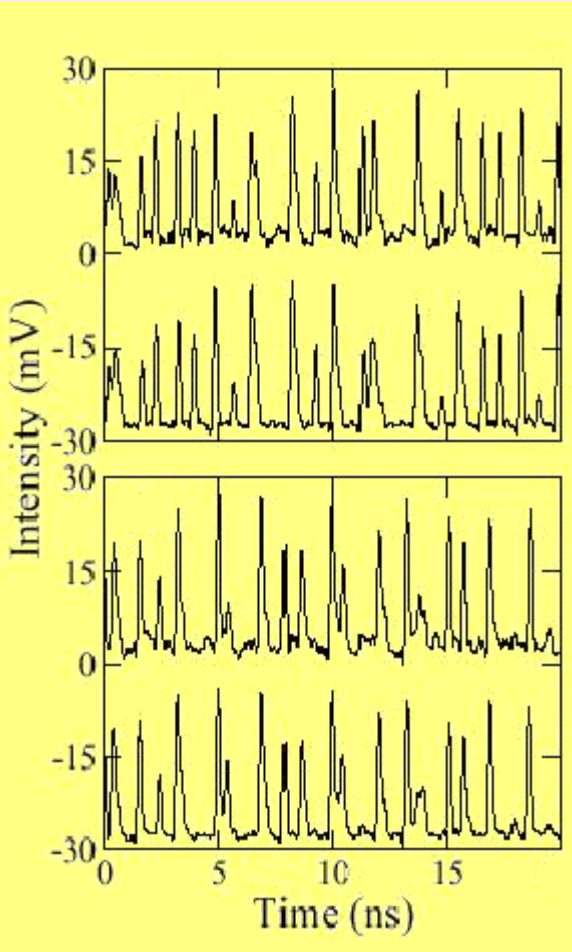


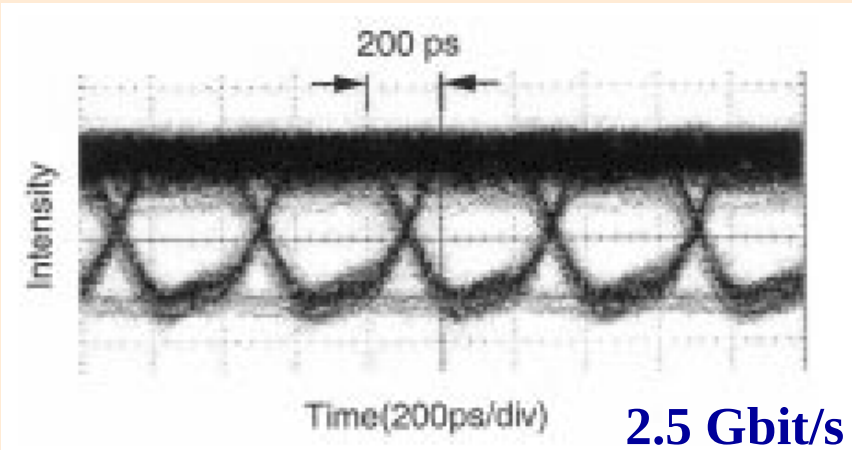


Chaos Generator / Receptor
Linear Electro-optical Feedback

J.L. Liu Group
USA (Experimental)



