Telecommun Syst (2017) 64:279–291
DOI 10.1007/s11235-016-0175-1

A new DNA cryptosystem based on AG codes evaluated in gaussian channels

Ivan Jiron[1] · I. Soto[2] · Cesar A. Azurdia-Meza[3] · A. Valencia[3] · R. Carrasco[4]

Published online: 24 May 2016

Abstract This paper proposes a new cryptosystem system that combines DNA cryptography and algebraic curves defined over different Galois fields. The security of the proposed cryptosystem is based on the combination of DNA encoding, a compression process using a hyperelliptic curve over a Galois field $GF\left(2^{p}\right)$, and coding via an algebraic geometric code built using a Hermitian curve on a Galois field $GF\left(2^{2q}\right)$, where $p > 2q$. The proposed cryptosystem resists the newest attacks found in the literature because there is no linear relationship between the original data and the information encoded with the Hermitian code. Further, the work factor for such attacks increases proportionally to the number of possible choices for the generator matrix of the Hermitian code. Simulations in terms of BER and signal-to-noise ratio (SNR) are included, which evaluate the gain of the transmitted data in an AWGN channel. The performance of the DNA/AG cryptosystem scheme is compared with un-coded QPSK, and the McEliece code in terms of BER. Further, the proposed DNA/AG system outperforms the security level of the McEliece algorithm.

Keywords AG codes · Bit error rate (BER) · DNA cryptosystem · Gaussian channel · Galois fields · Information security, McEliece algorithm

1 Introduction

Future communication networks could explore the use of new source and channel coding methods, which would be vital in reducing the bandwidth and in increasing the security of the information during the transmission of the data in a public key cryptosystem. One of these techniques consists on using deoxyribonucleic acid (DNA) and molecular methods.

In Adleman [1], presented a method for solving the directed Hamiltonian path problem using DNA and molecular techniques, leading to the creation of DNA computing. There are two reasons behind the use and development of DNA computing. Firstly, DNA computing possesses a larger storage capacity compared to traditional storage media; such as optical and magnetic storage media, among others. Secondly, DNA computing requires less computational power compared to other techniques. Some of the techniques used in DNA computing are gel electrophoresis, polymerase chain reaction (PCR), and DNA Chip technology [2,22,32]. For these reasons DNA computing presents serious challenges to traditional cryptography based on math primitives, since the reverse is easy to calculate. For example, the reverse of the popular RSA algorithm is the factorization of very large numbers in their prime factors. While the reverse of the Diffie–Hellman key exchange algorithm is the solution of

Electronic supplementary material The online version of this article (doi:10.1007/s11235-016-0175-1) contains supplementary material, which is available to authorized users.

✉ Cesar A. Azurdia-Meza
cazurdia@ing.uchile.cl

Ivan Jiron
ijiron@ucn.cl

I. Soto
ismael.soto@usach.cl

A. Valencia
alvalenc@ing.uchile.cl

R. Carrasco
r.carrasco@ncl.ac.uk

[1] Universidad Catolica del Norte, Antofagasta, Chile

[2] Universidad de Santiago de Chile, Santiago, Chile

[3] Universidad de Chile, Santiago, Chile

[4] University of Newcastle upon Tyne, Tyne and Wear, UK

the Discrete Logarithm Problem (DLP). These two problems are considered very difficult to solve using current traditional computers [23,28,31], but not for DNA cryptoanalysis [6,7,15]. Thus, DNA cryptography is an excellent alternative to traditional cryptography, although it has to be concatenated with an encoding source or channel method for introducing a higher security level.

The use of the Diffie–Hellman trading key scheme using DNA was proposed in [2]. In this scheme, each of the original data symbols are replaced by a sequence formed of Adenine (A), Thymine (T), Cytosine (C), and Guanine (G). Then, the DNA sequence will add two primers, starting with $ForwardPrimer\ (F_{pr})$ and ending with $EndPrimer\ (E_{pr})$. Each DNA symbol $(A, T, C$ and $G)$ is converted to its binary equivalent according to a preset rule.

