ON THE POSTQUANTUM CIPHER SCHEME

Jaroslav HRUBY
Institute of Physics
Czech Academy of Sciences, Czech Republic

July 2006

Abstract

We discuss the general theoretical ideas of the possibility using cryptosystems based on the partial differential equations (PDE) and the role of inverse scattering problem for the cryptanalysis as the possible way to the postquantum cipher scheme. An application of the nonlinear Schrödinger equation and optical fibre technology in cryptology is presented.

1 Introduction

Classical cryptography based on asymmetric or symmetric ciphers have become a key technology for making the Internet and other IT infrastructures secure. For example digital signatures provide long term authenticity, integrity, and support for non-repudiation of data. Digital signatures are widely used in identification and authentication protocols for example for software downloads and also for long term archiving. Therefore, secure of digital signature algorithms are crucial for maintaining IT security. But quantum information science now has the dynamical develop and it is showed that quantum computers can break all digital signature via Shor's algorithm. The Grover's algorithm can make symmetric cipher also vulnerable.

Physicists predict that within the next 15 to 20 years there will be quantum computers that are sufficiently large to implement Shor's ideas for breaking digital signature schemes used in practice for example in e-archiving.

Naturally the following questions arise: What kind of cipher schemes do we use when quantum computers exist? What do we know about their security and their efficiency?

Here we have to design a postquantum cipher schemes based on continuous mathematics and to investigate their security and efficiency.

In cryptology the conventional way is using the discrete mathemathics to obtain the information security. It is obviously connected and limited via electronic technology.

Unconventional way in this direction is using ideas related to ill-posed problems in differential equations, which can describe an evolution.Such evolution eqs. very often describe the physical systems and it can give the way to the crypto-techniques, which are based on the purely analog methods.

Today these methods are available in optoelectronics and nonlinear optics [1, 2, 3].

The nice idea of cryptosystems based on an analog of heat flow was firstly presented by G.R.Blakley in the work [4].

There was demonstrated the feasibility of using cryptosystems on a circle of hard problems arising in the theory of PDE. There was shown why it is hard to avoid the use of nonlinear pseudoparabolic PDE and the possibility of nonlinear boundary conditions in formulating such a cryptosystem. The feature of this approach is its neutrality between continuous or discrete messages and using purely analog methods.

The aim of this paper is a discussion of cryptosystems based on nonlinear PDE from the point of view of inverse problems, which are crucial for cryptanalysis of these cryptosystems.

For example an inverse problem for the heat eq. was solved [5], and it can break cryptosystems, and it can break cryptosystems, based on an analog of heat eq. expeditiously.

We want to remaind the role of the Inverse Scattering Transform (IST) method for obtaining the solitonic solutions of certain nonlinear PDE and their application for cryptology.

We also mention the natural extension of cryptosystems based on nonlinear PDE to multidimensional or vector case.

An interesting role in such an application of the nonlinear Schrödinger eg. (NLS) is presented and connection with optoelectronics technology is shown.

2 A review of basic ideas on PDE and the role of nonlinearity

Following interesting work [4] we simply speak of encoding and decoding a message f, it is a function

$f : D \to C$,

whose domain D and codomain C have some useful structure, usually group-theoretic.

An encode,decode pair (c, d) is a pair of functions:
$c : C^D \to E, d : E \to C^D$,
where E is some appropriate set of encoded messages and $d(c(f)) = f$, or at least such that $d(c(f))$ is usually fairly near f. Consider for simplicity an encode map $C : R\langle 0, 1\rangle \to R\langle 0, 1\rangle$.

The encoding process stars via choosing the governing evolution equation, which can have for example the form of pseudoparabolic eq.:

$$(L - I)u_t + Lu = 0, \tag{1}$$

where $u(x, t)$ is a function whose domain is semiinfinitive strip $\langle 0, 1\rangle \times \langle 0, \infty\rangle$; I is the identity map, L is the linear operator

$$Lu = (K_1 u_x)_x - K_2 u \tag{2}$$

in which $K_1 = K_1(x), K_2 = K_2(x)$ play the role of key material and $K_1(x)$ is strictly positive for every $x \in \langle 0, 1\rangle$. The notation $u_t = \partial_t u, u_x = \partial_x u$ is used (see [4] for more details).

