Construction of a New Cryptographic Method, Employing Pseudoanalytic Function Theory

A. Bucio R. *IAENG, Member*, A. Hernandez-Becerril *IAENG, Member*,
C. M. A. Robles G. *IAENG, Member*, M. P. Ramirez T. *IAENG, Member*, A. Arista-Jalife.*

***Abstract*—Employing the Pseudoanalytic Function Theory, and based upon the inverse Dirichlet boundary value problem for the two-dimensional Electrical Impedance Equation, an open problem also known as Electrical Impedance Tomography, we propose a new cryptographic method whose main characteristics are the Confidentiality and the Data Integrity.**

***Index Terms*—Cryptography, Electrical Impedance Tomography, Pseudoanalytic Functions, Vekua Equation.**

I. Introduction

THE study of techniques for secure communication is the main goal of Cryptography [6]. That is why this discipline is strongly related with other branches of Science, as Applied Mathematics and Computation. There are many other disciplines on which the Cryptography can be based on. Yet, the paragraphs shown further will show that, in this particular proposal, both Mathematics and Computes Sciences will provide enough material to ensure the successful performance of the novel method. Therefor, the Figure 1 shall be adequate to appoint the basic execution of a ciphering method.

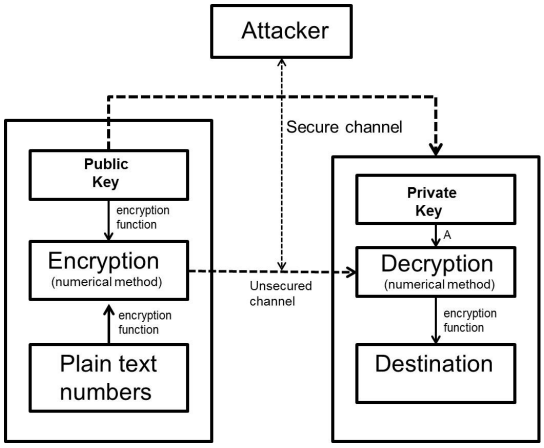

Fig. 1: A general description of a cryptographic method.

This work pays particular attention to the Pseudoanalytic Function Theory [3], that has recently proved to be an important tool in Theoretical Physics, and Applied Mathematics (see *e.g.* [4], [11], and [15]). More precisely, since the pseudoanalytic functions have been employed for analyzing the Electrical Impedance Tomography [18] (a mathematical problem that remains open), it is possible to propose a new cryptographic method that will positively posses characteristics as Confidentiality and Data Integrity.

From the scope of these pages, a cryptographic algorithm will be considered a mathematical method whose main purpose is to convert information into encrypted data, such that the decryption is available only for those that posses the key. For that, the cryptographic algorithm will arise employing numerical techniques that allowed the approaching of the so-called Taylor Series in Formal Powers.

Starting with a brief study of the Pseudoanalytic Function Theory, and its relation with the two-dimensional Electrical Impedance Equation, we expose the details of the methodology for constructing a cryptographic method.

Based upon the material previously posed in a variety of works, fully dedicated to the forward Dirichlet boundary value problem for the Electrical Impedance Equation, we explain that this method is effective for ciphering numerical data whose values are significantly bigger than 10^{-12}. Thus, the variety of data classes on which this method could be useful, can be considered wide enough for engineering applications.

II. The Cryptographic Proposal.

The idea of proposing a new cryptographic algorithm arises from the study of the Electrical Impedance Tomography problem, employing modern elements of the Pseudoanalytic Functions [11]. Nevertheless, we shall appoint that these numerical techniques do not provide yet an adequate solution for the problem.

As a matter of fact, most works (see *e.g.* [4] and [13]) mainly analyze the forward Dirichlet boundary value problem for the Electrical Impedance Equation (the Electrical Impedance Tomography constitutes the inverse problem, correctly posed in mathematical form by A.P. Calderon in [5]). Thus, even the new techniques do provide additional information for better understanding the field, it is impossible to assert that the Electrical Impedance Tomography problem could be solved for arbitrary cases.

Taking into account the last statement, we shall propose the employment of the Pseudoanalytic Function Theory for constructing a cryptographic method, because any attempt to unlock the encrypted information would be equivalent to fully solve an arbitrary case of the Electrical Impedance Tomography problem.

A. Bucio R. is with the National Polytechnique Institute, UPIITA, Mexico, ari.bucio@gmail.com
C. M. A. Robles G. and A. Hernandez-Becerril are with the National Polytechnique Institute, ESIME C. Mexico, cesar.robles@lasallistas.org.mx
M. P. Ramirez T. and A. Arista-Jalife are with the Communications and Digital Signal Processing Group, Engineering Faculty of La Salle University, Mexico, marco.ramirez@lasallistas.org.mx.
*Each author equally contributed to the research work.