The use of the Diffie–Hellman scheme combined with elliptic curves over finite fields was proposed in [24]. This work developed an image encryption algorithm, which separates the image into Red, Green and Blue images, then applies DNA encoding to an interleaving process over these images. Finally these images are encrypted using the Diffie–Hellman scheme.

In [25], the authors proposed an encryption method that represents the key and the encrypted message using a single stranded DNA (ssDNA). The original binary data is arranged according to the Feistel structure. The decryption is done using the hybridization technique. In order to get a better security system, the authors suggest the use a random key mode known as One Time Pad, which consists on destroying the key after being used and using a new key in the next transmission.

In steganography there are some studies that propose improvements in safety in DNA cryptography. In [30], the authors generated a private key from a chaotic function by using the logistic mapping function. A chaotic DNA mask sequence is used to encrypt the picture, whereas the best encryption mask is obtained by using genetic algorithms. This algorithm is able to resist attacks because it introduces a higher entropy and a lower correlation between pixels.

In [14], the authors presented an algorithm that encrypts gray scale images of any size. This algorithm, as a first step, uses a DNA sequence matrix operation. Later, the pixels are scrambled, obtaining the encrypted image. This algorithm is able to resist attacks and is categorized as a comprehensive statistical algorithm, although does not produce channel gain [14].

In the context of AG codes, we have modified and optimized the algorithm proposed by Sakata to design new Hermitian codes [5,8,9] over Galois fields. Further, we have simulated the performance curves of different codes using algebraic curves; such as Elliptic [27] and Hyperelliptic curves [19,35]. Also, in previous papers we have explored the use of reduced divisors for compression, but with other cryptographic schemes, for example, Diffie Hellman and ElGamal, which are based on DLP [19].

It should be noted that in [5], the Hermitian codes were used only for channel coding or data storage. In [19] a cryptographic system is constructed using a combination of a hyperelliptic and a Reed-Solomon code, whereas in [35] those results were extended to a Low density Parity Check Code (LDPC) code.

In the context of security using AG codes, one of the newest attacks found in literature focuses on a structural attack to the McEliece cryptosystem. This new attack uses AG codes, avoiding the re-construction of the decoding matrix $\boldsymbol{G}$, from public data and duality [11].

In [33] we presented preliminary results of this DNA/AG methodology in fading channels, but without proof or further justification of the results. In that system, the attack reported in [11] fails because the data that enters the decoder is protected by the keys F_{pr} and E_{pr}, compressed by the hyperelliptic curve and the mapping. Therefore, the original data is not available.

In this paper we present the proof and details of the proposed method in a Gaussian channel. The proposed method allows the generation of public and private keys for DNA/AG packing. Further, details of the compression/encryption algorithms and the decryption/decompression algorithms used to generate channel encoding and security in parallel are given. The DNA/AG cryptosystem outperforms the McEliece cryptosystem in terms of power consumption by approximately 50 % during the delivery of the keys and data transmission. Efficiency studies are given in terms of BER and security by using computational simulations. This is because the proposed encryption process is a concatenation of data encoding using DNA strands, data compression using a Hyperelliptic curve over a Galois field $GF(2^p)$, and data encoding using a Hermitian algebraic geometric code (HAGC) over a Galois field $GF((2^q)^2)$, with $p > 2q$. Thus, the original data are protected by these three stages, where the decoding of the HAGC is a NP-complete problem. While data compression and encoding data using DNA prevent attacks on the HAGC, as described in reference [11].

The remainder of this paper is organized as follows. Section 2 introduces the mathematical preliminaries that will be used in this article. Section 3 presents a description of the proposed cryptosystem. Section 4 evaluates the performance and security of the proposed DNA/AG cryptosystem. While Sect. 5 presents a discussion of the results using computer simulations. Finally, Sect. 6 presents the conclusions.

2 Algebraic curves over a field

In this section we present the mathematical framework in which the DNA/AG cryptosystem operates, including the definitions of the Hyperelliptic and Hermitian curves, accompanied by a couple of examples and some results regarding these curves over a field. For more details the reader is referred to references [12,17,23] and [26].

