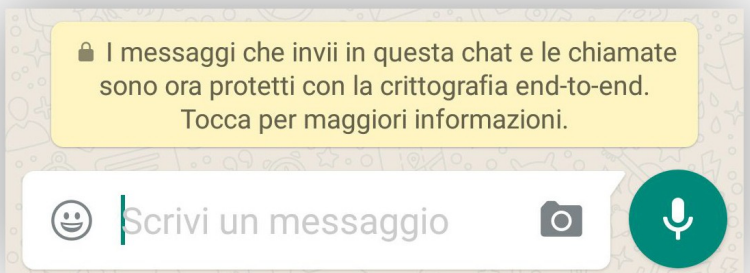
Crittografia e sicurezza

Proteggere la rete internet con il caos

Mattia Lenoci

Crittografia dei dati

- E’ una **tecnica fondamentale** utilizzata nella trasmissione di informazioni e dati che consente di avere **connessioni sicure** all’interno di una rete insicura. In breve permette di celare le informazioni a lettori “indesiderati”.



Tecniche di crittografia

Esistono due tecniche di crittografia:

- **Software**

  I messaggi vengono cifrati attraverso algoritmi o software

- **Hardware**

  La crittografia viene applicata a livello del mezzo di trasmissione “fisicamente” (es. caos)

  Le due tipologie possono essere tra loro **complementari** per avere un livello di sicurezza maggiore.

Crittografia software

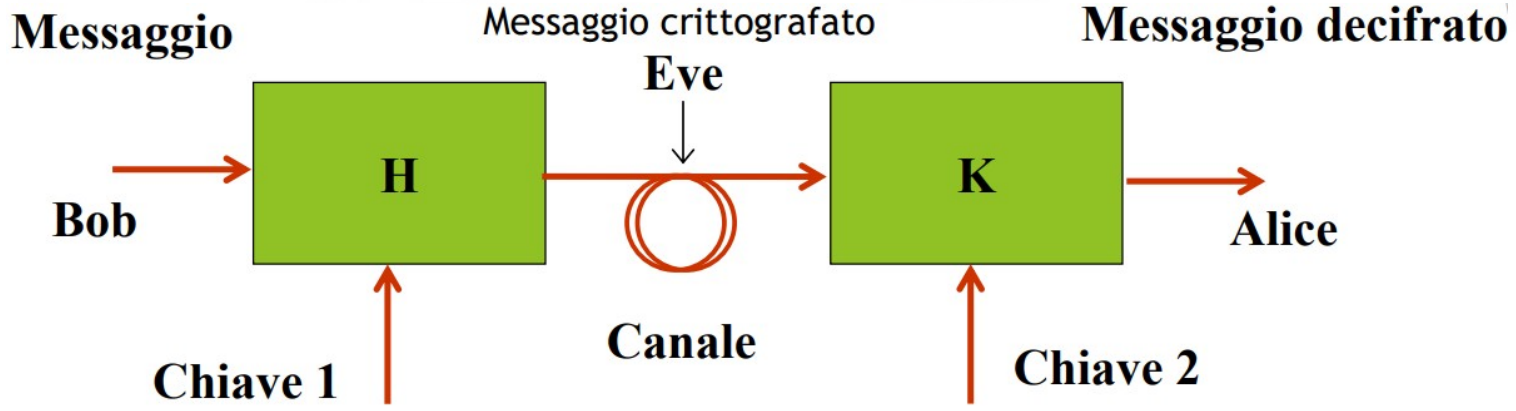
Esistono due tipi di crittografia software

- **Crittografia simmetrica**
- **Crittografia asimmetrica (o RSA)**

Le due tipologie variano in base al modo in cui l'algoritmo viene applicato e alla trasmissione della chiave di cifratura: nel primo caso questa deve essere comunicata segretamente, mentre nel secondo viene trasmessa pubblicamente.

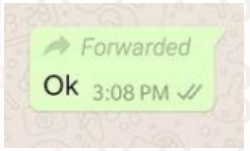
Crittografia simmetrica (chiave segreta)

- Il mittente al momento dell'invio del messaggio **genera una chiave**, lunga quanto i bit del messaggio, e cifra il messaggio **sommando** i bit di quest'ultimo a quelli della chiave.
- Il destinatario effettua la **sottrazione** tra i bit del messaggio criptato, e quelli della chiave, che deve essere ricevuta segretamente.



Crittografia simmetrica

- Mittente



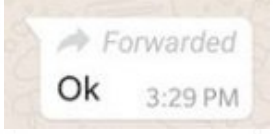
	0	1	1	0	1	1	1	1	0	1	1	0	1	0	1	1
Chiave generata	1	0	1	1	1	0	0	1	0	1	0	0	1	1	1	0
Messaggio criptato	1	1	0	1	0	1	1	0	0	0	1	0	0	1	0	1

+

- Destinatario

Messaggio criptato	1	1	0	1	0	1	1	0	0	0	1	0	0	1	0	1
Chiave segreta	1	0	1	1	1	0	0	1	0	1	0	0	1	1	1	0
	0	1	1	0	1	1	1	1	0	1	1	0	1	0	1	1

-



Per ogni messaggio deve essere generata una chiave segreta differente per evitare che un malintenzionato possa trovare nel tempo delle corrispondenze

Crittografia asimmetrica (RSA)

- E’ nota anche come RSA dal nome dei suoi inventori: Ronald Rivest, Adi Shamir, Leonard Adleman.
- E’ la tipologia di crittografia più diffusa dato che risolve il problema più grande della crittografia simmetrica: **la chiave di criptazione non deve essere comunicata segretamente**.
- La sicurezza è garantita dalla complessità del calcolo computazionale e dalla lunghezza della chiave di criptazione.