ISBN: 978-988-19252-3-7
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

III. Elements of Pseudoanalytic Function Theory and their relation with the Electrical Impedance Equation.

Let us consider the two-dimensional case of the Electrical Impedance Equation:

$$\nabla \cdot (\sigma \nabla u) = 0, \tag{1}$$

where u is the electric potential and σ is a separable-variables non-vanishing function within a bounded domain Ω, with boundary Γ, such that:

$$\sigma = \sigma_1(x)\sigma_2(y). \tag{2}$$

By introducing the notations:

$$W = \sqrt{\sigma}\partial_x u - i\sqrt{\sigma}\partial_y u, \quad p = \sqrt{\frac{\sigma_2(y)}{\sigma_1(x)}}, \tag{3}$$

where $i^2 = -1$, $\partial_x = \frac{\partial}{\partial x}$ and $\partial_y = \frac{\partial}{\partial y}$; the equation (1) can be rewritten into a Vekua equation [17] of the form:

$$\partial_{\overline{z}} W - \frac{\partial_{\overline{z}} p}{p}\overline{W} = 0, \tag{4}$$

where $\partial_{\overline{z}} = \partial_x + i\partial_y$, and $\overline{W}$ represents the complex conjugation of W: $\overline{W} = \mathrm{Re}W - i\,\mathrm{Im}W$.

The general solution of this equation can be expressed by means of the Taylor series in formal powers [3]:

$$W = \sum_{n=0}^{\infty} Z^{(n)}(a_n, z_0; z). \tag{5}$$

This is, indeed, a generalization of the classical postulates of Complex Analysis, that was mainly developed by L. Bers [3]. The following paragraphs contain a condensed description of the material that will be needed for our further discussions. The reader can find a complete and detailed explanation of these postulates in [3] and [11].

A. Formal Powers.

The formal power $Z_0^{(0)}(a_0, z_0; z)$ with complex constant coefficient a_0, center at z_0, depending upon z, formal exponent 0, and corresponding to the generating pair (F_0, G_0); is expressed as:

$$Z_0^{(0)}(a_0, z_0; z) = \lambda_0 F_0 + \mu_0 G_0;$$

where λ_0 and μ_0 are real constants such that

$$\lambda_0 F_0(z_0) + \mu_0 G_0(z_0) = a_0;$$

and

$$F_0 = p, \quad G_0 = \frac{i}{p}.$$

where p possesses the form (3).

The formal powers with higher formal exponents n, are defined by the recursive integral expressions:

$$Z_{j_0}^{(n)}(a_n, z_0; z) = n\int_{z_0}^{z} Z_{j_1}^{(n-1)}(a_0, z_0; z) d_{(F_{j_0}, G_{j_0})} z. \tag{6}$$

where $j_0 = 0, 1$ and $j_1 = 1, 0$. This is, if $j_0 = 0$ then $j_1 = 1$, and if $j_0 = 1$ then $j_1 = 0$. The integral expressions in the right-hand side of (6) are what can be considered antiderivartives in the sense of Bers [3]:

$$\int_{z_0}^{z} Z_{j_1}^{(n-1)}(a_0, z_0; z) d_{(F_{j_0}, G_{j_0})} z =$$

$$= G_{j_0}\mathrm{Re}\int_{\Lambda} F_{j_0}^{*} Z_{j_1}^{(n-1)}(a_0, z_0; z)dz +$$

$$+ F_{j_0}\mathrm{Re}\int_{\Lambda} G_{j_0}^{*} Z_{j_1}^{(n-1)}(a_0, z_0; z)dz.$$

Here, Λ is a rectifiable curve going from z_0 upto z, and:

$$F_1 = \sqrt{\sigma}, \quad G_1 = \frac{i}{\sqrt{\sigma}}.$$

whereas

$$F_{j_0}^{*} = -iF_{j_0}, \quad G_{j_0}^{*} = -iG_{j_0},$$

as well

$$F_{j_1}^{*} = -iF_{j_1}, \quad G_{j_1}^{*} = -iG_{j_1}.$$

Once more, the detailed description of the construction and characteristics of the formal powers can be found in [3] and [11]. Here we will only enhance two fundamental properties for our discussions.

