Reprint from: *Proceedings Fotonica 95,* Sorrento 1995, pp.463-466, published by AEI Milano

CRITTOGRAFIA OTTICA CAOTICA

S. Donati, V. Annovazzi Lodi
Dipartimento di Elettronica, Università di Pavia
27100 Pavia, tel. 0382 505 204

ABSTRACT: Chaotic phenomena (such those found in coupled laser sources and nonlinear feedback interferometers) can be used for the cryptography of optical signals. In addition to give a further method to increase security of communications, chaotic cryptography offers the unique advantage of being capable to spread the signal on a so large optical bandwidth (i.e. >100 GHz) that the signal cannot be recovered by electrical-domain techniques by the eavesdropper.

1. INTRODUZIONE

I primi esempi storici di crittografia delle comunicazioni scritte risalgono ai tempi degli antichi egizi. Anche dei romani sono riportati esempi di crittografia per sostituzione e per trasposizione dei simboli. Nel Rinascimento, la tavola alfabetica di Cardano ha costituito per lungo tempo un semplicissimo ed efficace metodo di crittografia a sostituzione ciclica.

Oggigiorno, con lo sviluppo dei servizi di comunicazione ad accesso libero da parte di un numero elevatissimo di utenti, il problema della protezione dei dati diventa sempre più importante e potrebbe costituire il vero collo di bottiglia per lo sviluppo estensivo delle applicazioni di affari. Da qui la necessità di sviluppare efficienti tecniche di crittografia ad alta resistenza all'intrusione [1].

Ricordiamo che, dal punto di vista di sistema, esistono differenti livelli ai quali la crittografia della comunicazione può essere effettuata e cioé:

- contenuto del messaggio
- simboli del messaggio
- codifica
- modulazione
- portante

A livello di contenuto appartengono le cosidette tecniche *subliminali* - che consistono nel nascondere il vero messaggio in un altro innocuo o inutile, e come tale riconosciuto e perciò scartato dalla spia [come semplici esempi, sono subliminali la scrittura con inchiostro simpatico o la codifica a punti e linea Morse con le i e le t di un messaggio, usato nella seconda guerra mondiale]. E' ovvio che in tal caso la chiave di decifrazione è il punto debole di sistema.

La crittografia dei simboli (dell'alfabeto usato) e della codifica (di trasmissione) sono le più usate e meglio si prestano all'implementazione di sofisticate tecniche di

elaborazione, ad es. con livello multiplo di crittografia, che rendono difficile la decifrazione. Ma poichè la spia si presume conosca tutte le tecniche applicabili di crittografia e abbia a disposizione gli stessi strumenti di elaborazione del cifratore, il confronto tra i due è solo sui tempi d'attesa necessari a scoprire la chiave e decifrare il messaggio, una volta che questo è stato acquisito dalla spia.

Contro l'acquisizione del messaggio si possono usare tecniche di crittografia della modulazione (ad es. con modulazioni esotiche) o della portante (spread-spectrum), oggetto di notevole lavoro di sviluppo in ambito di applicazioni militari. Anche in questo contesto, tuttavia, il lavoro dei crittografi progredisce parallelamente a quello dei decrittografi e soltanto il continuo sforzo innovativo può rendere ragionevolmente sicura la trasmissione crittografata. E' da notare che queste tecniche spostano la chiave di decifrazione dal software all'hardware, e che, contrariamente alle applicazioni usuali, lo schema più complicato è il preferibile - purchè robusto - perchè più difficile da individuare.

In questo contesto rientra la *crittografia ottica* mediante *caos*. L'idea di base consiste sostanzialmente nell'impiegare come portante l'uscita (ottica) di un sistema che genera il caos. In tali sistemi, ampiezza e fase sono variabili nel tempo, con andamento e con spettro di potenza del tutto simili a quelli di un rumore a largo spettro; a differenza però del rumore, ampiezza e fase del sistema caotico sono deterministiche nel senso che hanno la stessa evoluzione a partire da una stessa condizione iniziale.

Se l'informazione viene impressa al trasmettitore sulla sorgente caotica attraverso l'ampiezza o la fase in modo appropriato, si può ottenere che né l'evoluzione nel dominio del tempo, né lo spettro di potenza rivelino l'avvenuta modulazione. Viceversa, il ricevitore che dispone di un identico (nominalmente) sistema caotico è in grado di rivelare l'informazione attraverso le variazioni di evoluzione osservate.

Ovviamente, la crittografia caotica può essere usata anche a livello di codifica, su un normale segnale elettrico a frequenza molto più bassa dell'ottico (CSK, chaos shift keying) e in tal caso è la simulazione numerica a calcolatore a fornire la forma d'onda caotica. Rispetto a tale approccio, il sistema *caotico ottico* ha un *definito vantaggio*: esso può essere fatto emettere su una banda di frequenza elevatissima (ad es. 100 GHz) che rende molto ardua l'acquisizione del segnale mediante fotorivelazione prima ancora che la sua decifrazione.