- Il destinatario elabora una chiave segreta tramite la quale ne calcola una pubblica che invia al mittente.
- Il mittente offusca il messaggio con la chiave pubblica ricevuta.
- Il destinatario riceve il messaggio criptato con la chiave pubblica ed è l'unico in grado di decriptarlo perché in possesso della chiave segreta di partenza.

Proteggere la rete con il caos

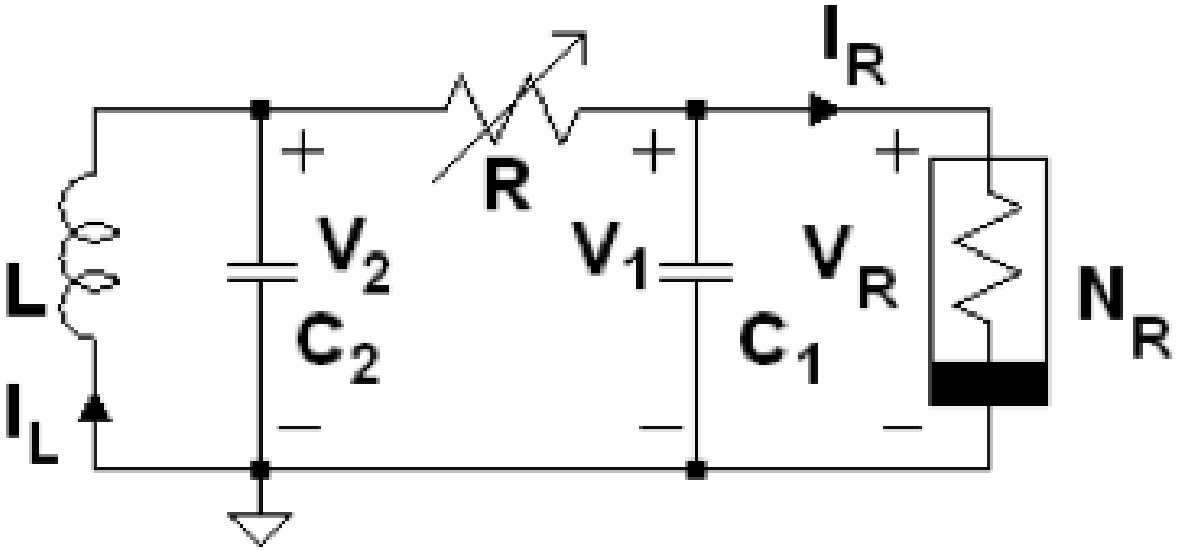
- E’ una **tecnica hardware** che permette di celare le informazioni al livello del mezzo di trasmissione.

  Cos’è il caos?

- Nelle antiche cosmologie il caos individuava il complesso degli elementi materiali senza ordine mentre in campo scientifico un sistema tende al caos quando tende al disordine con **comportamenti irregolari** e **non prevedibili**.
- Applicato alla crittografia sarebbe come **disordinare le informazioni** in modo da renderle **illeggibili**.

Il circuito di Chua

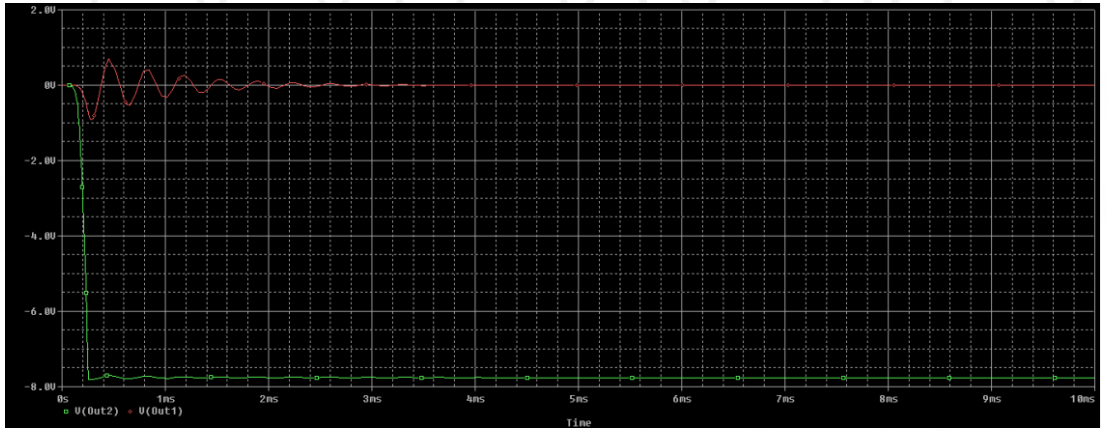
- E’ un **circuito molto semplice** in grado di eseguire **fenomeni caotici** e fu realizzato nel 1983 dal professore **Leon Ong Chua**.