1)
$$\lim_{z \to z_0} Z^{(n)}(a_n, z_0; z) = a_n(z - z_0)^n. \tag{7}$$

2) Let $a_n = a_n' + ia_n''$, where a_n' and a_n'' are both real constants. Thus

$$Z^{(n)}(a_n, z_0; z) =$$
$$= a_n' Z^{(n)}(1, z_0; z) + a_n'' Z^{(n)}(i, z_0; z). \tag{8}$$

The absence of the subindex j_0 and j_1 indicates that the properties are valid for all formal powers.

Notice the last statement establishes that any formal power $Z^{(n)}(a_n, z_0; z)$ can be approached by the linear combination of $Z^{(n)}(1, z_0; z)$ and $Z^{(n)}(i, z_0; z)$, thus the numerical calculations shall be exclusively performed to approach these two classes of formal powers.

Moreover, in [8] was provided the proof about the completeness of the set:

$$\left\{\mathrm{Re}\, Z^{(n)}(1, z_0; z)|_{\Gamma}, \mathrm{Re}\, Z^{(n)}(i, z_0; z)|_{\Gamma}\right\}_{n=0}^{\infty}, \tag{9}$$

for approaching solutions of the forward Dirichlet boundary value problem corresponding to the equation (1).

This is, given a non-vanishing function σ within a bounded domain Ω, with boundary Γ, any boundary condition $u|_{\Gamma}$ can be approached by the linear combination of the elements belonging to (9), that are the real parts of the formal powers with coefficients 1 and i, valued at the points belonging to the boundary Γ:

$$u|_{\Gamma} = \sum_{n=0}^{\infty} c_n^{(1)}\mathrm{Re}\, Z^{(n)}(1, z_0; z)|_{\Gamma} +$$
$$+ \sum_{n=0}^{\infty} c_n^{(i)}\mathrm{Re}\, Z^{(n)}(i, z_0; z)|_{\Gamma}, \tag{10}$$

where $c_n^{(1)}$ and $c_n^{(i)}$ are all real constant coefficients.

A final statement is in place before studying the numerical method for approaching the elements of (9).

It is a conjecture posed first in [15], and employed to analyze a wider class of conductivity functions and domains in [14]. It establishes that any function σ, fully defined within a domain Ω, can be considered at every single point, a special separable-variables function for which $j_0 = j_1$, thus it can be employed for numerically approaching the elements of (9).

ISBN: 978-988-19252-3-7
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

B. Numerical approaching of the formal powers.

This Section is dedicated to briefly explain the numerical method for approaching integral expressions corresponding to (6). We will only expose the procedure for calculating the formal powers with coefficient 1, since there are not relevant logical variations when taking into account the coefficient i.

Since the integral expressions of (6) are path-independent, as proved in [3], let us consider a collection of $\mathbf{Q} = Q + 1$ points:

$$\{x[q], y[q]\}_{q=0}^{Q};$$

located in the closed interval $[0, 1]$; corresponding to a parametric radius of magnitude $\mathbf{R}$, traced into a circle with center at $z_0 = 0$, and with some angle θ, such that:

$$x[q] = r[q]\cos\theta,\ y[q] = r[q]\sin\theta, \tag{11}$$

where $r[q]$ are points located upon the radius $\mathbf{R}$, traced equidistantly among each other.

Then, the elements of the array $Z^{(0)}[q]$, corresponding to the numerical approach of the formal power $Z^{(0)}(1, 0; z)$, will be defined as follows:

$$Z^{(0)}[q] = \sqrt{\sigma(x[q], y[q])}. \tag{12}$$

Notice that according to (7), for $k = 0$ and every $n > 0$, we will have that:

$$Z^{(n)}[0] = 0.$$

The subsequent elements q of the arrays $Z^{(n)}[q]$ will be approached according to the following variation of the classical trapezoidal integration method:

$$Z^{(n)}[q] = F[q]\cdot$$
$$\cdot\mathrm{Re}\sum_{h=0}^{q}\left(G^{*}[h]Z^{(n-1)}[h] + G^{*}[h+1]Z^{(n-1)}[h+1]\right)\cdot$$
$$\cdot\left(x[h+1] - x[h] + i\left(y[h+1] - y[h]\right)\right) +$$
$$+G[q]\cdot$$
$$\cdot\mathrm{Re}\sum_{h=0}^{q}\left(F^{*}[h]Z^{(n-1)}[h] + F^{*}[h+1]Z^{(n-1)}[h+1]\right)\cdot$$
$$\cdot\left(x[h+1] - x[h] + i\left(y[h+1] - y[h]\right)\right). \tag{13}$$

On behalf of briefness, we will denote these calculations in operational form:

$$Z^{(n)}[q] = \mathcal{B}\left[Z^{(n-1)}[q]\right]. \tag{14}$$

where $n = 1, 2, ..., N$.