The plaintext message f is the initial condition of eg.(1)for $t = 0$ (the beginning of the evolution eq.)

$$f(x) = u(x, 0), x \in \langle 0, 1\rangle \tag{3}$$

and the encoded text g corresponding to the f is just the restriction of the solution u to the set $\{(x, t), t = 1\}$:

$$g(x) = u(x, 1), x \in \langle 0, 1\rangle. \tag{4}$$

The encoding process via eq.(1) has good cryptographical symptoms as intersymbol dependence, smearing and this process appears a one-way function especially, if the ordinary boundary condition

$$u(0, t) = u(1, t) = 0, t \geq 0 \tag{5}$$

is generalized to the nonlinear form.

Of course, if we want to make the process more cryptographically strong, we have to put the nonlinear term on the right side of the eq.(1). In such a way the encoding process cryptographically strong is realized via the nonlinear PDE. We have to take the governing eq. and the nonlinearities resistible to inverse methods and computerised inversion of data. It will be explain in the next section.

At first we repeat some basic facts.A designated decoder knowing the type of nonlinear PDE, the form of L, the boundary condition and the encoded message $g(x) = u(x, 1)$ can hope to recover a good approximation to plaintext message $f(x) = u(x, 0)$ by the following way:

Let us suppose a pseudoparabolic PDE

$$u_t + (L - I)^{-1} Lu = 0, \tag{6}$$

where the operator $(L-I)^{-1}L$ has an extension to a bounded operator on all of $Ł^2$ or of $C^{0+\alpha}$ on Sobolev space ${H_0}^1 \cap H^2$ or Schauder space ${C_0}^{2+\alpha}$ and the operator $(L-I)$ turns to be invertible if $K_2(x) \geq -1$.

Coupled with the boundary condition (5) and the initial condition (3) the eq.(6) has the solution

$$u(x,t) = exp[-t(L-I)^{-1}L]f(x) = exp[-tA]f(x), \tag{7}$$

where $\{exp[-tA]; t \in \Re\}$ is a group of operators generated by A.

The plaintext message

$$f(x) = u(x,0) = exp[0]f(x), \tag{8}$$

gives rise to the cryptext message

$$g(x) = u(x,1) = exp[-A]f(x), \tag{9}$$

and vice versa:

$$f(x) = exp[A]g(x), \tag{10}$$

Under the substitution

$$u(x,t) = exp[-t]v(x,t), \tag{11}$$

the eq. (6) becomes

$$v_t + (L-I)^{-1}v = 0, \tag{12}$$

Noting that $v(x,0) = f(x)$ and $g(x) = exp[-1]v(x,1)$ we can see from eq.(12):

$$v(x,t) = exp[-t(L-I)^{-1}]v(x,0), \tag{13}$$

and

$$g = exp[-(L-I)^{-1} - 1]f = exp[-1]exp[-(L-I)^{-1}]f, \tag{14}$$

and since $\Lambda = -(L-I)^{-1}$ is a bounded operator

$$g = exp[-1](\sum_{k=0}^{\infty} \frac{\Lambda^k}{k!})f. \tag{15}$$

The action

$$\Lambda f = -(L-I)^{-1}f = \int_0^1 G(x,s)f(s)ds, \tag{16}$$

where $G(x,s)$ is the Green function. So g can be computed by truncating the exponential series and the k-th term of this series consists of k consecutive integration of the function f(s) with G(x,s), depending on the key material. It is this integration process that provides the "smearing" of the function f(x).

The nonlinear case of eg.(1) has the form

$$(L-I)u_t + Lu = F(u), \tag{17}$$

with the boundary condition

$$u_x + K_3(t)u = K_4(t), \tag{18}$$

where K_3 and K_4 could form a part of key material and they could also be made nonlinear.

The eq.(17) has the form

$$u_t + Au = (L-I)^{-1}F(u) = \tilde{F}, \tag{19}$$

where $\tilde{F}$ depends on (x, t, u, u_x).