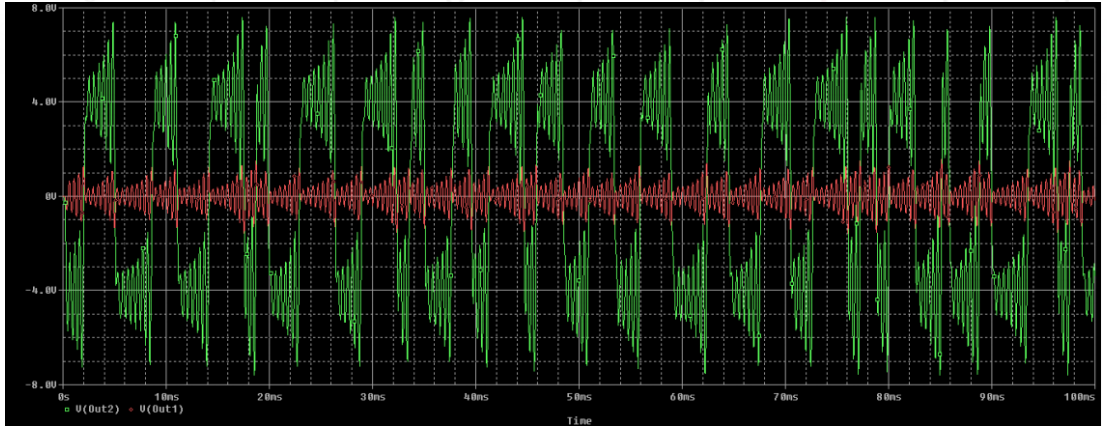
Il circuito di Chua e l’effetto “farfalla”

- L’effetto “farfalla” fu studiato per la prima volta dal meteorologo Edward Lorenz nel 1962 il quale osservò che una **piccola varizazione nelle condizioni iniziali** di un sistema producono **grandi variazioni a lungo termine**.
- Il circuito di Chua risponde di questo fenomeno: variando anche di poco i valori delle resistenze si generano **fenomeni caotici molto diversi tra loro**.