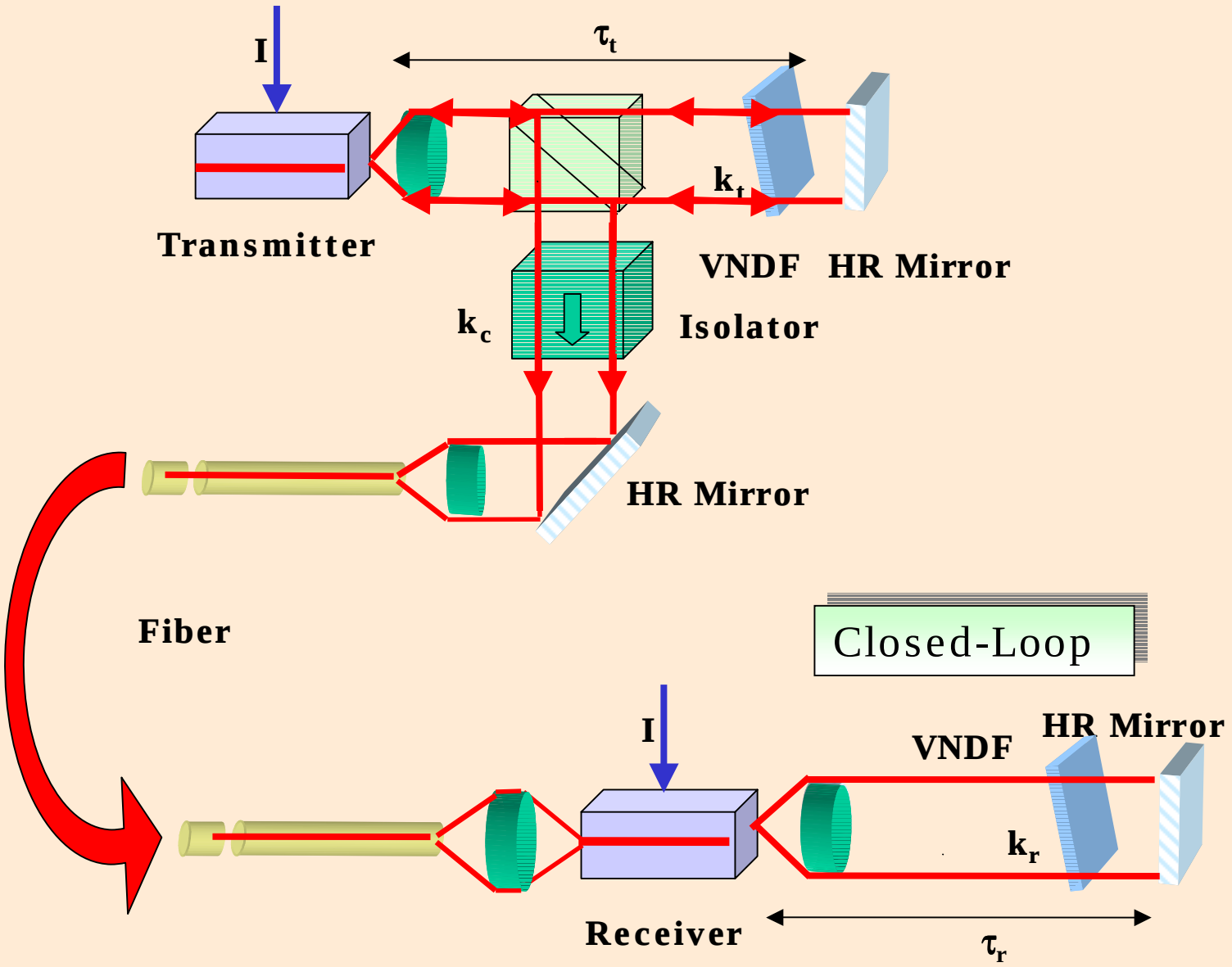




2.5 Gbit/s message

Chaos Generator / Receptor
All-optical Feedback

Several Groups
(Experimental)



Open vs. closed loop receivers

Open loop receiver

- The external cavity has been removed
- Good synchronisation quality is obtained
- Easier to implement and feedback phase independent
- Synchronisation properties robust against detunings of several GHz and small parameter deviations
- Short re-synchronization times (~ hundred ps)

Closed loop receiver

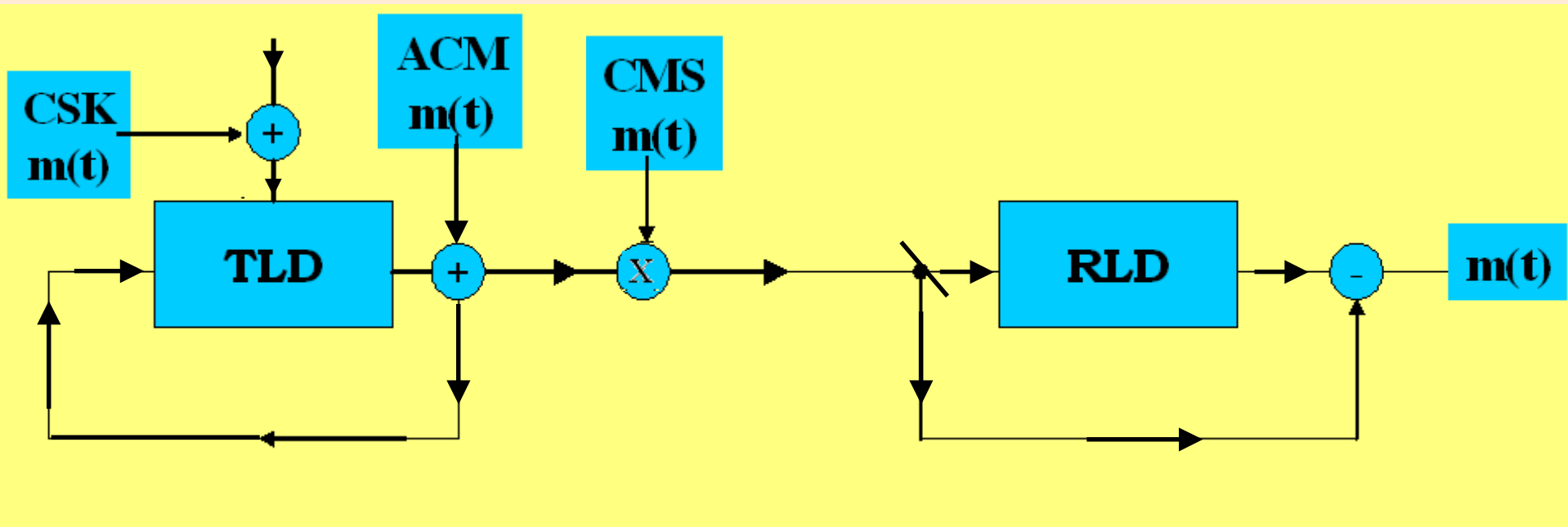
- External cavity lengths have to be adjusted within tens of nm
- Very good synchronization for $F_{rel} = 0$ and very low for $F_{rel} \sim \pi$
- Synchronisation properties robust against detunings of several GHz and small parameter deviations
- Long re-synchronization times (~ hundred ns)