Definition 1 Given a set F and two operations $+ : F \times F \rightarrow F$ and $* : F \times F \rightarrow F$. The tuple $(F, +, *)$ is a field if satisfies the following properties: $(F, +)$ and $(F - \{0\}, *)$ are commutative groups, and $*$ is distributive over $+$, i.e., $\forall x, y, z \in F : x * (y + z) = x * y + x * z$. Where $0 \in F$ is the additive identity element.

A Galois field $GF(2^m)$ is a finite field with 2^m elements, with $m \in \mathbb{N}, m \geq 1$. In reference [26] a construction method allows to build a field $GF(2^m)$ as an extension field of $GF(2) = \{0, 1\}$.

Definition 2 A Hyperelliptic Curve H_yC of genus $g \geq 1$ over a field $(F, +, *)$ is given by the solutions to the equation of the form:

$$H_yC : v^2 + h(u)\,v = f(u) \tag{1}$$

where $h(u)$, $f(u)$ are polynomials with coefficients in F. Particularly, these polynomials have degrees $deg(h) \leq g$ and $deg(f) = 2g+1$. In addition, the coefficient of u^{2g+1} is equal to 1 in the polynomial $f(u)$. Furthermore, the solutions $(u, v) \in \overline{F} \times \overline{F}$ can not satisfy simultaneously the Eq. (1) and their partial derivatives with respect to variables v and u. And these solutions $(u, v) \in \overline{F} \times \overline{F}$ are called rational points. Here, $\overline{F}$ is the algebraic closure of F.

For a Hyperelliptic curve H_yC of genus g a divisor is given by a formal sum $D = \sum m_i P_i$, where $P_i \in H_yC, m_i \in \mathbb{Z}$ and a finite amount of m_i are nonzero. Furthermore, a divisor D can be represented as a unique pair of polynomials $a(u)$ and $b(u)$ over the field $(F, +, *)$. To see more details about this polynomial representation we recommend see reference [23]. The Example (1) shows a particular case of a reduced divisor as two polynomials $a(u)$ and $b(u)$.

Example 1 Let the curve $H_yC : v^2+(u^2+u)v = u^5+u^3+1$ of genus $g = 2$ over the field $GF(2^5)$, with $p = 5$. This curve has 32 rational points, some of them are: $(0, 1)$, (α^5,α^{15}), (α^5, α^{27}), $(\alpha^{10}, \alpha^{23})$, $(\alpha^{10}, \alpha^{30})$, (α^{14}, α^8), $(\alpha^{30}, 0)$. Let $D = (\alpha^7, \alpha^4) + (\alpha^9, \alpha^{27}) - 2\infty$ a reduced divisor with points $P_1 = (\alpha^7, \alpha^4)$ and $P_2 = (\alpha^9, \alpha^{27})$, and $m_1 = m_2 = 1$. Then $a(u) = (u + \alpha^7)(u + \alpha^9)$ and $b(u) = \alpha^4 u + \alpha^{26}$.

Definition 3 A Hermitian Curve H_eC over a field $GF(r^2)$ is given by the solutions to the equation of the form:

$$H_eC : x^r - y^{r-1} - y = 0 \tag{2}$$

where r is a power of some prime number, the genus is $g_e = \frac{(r^2-r)}{2}$, and degree $d_{He} = r + 1$. Note that the rational points satisfy Eq. (2) and $\frac{\partial}{\partial x}(H_eC) \neq 0$ or $\frac{\partial}{\partial y}(H_eC) \neq 0$ [16,20,34].

The Example (2) shows a Hermitian curve and some of their rational points.

Example 2 Let Hermitian curve $H_eC : y + y^4 = x^5$ over $GF\left(\left(2^2\right)^2\right)$, with $r = 2^2$, and α is a root of the primitive polynomial $P(x) = x^4+x+1$, $d_{He} = 5$, and $g_e = 6$. Some rational points on H_eC are:$\left(\alpha^4, \alpha^6\right)$, $\left(\alpha^5, \alpha^3\right)$, $\left(\alpha^6, \alpha\right)$, $\left(\alpha^{11}, \alpha^3\right)$, $\left(\alpha^{14}, \alpha^3\right)$.