This process will be performed for every angle θ on which the close interval $[0, 2\pi)$ is subdivided. Particularly, we will consider an array of $\mathbf{S}$ angles, such that:

$$\left\{\theta[s] = \frac{2\pi s}{\mathbf{S}}\right\}_{s=0}^{\mathbf{S}}. \tag{15}$$

In other terms, we will consider $\mathbf{S}$ angle intervals, over which N formal powers will be numerically approached, considering $\mathbf{Q}$ equidistant points on every radius.

After obtaining N formal powers for the coefficient 1, and N formal powers for the coefficient i, each one composed by $\mathbf{S}$ arrays of $\mathbf{Q}$ elements, we shall collect the real values of $Z^{(n)}[\mathbf{Q}; s]$, $s = 0, 1, 2, ..., \mathbf{S}$; as posed in the equation (9).

Thus, we will obtain a linear independent system of $\mathbf{N} = 2N + 1$ vectors, each one with $\mathbf{S}$ elements.

Moreover, we can apply a standard Gram-Schmidt orthonormalization process to the set:

$$\left\{Z^{(n)}[\mathbf{K}; s]\right\}_{n=0,s=0}^{\mathbf{N},\mathbf{S}},$$

from which it will upraise a matrix:

$$\mathbf{U}_{[\mathbf{N},\mathbf{S}]}; \tag{16}$$

whose lines will constitute a set orthonormal vectors. This is:

$$\langle U^{n_1}, U^{n_2}\rangle = \sum_{s=0}^{\mathbf{S}} U^{n_1}[s]U^{n_2}[s] = \begin{cases} 0;\ n_1 \neq n_2, \\ 1;\ n_1 = n_2; \end{cases}$$

where U^n represents a vector of $\mathbf{S}$ elements, containing all numbers of the n-line corresponding to the matrix $\mathbf{U}_{[\mathbf{N},\mathbf{S}]}$; whereas $U^n[s]$, $s = 0, 1, 2, ..., \mathbf{S}$; represent each element of the vector U^n.

IV. Construction of the cryptographic algorithm.

We propose a *Private Key Algorithm*, because the encryption key is not publicly known. In other words, not any person can employ the encryption key to cipher a message, and only who has the corresponding decryption key will be able to decipher the information. In these kind of algorithms, the cipher key and the decryption key compose the *Private Key*.

Thus, let us consider a random matrix $\mathbf{A}_{[\mathbf{Q},\mathbf{S}]}$, whose elements will be suppose to be the collected values of the function σ, introduced in (2), such that every line $q = 0, 1, 2, ..., Q$; contains the conductivity values corresponding to every radius $s = 0, 1, 2, ..., \mathbf{S}$ (notice every value must be positive and bigger than zero). We shall denote the total number of lines as $\mathbf{Q} = Q + 1$.

Thus, by applying the full procedure described in the Section III, we can obtain the matrix $\mathbf{U}_{[\mathbf{N},\mathbf{S}]}$ posed in (16).

Suppose there is as set of $\mathbf{M} \times \mathbf{N}$ values to be encrypted, where $\mathbf{M} = M + 1$. They can be always organized into a matrix $\mathbf{B}_{[\mathbf{M},\mathbf{N}]}$, thus every element $b_{m,n} \in \mathbf{B}_{[\mathbf{M},\mathbf{N}]}$ will represent a number to encrypt. Here $n = 0, 1, 2, ..., \mathbf{N} - 1$; and $m = 0, 1, 2, ..., M$.

The encryption idea arises as follows. Let us consider the vector C^m, composed by $\mathbf{S}$ elements, upcoming from the linear combination:

$$C^m = \sum_{n=0}^{\mathbf{N}} b_{m,n}U^n. \tag{17}$$

If this operation is performed considering $m = 0, 1, 2, ..., M$; we will obtain a set of $\mathbf{M}$ vectors with form (17), each one containing $\mathbf{S}$ elements.

Thus we can introduce a matrix:

$$\mathbf{C}_{[\mathbf{M},\mathbf{S}]} = \left[C^0; C^1; C^2; \ldots; C^M\right], \tag{18}$$

that, as a matter of fact, is the encryption of the data contained into the matrix $\mathbf{B}_{[\mathbf{M},\mathbf{N}]}$.