Simulazioni caos generato

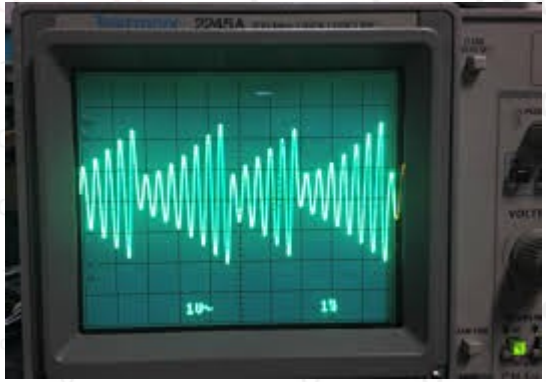


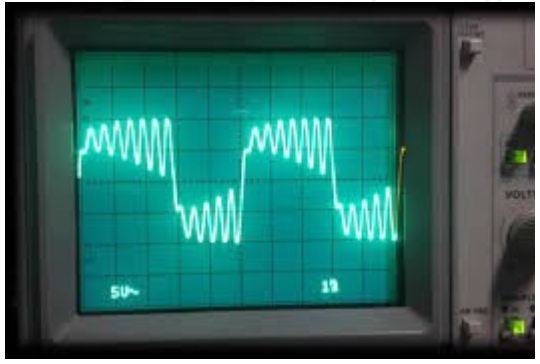
→ **R1 = 3 kΩ**

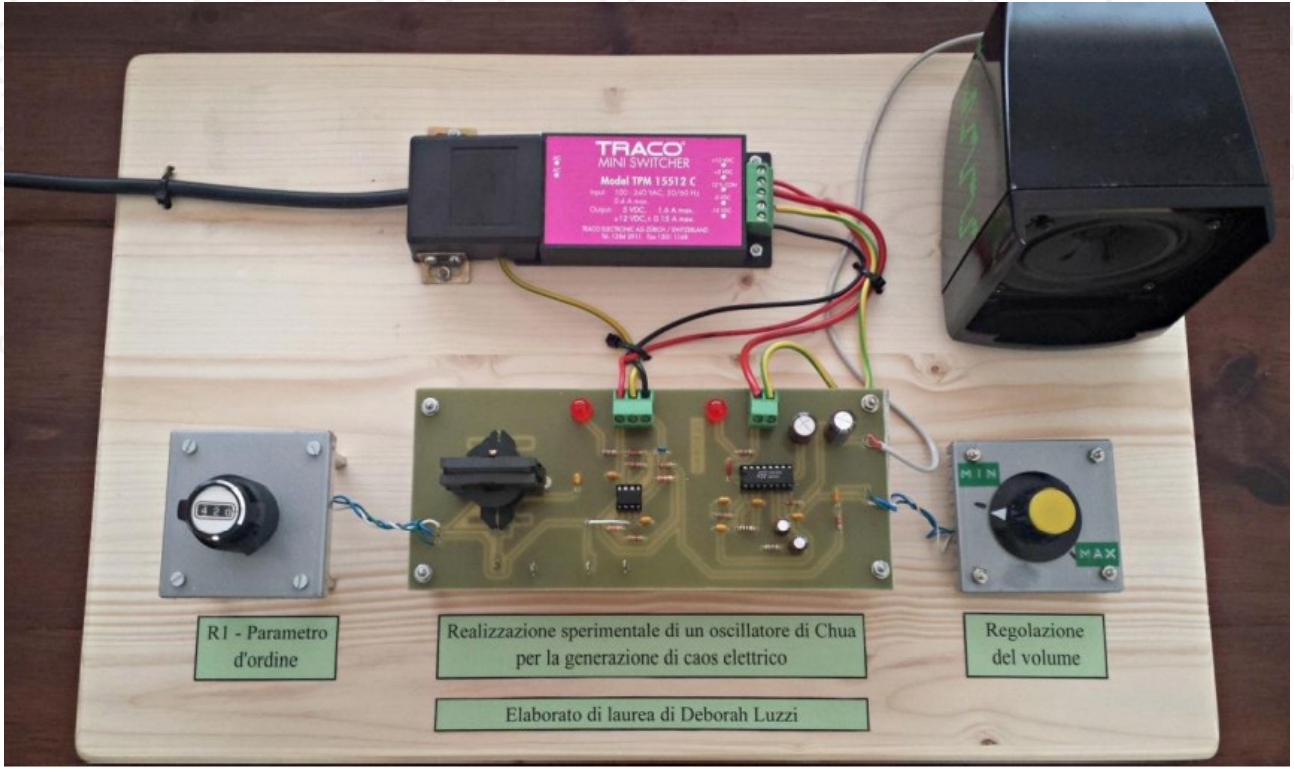


→ **R1 = 2 kΩ**

Il circuito in pratica

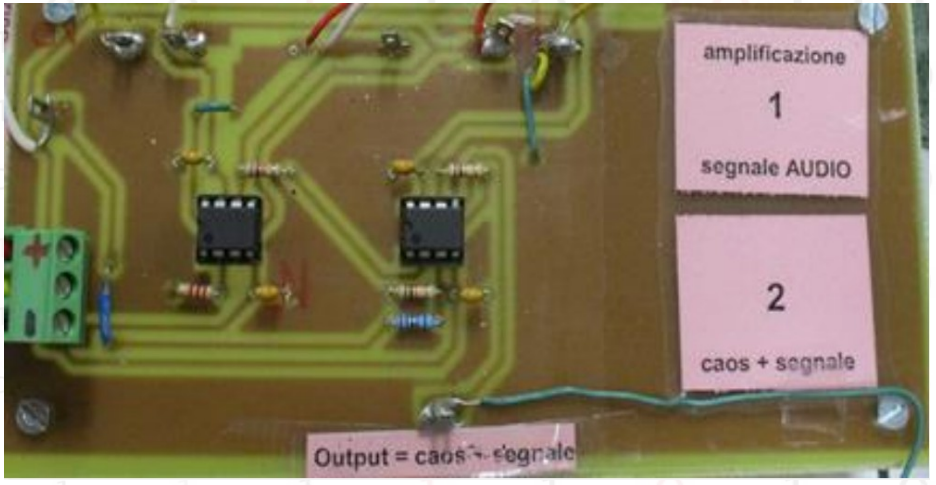


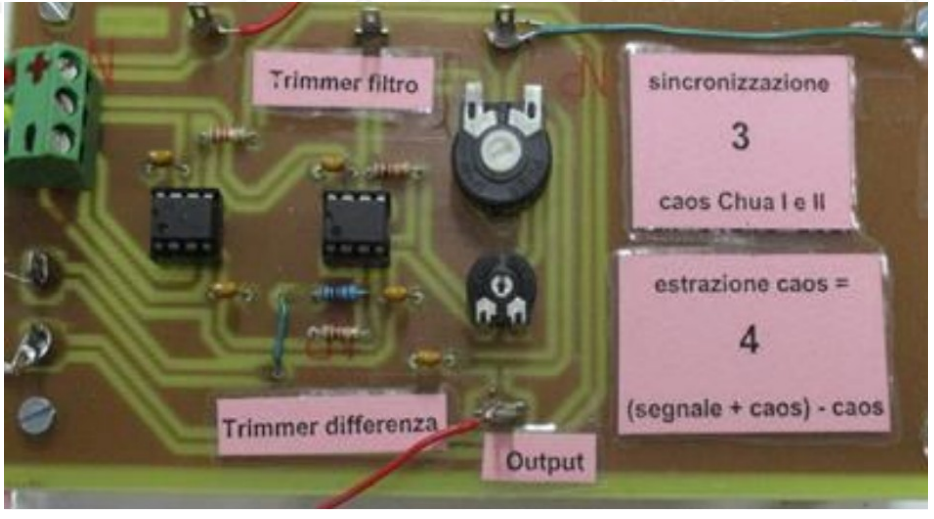




Crittografia con caos elettrico

- Il circuito di Chua genera un caos elettrico, ovvero un segnale in tensione. Il messaggio che si vuole inviare viene tradotto anch'esso in un segnale elettrico, in tensione.
- Il segnale in tensione del caos (chiave) viene sommato a quello del messaggio e così la comunicazione viene offuscata.
- Il destinatario può decriptare il messaggio effettuando la sottrazione tra la tensione del segnale offuscato e quella del caos (chiave), solo se è in grado di generare lo stesso caos del mittente.
- I due circuiti di Chua devono avere gli stessi parametri ed essere sincronizzati.