The eq.(17) has the solution

$$u_t = exp[-tA]f + \int_0^t exp[-(t-\tau)A]\tilde{F}(u(\tau))d\tau. \tag{20}$$

It represents a nonlinear integral eq. for $u(x,t)$ whose free term is $exp[-tA]f$ and whose kernel is $exp[-(t-\tau)A]\tilde{F}$. This can be solved by the method of succesive approximation under mild conditions on the function $\tilde{\mathrm{F}}$ (smoothness in x,t, Lipschitz continuity in the variable u,u_x):

$$u_0(t) = exp[-tA]f, \tag{21}$$

$$u_{n+1}(t) = u_0(t) + \int_0^t exp[-(t-\tau)A]\tilde{F}(u_n(\tau))d\tau, \tag{22}$$

for $n \geq 0$.

In practise a finite difference scheme [6] would be used and the nonlinear term would be evaluated by succesive approximation in a subloop. The possibility of recovering a function $\tilde{\mathrm{F}}$ from measurements of f, g pairs lies for most cases outside the scope of present research in the area of undetermined coefficients problems in PDE.

For some cases of nonlinear PDE there exists "complete integrability", which is normally associated with the identification of an infinite number of nontrivial conservation laws (integrals).

It would appear that such systems can be solved by the IST method, the scattering data of which may be shown to be related to the integrals [7,8].

The NLS eq. plays the crucial role for the application of nonlinear PDE in cryptology. The NLS eq. describes the evolution of the light wave in an optical fibre and can be written in the form [9]:

$$2iE_x - (\frac{d^2k}{d\omega^2})E_{tt} + \gamma E| \ E \ |^2 = 0, \tag{23}$$

where γ is a constant.

$E(x,t)$ represents the field envelope and the nonlinear term $F = \gamma E| E |^2$ arises from the field dependent refractive index $n = n_0 + n_2| E |^2$.

The important role plays the coefficient $(\frac{d^2k}{d\omega^2})$ if the optical wavelength $\lambda = \frac{2\pi}{k}$ of the carrier frequency is such that $(\frac{d^2k}{d\omega^2}) < 0$. In this case there appear the solitonic solutions [2] of NLS eq.(23). This will be discussed later and it is connected with IST.

For encoded and decoded messages eq.(23) can play the crucial role with an application of optical phase conjugation [1], where optical fibre can be used as an analog of operators c and d.

Now we shall concentrate on general inverse scattering problem, which can be useful for recovering the form of operator L.

3 An inverse problem as a tool for codebrakers

First we mention the role of IST for obtaining solutions of certain nonlinear PDE.

In 1811 the Fourier series was introduced to treat the diffusion eq. The IST method is an extension of the Fourier transform, when we regard the scattering data as the generalization of momentum space. It has been a unique method whereby the initial value problem of nonlinear evolution eqs. can be solved.

The IST method as expounded in the classic paper of Ablowitz et al [7], was seen essentially as an extension of the Fourier transform to certain nonlinear problems. As such it consists of the linear Zakharov-Shabat [9], which act as a direct transform to map the unknown solution of a nonlinear eq. on to a set of "scattering data", and the Marchenko eq., which acts as an inverse transform to reconstruct the solution from this data, using linear integral eq.

This IST method is useful for obtaining the solutions of certain nonlinear PDE as for example the NLS eq.

Here is also another inverse method namely the inverse scattering method. Namely this can be a useful tool for the selection of the cryptographically strong governing nonlinear PDE for cryptosystem.

As example we mention the heat eq. in the form [4]

$$u_t - u_{xx} - q = 0., \tag{24}$$

The codebrakers using inverse method cam determine as unknown source (key material) in the heat eq. (24) from the overspecified data for certain types of function q [5].

Theoretically one can successfully use a system of PDE to built corresponding cryptosystem , but he must be sure that inverse method for such eqs. cannot determine their form.

