Serial key based all-optical cryptographic device for security applications

Fabio Garzia*, Mario Bertolotti

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

ABSTRACT

An all-optical cryptographic device for security applications, based on the properties of soliton beams, is presented. It is able to codify a given bit stream of optical pulses, changing their phase and their amplitude as a function of one or more encryption serial keys that merge with the data stream, generating an incomprehensible stream.
Its great advance is represented by its capability of encrypting in real time, without slowing the data flow that can be transmitted with its original velocity.

Keywords: cryptographic device, security device, soliton interaction, all-optical switching, spatial soliton, all-optical device.

1. INTRODUCTION

The device described in this paper is capable of codifying a given bit stream of optical pulses, changing their phase and their amplitude as a function of one or more encryption serial keys that merge with the data stream, generating an incomprehensible stream. It is based on the special properties of spatial solitons that are, as well known, self-trapped optical beams able to propagate without any change of their spatial shape, thanks to the equilibrium, in a self-focusing medium, between diffraction and nonlinear refraction[1].
Their interesting properties have allowed to design a certain number of spatial optical switches which utilise the interaction between two bright or dark soliton beams, and the waveguide structures induced by these interactions[2-6]. Two distinct parallel solitons are generally used as initial condition for such interactions. In fact it is well known that when two distinct bright spatial solitons are launched parallel to each other, the interaction force between them depends on their relative distance and their phase[7,8].
A variety of useful devices can be thought and designed using the properties of solitons. One of the most important features is their particle-like behaviour and their relative robustness to external disturbs.
Interesting effects have been found in the study of transverse effects of soliton propagation at the interface between two nonlinear materials[9-11] or in a material in the presence of a gaussian refractive index profile, that is in low perturbation regime[9].
It has been shown that it is possible to switch a soliton, in the presence of a transverse refractive index variation, towards a fixed path, since the index variation acts as a perturbation against which the soliton reacts as a particle, moving as a packet without any loss of energy. This last property makes possible to design useful all optical devices such as a filter[13] or a high speed router[14].
The general problem of encrypting the binary data transmitted on an optical channel is very felt in the security field.
The aim of the present work is to find a new approach to this problem, studying a device that is able to increase the security level of an optical channel, extending the modulation also to the phase of the output pulses. It acts as an amplitude/phase converter accepting two binary modulated stream of pulses as inputs and generating a unique phase modulated stream of pulses as output. The first stream is related to the data stream while the second stream is related to the serial cryptographic key. The device can be properly cascaded, adding further serial cryptographic keys, generating a unique stream of pulses characterized by a higher security level. The great advantage is that the device is totally passive, which means that is does not need extra energy to work properly. The working principle is shown in fig.1.

*fabio.garzia@uniroma1.it; phone +39 06 4991 6543; fax +39 06 44240183; http://www.securitylab.org; Dipartimento di Energetica & INFM; Università degli Studi di Roma "La Sapienza", Via A. Scarpa, 16, 00161 Roma, Italy

In its basic geometry a soliton beam travels in a waveguide which, in the plane between the cladding and the substrate, has a distribution of refractive index which follows a triangular curve, with a modified parabolic profile.
We start studying the general structure of the device. Then the transverse behaviour of a soliton in a triangular profile[13], whose longitudinal profile is parabolic[14], is discussed. Once the properties of motion are derived, we investigate the structure from the global point of view, deriving all the properties and the operative conditions, that represents the scope of this paper.

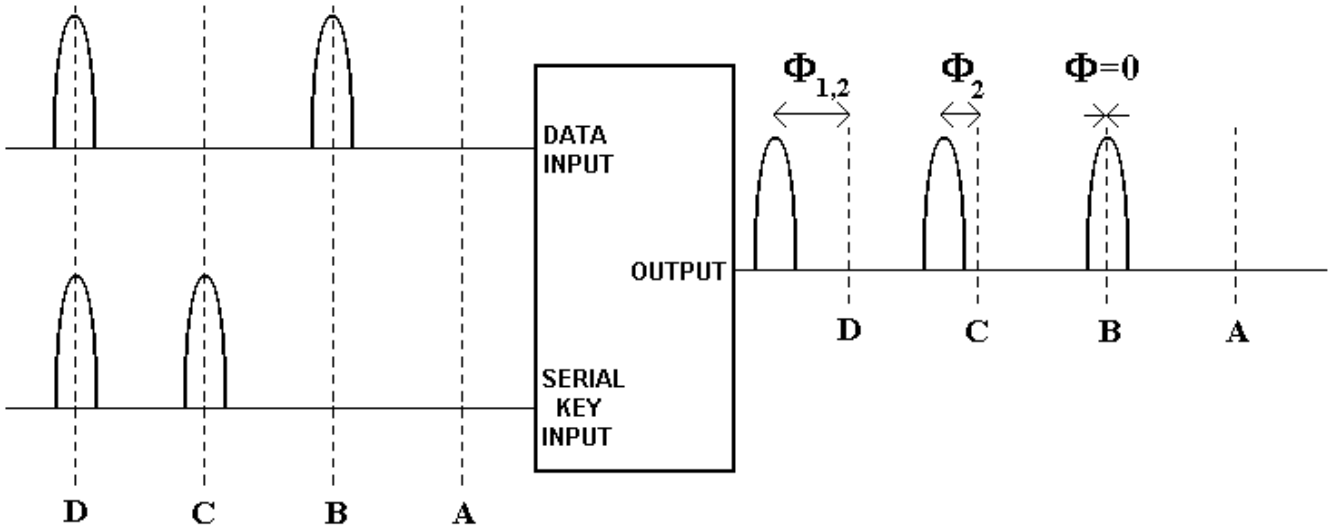

Fig.1 Working principle of the device

2. STRUCTURE OF THE DEVICE

To simplify the development of the theory we consider only a 2 inputs -1 output device. The purpose of the device is to generate a phase modulated pulse according to the different combinations of amplitude of input pulses, that represent the data stream and the cryptographic stream.