Mittente

Caos
+
Segnale messaggio

Segnale offuscato

Destinatario

Segnale offuscato
-
Caos sincronizzato

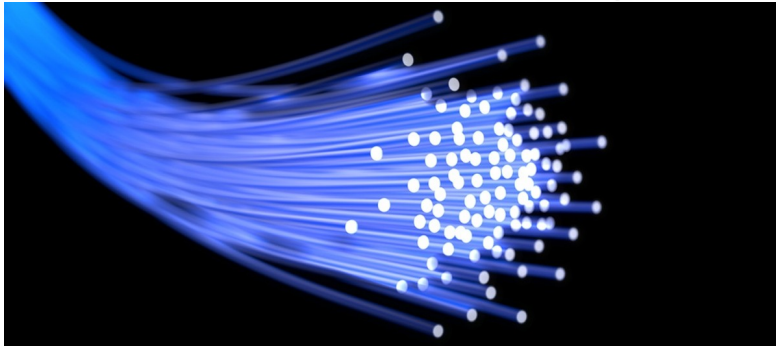
Segnale messaggio

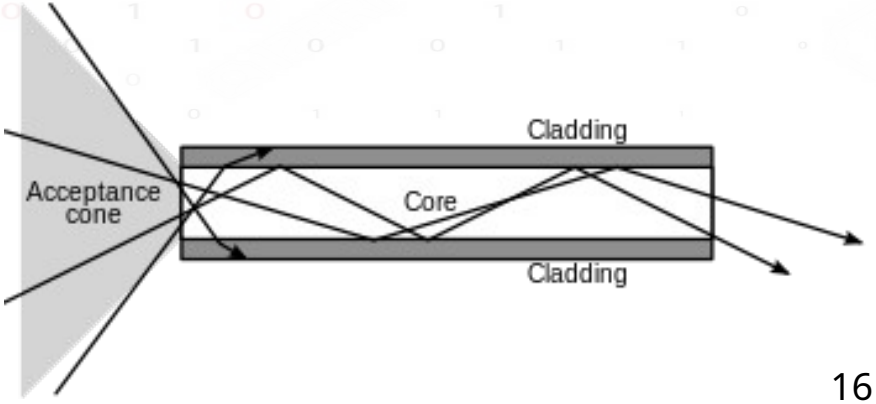
Crittografia caotica ottica

- Il caos per mascherare il messaggio non viene più generato dal circuito di Chua ma da un **laser** che viene portato al **caos**.

Mezzo di trasmissione

- Il mezzo di trasmissione più diffuso per comunicazioni ottiche è rappresentato dalla **fibra ottica**.