1. SISTEMI CAOTICI OTTICI

Numerosi sono gli esempi proposti o proponibili di sistemi ottici attivi o passivi in grado di generare fenomeni pseudocasuali caotici. Tra quelli attivi, ad es., un laser a semiconduttore con retroriflessione da uno specchio esterno, e una coppia di laser leggermente dissonanti e mutuamente accoppiati, mostrano il classico compor-

tamento dei diagrammi di stato con biforcazioni e ampie regioni caotiche intervallate da regioni di multiperiodicità [2,3]. Tra quelli passivi, ampiamente studiato è il modulatore Mach-Zehnder con elettrodi alimentati dal segnale rivelato da un fotodiodo, e con un laser come sorgente esterna.

Esempi di diagrammi di stato, forme d'onda e spettri nella regione caotica sono riportati in fig.1 per un sistema con laser mutuamente accoppiati. Questo sistema può essere generalizzato come in fig.2 che identifica due separati cammini di iniezione nei laser DL1 e DL2, comprendenti un isolatore ottico e un modulatore di fase (MΦ), e che possiede un'uscita e un ingresso ausiliari IN e OUT. Il messaggio da crittografare caoticamente entra all'ingresso Φ del modulatore di fase (fig.2).

La modulazione di fase genera una variazione di evoluzione delle forme d'onda, che tuttavia mantengono lo stesso carattere pseudocasuale senza apparente variazione delle loro caratteristiche temporali o di spettro. Inoltre, se il parametro K di retroriflessione è scelto all'interno di una regione di funzionamento caotico ampia (fig.1), il sistema è in grado di sincronizzarsi su forme d'onda caotiche della stessa classe (cioè con K vicini a quello dato).

Per sfruttare la proprietà della sincronizzazione, si fa uso di un doppio sistema (master-slave) per il trasmettitore (fig.3), e dopo la propagazione in fibra si usano come ricevitore due sistemi identici al trasmettitore ed alimentati rispettivamente da zero e uno al modulatore di fase. Quello dei due che è alimentato con un bit uguale a quello trasmesso si sincronizza sulla forma d'onda caotica ricevuta e fornisce perciò un'uscita identica all'ingresso. Dal confronto ingresso/uscita dei ricevitori si può così ricostruire il messaggio nonostante l'evoluzione caotica.

I risultati preliminari di simulazione numerica sinora ottenuti per questo sistema di crittografia ottica sono incoraggianti anche se rappresentano solo il primo passo per una valutazione completa delle prestazioni.

BIBLIOGRAFIA

[1] W.Wolfowicz, R.A.Rueppel: Focus on Cryptography, *ETT*, 5 (1994), p.419.

[2] V. Annovazzi Lodi, S. Donati, M.Manna: Transizione al caos di sorgenti laser in regime di iniezione, *Fotonica 93*, Arezzo 28-30 apr. 1993, pp.347-350.

[3] V. Annovazzi Lodi, S. Donati, M.Manna: Chaos and Locking in a Semiconductor Laser due to External Injection, *Journal of Quantum Electronics*, vol. QE-30 (1994), pp.1537-1541.

[4] M.P.Kennedy, M.Hasler: CSK: Modulation and Demodulation of Chaotic Carrier using a Self-Synchronising Circuit, *Trans. on CAS*, 40 (1993), 1577.

[5] C.W.Wu, L.O.Chua: A simple way to Synchronize Chaotic Systems with Application to Secure Communications, *J. Bifurc. and Chaos*, 3 (1993), pp.1619-27.