From this point of view, the decryption process is simple. Since all lines of the matrix $\mathbf{U}_{[\mathbf{N},\mathbf{S}]}$, introduced in (16),

ISBN: 978-988-19252-3-7
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

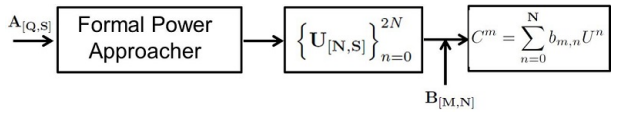

Fig. 2: Simplified illustration of the encryption process, employing the algorithm based on pseudanalytic approach.

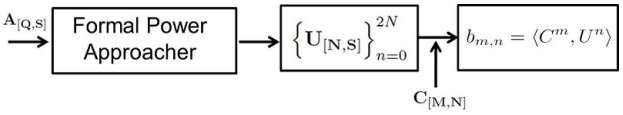

Fig. 3: Brief illustration of the decryption process.

are orthonormal vectors, the encrypted data $b_{m,n}$ can be recovered by simply considering the inner products:

$$b_{m,n} = \langle C^m, U^n \rangle = \sum_{s=0}^{\mathbf{S}} C^m[s]U^n[s]; \qquad (19)$$

where $C^m[s]$, $s = 0, 1, 2, ..., \mathbf{S}$; represent each element of the vector C^m.

On the light of the previous paragraphs, we can propose the elements of the *Private* and the *Public Keys*.

Private Key

- A random matrix $\mathbf{A}_{[\mathbf{Q},\mathbf{S}]}$.
- A maximum number N of formal powers.
- A set of $\mathbf{M} \times \mathbf{N}$ values to be encrypted; all contained into a matrix $\mathbf{B}_{[\mathbf{M},\mathbf{N}]}$.

Public Key

- A matrix $\mathbf{C}_{[\mathbf{M},\mathbf{S}]}$.

A. Encryption Process.

We shall now summarize the encryption and decryption processes. First, in order to perform the encryption process, we follow the next steps:

1) Construct the random matrix $\mathbf{A}_{[\mathbf{Q},\mathbf{S}]}$, that will be part of the *Private Key*.
2) Employing the $\mathbf{A}_{[\mathbf{Q},\mathbf{S}]}$ matrix, and using the number N (the second part of the *Private Key*), approach $\mathbf{N}$ formal powers, employing the procedure described in the Section III, taking also into consideration the postulates of the Section IV.
3) Applying a Gram-Schmidt process, obtain an orthonormal system $\mathbf{U}_{[\mathbf{N},\mathbf{S}]}$, as posed in (16).
4) Introduce a matrix $\mathbf{B}_{[\mathbf{M},\mathbf{N}]}$, containing the data $b_{m,n}$ to be encrypted.
5) Construct a matrix $\mathbf{C}_{[\mathbf{M},\mathbf{N}]}$, containing the encrypted data, according to ideas exposed in the Section IV. This matrix will be the *Public Key*.

B. Decryption Process.

1) Employing the matrix $\mathbf{A}_{[\mathbf{Q},\mathbf{S}]}$, employed in the Encryption Process, construct $\mathbf{N}$ formal powers.
2) Approach the orthonormal system $\mathbf{U}_{[\mathbf{N},\mathbf{S}]}$.
3) Finally, for recovering the encrypted data, calculate the inner products between the vectors C^m belonging to $\mathbf{C}_{[\mathbf{M},\mathbf{N}]}$ in (18), and U^n belonging to $\mathbf{U}_{[\mathbf{N},\mathbf{S}]}$ in (16):

$$b_{m,n} = \langle C^m, U^n \rangle .$$

A brief illustration of the encrypting process is plotted in Figure 2, whereas the Figure 3 illustrates the decoding procedure.

On behalf of clarity, it is also useful to expose the full procedure in the Algorithm 1. We shall remark that the numerical values appearing on it, are purely illustrative.

Algorithm 1 Cryptographic Algorithm

function FORMAL POWER APPROACHER
$\mathbf{S} \leftarrow 501$; (Maximum number of radii)
$\mathbf{Q} \leftarrow 101$; (Maximum number of points per radius)
$N \leftarrow 250$; (Maximum number of Formal Powers)
while $n = 0 \rightarrow N$ **do**
  while $s = 0 \rightarrow \mathbf{S}$ **do**
    while $q = 0 \rightarrow Q$ **do**
      $Z^{(n)}[q] = \mathcal{B}\left[Z^{(n-1)}[q]\right]$; (see equation (14))
    end while
  end while
end while
function ORTHONORMALIZATION
  (Gram-Schmidt process reaching $\mathbf{U}_{[\mathbf{N},\mathbf{S}]}$)
end function *ORTHONORMALIZATION*
end function *FORMAL POWER APPROACHER*
function ENCRYPTION PROCESS
$M \leftarrow 501$;
while $m = 0 \rightarrow M$ **do**
  $C^m = \sum_{n=0}^{2N} b_{m,n}U^n$;
end while
end function *ENCRYPTION PROCESS*
function DECRYPTION PROCESS
while $m = 0 \rightarrow M$ **do**
  while $n = 0 \rightarrow 2N$ **do**
    $b_{m,n} = \langle C^m, U^n \rangle$;
  end while
end while
end function *DECRYPTION PROCESS*