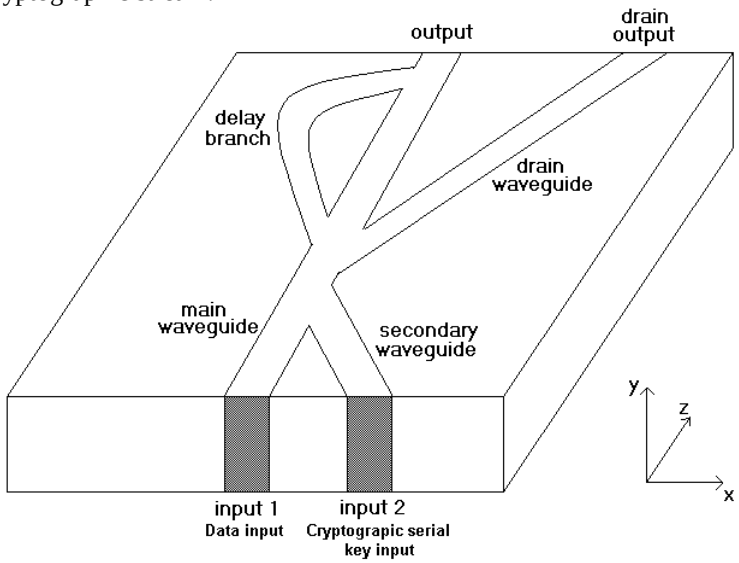

Fig.2 Structure of the device.

In the following we briefly call them input 1 and input 2. This is equal to say that, in the presence of two binary inputs, the possible amplitude combinations are 4, and the output pulse has to assume 4 different phase values, without requesting auxiliary energy.

We suppose to work with soliton beams to use their attracting or repelling properties[7] and their particular behaviour when they propagate in a transverse refractive index profile[13]. The structure we want to study is shown in fig. 2.
We also suppose that the two input pulses enter in the relative inputs of the device with the same phase. This is not a restriction since any phase difference can be properly compensated.
Owed to the fact that we deal with equal streams of pulses the last condition is that the input pulses are characterised by the same amplitude.
The device is composed by 4 parts: the main waveguide, the secondary waveguide, the delay branch and the drain waveguide. The geometry and the refractive index values of these four components strictly determine the feature of the device and their values will be designed as discussed in the following.
Let us analyse the behaviour of the device in the four possible input situations. Since we deal with binary input pulses we consider the two values of logical zero (absence of pulse) and logical one (presence of pulse). We refer to them as zero and one.
The first situation is when the two inputs are equal to zero. In this case, due to the passive nature of the device, we obtain a zero in the output.
The second situation is when the first input is equal to one and the second input is equal to zero. In this case, if the refractive index of both the delay branch and the drain waveguide is less or equal to the refractive index of the main waveguide, the pulse propagates undisturbed and it reaches the output, with a phase that is equal to the propagation phase along the main waveguide. If the length of this waveguide is properly chosen, according to the wavelength of the beam, the phase of the output pulse is equal to the phase of the input pulse. In the first situation there was an absence of pulse and its phase value was virtually equal to zero. In this case the phase value variation has been chosen equal to zero but we are in the presence of a pulse. The phase variation could anyway be chosen at will, but we keep it fixed at zero for simplicity. The behaviour of this kind of waveguide has already been studied[13].
The third situation is when the first input is equal to zero and the second input is equal to one. In this case, since we are in the proper refractive index conditions of the waveguide and the delay branch is properly shifted with respect to the input point of the secondary wave, the second input pulse is trapped in the main waveguide and it reaches the output with a certain phase difference, that we define later, respect to the previous case due to the fact that it propagates, in the initial part, into the secondary waveguide.
The fourth situation is when both the inputs are equal to one. In this case the two pulses meet at the converging point between the main waveguide and the secondary waveguide. In this case, since we are in soliton propagation condition, they can attract if their relative phase is included between zero and $\pi/2$ or between $3\pi/2$ and 2π, or they can repel if their relative phase is included between $\pi/2$ and $3\pi/2$. If the length of the secondary waveguide is chosen to generate a repulsive condition, the two solitons propagate in the main waveguide properly separated until reaching the bifurcation point between the main waveguide, the delay branch and the drain waveguide. At this point the two solitons detach: the first one enters the delay branch while the second one enters the drain waveguide.
The first soliton propagates in the delay branch experiencing a phase variation that depends on the length of the branch and therefore is properly selectable and can be chosen different from the previous cases, generating the fourth phase condition. The second pulse, on the contrary, propagates in the drain waveguide where it reaches the proper drain output.

N°.	**INPUT 1 (INTENSITY)**	**INPUT 2 (INTENSITY)**	**OUTPUT INTENSITY**	**OUTPUT PHASE**	**PHASE CONDITION**
1	0	0	0	0	-
2	I_1	0	I_1	0	-
3	0	I_2	I_2	φ_2	$\frac{\pi}{2} < \varphi_2 < \frac{3\pi}{2}$
4	I_1	I_2	I_1	$\varphi_{1,2}$	-

Table 1 Working scheme of the device

The delay branch is composed by a properly modified longitudinal parabolic waveguide, whose purpose is to accept the beam from the main waveguide with an angle that respects the paraxial approximation, to propagate it changing its

direction until reaching a straight longitudinal direction and to reverse this sequence until carrying the pulse inside the main waveguide with a certain phase difference. The behaviour of this modified parabolic waveguide is studied later.
The situation is summarised in table 1, where it is also pointed out the pulse that reaches the output to provide more details about the working principles of the device, even if we consider input pulses with the same amplitude.
We will now define better the profile of the refractive index of the waveguides and the properties of the longitudinal modified parabolic waveguide that compose the delay branch.

