

# DISPOSITIVI OTTICI PER APPLICAZIONI DI SICUREZZA

F. GARZIA, M. BERTOLOTTI, E. FAZIO

INFM Dipartimento di Energetica, Università degli Studi di Roma "La Sapienza"

Via A.Scarpa 16 - 00161 Roma (E-mail fabio.garzia@uniroma1.it)

## ABSTRACT

Nel presente articolo verrà presentato un dispositivo che funziona come una chiave di sicurezza totalmente ottica in grado di generare un suo codice di uscita quando viene opportunamente interrogata da una sequenza di impulsi in ingresso. Tale dispositivo può essere riadattato per ottenere un dispositivo per crittografia in grado di alterare l'ordine di una sequenza di impulsi di ingresso al fine di rendere incomprensibile il messaggio in ingresso se non all'utilizzatore finale.

## 1. INTRODUZIONE

L'ottica può essere proficuamente utilizzata per la realizzazione di dispositivi di sicurezza. In particolare è possibile utilizzare impulsi laser di intensità opportuna per ottenere solitoni ottici spaziali da utilizzare in opportune strutture guidanti [1-4] in grado di commutare in maniera totalmente ottica [5-7].

Nel presente articolo si utilizzeranno le proprietà di propagazione dei solitoni ottici spaziali in gradienti di indice di rifrazione trasversali, al fine di proporre dispositivi di sicurezza totalmente ottici quali chiavi o criptatori di messaggi.

## 2. STRUTTURA DELLA CHIAVE OTTICA

La chiave ottica è composta da N celle elementari opportune, essendo N il numero di impulsi che compongono il codice di uscita. Tale chiave viene interrogata mediante una sequenza composta da N impulsi equispaziati temporalmente, detti anche bit, in grado di trasportare ciascuno un'informazione binaria in funzione della loro presenza o assenza. Nella fig.1 viene mostrata la struttura di una chiave di sicurezza a 2 bit.

Quando il primo impulso entra nella chiave, esso viene attratto dall'anello più esterno, caratterizzato da un indice di rifrazione più elevato rispetto alla guida di ingresso, la cui lunghezza è calcolata in maniera tale che il solitone che si propaga all'interno di esso si ripresenti nel punto di partenza con fase repulsiva rispetto all'impulso seguente con il quale interagisce, respingendolo. In tale situazione il secondo impulso rimane sulla guida principale raggiungendo lo stadio successivo dove si ripete il medesimo processo che avviene nel primo stadio mentre il primo impulso viene spinto verso l'anello inferiore, la cui lunghezza è tale che il solitone che si propaga al suo interno si ripresenti nel punto di partenza con la medesima fase iniziale, la quale è comunque repulsiva rispetto agli impulsi seguenti, ripetendo lo stesso processo tante volte fino all'esaurimento degli impulsi di interrogazione del codice.

Quando tutti gli impulsi di interrogazione sono entrati all'interno della chiave il primo solitone si ripresenta al punto di ingresso dell'anello dove non sono più presenti impulsi che lo respingono verso l'anello interno: in tali condizioni l'impulso esce spostandosi obliquamente verso la guida d'uscita dove viene trattenuto se tale impulso deve appartenere al codice della chiave, raggiungendo l'uscita, in funzione delle proprietà di propagazione della giunzione  $\bar{A}$ . Se tale impulso non deve appartenere al codice della chiave allora la giunzione viene realizzata in maniera tale da inviarlo verso la guida di uscita del codice complementare.