V. Conclusions: Advantages of the proposed method.

In general, it is required that the cryptographic algorithms preserve the security of the encrypted information from several points of view. Among those, we shall remark the Confidentiality and the Data Integrity. Taking this into account, we will describe the performance of this ciphering method.

About Confidentiality, we might appoint that to decipher the encrypted data $b_{m,n}$, employing any different method to the posed in (19), would be totally equivalent to solve the *Electrical Impedance Tomography* problem, posed in [5].

It is true that most of the material analyzed in the Section III is part of a new theory dedicated to study, and eventually to solve this problem. Nevertheless this achievement is far to be complete, when considering arbitrary cases. Moreover, the existing computational tools (see *e.g.* [10] and [18]) provide very low image resolution, when this technique is applied for medical purposes.

Then, if the decryption process of the matrix $\mathbf{C}_{[\mathbf{M},\mathbf{N}]}$ was attempted through novel or current algorithms for solving the Electrical Impedance Tomography problem, the random matrix $\mathbf{A}_{[\mathbf{Q},\mathbf{S}]}$ would play the role of the conductivity σ, and since it is randomly introduced, its complexity would

ISBN: 978-988-19252-3-7
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

be so high, that the probability of recovering the encrypted values from one single line C^m of the matrix $\mathbf{C}_{[\mathbf{M},\mathbf{N}]}$, would numerically vanish.

Beside, the procedure for solving the Electrical Impedance Tomography problem would have to be performed for each vector C^m, thus the necessary computational resources would provoke any attempt to become profitless.

The reader can verify the veracity of this statements, examining the modern literature dedicated to the Electrical Impedance Tomography problem, contained in *e.g.* [9] and [16].

Related to the Data Integrity, it is convenient to remark that the numerical tools employed for the construction of the new cryptography method, are a variation of the methods employed in [13] and [14], which have proved to be efficient for solving the forward Dirichlet boundary value problem of (1). Yet, for ciphering purposes, additional considerations may be taken into account when performing the numerical calculations.

Specifically, since the orthonormal vectors U^n, belonging to the matrix $\mathbf{U}_{[\mathbf{N},\mathbf{S}]}$, are expected to be high-dimensional, in order to warrant the Confidentiality, a standard Gram-Schmidt orthonormalization method could not be enough to ensure the Data Integrity.

For instance, if performing the full procedure described in the Algorithm 1, considering a random matrix $\mathbf{A}_{[\mathbf{Q},\mathbf{S}]}$ whose values are located in the closed interval $[1, 100]$, with $\mathbf{Q} = 101$ and $\mathbf{S} = 501$, and approaching $\mathbf{N} = 501$ base functions, when examining the set of inner products:

$$\left\{\left\langle U^{\mathbf{N}}, U^0\right\rangle, \left\langle U^{\mathbf{N}}, U^1\right\rangle, \left\langle U^{\mathbf{N}}, U^2\right\rangle, ..., \left\langle U^{\mathbf{N}}, U^{\mathbf{N}}\right\rangle\right\}; \quad (20)$$

we will find that:

$$\left\langle U^{\mathbf{N}}, U^0\right\rangle \sim 6.878 \times 10^{-15}.$$

Nevertheless for $n > 90$, we obtain

$$\left\langle U^{\mathbf{N}}, U^n\right\rangle \sim 1;$$

which is unacceptable to warrant the Data Integrity. An illustration of the random matrix $\mathbf{A}_{[\mathbf{Q},\mathbf{S}]}$ is provided in the Figure 4.

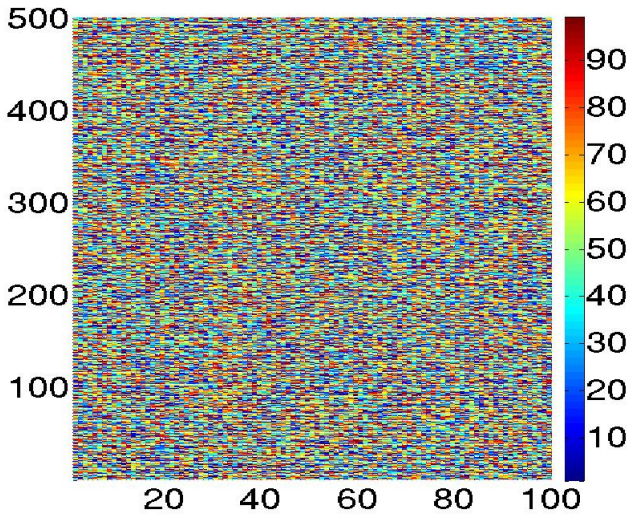

Fig. 4: Example of a random matrix $\mathbf{A}_{[\mathbf{Q},\mathbf{S}]}$.