3. PROPERTIES OF A SOLITON IN A MODIFIED LONGITUDINAL PARABOLIC WAVEGUIDE

We want now to define the structure of the modified parabolic waveguide composing the delay branch to find its peculiar properties that allow the loop to work properly.
We choose this kind of waveguide because it is the simplest curve that carries progressively the soliton beam from a propagation angle that respects the paraxial approximation until a angle that respects a parallel longitudinal propagation and vice versa.
This curve could be roughly approximated with a linear curve, but the final result would be a too sharp path, since the soliton reaches the reversing point with a certain inclination. Further the parabolic path is the trajectory followed from a soliton beam that is injected into a linear transverse refractive index profile, that is the transverse profile that we are going to consider.
Let us consider a soliton beam propagating in the z-direction, whose expression of the field Q at the beginning of the structure is:

$$Q(x,0) = C\,\mathrm{sech}\left[C(x - \bar{x})\right], \tag{1}$$

where $\bar{x}$ is the position of the centre of the beam and C is a real constant from which both the width and the amplitude of the field depend. The variables x and z are normalised with respect to the wavevector of the wave and therefore they are adimensional quantities.
When the soliton beam is propagating in a triangular transverse index profile, whose maximum value is Δn_0 and whose maximum width is 2b, it is subjected to a transverse acceleration equal to [13-16]:

$$a_T = \frac{2\Delta n_0}{b} C^2 . \tag{2}$$

We use, for our analysis, a dynamic point of view, that is to consider the step by step transverse relative position of the waveguide with respect to the beam using the z variable as a time parameter.

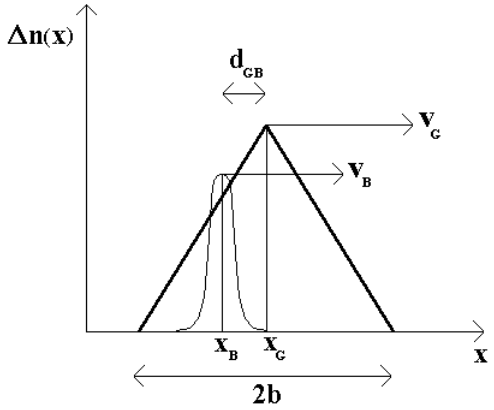

Fig.3 Relative distance waveguide-soliton at some propagation distance z.

If $x_G(z)$ is the position of the central part of the waveguide profile with respect to z, the longitudinal form of the waveguide is chosen to be a modified parabolic:

$$x_G(z) = \frac{z^2}{a^2} - \frac{2\sqrt{d}}{a} z , \tag{3}$$

where 'a' is a real constant responsible for the curvature of the waveguide and 'd' is a real constant responsible for the position of the curve. Equation (3) can be better understood if it is expressed as a function of z, that is:

$$z = -a\sqrt{x_G + d} + a\sqrt{d} \ . \tag{4}$$

It is possible to see that it is positioned in the second quadrant of the Cartesian plane, it has a vertical asymptote at $x_G(z) = d$ when $z \to a\sqrt{d}$. It shows a gradually increasing derivative, growing from a starting angle at x=0, chosen to be below the maximum angle allowed from the paraxial approximation, until reaching a vertical alignment at $x_G(z) = d$, that is what we want to make the device work properly. To respect this term it is necessary to impose a certain condition to the 'a' and 'd' parameters, as we show later. A graphical representation of equation (4) is shown in fig. 4 for a=16.9 and d=1.4.

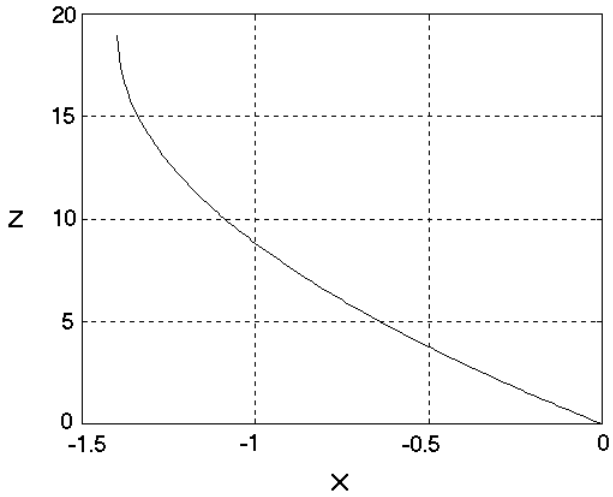

Fig.4 Graphical representation of the modified parabolic waveguide for a=16.9, d=1.4.

The local inclination of the waveguide with respect to the longitudinal axis z, can be regarded as the transverse relative velocity of the waveguide that appears to the beam that propagates longitudinally:

$$\mathrm{v}_G = \frac{dx_G(z)}{dz} = \frac{2z}{a^2} - \frac{2\sqrt{d}}{a} \ . \tag{5}$$

Using equation (2) it is possible to calculate the transverse relative velocity:

$$\mathrm{v}_B = \int_0^z a_T \, d\zeta = \frac{2\Delta n_0}{b} C^2 z \tag{6}$$

and the position of the beam

$$x_B = \int_0^z \mathrm{v}_B \, d\zeta = \frac{\Delta n_0}{b} C^2 z^2 \ . \tag{7}$$

Equation (7) is valid for a propagation in the first quadrant of Cartesian plane. Since we consider, in our case, a propagation in the second quadrant, we must reverse the sign of the second member of the equation considered.

Initially the beam is positioned in the centre of the waveguide. Since the waveguide appears to move, with respect to an observer that follows the longitudinal direction, with a relative velocity expressed by equation (5), the soliton beam enters in the constant acceleration zone, where its velocity increases linearly with z. It also follows a parabolic trajectory, according to equation (7), until it remains in this part of the waveguide.