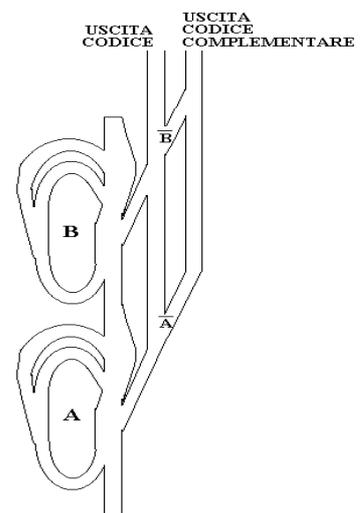


FIG.1 SCHEMA DI UNA CHIAVE A 2 BIT

La chiave è dunque concepita in maniera tale che la struttura di base è la medesima per tutte le chiavi mentre il codice specifico di ciascuna di esse viene scritto all'interno, aprendo o chiudendo opportunamente le giunzioni che connettono la guida di uscita del codice alla guida di uscita del codice complementare. Tale operazione di programmazione può essere eseguita in fase di produzione o in una seconda fase. Il processo di emissione del codice avviene secondo la medesima sequenza di ingresso, selezionando opportunamente gli impulsi di ingresso come appartenenti o non appartenenti al codice di uscita mediante le giunzioni menzionate sopra. L'ultimo impulso della sequenza di ingresso deve comunque anch'esso propagarsi all'interno di un anello al fine di preservare la relazione temporale con gli altri impulsi del codice.

Vediamo ora nei dettagli i meccanismi di interazione all'interno della cella elementare che viene mostrata in fig.2.

Poiché è necessario sfasare opportunamente una sola volta l'impulso che entra all'interno dell'anello, si ricorre a una struttura a due rami. Quando il primo impulso entra all'interno della guida 1 esso si propaga nella guida 3, passando oltre l'ingresso della guida 4 e l'ingresso del ramo 6 dell'anello, dal momento che tutte le strutture suddette sono caratterizzate dal medesimo indice di rifrazione della guida d'onda principale. Poiché il ramo 8 dell'anello è caratterizzato da un indice di rifrazione più elevato, l'impulso viene attratto all'interno di esso. La lunghezza di tale ramo è calcolata in maniera tale che l'impulso che si propaga all'interno di esso, tornando al punto di partenza, subisca una variazione di fase relativa tale da respingere gli impulsi seguenti (fase repulsiva).

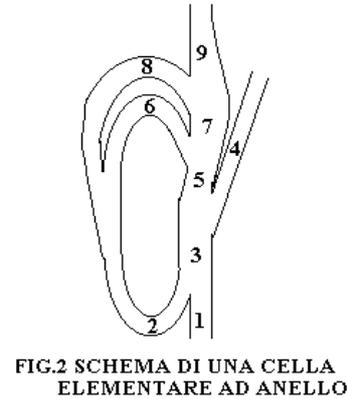


FIG.2 SCHEMA DI UNA CELLA ELEMENTARE AD ANELLO

Poiché tale impulso si propaga parallelo e leggermente sovrapposto all'impulso seguente a partire dal punto 3, la mutua azione repulsiva impedisce al primo impulso di raggiungere l'uscita 4. Essi raggiungono il punto 5 dove la guida si restringe, aumentando la forza repulsiva [7], spingendo il primo impulso all'interno del ramo 6 dell'anello e l'impulso seguente verso il lato destro del punto 7 della guida che si allarga nella suddetta zona: in tale situazione esso è sufficientemente distante dall'ingresso 8 del ramo dell'anello per esserne attratto all'interno e può raggiungere il punto 9 dove esce dalla cella elementare per raggiungere la cella successiva.

Il primo impulso si propaga invece all'interno dell'anello 6 la cui lunghezza è calcolata in maniera tale da farlo ritornare nella posizione di partenza con la medesima fase (repulsiva) rispetto agli impulsi seguenti, dove si ripete il processo. Quando tutti gli impulsi sono entrati all'interno della chiave il primo impulso non trova più nessun altro impulso che possa esercitare azioni repulsive ed è quindi libero di propagarsi obliquamente fino a raggiungere la guida 4 che lo conduce verso la guida di uscita del codice dove viene selezionato come appartenente o non appartenente al codice, in funzione delle proprietà di propagazione della giunzione.