The name of the inverse scattering method (or problem) follows from Physics. Here in the usual scattering theory, the hamiltonian of the system (corresponding the evolution eq.) or the interparticle forces are known. Physical quantities the cross section, polarization etc. are to be calculated and subsequently confronted with experimental results. The "inverse" problem is posed in the opposite direction:

given certain kinds of information obtained more or less directly from scattering experiments, we are to determine the interparticle forces.

The same situation arises in crypto application, which we discuss.

For the codemaker the inverse method can be an antitool, which can be used for the selection from nonlinear PDE, which are not applicable in crypology.

Let codemakers assume a nonlinear PDE that contains certain parameters and a number of arbitrary function (for example the form of L, key material, the form of F from sect.2), which we shall refer as the "cryptoforces". Also included are boundary conditions of a given kind on arbitrary surfaces.

The solution of this systems gives rise to a set of functions that are more or less directly observable (encoded message). Let us collectively refer to these functions as the "encoded data".

Let the plaintext message f is evaluated under this "cryptoforces" to the codetext g. Thus the solution of the direct problem of solving PDE establishes a map $c : C^D \to E$, which consists of the cryptoforces, to the "data", which are the codetext E.

The inverse problem is to find the inverse c^{-1} of this map starting from the codetext. The first step in solving the inverse problem must be to answer the question whether the map c^{-1} is one-to-one. We will take it for granted that c is well-defined so that it assigns to each point C^D a unique way. If there is no uniqueness there can obviously be no inverse.

If the one-to-one of c is established, the inverse map c^{-1} exists.

The set E, i.e. the set of admissible data may be difficult to define in terms other than its definition. Often encoded messages look just like plaintext messages $E = C^D$.

The problem how to characterize admissible data intrinsically without the reference to the set C^D and the map c, is the so called characterization or existence problem. For cryptosystem application the existence problem does not arise because the aim is to reconstruct the cryptoforces and here the cryptodata are constructed solving the direct problem.

The next step in solving the inverse problem is the stability of the mapping. This is the question of its continuity in some suitable topology.

The continuity of the map c may be well established but that does not necessarily tell us if the c^{-1} is continuous and in what topology.

This question is particularly important in cryptosystems application because it is necessary here to retain codetext to sufficient accuracy so one can invert to recover plaintext.

For example let the two sets of g will differ by small unknown amounts. If the inversion is not continuous, this small difference in g may be correlated with a large difference in the f.

Once existence, uniqueness and stability have been established the problem is well posed in the sense Hadamard.

Generally the inverse problems are notoriously ill posed. Thus it may well happen that one or more Hadamard's criteria for well-posed problem will be found to be violated. It is instructive to see general discussion of inverse problems [10]. Of course the class of ill-posed problems is larger then the class of inverse problems.

For codebrakers the most important task is to find an actual reconstruction procedure for the map c^{-1} from measurements of plaintext/codetext pairs.

For codemakers it is important to choose the governing nonlinear PDE in such a way that the reconstruction procedure for the map c^{-1} is impossible. The complexity theory has little to say about the difficulty of such problems. It belongs to the realm of discrete mathematics and an application on the hard problems in continuous mathematics is not known.

The governing eq. could be for example the hyperbolic eq.

$$(\partial_{tt} - L)u = F(u) \tag{25}$$

defined at the domain $0 \leq x \leq 1, 0 \leq t \leq 1$ and then this procedure would share many of these ideas of cryptosystems from sect.2. Even if an eaversdropper could determine all eigenvalues of L for the linear system $F = 0$, this is generally insufficient to recover L, what is the statement of the classical inverse Sturm-Liuville problem.

When the energy in each eigenmode is added, then recovery methods are possible in one space dimension. In higher space dimensions the determination of L from such spectral data remains an enigma.

The instructive example could be also the ordinary Schrödinger equation from quantum mechanics

$$(i\partial_t - \partial_{xx} + F(x))u = F(u), \tag{26}$$

where $F(x)$ is a potential.

The solution of the inverse scattering problem for the eq.(26) (with a reflection coefficient given as a function of the wave number) is not unique if there are bound states (discrete eigenvalues). The same is true for three dimensions. In order to make it unique the data have to include the eigenvalues and one additional parameter for each [11].