Still, this numerical inconvenience, emerging when employing basic Gram-Schmidt orthonormalization processes, can be easily overpass by using a variety of well known improved techniques (see *e.g.* [2]), whose computational requirements do not significantly increase the total cost of applying the ciphering method.

On the other hand, if the values $a_{q,s}$ of the matrix $\mathbf{A}_{[\mathbf{Q},\mathbf{S}]}$ are produced according to the exact expressions:

$$a_{q,s} = \left(\frac{q}{\mathbf{Q}}\cos\frac{2\pi}{\mathbf{S}}s + 0.5\right)^{-1}\left(\frac{q}{\mathbf{Q}}\sin\frac{2\pi}{\mathbf{S}}s + 0.5\right)^{-1}, \quad (21)$$

we will find that the elements of the set (20) are all smaller than 1×10^{-16}, when employing the same Gram-Schmidt method of the previous example. It is clear that the values produced with the formulas shown above are not random. Nonetheless the reader can verify in, *e.g.* [9], that even for this exact case, the Electrical Impedance Tomography problem has not been adequately solved, thus the Confidentiality and the Data Integrity are assured. The Figure 5 plots an example of $\mathbf{A}_{[\mathbf{Q},\mathbf{S}]}$ generated by the formula (21).

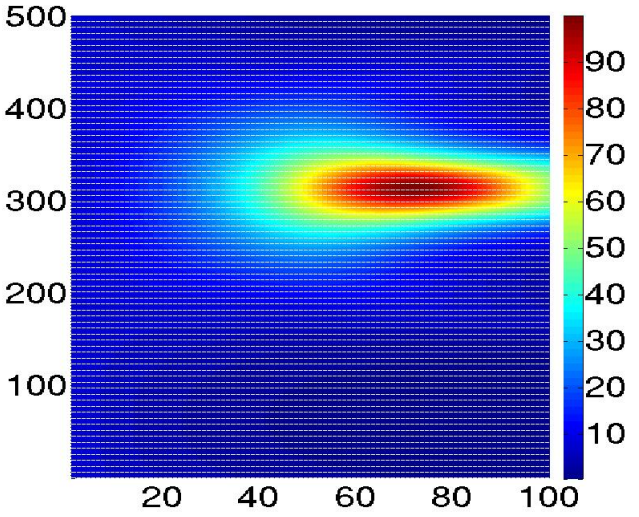

Fig. 5: Example of a matrix $\mathbf{A}_{[\mathbf{Q},\mathbf{S}]}$ constructed according to the expression 21.

As a final remark, related to the time-viability of the method, taking into account the explanations posed in the Section III-B, it is possible to verify that the calculation of the formal powers can be performed employing parallel computing tools. This would immediately allow a reduction of the computational time required for the construction the matrix $\mathbf{U}_{[\mathbf{N},\mathbf{S}]}$.

Moreover, the matrix $\mathbf{U}_{[\mathbf{N},\mathbf{S}]}$ not necessarily shall be approached every time we desire to encrypt different data sets, contained into the matrix $\mathbf{B}_{[\mathbf{M},\mathbf{N}]}$.

Since $\mathbf{U}_{[\mathbf{N},\mathbf{S}]}$ is part of the *Private Key*, as explained in the Section IV, and given the Confidentiality provided by the method, subsequent encryption processes could well employ the same matrix $\mathbf{U}_{[\mathbf{N},\mathbf{S}]}$, without compromising the security of the ciphering algorithm. In this sense, the computational cost would be reduced considerably.

It is clear that many other parameters could be introduced for increasing the confidentiality of the method. Nonetheless, the information provided in the paragraphs above might be

ISBN: 978-988-19252-3-7
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

enough to clearly illustrate the effectiveness of the new encryption method.