We end this section by recalling the following theorems to determine bounds for the number of rational points over an algebraic curve with genus greater or equal to 1, defined over a Galois field $GF(r^m)$, where r is a power of some prime number [18].

The number of rational points N_r can be bounded by the Serre bound, which is given at (3):

$$\left|N_r - \left(r^m + 1\right)\right| \leq g\left\lfloor 2\sqrt{r^m}\right\rfloor \tag{3}$$

where $\lfloor x \rfloor$ is the largest integer less than or equal to x.

In [13] is presented an example to calculate the number N_r of rational points of hermitian curve H_eC over a field $GF(r^2)$ by the equation

$$N_r = 1 + r^3 \tag{4}$$

Here, these curves have exactly $N_r = r^3$ rational points and one point is at infinity.

3 System description

Figure 1 shows the system description of an artificial DNA communications system over $GF(2^p)$ and $GF((2^q)^2)$, where T_x is the transmitter side and R_x is the receiver side. It is assumed that the key $(\widetilde{\boldsymbol{G}}, \boldsymbol{Z}, t)$ of the receiver is public, also F_{pr} and E_{pr} were negotiated in advance, or can be modified after the the private key $(\boldsymbol{S}, \boldsymbol{G}, \boldsymbol{P})$ is computed [33].

In the $DNA\ encoder$ block, a binary data is encoded using DNA symbols, and then this DNA sequence is introduced into the reduced divisors of a Hyperelliptic curve over $GF(2^p)$. For T_x, the transmitted data is a binary data sequence represented by $d = d_{\delta_0-1}, \ldots, d_1 d_0$ with an arbitrary length $\delta_0 = \rho_0 * p$, with $\rho_0 \in \mathbb{N}$. The language symbols are encoded by the DNA codes in Table 1. Whereby the DNA basis elements are represented by a couple of bits, but using polynomial notation Adenine $A = 0$, Thymine $T = 1$, Cytosine $C = \alpha$ and Guanine $G = \alpha^2$, where $GF(2^2) = \left\{0, 1, \alpha, \alpha^2\right\}$. The transmitter first generates a random DNA carrier $S_c = s_{\delta_1-1}, \ldots, s_1 s_0$ with a length $\delta_1 = \rho_1 * p$, with $\rho_1 > \rho_0$, $\rho_1 \in \mathbb{N}$. For example, if there is a desire to transmit the short word "FOR", by using the ASCII