Studying the inverse Schrödinger scattering in three dimensions it gives a view on methods, which can be generally used as the tools for codebrakers in other cases. The methods are based on a Marchenko-procedure, a Gelfand-Levitan procedure or a δ procedure (see for example [12]).

An important example of an inverse eigenvalue problem is provided by the mentioned Sturm-Liouville problem on the finite line. The problem is to construct the potential $q(x)$ in eq.

$$\partial_{xx}u(x) + (\lambda - q(x))u(x) = 0, \tag{27}$$

from eigenvalue data relating to the end conditions $u_x(0) = 0 = u(1)$.

The function q(x) may be constructed uniquely from the eigenvalues, ${\{\lambda_i\}_1}^{\infty}$, and the norming constant

$$\rho_i = \int_0^1 [u_i(x)]^2 dx, \tag{28}$$

of the eigenfunctions $u_i(x)$, chosen to satisfy $u_i(0) = 1$. The fundamental step in the solution of the inverse problem is, that before constructing q(x), we first construct the eigenfunctions, ${\{u_i(x)\}_1}^{\infty}$, and we do this by seeking $u_i(x)$ in the form

$$u_i(x) = \cos(\sqrt{\lambda_i}x) + \int_0^x H(x,s)\cos(\sqrt{\lambda_i}s)ds. \tag{29}$$

We are not concerned with the details of the procedure, but we point out some features:

1. The functions $\cos(\sqrt{\lambda_i}x)$ are the solutions of the eq. $\partial_{xx}u + \lambda_i u = 0, u_x(0) = 0$.

2. Expression (29) has a "triangular" form, i.e. $u_i(x)$ is made up form values of $\cos(\sqrt{\lambda_i}s)$ in the interval $0 \leq s \leq x$.

3. The functions $H(x,s)$ must be found so that the resulting $u_i(x)$ form a complete orthogonal set. This requires that $H(x,s)$ satisfy an integral eq.

$$P(x,y) + \int_0^x P(y,s)H(x,s)ds + H(x,y) = 0, 0 \leq y \leq x, \tag{30}$$

   where $P(x,y)$ can be constructed from the spectral data ${\{\lambda_i, \rho_i\}_1}^{\infty}$.

4. If only a finite set ${\{\lambda_i, \rho_i\}_1}^{m}$ is specified, then the data can be "completed" by using the spectral data ${\{\lambda_i, \rho_i\}_{m+1}}^{\infty}$ of the eq. $\partial_{xx}u + \lambda_i u = 0$.

McLaughlin [13] has shown that a Gelfand-Levitan-like procedure may be developed for the alternative form of the Sturm-Liouville problem.

On this simple example we demostrated the way how codebraker obtain the key material if the governing eq. for the cryptosystem has the form of eq.(26) plus the term of the time evolution.

Here the important role can play also the q-deformed inverse scattering problem [14]. There is shown how from the known spectral data $\{E_n\}$ via a general q-deformation we can obtain the unknown potential with the spectrum $\{{E_n}^*\}$, which is connected with $\{E_n\}$ via q-deformation.

Of course for higher dimensions and nonlinear PDE the solving of the inverse problem in most cases represents long standing hard problem in continuous mathematics.

Here we can see also the possibility to combine a few nonlinear PDE into a system, or use the vector extension of these eqs. or other discretization to mix such hard problems with complexity theory in discrete mathematics.

4 An application of the nonlinear Schrödinger equation in cryptology

As was mentioned the most interesting perspective of the application of nonlinear PDE in cryptology is a possibility of realization an optoelectronic purely analog crypto-device with optical fibres.

Of course such crypto device can be constructed also using a optical hologram as one time pad, what it is another interesting application of optolectronics for information security.

The advantage of such devices is that it would be possible make the crypto information at rates Gbit/s. Today the technology is giving the optical fibres with enough precision for using them for crypto application. Now exists interferometric quantum cryptography devices [15], what is a nice application of optoelectronics in quantum cryptography.

Here we are interesting about the application of optoelectronics in classical cryptography, namely we propose to use optical phase conjugation (multimode fibres) [1] or on solitons based communication system for crypto application.