Disclosure: As it was appointed in [14] and [15], the numerical methods used for approaching the formal powers in Section III-B, were fully developed in GNU C/C++ Compiler, employing a CPU64B@2.4GHz, on SLACKWARE 13.37 LINUX operating system. The experimental procedures showed that the numerical results can vary when using different platforms, based on 32 B and 64 B processor architecture, or compilers between other operating systems, including different LINUX distributions or Registered Trade Mark operating systems. If the reader wishes to perform his own numerical trials, please contact the authors to obtain the resource codes.

Acknowledgements: The authors would like to acknowledge the support of CONACYT projects 81599, and 106722; A. Bucio R., A. Hernandez-Becerril, C. M. A. Robles G. would like to thank the support of CONACYT; M. P. Ramirez T. thanks the support of HILMA S.A. de C.V., Mexico.

REFERENCES

[1] K. Astala, L. Päivärinta (2006), *Calderon's inverse conductivity problem in the plane*, Annals of Mathematics, Vol. 163, pp. 265-299.
[2] J. L. Barlow, A. Smoktunowicz, H. Erbay (2005), *Improved Gram-Schmidt Type Downdating Methods*, BIT Numerical Mathematics, Volume 45, Issue 2, pp 259-285.
[3] L. Bers (1953), *Theory of Pseudoanalytic Functions*, IMM, New York University.
[4] A. Bucio R., R. Castillo-Perez, M.P. Ramirez T. (2011), *On the Numerical Construction of Formal Powers and their Application to the Electrical Impedance Equation*, 8th International Conference on Electrical Engineering, Computing Science and Automatic Control, IEEE Catalog Number: CFP11827-ART, ISBN:978-1-4577-1013-1, pp. 769-774.
[5] A. P. Calderon (1980), *On an inverse boundary value problem*, Seminar on Numerical Analysis and its Applications to Continuum Physics, Soc. Brasil. Mat., pp 65-73.
[6] Z. Cao (2012), *New Directions of Modern Cryptography*, CRC Press, Shanghai Jiao Tong University, China.
[7] H. M. Campos, R. Castillo-Perez, V. V. Kravchenko (2011), *Construction and application of Bergman-type reproducing kernels for boundary and eigenvalue problems in the plane*, Complex Variables and Elliptic Equations, 1-38.
[8] R. Castillo-Perez., V. Kravchenko, R. Resendiz V. (2011), *Solution of boundary value and eigenvalue problems for second order elliptic operators in the plane using pseudoanalytic formal powers*, Mathematical Methods in the Applied Sciences, Vol. 34, Issue 4.
[9] S. Kaufhold (Editor) (2013), *Proceedings of the XVth International Conference on Electrical Bio-Impedance (ICEBI) and the XIVth Conference on Electrical Impedance Tomography 2013*, Heilbad Heiligenstadt, Germany.
[10] Y. Kim, J. G. Webster, W. J. Tompkins (1983), *Electrical impedance imaging of the thorax*, J Microw Power.
[11] V. V. Kravchenko (2009), *Applied Pseudoanalytic Function Theory*, Series: Frontiers in Mathematics, ISBN: 978-3-0346-0003-3.
[12] V. V. Kravchenko (2005), *On the relation of pseudoanalytic function theory to the two-dimensional stationary Schrödinger equation and Taylor series in formal powers for its solutions*, Journal of Physics A: Mathematical and General, Vol. 38, No. 18, pp. 3947-3964.
[13] C. M. A Robles G., A. Bucio R., M. P. Ramirez T., (2013), *New Characterization of an Improved Numerical Method for Solving the Electrical Impedance Equation in the Plane: An Approach from the Modern Pseudoanalytic Function Theory*, IAENG International Journal of Applied Mathematics, Volume 43, Issue 1.
[14] M. P. Ramirez T., M. C. Robles G., R. A. Hernandez-Becerril (2012), *Study of the forward Dirichlet boundary value problem for the two-dimensional Electrical Impedance Equation*, Mathematical Methods in the Applied Sciences (submitted for publication), available in electronic at http://arxiv.org
[15] M. P. Ramirez T., M. C. Robles G., R. A. Hernandez-Becerril, A. Bucio R. (2013), *First characterization of a new method for numerically solving the Dirichlet problem of the two-dimensional Electrical Impedance Equation*, Journal of Applied Mathematics, Volume 2013, Article ID 493483, 14 pages, Hindawi Publishing Corporation.
[16] M. Soleimani (Editor), *Proceedings of the 12th International Conference in Electrical Impedance Tomography*, University of Bath, U.K.
[17] I. N. Vekua (1962), *Generalized Analytic Functions*, International Series of Monographs on Pure and Applied Mathematics, Pergamon Press.
[18] J. G. Webster (1990), *Electrical Impedance Tomography*, Adam Hilger Series on Biomedical Engineering.