After that the beam has propagated for a certain z distance, two different situations may happen: the beam leaves the acceleration zone without reaching the velocity of the waveguide at that z, or the beam acquires a velocity that is greater than or equal to the velocity of the waveguide. The first event may called ‘detach situation’, since the beam leaves the waveguide, while the second one may be called ‘lock-in situation’ since the beam reaches the other side of the waveguide where it is stopped, reversing its path and so on.

At any value of z, as shown in fig. 3, the distance d_{BG} between the beam and the waveguide is:

$$d_{BG} = x_B - x_G = -\frac{\Delta n_0 C^2}{b} z^2 - \frac{z^2}{a^2} + \frac{2\sqrt{d}}{a} z = -z^2 \left(\frac{b - a^2 \Delta n_0 C^2}{a^2 b} \right) + \frac{2\sqrt{d}}{a} z . \quad (8)$$

A detach situation takes place when:

$$d_{BG} = b . \quad (9)$$

If we solve equation (9) with respect to z we can calculate, if it exists, the propagation distance where the detachment begins:

$$z_D = \frac{\sqrt{d} \pm \sqrt{d - b - a^2 \Delta n_0 C^2}}{\frac{b + a^2 \Delta n_0 C^2}{ab}} . \quad (10)$$

The two solutions refer to the detach situation (when the negative sign of the root is considered) or to the first cross of the centre of the waveguide in the lock-in situation (when the positive sign of the root is considered). Studying the discriminator of equation (10) it is possible to derive the value of the amplitude C_D that divides the lock-in values from the detach values:

$$C_D = \frac{1}{a} \left(\frac{d - b}{\Delta n_0} \right)^{1/2} . \quad (11)$$

It is possible to see, from equation (11) that the more the curvature of the waveguide ('a' parameter) increases or the more the refractive index decreases and the more C_D increase. This behaviour agrees with what one could expect.

We want now to calculate the inclination according to which a soliton, whose amplitude is smaller than the detach amplitude, leaves the waveguide. Since the mentioned angle is equal to the detach velocity, substituting equation (11) into equation (6), we have:

$$\Phi = \tan^{-1} \mathrm{v}_D \quad (12a)$$

and

$$\mathrm{v}_D = \mathrm{v}_B(z_D) = \frac{2\Delta n_0 C^2 a}{b + a^2 \Delta n_0 C^2} (\sqrt{d} - \sqrt{d - b - a^2 \Delta n_0 C^2}) . \quad (12b)$$

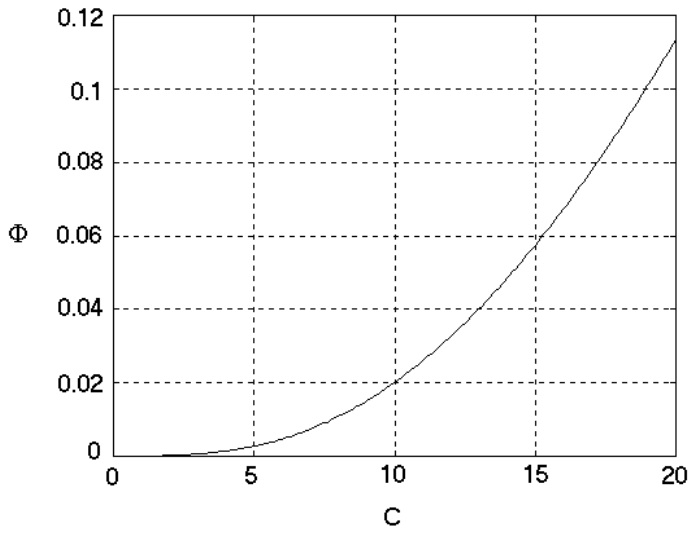

Fig.5 Detach angle Φ in degrees, equal to $\mathrm{atan}(\mathrm{v}_D)$, versus C for a=16.9, d=1.4, b=0.25, $\Delta n_0 = 1 \cdot 10^{-5}$.

In fig. 5 it is shown the graphical behaviour of equation (12) for a=16.9, d=1.4, b=0.25, $\Delta n_0 = 1 \cdot 10^{-5}$. The detach value C_D can be calculated by means of equation (11) and it is equal to 20.

Due to the absence of restrictions about the length L of the waveguide, the lock-in value C_D of the amplitude, expressed from equation (11), does not depend on L. This means that, given a certain waveguide whose length is equal

to L, we can obtain a lock-in value C_D whose detachment distance, calculated from equation (10), is longer than L. In this situation, due to the restriction imposed from the waveguide length L, the detach value C_D obviously decreases. In fact, even if the beams characterised from an amplitude lesser than C_D tend to be expelled from the waveguide, the detachment takes place at a distance that is longer than the waveguide length L and the beam remains locked-in. The new value C_{DL}, that is lower than C_D, can be calculated from equation (10) setting $z_D = L$ and solving respect to C:

$$C_{DL} = \sqrt{\frac{-B + \sqrt{B^2 - 4AC}}{2A}} \,. \tag{13}$$

where

$$A = a^4 \Delta n_0^2 L^2 \tag{13a}$$

$$B = 2a^2 bL^2 \Delta n_0 - 2a^3 b\sqrt{d}\, L\Delta n_0 + a^4 b^2 \Delta n_0 \tag{13b}$$