Illustriamo ora le proprietà di propagazione dei solitoni all'interno delle guide d'onda longitudinalmente paraboliche che compongono l'anello e l'espressione della mutua forza di interazione dei solitoni, che sono fondamentali per il corretto dimensionamento del dispositivo.

Il profilo trasversale di indice di rifrazione di tali guide segue una distribuzione triangolare [5] e la loro configurazione longitudinale viene scelta essere di tipo parabolico in quanto coincide con la traiettoria seguita dai solitoni quando vengono inseriti in gradienti di indice lineari come quelli che si utilizzano[6]. L'inclinazione locale rispetto all'asse longitudinale di tali guide aumenta progressivamente con la distanza di propagazione: ciò significa che è necessario imporre dei limiti alla loro lunghezza per evitare di superare l'approssimazione parassiale con la quale viene sviluppata l'equazione di Schroedinger non lineare (NLSE) che descrive il processo di propagazione solitonica. Per tale motivo non si utilizzano interamente tali curve, ma solo due tratti di esse quasi paralleli all'asse longitudinale e due specchi per chiudere l'anello [6,7].

Un solitone che si propaga nella direzione dell'asse longitudinale  $z$  è caratterizzato dalla seguente espressione del campo  $Q$  all'ingresso della struttura:

$$Q(x,0) = C \operatorname{sech}[C(x - \bar{x})], \quad (1)$$

dove  $\bar{x}$  è la posizione del centro del fascio e  $C$  una costante reale dalla quale dipendono sia la larghezza che l'ampiezza del fascio. Le variabili  $x$  e  $z$  sono normalizzate rispetto al vettore d'onda. Quando un fascio solitonico si propaga in un indice di rifrazione trasversale a profilo triangolare il cui massimo è pari a  $\Delta n_0$  e la cui larghezza è pari a  $2b$ , esso è soggetto a un'accelerazione trasversale [5,8,9]. Se la guida viene scelta essere longitudinalmente parabolica, la posizione del centro del profilo trasversale della guida  $x_G(z)$  varierà con  $z$  secondo la:

$$x_G(z) = az^2, \quad (2)$$

dove "a" è una costante da cui dipende l'inclinazione locale della guida rispetto all'asse longitudinale. In tale situazione è possibile dimostrare che il fascio resta intrappolato all'interno della guida se la sua ampiezza è maggiore di:

$$C_D = (ab/\Delta n_0)^{1/2}. \quad (3)$$

Si è già detto che si utilizza una guida d'onda parabolica la cui inclinazione rispetto all'asse longitudinale aumenta con la distanza di propagazione, per cui esisterà una distanza massima oltre la quale la guida esce dalle condizioni parassiali che sono valide sino a  $8^\circ$ - $10^\circ$  rispetto all'asse  $z$ . Una volta scelta la forma della curva mediante il parametro "a" dell'eq.(2), la massima lunghezza di propagazione  $z_{\max}$  dipende dalla derivata prima dell'eq.(2) mediante la:

$$x'_G(z_{\max}) = \tan 8^\circ = 0.14 = 2az_{\max}, \quad (4)$$

che può essere risolta rispetto a  $z_{\max}$  fornendo:

$$z_{\max} = 7 \cdot 10^{-2} / a. \quad (5)$$

Ciò significa che, una volta scelto il profilo parabolico della guida mediante il parametro "a", il solitone si può propagare all'interno della stessa sino a una distanza pari a  $z_{\max}$ , valore che deve essere rispettato nella progettazione dell'anello del dispositivo.

Poiché si utilizza un processo di interazione tra solitoni per il corretto funzionamento del dispositivo, l'espressione della corrispondente accelerazione è stata dimostrata essere una funzione esponenziale della distanza relativa  $d$  e una funzione cosinusoidale della fase relativa  $\varphi$  [7]:

$$a(d, \varphi) = (C^2/5) \exp(-C(d - 2x_{\text{HHHW}})) \cos \varphi, \quad (d \geq 2x_{\text{HHHW}}) \quad (6)$$

dove  $x_{\text{HHHW}}$  è la larghezza a metà altezza del fascio che è pari a:  $x_{\text{HHHW}} = (1/C) \log(2 + \sqrt{3})$ .