We concern on a skeleton of mathematical description of such a theoretical optoelectronic crypto-device, combining optical phase conjugation via multimode fibres with solitons in optical fibres.

For solitons the optical fibre is one-dimensional world, where the developing of light pulses is given by NLS eg.(23). Solitons, what are the special solutions of some nonlinear PDE, can be described by the following way.

Let us use a normalized form of eq.(23) with $(\frac{d^2k}{d\omega^2}) = -1, \gamma = 2$ such that solitons are possible

$$iE_x - \frac{1}{2}E_{tt} + E|\ E\ |^2 = 0. \tag{31}$$

J.Satsuma and N.Yajima [16] have used IST on eq.(31), with the initial pulse profile

$$E(0,t) = \frac{N}{T}sech(\frac{t}{T}), \tag{32}$$

where T denotes pulse width and N is an integer. They showed that this initial data produces N zeros of the transmission coefficient in the complex plane each of which have zero real part. This is caused by the fact that the initial profile has zero phase. We shall call this "N-soliton" case even though the solitons are not comletely independent.For integer N, analytic solutions of the NLS exist and are presented in [17]. There a vector extension of NLS is used in the form

$$iu_{Nt} + u_{Nxx} + (\bar{u}_N u_N)u_N = 0, \tag{33}$$

where

$$u_N(x,t) = (u_{N,1}, u_{N,2}...u_{N,m})^{Tr.}, \tag{34}$$

$$\bar{u}_N u_N = \sum_{j=1}^{m} \mid u_{N,j} \mid^2, m \geq N. \tag{35}$$

N-soliton pulses for $N \geq 2$ are deeply modulated pulses which are periodic in x and therefore return to the same initial profile for distances

$$x_0 = \frac{nT^2\pi}{2}, \text{n integer.} \tag{36}$$

Note that x_0 scales with T^2, a broader pulse requires a longer distance to execute one period. Hence every fibre of a given length has a particular pulse which resonates exactly with it. L.Mollenauer and R.Stolen [18] have exploited this facts in building a soliton laser and we can it use for cryptosystem.

Let us suppose a two-dimensional plane with plaintext f divided on j subplanes. Each subplane will be transmitted by the optical system , which consists from single-mode fibres (I) , corresponding one-to-one map ${c_{\lambda j}}^{IN}$ from the j subplane with single mode λ_j on ${g_{\lambda j}}^{IN}$, where N denotes N solitonic pulses, which are determined by the length of the single mode fiber.

On each monovide fiber we can put the key material via optical sensors [19] for example from the quantum optical chaotic generator (which are usual for the optical experiments on the verification local realism in quantum physics) or another with the chaotic behavior [3].

In the optical system it will be transmitted due the multimode optical fibre (II), where the distortion arise (c^{II}), because a spatial image sent down optical fibre cable travels via many optical modes. Each mode correspondes to a given ray that zigzags down the fiber. Since all the mode traverse different paths, by the time they reach the end of the fiber they are out of step, producing unrecocgnizable image .

This multimode optical cable represents cryptoforces map where also key material (for example hologram) can be added. Such encoded image represents cipher image which can be transmitted via telecommunication media.

The decrypted image can be obtained if it is phase-conjugated in inverse order. It must be sent down through an identical optical system in inverse order so $d^{II} = (c^{II})^{-1}$, which produce ${g_{\lambda j}}^{IN}$ and ${d_{\lambda j}}^{IN} = ({c_{\lambda j}}^{IN})^{-1}$ such that

$$ {d_{\lambda j}}^{IN} d^{II}[c^{II}({c_{\lambda j}}^{IN} f)] = f. \tag{37} $$

The idea of such optoelectronical crypto-device is simple in principle although in practice, it is much harder to achieve this. From cryptanalytical point of view such system combine hard problems from the complexity theory with hard inverse problem and it can represents a superenigma also for the quantum computer in future.