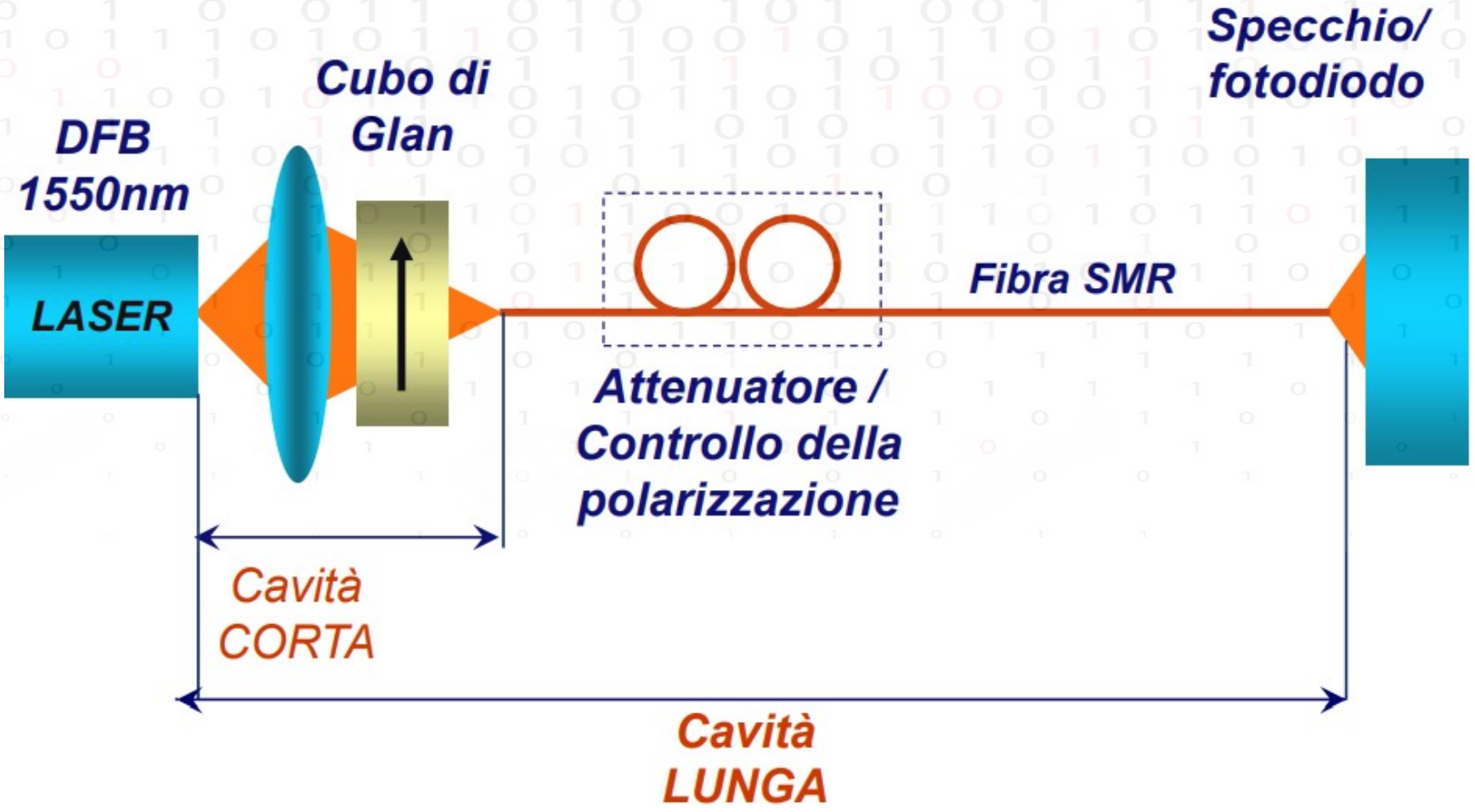
Il laser

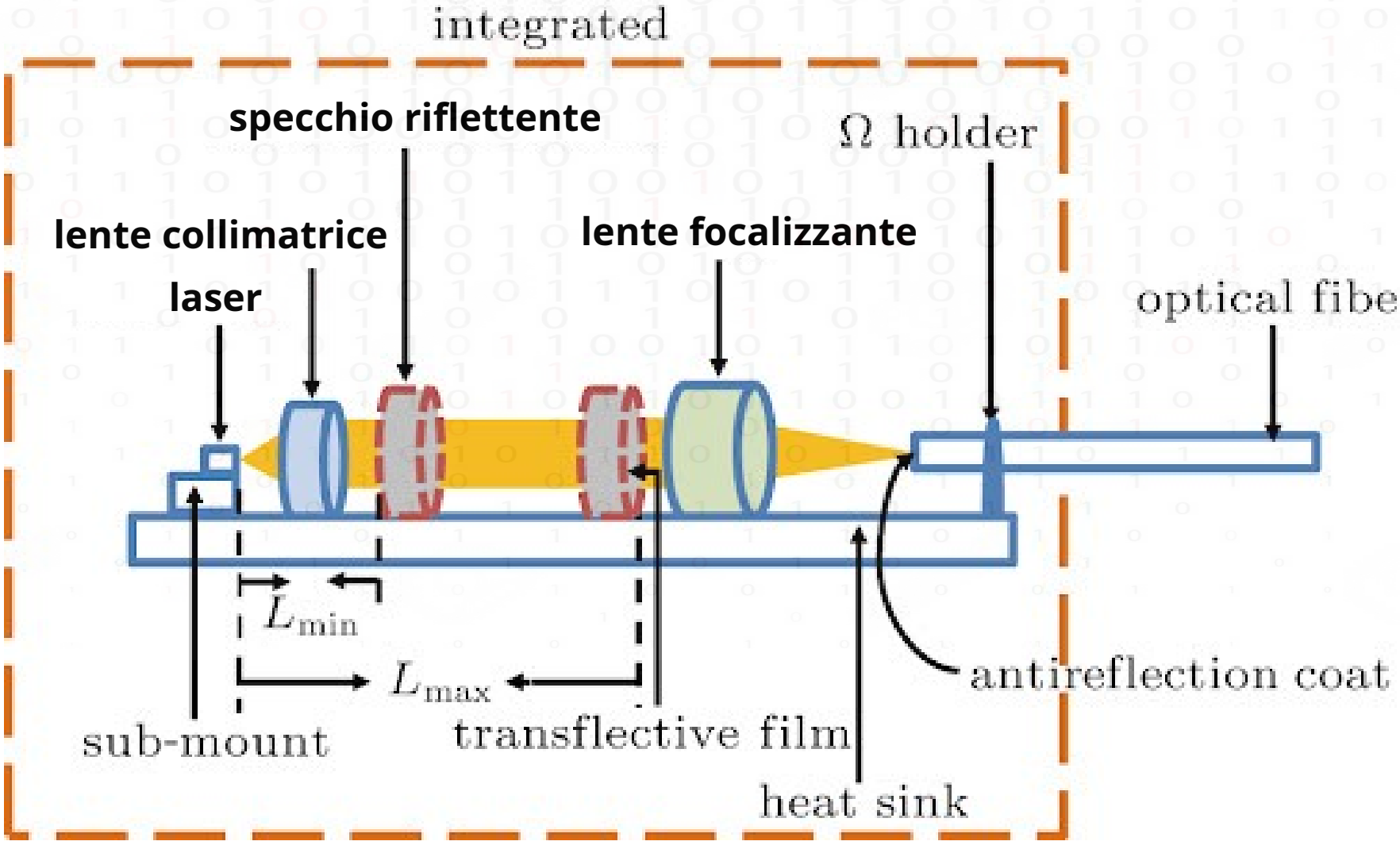
- Il laser è un dispositivo optoelettronico in grado di emettere un fascio di **luce coerente**.

Come portarlo al caos?

- Tramite **retroriflessione con uno specchio remoto**.
- Iniezione da altra sorgente.
- Modulazione della corrente di pompa.