L'accelerazione espressa dall'eq.(6) si rivela essere di fondamentale importanza per la progettazione pratica della chiave ottica di sicurezza.

La progettazione della chiave ottica risulta essere un procedimento abbastanza complesso in quanto è necessario tenere conto di molteplici parametri, talora reciprocamente contrastanti [8]. Tale procedimento non viene riportato per brevità. Una volta progettato il dispositivo esso è stato simulato numericamente utilizzando un algoritmo di tipo FD-BMP. La struttura del dispositivo è mostrata in fig.3a, dove si può vedere come non sia stata considerata la parte sinistra dell'anello in quanto gli effetti di interazione avvengono nella parte destra del dispositivo. Sono state simulate l'ingresso del primo solitone all'interno dell'anello, la commutazione operata dal primo solitone rispetto al solitone seguente e l'uscita del primo solitone dall'anello, al fine di raggiungere la guida di uscita. I risultati sono mostrati nelle figure 3.

### 3. IL DISPOSITIVO CRIPTOGRAFICO

Un'interessante variante della chiave ottica è rappresentata dal dispositivo criptografico, in grado di alterare il normale ordine del flusso di impulsi rendendo il messaggio incomprensibile ad eccezione del destinatario finale. Se si utilizza la medesima struttura della chiave ottica con la variante che l'indice di rifrazione dell'anello è tale che il solitone resta intrappolato al suo interno sino a che la sua intensità non scende al di sotto di un certo livello di soglia a causa dell'assorbimento dal valore

ben definito, è possibile stabilire quanto tempo l'impulso si propaga all'interno della singola cella. Una volta che tutti gli impulsi sono entrati all'interno dei rispettivi anelli, inizia l'uscita da tali strutture secondo un ordine stabilito dall'indice di rifrazione, o alternativamente dalla curvatura dei vari anelli: variando l'ordine di uscita è possibile variare l'ordine degli impulsi del messaggio di ingresso, criptandolo opportunamente secondo una sequenza nota solo al mittente e al destinatario e operando in tempo reale, senza alcun rallentamento dovuto ad elaborazioni intermedie.