$$C = b^2 L^2 - 2ab^2 L\sqrt{d} + a^2 b^3 \,. \tag{13c}$$

We want now to make some considerations about the paraxial approximation.
Since we deal with a modified parabolic waveguide, we are in the presence of a curvature, with respect to the z axis, that increases with z. We have not to forget that we are in a paraxial approximation, that is the derived equation s are valid until the angle between the propagation direction and the longitudinal direction is lesser than 8°÷10°. This means that, due to the analytical expression of the waveguide, expressed from equation (3) or equation (4), once the 'a' or 'd' parameter has been chosen the other parameter is unavoidably fixed. The condition must be imposed only at the entrance of the waveguide, where the curvature, with respect to the longitudinal direction is maximum and decreases up to zero at the end. In analytical terms this means that it is possible to impose this condition to the first derivative of equation (3) to calculate the maximum propagation distance:

$$\left| x'_G(0) \right| = \frac{2\sqrt{d}}{a} \le \tan 8° = 0{,}14 \,, \tag{14}$$

that gives:

$$\frac{\sqrt{d}}{a} \le 7 \cdot 10^{-2} \,. \tag{15}$$

This condition must be considered in the project of the delay branch.
We want now to calculate the length of the curve expressed by equation (3), since it is necessary to control the optical path, and therefore the phase variation, of the beam that propagates inside it.
Considering equation (4), the first derivative of z with respect to x is:

$$\frac{dz}{dx} = -\frac{a}{2\sqrt{x+d}} \tag{16}$$

and the elementary length of the curve, as a function of x is:

$$dl = \sqrt{dx^2 + dz^2} = \sqrt{dx^2 + \frac{a^2}{4(x+d)} dx^2} \,. \tag{17}$$

Integrating equation (17) we have:

$$I(x) = \frac{(x+d)\sqrt{\frac{4x+4d+a^2}{x+d}}}{2} + \frac{a^2}{8}\log(8x+8d\ +a^2\ +4(x+d)\sqrt{\frac{4x+4d+a^2}{x+d}}) + \text{constant} \,. \tag{18}$$

It is possible to see that the integral becomes indefinite when x tends to -d, as one could expect due to the structure of the curve. To define the constant that is present in equation (18) it is necessary to calculate the limit of the integral when x tends to -d:

$$\lim_{x \to -d} I(x) = \frac{a^2}{4} \log a \,. \tag{19}$$

The length of the curve is therefore equal to:

$$L_G = I(0) = \frac{d}{2}\sqrt{\frac{4d+a^2}{d}} + \frac{a^2}{8}\log(8d + a^2\ + 4d\sqrt{\frac{4d+a^2}{d}}) - \frac{a^2}{4}\log a \,, \tag{20}$$

that is obviously a complex function of 'a' and 'd' parameters.

4. NUMERICAL SIMULATION OF THE EFFECT

We have simulated the device from the numerical point of view using a FD-BPM algorithm to study its behaviour and to see if it agrees with the developed theory.
At first the design does not consider the physical limitations that can arise when we deal with technological fabrication problems. In the next paragraph we will consider this kind of problems.
We use, in this situation, a geometrical approach, that is we do not care of imposing particular conditions that would be necessary in a real situation, such us to use the same Δn_0 for all the waveguides, letting us a higher number of degrees of freedom. We are further free of using the wavelength we need to generate the proper phase variation according to our needs. This is not obviously possible in a real case where the wavelength is given
Let us choose for example the half length of the delay branch waveguide equal to 20:

$$a\sqrt{d} = 20 . \tag{21}$$

Since we have to respect, even in this design approach, the paraxial condition, we have to solve the system of equation s composed by equation (21) and equation (15) that gives a=16.9, d=1.4.
The width of the waveguide must obviously be less than 'd' and we choose, for example b=0.25, that is to suppose a waveguide width equal to 2b=0.5.
The spot size of the beam must be less or equal to 'b'. Since we deal with a hyperbolic secant profile, expressed by equation (1), the width is linked to the amplitude C, that is the greater is C the narrower is the beam. A proper value is C=20.
The difference of length between the interested part of the main waveguide and the delay branch can be calculated using equation (20) that gives $\Delta L_G = 0.1305$. Once chosen the wavevector we have immediately the phase difference.
We have not, until this point, chosen the phase values to code. We decide to generate a phase difference a bit greater than $\pi/2$ for the passage through the secondary waveguide and a phase difference a greater than π for the passage through the delay branch. This is equal to say that the length of the delay branch must almost be twice the length of the secondary waveguide. Since the length of the delay branch has already been chosen we have to design the secondary waveguide. A proper structure is for example the one whose projections on the longitudinal and transversal directions are respectively equal to 35 and 2, that gives a difference of length between the interested part of the main waveguide and the secondary waveguide equal to 0.0571, that is less than one half of the relative difference of length of the delay branch.
We have now to find the value of the wavevector that allows to obtain the chosen phase values. A good values is β=30, that gives a phase value of 1.24 π for the delay branch and a phase value of 0.55 π (a bit larger than the minimum value of $\pi/2$ that allows the repulsion between two close soliton beams) for the secondary waveguide.
Once chosen all the geometrical values of the structure it is necessary to select the refractive index of the waveguides to ensure the correct trapping of the beams inside them.
From equation (11) we have:

$$\Delta n_{0G} = \frac{d-b}{a^2 C_D^2} . \tag{22}$$

Substituting the numerical values we have $\Delta n_{0G} = 1 \cdot 10^{-5}$.
Since for the secondary waveguide we have[13]:

$$C_D = \frac{\mathrm{v}_G}{2(\Delta n_{0S})^{\frac{1}{2}}} , \tag{23}$$

where v_G is the tangent of the angle between the waveguide and the longitudinal direction, it is possible to solve equation (23) with respect to Δn_{0S} giving:

$$\Delta n_{0S} = \left(\frac{\mathrm{v}_G}{2C_D} \right)^{\frac{1}{2}} . \tag{24}$$

Substituting the numerical values we have $\Delta n_{0S} = 2.04 \cdot 10^{-6}$, that is 5 times less than the value found for the delay branch. This difference reflects the different geometry, and therefore the different propagation conditions, of the two

considered optical structures. We further choose for the main waveguide a refractive index value equal $\Delta n_{0G} = 1 \cdot 10^{-5}$, so that the beam that propagates inside the main waveguide does not enter in the delay branch unless it is pushed inside it.
The design approach used until this point is obviously practical for the numerical simulations since, as we already said, we have no physical restrictions, but absolutely impossible to be used in a real device design due to the greater number of limitations that is necessary to respect. We show a real design approach in the following.