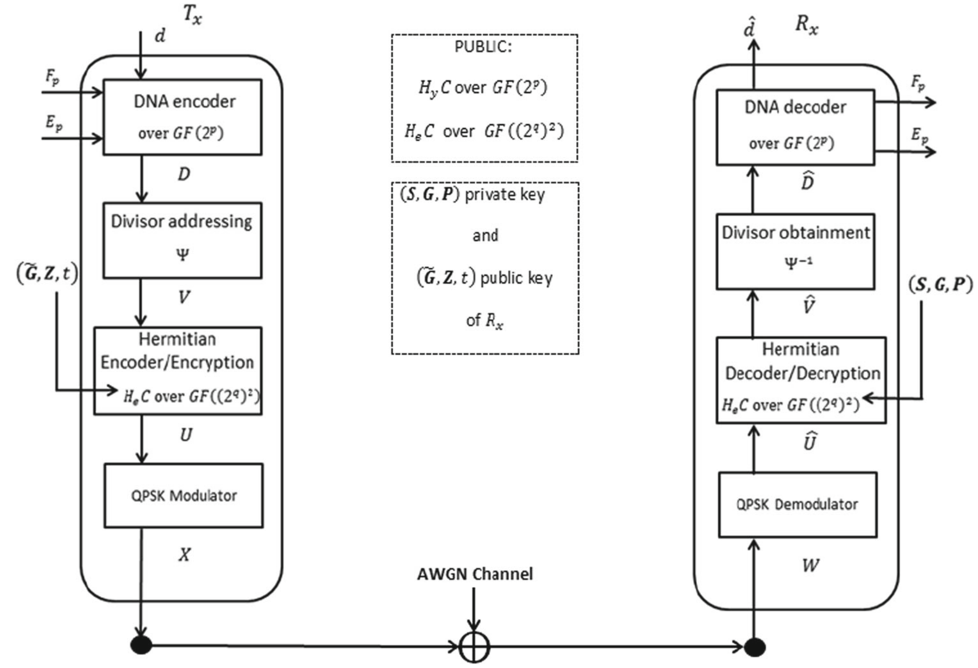
T_x
d
F_p
E_p
DNA encoder over $GF(2^p)$
D
Divisor addressing Ψ
$(\tilde{G}, Z, t)$
V
Hermitian Encoder/Encryption
H_eC over $GF((2^q)^2)$
U
QPSK Modulator
X
PUBLIC:
H_yC over $GF(2^p)$
H_eC over $GF((2^q)^2)$
(S, G, P) private key
and
$(\tilde{G}, Z, t)$ public key
of R_x
AWGN Channel
$\hat{d}$
R_x
DNA decoder over $GF(2^p)$
F_p
E_p
$\hat{D}$
Divisor obtainment Ψ^{-1}
$\hat{V}$
(S, G, P)
Hermitian Decoder/Decryption
H_eC over $GF((2^q)^2)$
$\hat{U}$
QPSK Demodulator
W

Fig. 1 Description of an artificial DNA communications system over $GF(2^p)$ and $GF((2^q)^2)$

Table 1 DNA encoder over $GF(2^2)$

Symb	Code	Symb	Code	Symb	Code	Symb	Code
A	$0\ \alpha^2\ \alpha$	H	$\alpha\ 0\ 1$	O	$\alpha^2\ 0\ 1$	W	$\alpha\ \alpha^2\ 1$
B	$\alpha^2\ \alpha\ 1$	I	$1\ 0\ \alpha$	P	$0\ 0\ \alpha^2$	V	$\alpha^2\ 1\ \alpha$
C	$\alpha\ 1\ 0$	J	$\alpha^2\ \alpha^2\ 0$	Q	$\alpha^2\ 1\ 1$	X	$1\alpha^2\ 0$
D	$1\ 0\ \alpha^2$	K	$0\ \alpha\ 1$	R	$\alpha\ 0\ \alpha^2$	Y	$1\ \alpha^2\ \alpha^2$
E	$\alpha^2\ 0\ \alpha$	L	$\alpha^2\ \alpha^2\ \alpha$	S	$1\ 1\ \alpha$	Z	$\alpha^2\ \alpha\ \alpha^2$
F	$0\ 1\ 1$	M	$\alpha\ \alpha^2\ \alpha$	T	$\alpha\ 0\ 0$	Blank space	$\alpha^2\ \alpha\ \alpha$
G	$\alpha^2\ \alpha\ \alpha$	N	$1\ 0\ 1$	U	$0\ \alpha^2\ \alpha^2$	.	$\alpha\ \alpha\ 0$

code it would be 24 bits, but by using Table 1 it is reduced to 18 bits [33]. Assume that the carrier S_c has $\delta_1 = 5 * 5 = 25$ bits, 18 bits of which are data d, i.e. $\delta_0 = 18$ and the remaining 7 bits are F^1_{pr} and E^1_{pr}, but concatenated as $F^1_{pr}\&E^1_{pr}$.

Then, in the case of a sentence, such as "FOR ME", the carrier would have 50 bits, and 36 of them are data d_1 and d_2, respectively, including blank ($\alpha^2\ \alpha\ \alpha$), given in Table 1. Whereas the remaining 14 bits are F^1_{pr}, E^1_{pr}, F^2_{pr} and E^2_{pr}, then $F^1_{pr}\&E^1_{pr}\&d_1\&F^2_{pr}\&E^2_{pr}\&d_2$, and so on for longer word sequences [33].