Chaos Modulation Schemes

Chaos Modulation (CM)

Chaos Masking (ACM)

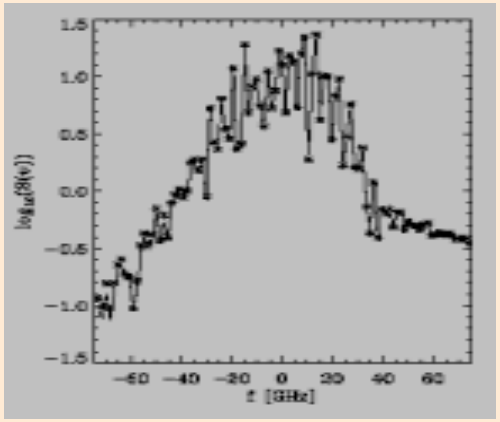
Chaos Shift Keying (CSK)



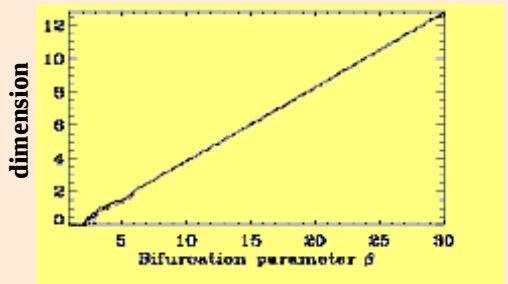
Eavesdropper attacks

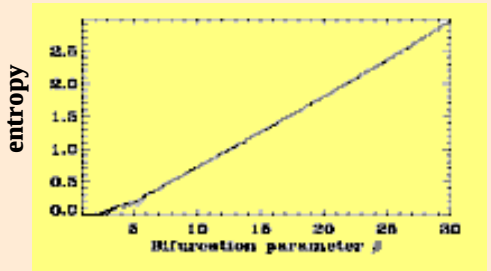
- Very fast pulsations (GHz) very difficult to detect.

- Fourier analysis or linear filtering process would fail since the amplitude of the message is very small.