5 Discussion

This paper presents to main goals:

1. presents the role of inverse problems and inverse methods in cryptological application of nonlinear PDE, which was established by G.R.Blakley [4]. On simple example of one dimensional heat eq. we show, how the key material can be obtained via inverse method. Of course using inverse methods we can analyze the effect of particular differences in f pairs on the differences of the g pairs. These differences can be used to assign probabilities to obtain the possible potentials (key materials) and to determine the most probable one. This idea was rediscovered in cryptology as differential cryptanalysis [20]. We mentioned also IST method which is connected with the solitonic solutions for some nonlinear PDE and NLS eq. in crypto application was discussed.

2. presents new application of NLS eq. for the crypto device with optical fibres whose cryptoanalysis presents superenigma also for quantum computers in future [21].

This work was covered by grant GA AV CR number T300100403 .

References

[1] D.M.Pepper, Aplication of optical phase conjugation, Scientific American, 254, n.1 (1986) 74.

[2] E.M.Dianov, Optical Solitons in Fibres, Europhys. news 2 (1992)23.

[3] J. Lesurf, A spy's guide to chaos, New Scientist 1, February (1992) 29.

[4] G.R.Blakley, W.Rundell, Cryptosystems based on an analog of heat flow, CRYPTO 87, Lecture Notes in Comp.Sci.293, Springer-Verlag (1987)306.

[5] J.R.Cannon and S.P.Esteva, An inverse problem for the heat equation, Inverse Problem 2, n.4 (1986)395.

[6] D.M.Young and R.T.Gregory, A Survey of Numerical Mathematics, Vol.2, Addison-Wesley,Reading.Massachusetts (1973) pp.1078,1086-88.

[7] M.J.Ablowitz, A.Ramani and H.Segur, J.Math.Phys. 21, (1978) 715.

[8] V.E.Zacharov, A.B.Shabat, Sov.Phys.JETP,v.34,62 (1972).

[9] A.Hasegawa and F.Tappert, Appl.Phys.Lett 23 (1973) 142.

[10] P.C.Sabatier, Well-possed questions and exploration of the space of parameters in linear and nonlinear inversion, in Inverse Problems of Acustic and Elastic Waves, F.Santona et al., editors,SIAM,Philadelphia (1984) 82;

P.C.Sabatier, A few geometrical features of inverse and ill-posed problems, H.W. Engl and C.W.Groetsch, editors, Academic Press, New York (1987).

[11] K.Chadan and P.C.Sabatier, Inverse Problems in Quantum Scattering Theory, Springer-Verlag,New York (1977).

[12] Roger G.Newton, Scattering Theory of waves and Particles, second edition,Springer-Verlag,New York (1982);

R.Beals and R.R.Coifman,Linear spectral problems, nonlinear equations and the method,Inverse Problems, v.5, n.2 (1989)87.

[13] J.R.Mc Laughlin, An inverse problem of orders four,SIAM J.Math.Anal.7(1976)646;

J.R.Mc Laughlin, Bounds for constructed solutions of second and fourth order inverse eigenvalue problems,Diff.Eqs.ed I.W. Knowles and T.R.Lewis,Amsterdam: Elsevier , North Holland (1984)437.

[14] J.Hruby,Q-deformed inverse scattering problem,Suppl.ai Ren.del Circ.Matem.di Palermo,Ser.II.n.37(1994)103.

[15] R.J.Hughes et al.,Contemporary Physics,v.36, n.3 (1995)149;

J.Hruby, Lecture Notes in Computer Science 1029,(1995)282.

[16] J.Satsuma and N.Yajima,Progr.Teor.Phys.Suppl.55(1934)284.

[17] J.Hruby, J.Phys A:Math.Gen.22 (1989)1807.

[18] L.Mollenauer and R.Stolen, Optics. Lett (1984)13.

[19] S.Donati,V.Annovazi-Lodi,T.Tambosso,Magneto-optical fibre sensors for electrical industry: analysis of performance, IEEE Proceedings,v.135,Pt.J,n.5 (1988) 372.

[20] E.Biham and A.Shamir,Differential Cryptanalysis of DES-like Cryptosystems,J.Cryptology 4 (1991)3.

[21] J.Gruska, Quantum computing, McGraw-Hill(1999).