Then, the carrier S_c is embedded into the coefficients of the polynomial representation for the reduced divisors D of the Hyperelliptic curve H_yC over $GF(2^p)$. To do this, S_c is separated into groups of p bits, and each of these groups is embedded into the coefficients of the polynomials $a(u)$, $b(u) \in GF(2^p)[u]$, where $D = (a(u), b(u))$ [23].

The *Divisor addressing* block generates a cursor number V using a map Ψ over the set of all reduced divisors that belong to H_yC. That is, Ψ associates a unique cursor number V to each reduced divisor D. Then, each cursor number V is represented as a vector whose components are elements of the field $GF((2^q)^2)$, where $p > 2q$.

The *Hermitian Encoder/Encryption* block generates the codeword U from the keys $\left(\widetilde{\boldsymbol{G}}, \boldsymbol{Z}, t\right)$ and the cursor V using the Hermitian curve H_eC over $GF((2^q)^2)$. That is, $\boldsymbol{V}$ is encoded and encrypted using a McEliece cryptosystem constructed over a Hermitian curve H_eC, and the vector U is obtained. The components of U belong to field $GF((2^q)^2)$. The Hermitian curve H_eC is used to generate a secret generator matrix $\boldsymbol{G}$ and a public key matrix $\widetilde{\boldsymbol{G}}$. The components of these matrices are elements of $GF((2^q)^2)$.

The Hermitian codes have the following parameters: the length of a codeword $n = (2^q)^3$, the length of a message $k = (2^q)^3 - j\,(2^q+1) + \frac{2^q\,(2^q-1)}{2}$, and the designed distance of the code $d^* \geq (2^q + 1)\, j - 2^q\, (2^q - 1) + 2$, with $(2^q - 1) \leq j \leq \left\lfloor \frac{(2^q)^3}{2^q+1} \right\rfloor$ [16,20,21,34].

Thus, the generator matrix $\boldsymbol{G}$ for the code is constructed using rational points $P_1(x_1, y_1), \ldots, P_n(x_n, y_n)$ on H_eC, and a set of homogeneous monomials

$$H_o = \left\{ f_l(x, y) = x^i y^j \mid i, j \in \mathbb{N} \text{ and } 0 \leq i + j = l < k \right\} \tag{5}$$

Then, the generator matrix of order $k \times n$ for the code is given by:

$$\boldsymbol{G} = \left[f_l \left(P_\eta \right) \right], 0 \leq l \leq k - 1 \text{ and } 1 \leq \eta \leq n \tag{6}$$

In the key generation of the DNA/AG scheme, the McEliece public-key encryption algorithm was modified [31], introducing F_{pr}, E_{pr}, Ψ, and the Hermitian curve. Finally, in the transmitter side T_x, the $QPSK\ Modulator$ block produces the modulated codeword X, and it is sent through the AWGN channel using QPSK digital modulation. This modulated sequence X is corrupted by the noise in the channel and this is transformed into W.

In the receiver side R_x, the estimated transmitted codeword $\widehat{\boldsymbol{U}}$ is obtained after demodulation, and fed in the $Hermitian\ Decoder/Decryption$ block. Then, the data decryption process is developed in this block in three steps. The first step computes an internal matrix $\widehat{\boldsymbol{C}}$ using right multiplication by $\boldsymbol{P}^{-1}$ to recover the original order of columns in the generator matrix. The second step decodes the matrix $\widehat{\boldsymbol{C}}$ and computes an internal matrix $\widehat{\boldsymbol{N}}$. This matrix will be used in the third step to calculate an estimation $\widehat{\boldsymbol{V}}$ using right multiplication by $\boldsymbol{S}^{-1}$ to remove the scramble. The Sakata decoding algorithm is used in the second step, for more details about the Sakata decoding algorithm review [5].