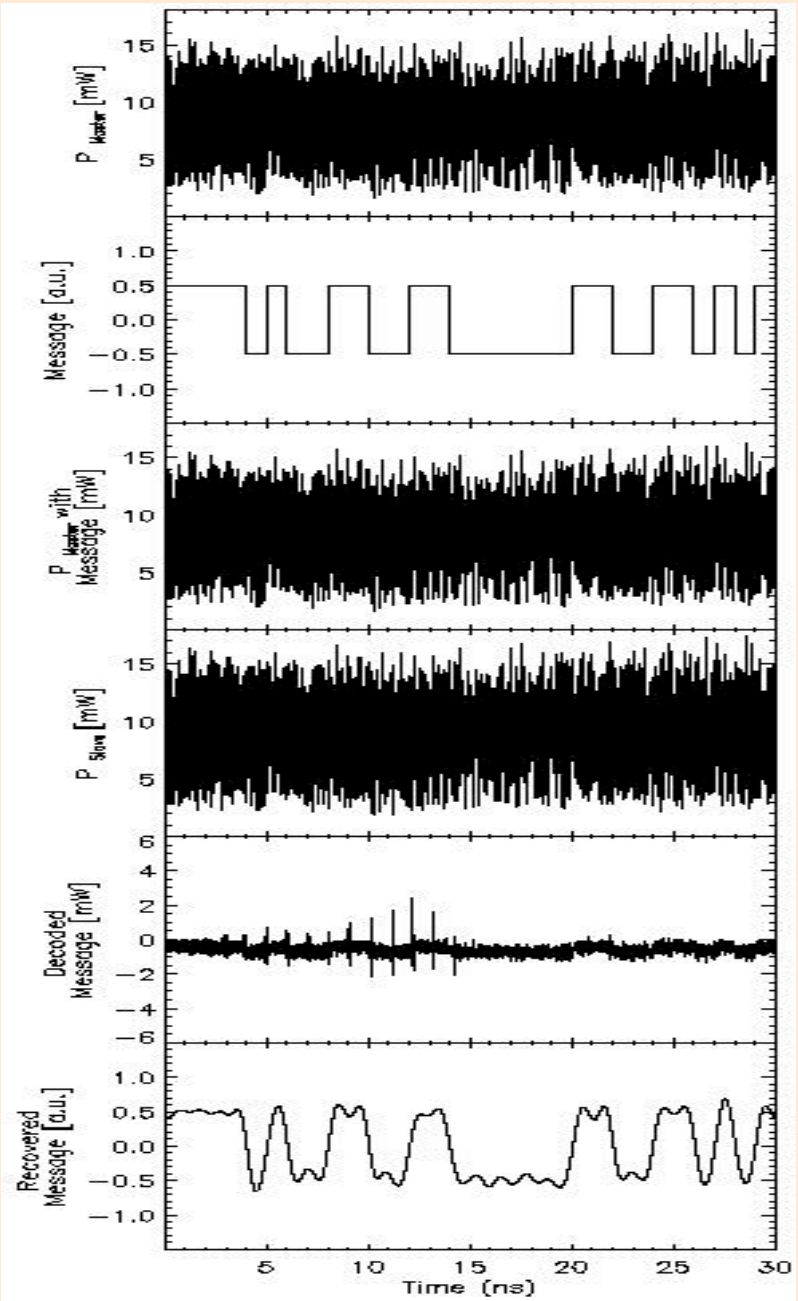


- High dimensional chaos can be generated whose complexity increases with the feedback strength but saturates with the delay time





Message encoding / decoding: Numerical Simulations



←Ouput of the transmitter

← Message to be encoded

← Ouput of the transmitter with message

← Ouput of the receiver

← Recovered message

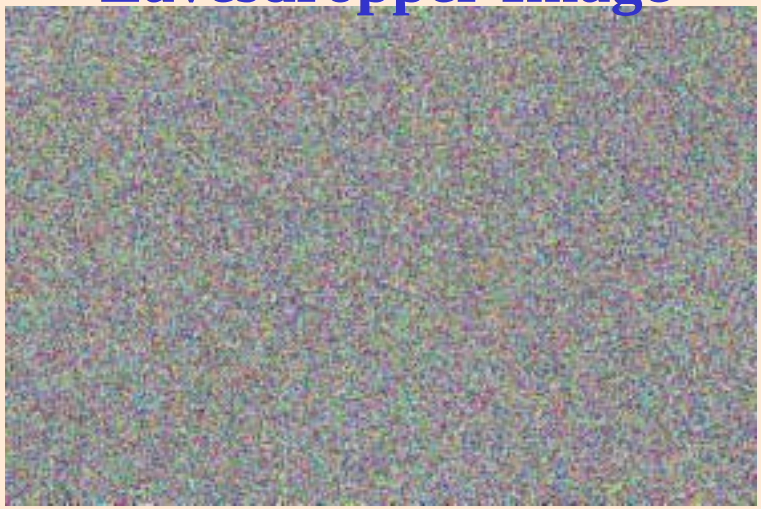
← Recovered message after filtering

Image Encoding / Decoding
(same conditions as previous example)

Encoded Image

Decoded Image

Eavesdropper Image



BER < 10^{-6}

Conclusions

- Optical chaos communications could be used as a complementary technique to improve privacy and security
- The technique can be very well combined with software encryption yielding a second level of security.
- Several ways of generating chaos can be implemented by using diode lasers: electro-optical (linear and non-linear) and all optical
- Receiver architectures have to match the emitters.
- Different techniques for encoding (CSK, ACM, CM)
- Synchronization and message encoding/decoding have been successfully achieved at laboratory level at high bit rate (100 Mbit/s – 1 Gbit/s), still with large BER.

IEEE J. Quantum Electron. Feature Section on “Optical Chaos and Applications to Cryptography”, Sep. 2002

Challenges for the Future

- Experiment with messages at higher bit rate
- Transmission of chaotic carriers through optical fibers
- Identification of parameters for key production
- Studies on eavesdropper attacks (neural networks)
- Integration in compact sources
- Analog/digital – Digital/analog conversion at high frequencies.