Generazione caos per retroriflessione

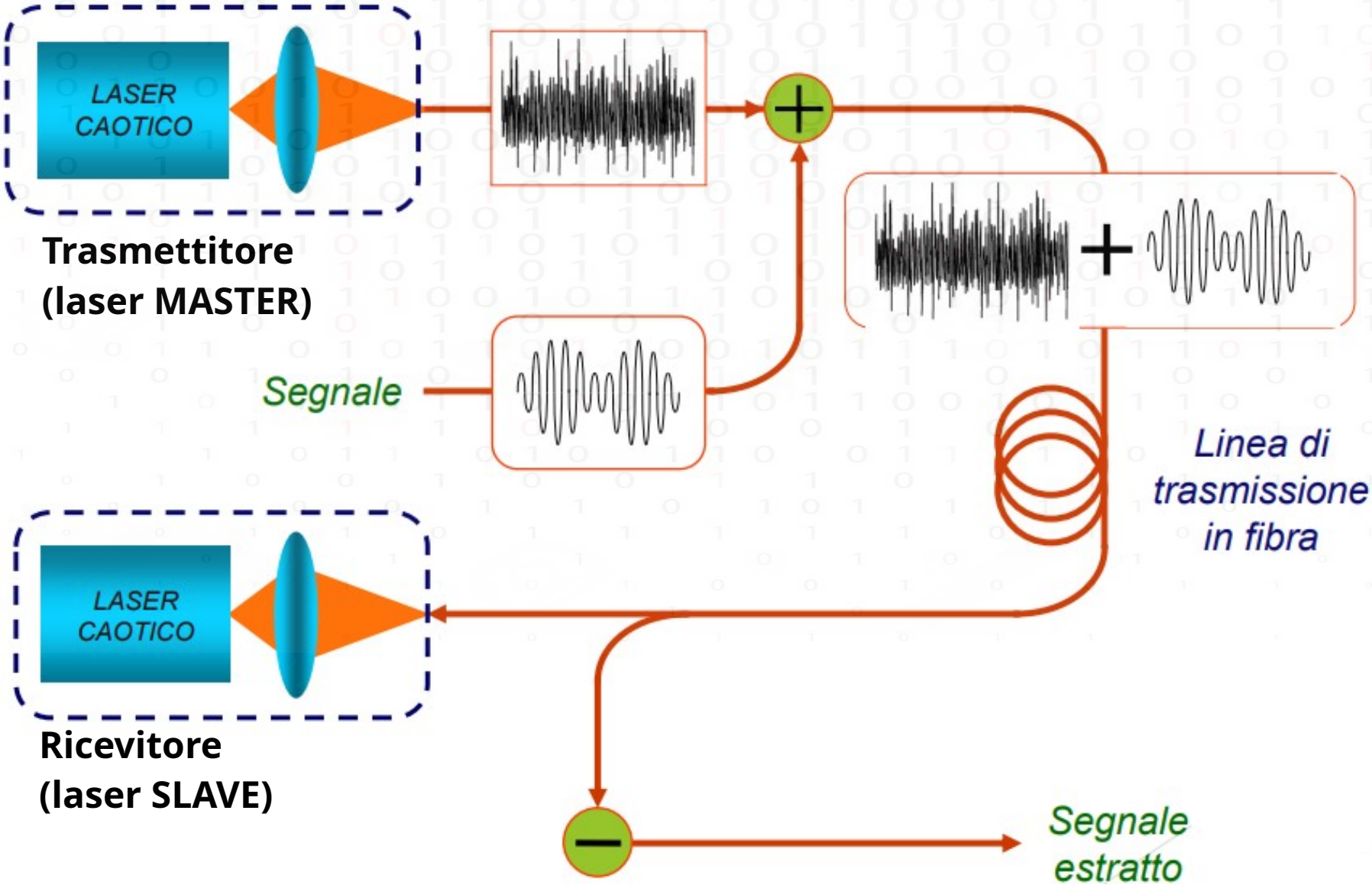



integrated
specchio riflettente
Ω holder
lente collimatrice
laser
lente focalizzante
optical fiber
L_{min}
L_{max}
antireflection coat
sub-mount
transflective film
heat sink

Crittografia ottica caotica

Funzionamento

- Il mittente è in possesso di un dispositivo **laser** che è stato portato al **caos**.
- Il messaggio viene sovrapposto al caos ottico (**mascheratura**) e la comunicazione via fibra ottica viene criptata.
- Il destinatario sarà in grado di estrapolare il messaggio solo se in possesso di un **laser gemello** che riesce a generare lo **stesso caos sincronizzato** da sottrarre alla comunicazione.


LASER CAOTICO
Trasmettitore (laser MASTER)
Segnale
Linea di trasmissione in fibra
LASER CAOTICO
Ricevitore (laser SLAVE)
Segnale estratto

Configurazioni

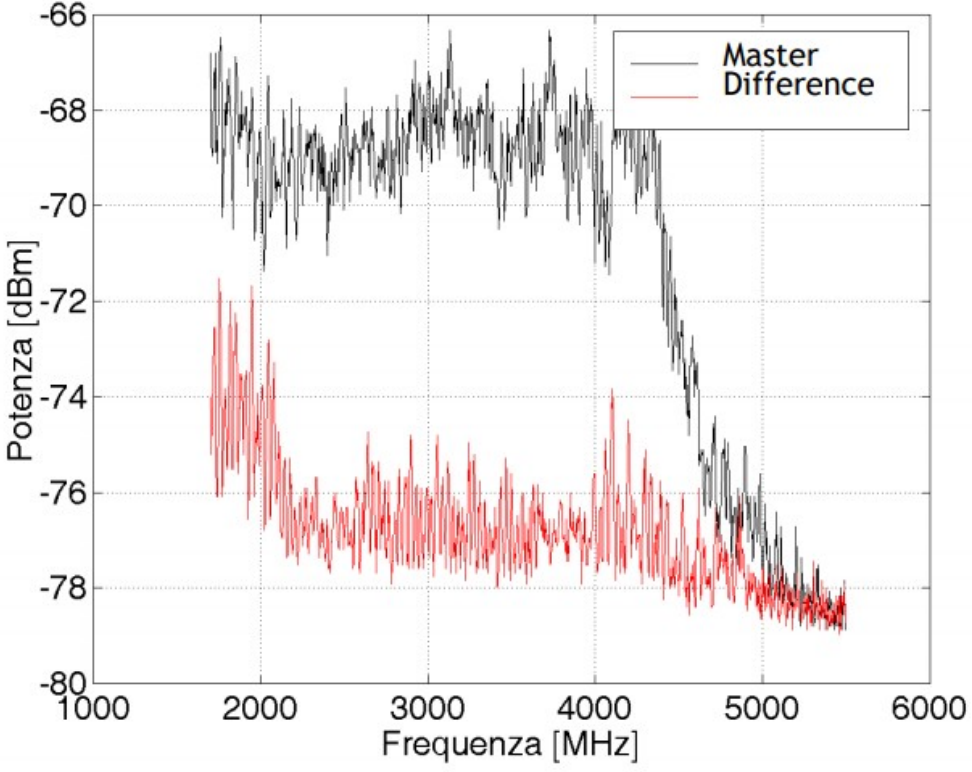
Esistono due tipi di configurazioni:

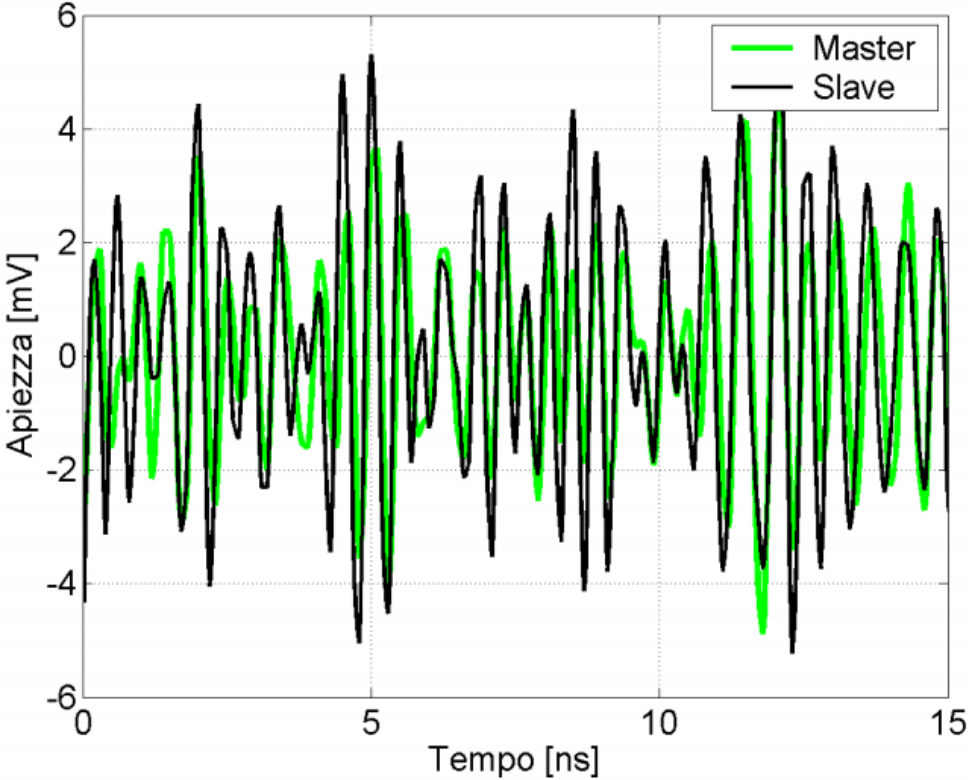
- **Anello chiuso**: master e slave sono entrambi caotici
- **Anello aperto**: master è caotico mentre lo slave no.

Sincronizzazione del caos

- Nei sistemi ad anello chiuso la sincronizzazione dipende dallo sfasamento dei campi retro iniettati di master e slave, ovvero dalla differenza delle loro lunghezze di cavità, per compensare la differenza temporale delle due uscite ed effettuare la cancellazione del caos.

- Configurazione ad **ANELLO CHIUSO** e **CAVITÀ CORTA**





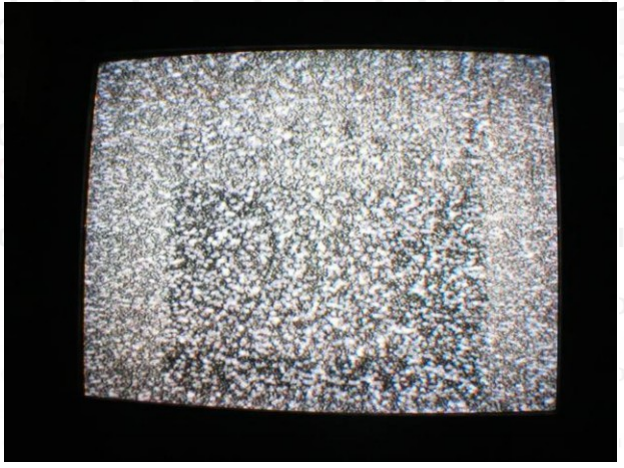
La configurazione migliore

La configurazione migliore del circuito per la crittografia ottica è ad **anello chiuso** e **cavità corta** per diversi motivi:

- **Maggiore sicurezza**: i due **laser** per generare la stessa forma d'onda devono essere prodotti appositamente per essere **gemelli**.
- Viene generato un **caos continuo** dove è più facile nascondere il messaggio.
- **Sincronizzazione** più **precisa** e **stabile**.
- **Realizzazione compatta**.

Applicazione crittografia ottica caotica

Messaggio in chiaro



Messaggio mascherato

Messaggio estratto