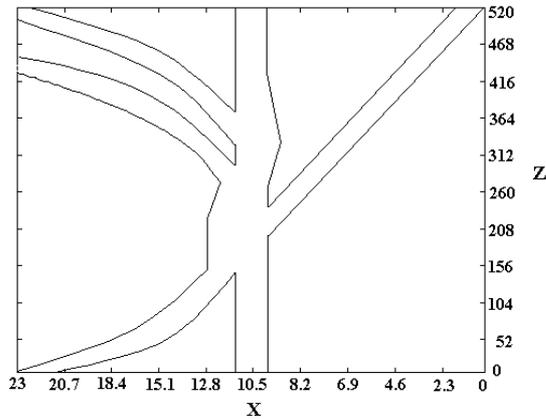


FIG. 3a VISTA SUPERIORE DEL DISPOSITIVO SIMULATO

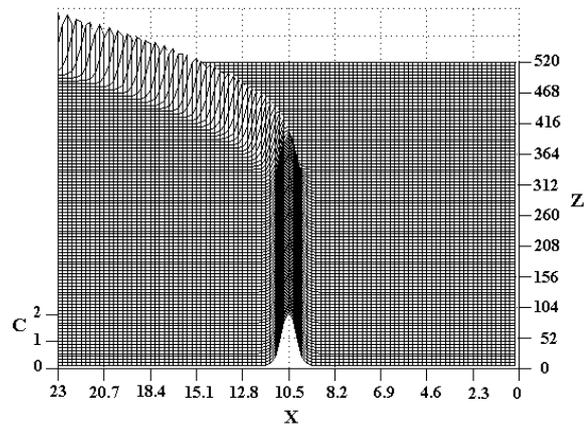


FIG. 3b INGRESSO DEL PRIMO SOLITONE ALL'INTERNO DELL'ANELLO

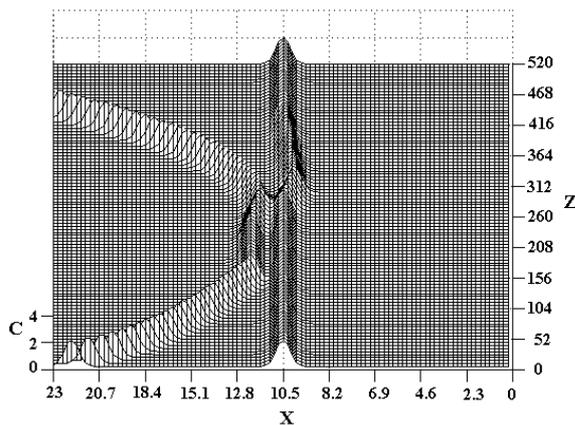


FIG. 3c COMMUTAZIONE OPERATA DAL PRIMO SOLITONE SUI SOLITONI SEGUENTI

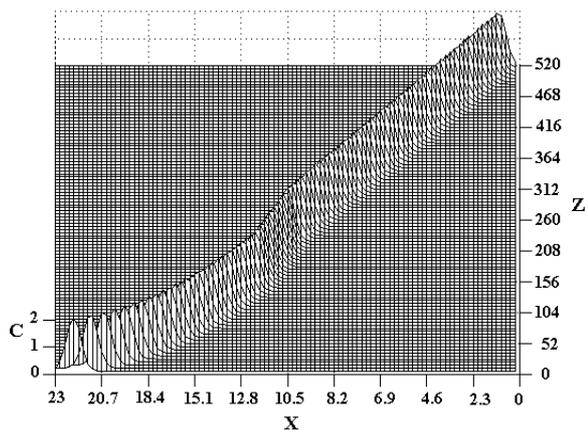


FIG. 3d USCITA DEL PRIMO SOLITONE DALL'ANELLO

#### 4. CONCLUSIONI

Sono stati presentati dei dispositivi totalmente ottici per applicazioni di sicurezza le cui proprietà di funzionamento si basano sull'interazione tra solitoni ottici spaziali. La loro frequenza operativa può essere molto elevata ed è limitata dalla geometria dei dispositivi, dal tempo di risposta del materiale non lineare e dalla frequenza operativa della sorgente.

#### BIBLIOGRAFIA

1. A. B. ACEVES, J. V. MOLONEY, A. C. NEWELL, *Opt. Lett.* 13, (1988) 1002.
2. P. VARATHARAJAH, A. B. ACEVES, J. V. MOLONEY, *App. Phys. Lett.* 54, (1989) 2631.
3. A. B. ACEVES, P. VARATHARAJAH, A. C. NEWELL, E. M. WRIGHT, G. I. STEGMAN, D. R. HEATLEY, J. V. MOLONEY, H. ADACHIHARA, *J. Opt. Soc. Am. B* 7, (1990) 963.
4. F. GARZIA, C. SIBILIA, M. BERTOLOTTI, *Optics Comm.* 139 (1997) 193.
5. F. GARZIA, C. SIBILIA, M. BERTOLOTTI, *Optics Comm.* 152 (1998) 153.
6. F. GARZIA, C. SIBILIA, M. BERTOLOTTI, *Optics Comm.* 168 (1999) 277.
7. F. GARZIA, C. SIBILIA, M. BERTOLOTTI, *Opt.&Quantum Electron.* 32 (2000) 781.
8. F. GARZIA, M. BERTOLOTTI, in stampa su *Opt.&Quantum Electron.*