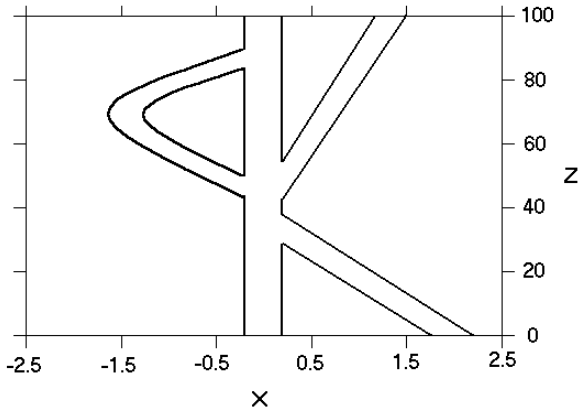

Fig.6a

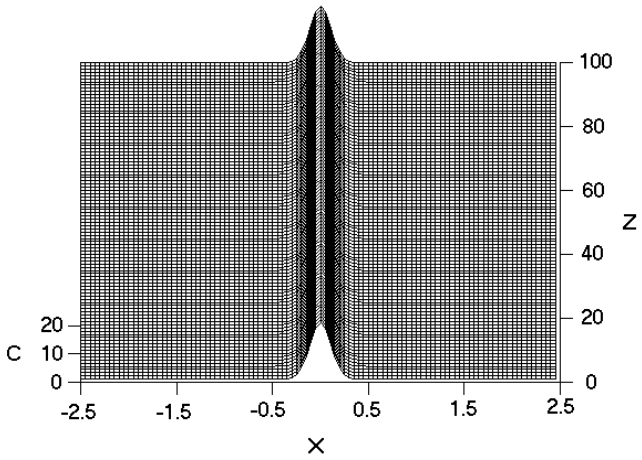

Fig.6b

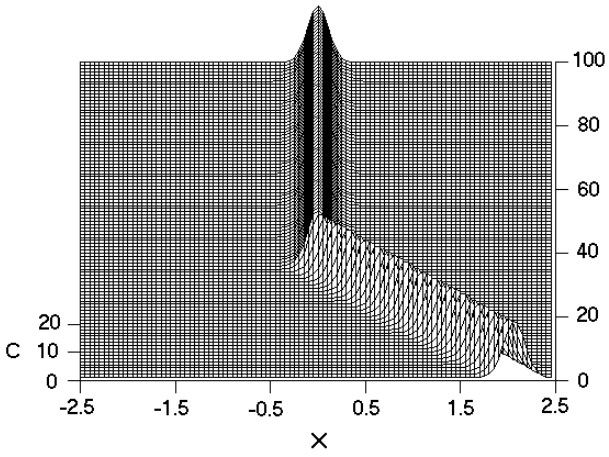

Fig.6c

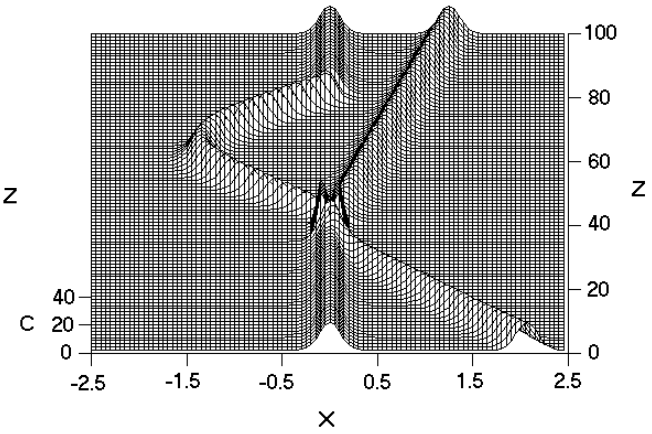

Fig.6d

Figs.6 Upper view and numerical simulations. The parameters of the waveguide are a=16.9, d=1.4, b=0.25, $\Delta n_0 = 1 \cdot 10^{-5}$.
(a) Upper view of the structure.
(b) Numerical simulation of the behaviour of the structure in the presence of the only input 1.
(c) Numerical simulation of the behaviour of the structure in the presence of the only input 2.
(d) Numerical simulation of the behaviour of the structure in the presence of both input 1 and input 2.

Further we neglect to insert at the end of the structure a proper propagation distance that allows to the beam that enters alone in the structure through input 1 to exit with the same input phase, since we are mainly interested to the phase variations. The drain waveguide has been designed in a way similar to the secondary waveguide.
The geometry of the designed structure is shown in fig. 6a.
Let us analyse the results of the numerical simulations for the three possible input combination to demonstrate the correctness of the developed theory, neglecting the situation of no inputs that represents the first combination according to table 1.