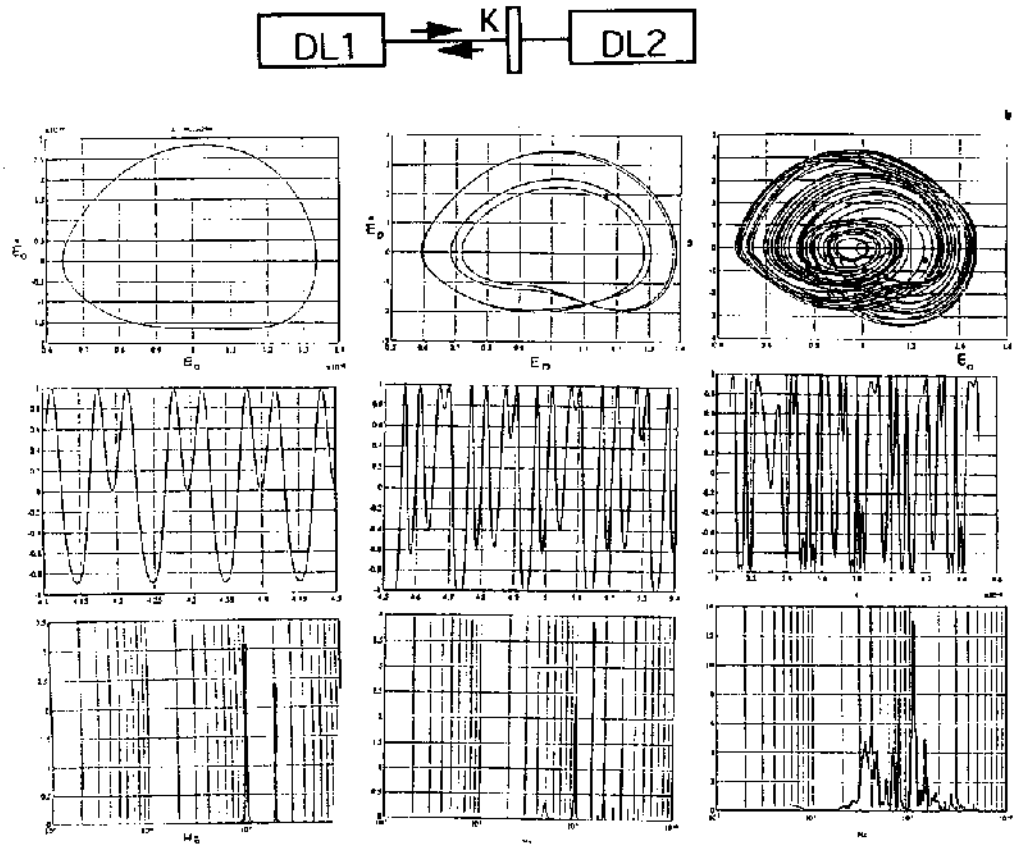

Fig.1 Laser accoppiati generanti caos (in alto) e comportamento a crescente (da sin a ds) livello di accoppiamento: in alto i diagrammi di fase, al centro le forme di battimento, in basso gli spettri di potenza.

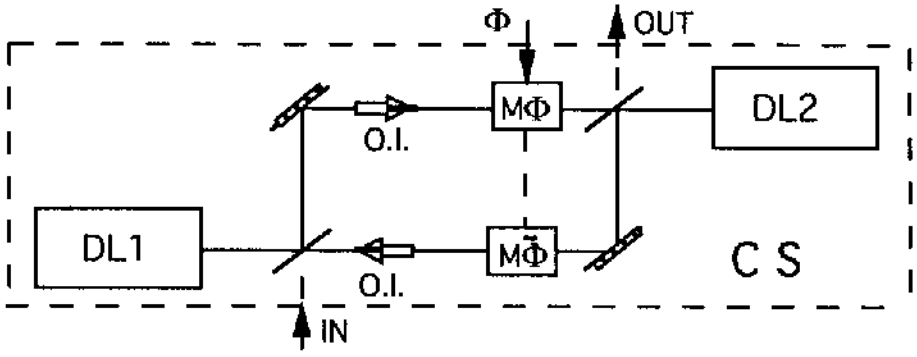

Fig.2 Sistema caotico generalizzato (CS)

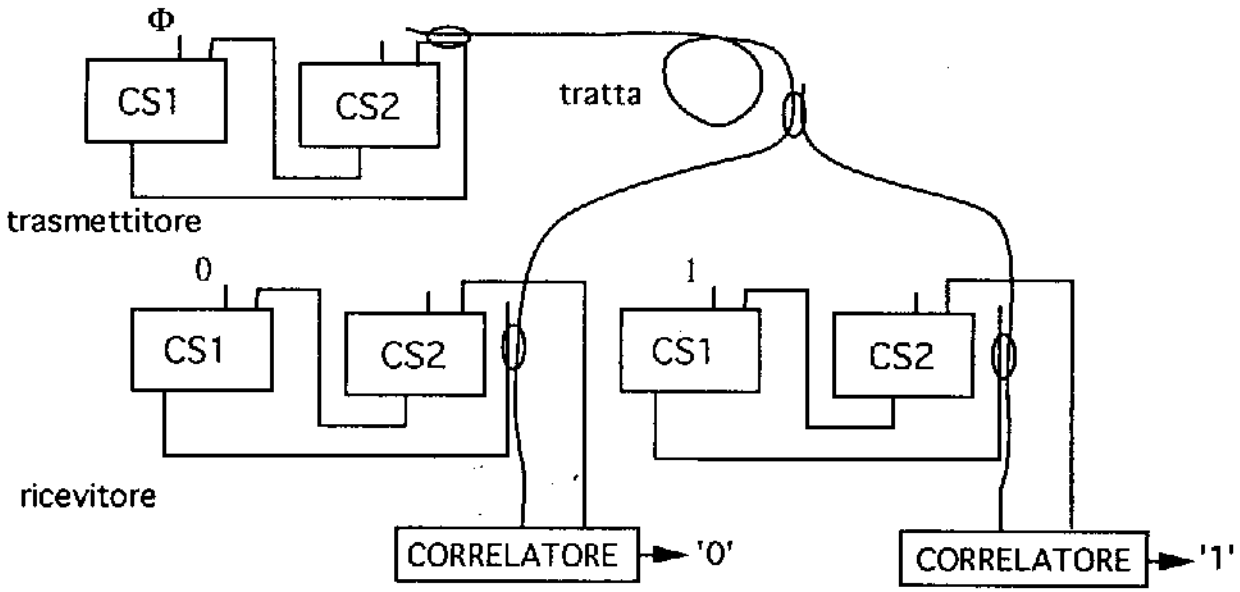

Fig.3 Sistema di rivelazione della crittografia caotica