In fig. 6b the numerical simulation in case of the presence of the only input pulse at the entrance 1 (the second input combination of table 1) is shown. In this case, since the refractive index variation is equal to the one of the delay branch, the beam propagates undisturbed and reaches the output, generating a proper phase coded pulse.
In fig. 6c the numerical simulation of the third input combination, that is the presence of only an input pulse at the entrance 2 is shown. In this case, the pulse first propagates properly trapped inside the secondary waveguide , due to the fact that the parameters of the structures have been designed to lock it. It reaches the main waveguide, with a certain phase difference that we have designed to be equal to 0.55 π, reaching the output, and generating a proper output phase coded pulse.
In fig. 6d the numerical simulation of the fourth input combination, that is the presence of both input pulses at the entrances is shown. In this case, the two pulses meet at the merging point between the main waveguide and the secondary waveguide with a relative phase difference greater than 0.55 π, that is in a repulsive situation. The two beams propagate parallel each other properly separated, until reaching the bifurcation point. In this zone the pulse relative to input 1 is pushed into the delay branch, while the pulse relative to input two is pushed inside the drain waveguide where it reaches the drain output. The first pulses, that propagates inside the delay branch, is trapped inside it since the structure has been properly designed and enters again inside the main waveguide with a relative designed phase difference equal to 1.24 π, reaching the output and generating a proper output phase coded pulse.
The numerical simulations, as shown in figures 6, confirm the theory developed.

5. A NUMERICAL DESIGN OF THE DEVICE

We want now to give a numerical example for the design of the considered device.
We suppose to have a Schott B 270 glass, whose optical parameters at $\lambda_0 = 620\text{nm}$ are $n_0 = 1.53$ and $n_2 = 3.4 \cdot 10^{-20}\,\text{m}^2/\text{W}$ being n_0 and n_2 are the linear and nonlinear refractive indices respectively[13]. Let us consider a spot size of the beam equal to $d_0 = 10\mu\text{m}$.
The design rules are very restrictive in a real situation since it is necessary to match different requests with a reduced free choice of parameters. In fact once fixed the source and the proper material for the given source it is necessary to design the geometry of the structure to trap the pulses with a proper soliton intensity level, generating the necessary coded phase variation. Further, since we use the same constructive technology, we suppose that the refractive index variation Δn_0 is the same for the delay branch and for the secondary waveguide, introducing another restriction.
It is well known that, given a certain material and a certain light source, the intensity necessary to generate a soliton beam is given by:

$$I_s = \frac{2n_0}{d_0^2 n_2 \beta^2} \tag{25}$$

where β is the wavevector of the beam. Substituting the numerical values into equation (17) we have $I_s = 3.74 \cdot 10^{15} W/m^2$.
Since the intensity of the beam I_s is related to its amplitude C from[13]:

$$I_s = \frac{1}{\left[\log\left(2+\sqrt{3}\right)\right]^2} \frac{n_0}{2n_2} C^2 , \tag{26}$$

it is possible to express eqs.(11) and (23) in term of the intensity of the beams.
We choose for example $\Delta n_0 = 1 \cdot 10^{-2}$ and we start with the design of the device. We want to code the third situation (only a pulse at the input 2) with a relative phase variation just greater than π/2 and the forth situation (both the input pulses) with a relative phase very close to π.
We choose $d = 2d_0 = 20\mu m$. Substituting this value into equation (15) we obtain a=0.0639. In this way the geometry of the delay branch is totally defined. If we choose $b = 19.96\mu m$, using equation (11) and equation (26) we obtain a lock-in value $I_D = 1.25 \cdot 10^{16} W/m^2$, that is a value above the soliton threshold calculated with equation (25) and below the second order soliton threshold.
We have now to check if, with these values, we have obtained a phase difference value very close to π, as we desire. The phase difference value can be calculated as the product of the wavevector and the difference of path between the delay branch and the main waveguide. Using equation (20) we obtain $\Delta\phi = 0.59\pi$. This value is very close to the other

phase value, generating two phase values very close each other. In this case it is necessary to make some correction to the geometry of the delay branch to correct the phase value to a value close to π, keeping at the same time the lock-intensity above the soliton generation threshold. We choose to increase the value of the "a" parameter, that allows the paraxial approximation to be conserved. If we increase this parameter by 1.53 times, the total length of the delay branch increases. The new intensity lock-in value decreases to $I_D = 5.36 \cdot 10^{15} W/m^2$, that is always above the soliton generation threshold. The phase value is in this case equal to π, as we desired at the beginning of our computation.
It is now necessary to project the secondary input waveguide. We want to obtain the same intensity lock-in value calculated for the delay branch and a phase difference value a bit greater than π/2.
This kind of waveguide as already been studied[13], showing a behaviour similar to the parabolic waveguide and a lock-in value equal to:

$$C_D = \frac{\mathrm{v}_G}{2(\Delta n_0)^{\frac{1}{2}}}, \tag{27}$$

where v_G is the tangent of the inclination angle with respect to the longitudinal direction. It is obviously necessary to respect, even in this case, the paraxial approximation; this means that once we have chosen the distance a_L between the second input and the main input, the longitudinal length b_L of the waveguide cannot be shorter than a minimum, calculated according to the paraxial limit, that is:

$$a_L \le b_L \tan 8° = 0.14 b_L \tag{28}$$

Since we suppose to generate this waveguide using the same physical procedure used for the delay branch, we have to suppose that the value $\Delta n_0 = 1 \cdot 10^{-2}$ is the same for both the waveguides. If we use as a first attempt value $a_L = d$, to generate a device whose lateral extensions with respect to the main waveguide are the same, we immediately obtain b_L from equation (28), that allows us to calculate v_G. Substituting these values into equation (27), using equation (26) we have an intensity lock-in value equal to $I_{DS} = 2.23 \cdot 10^{17} W/m^2$ and $\Delta\phi_S = 1.12\pi$. The waveguide designed according to these criteria is totally useless for our purpose since the lock-in value is greatly above the generation value of a second order soliton and consequently above the lock-in value calculated for the delay branch. Further, the phase value obtained is totally different with respect to the one we desire. It is therefore necessary to find another approach. If we impose the waveguide to have the same lock-in intensity of the delay branch, considering always $a_L = d$, we can calculate b_L, reversing the reasoning followed above. In this case we obtain $b_L = 5650 \ \mu m$ that satisfies the paraxial condition expressed by equation (27). If we calculate the phase difference we have $\Delta\phi_S = 0.175\pi$, that is not only a different value respect to the desired one but also a value that does not allow the repulsion between the two beams, that is a fundamental condition to make the device to operate correctly.
Consequently it is necessary to act also on a_L, considering a device that has not the same lateral extension with respect to the main waveguide. Fixing the intensity lock-in level to be equal to the one of the delay branch and fixing the phase difference $\Delta\phi_S$ to be as close as possible to 0.5 π, it is possible to demonstrate that a valid waveguide is the one characterised by $a_L = 3d = 60\mu m$ and $b_L = 16935 \ \mu m$, that provides a phase difference $\Delta\phi_S = 0.53\pi$, respecting the paraxial condition expressed by equation (27).
The problems found in the design of the secondary input waveguide could be avoided if we could act also on Δn_0, but this is very difficult to be made in a real situation where both the delay branch and the inclined waveguide are generated in the same process.
Different approaches can be used to design the device, as for example, to dimension first the secondary waveguide and the delay branch, but they are always subjected to different restrictions due to the physics of the waveguides generation process.
Further considerations about the temporal behaviour and the absorbing behaviour of solitons in transverse refractive index profile device have already been studied[13,14] and they are not repeated here for brevity.
This kind of device can be connected in a properly cascaded configuration[18] capable of accepting three input streams of pulses (a data stream and two cryptographic keys) and generating a unique stream of pulses characterized by a higher security level.

7. CONCLUSIONS

We have studied and designed a serial key based all-optical cryptographic device, whose working principles are based on the repulsive and propagation properties of solitons in a parabolic transverse refractive index profile, that we deeply analysed in the paper.
The switching properties have been studied in details, obtaining some useful design criteria for a practical device.
The device can be properly designed by means of the geometrical and optical parameters of the different structures that compose the modulator.
The device, as it stands, can be connected in an half cascade configuration, capable of accepting three input streams of pulses (a data stream and two cryptographic keys) and generating a higher security level output stream.

REFERENCES

1. R. Y. Ciao, E. Garmire, and C. H. Townes, "Self-trapping of optical beams", *Phys. Rev. Lett.*, **13**, pp. 479-482, 1964.
2. B. Luther-Davies and Y. Xiaoping, "Waveguides and Y junctions formed in self-defocusing dark spatial soliton", *Opt. Lett.*, **17**, pp. 496-498 ,1992; "Steerable optical waveguides formed in self-defocusing media by using dark spatial soliton", *Opt. Lett.*, **17**, pp. 1755-1757, 1992.
3. W. Krolikowski, and Y. S. Kivshar, "Soliton-based optical switching in waveguide arrays", *J. Opt. Soc. Am. B*, **13**, pp. 876-887, 1996.
4. N. N. Akhmediev, and A. Ankiewicz, "Spatial soliton X-junctions and couplers", *Opt. Comm.*, **100**, pp. 186-192, 1993.
5. W. Krolikowski, X. Yang, B. Luther-Davies, and J. Breslin, "Dark soliton steering in a saturable nonlinear medium", *Opt. Comm.*, **105**, pp. 219-225, 1994.
6. A. P. Sheppard, "Devices written by colliding spatial solitons: a coupled mode theory approach", *Opt. Comm.*, **102**, pp. 317-323, 1993.
7. J. P. Gordon, "Interaction forces among solitons in optical fibers", *Opt. Lett.*, **8**, pp. 596-598, 1983.
8. F. Garzia, C. Sibilia, M. Bertolotti, R. Horak, and J. Bajer, "Phase properties of a two-soliton system in a non linear planar waveguide", *Opt. Comm.*, **108**, pp. 47-54, 1994.
9. A .B. Aceves, J. V. Moloney, and A. C. Newell, "Reflection and transmission of self-focused channels at nonlinear dielectric interfaces", *Opt. Lett.*, **13**, pp. 1002-1004, 1988.
10. P. Varatharajah, A. B. Aceves, and J. V. Moloney, "All-optical spatial scanner", *App. Phys. Lett.*, **54**, pp. 2631-2633, 1989.
11. A .B. Aceves, P. Varatharajah, A. C. Newell, E. M. Wright, G. I. Stegman, D. R. Heatley, J. V. Moloney, and H. Adachihara, "Particle aspects of collimated light channel propagation at nonlinear interfaces and in waveguides", *J. Opt. Soc. Am. B*, **7**, pp. 963-974, 1990.
12. F. Garzia, C. Sibilia, and M. Bertolotti, "Swing effect of spatial soliton", *Opt. Comm.*, **139**, pp. 193-198,1997.
13. F. Garzia, C. Sibilia, and M. Bertolotti, "High pass soliton filter", *Opt. Comm.*, **152**, pp. 153-160, 1998.
14. F. Garzia, C. Sibilia, and M. Bertolotti, "All optical soliton based router", *Opt. Comm.*, **168/1-4**, pp. 277-285, 1999.
15. H. W. Chen, and T. Liu, "Nonlinear wave and soliton propagation in media with arbitrary inhomogeneities", *Phys. Fluids*, **21**, pp. 377-380, 1978.
16. P. K. Cow, N. L. Tsintsadze, and D. D. Tsakhaya, "Emission of ion-sound waves by a Langmuir soliton moving with acceleration", *Sov. Phys. JETP*, **55**, pp. 839- 843, 1982.
17. J. S. Aitchison, A. M. Weiner, Y. Silberberg, M. K. Oliver, J. L. Jackel, D. E. Leaird, E. M. Vogel, and P. W. E. Smith, "Observation of spatial optical solitons in a nonlinear glass waveguide", *Opt. Lett.*, **15**, pp. 471-473, 1990.
18. F. Garzia, C. Sibilia, and M. Bertolotti, “New Phase Modulation Technique Based on Spatial Soliton Switching”, *J.L.T.* , **19/7**, pp.1036-1050, 2001.