In the $Divisor\ obtainment$ block, the inverse of Ψ, denoted by Ψ^{-1}, is applied to estimate the reduced divisors $\hat{D}$; that is, $\Psi^{-1}\left(\widehat{\boldsymbol{V}}\right) = \hat{D}$. Finally, the $DNA - decoder$ block removes F_{pr} and E_{pr} and decode the estimated binary data sequence $\hat{d} = \hat{d}_{\delta_0 - 1}, \ldots, \hat{d}_1 \hat{d}_0$ using Table 1.

4 Performance and security of the DNA/AG cryptosystem

4.1 Modulation process and QPSK error probability of DNA/AG

In this subsection the expression for the error probability of the DNA/AG cryptosystem over an AWGN channel and QPSK modulation will be introduced. When two channel codes are concatenated, the total ratio corresponds to the product of the individual ratios, where each code has a ratio less than one, since parity symbols are introduced in each code [29]. However, when the source code is introduced in a hyperelliptic curve, a compression occurs and then the ratio is greater than one, when $p > 2q$ [19].

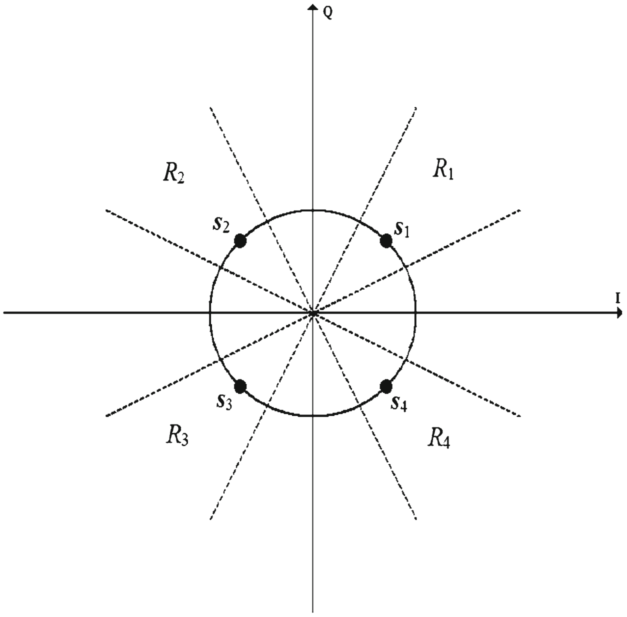

Fig. 2 Decision regions R_1, R_2, R_3 and R_4

Considering that $\boldsymbol{s}_m$ is the transmitted signal and the received signal $\boldsymbol{r} = \boldsymbol{s}_m + \boldsymbol{n}$, where $\boldsymbol{r}, \boldsymbol{s}_m, \boldsymbol{n} \in \mathbb{R}^N$ and $1 \leq m \leq M$. The components of $\boldsymbol{n}$ are Gaussian random variables with zero mean and variance $\frac{N_0}{2}$. Then, the space $\mathbb{R}^N$ is partitioned into the decision regions, which are defined as:

$$R_m = \left\{ \boldsymbol{r} \in \mathbb{R}^N / \Pr\left[\boldsymbol{s}_m \mid \boldsymbol{r}\right] > \Pr\left[\boldsymbol{s}_{\widehat{m}} \mid \boldsymbol{r}\right], \forall \widehat{m} : 1 \leq \widehat{m} \leq M \wedge \widehat{m} \neq m \right\} \tag{7}$$

for each of the transmitted signals $\boldsymbol{s}_m$, where $\Pr\left[\boldsymbol{s}_m \mid \boldsymbol{r}\right]$ is the conditional probability of the transmitted signal $\boldsymbol{s}_m$ and the received signal $\boldsymbol{r}$ affected by the channel. Figure 2 shows $M = 4$ decision regions. Thus, an error occurs when the signal $\boldsymbol{s}_m$ and $\boldsymbol{r} \notin R_m$ are transmitted. Then, the bit error probability can be calculated as

$$P_e = \sum_{m=1}^{M} Pr_m \cdot Pr\left[\boldsymbol{r} \notin R_m | \mathbf{s}_m\right] = \sum_{m=1}^{M} Pr_m \cdot \sum_{1 \leq \beta \leq M; \beta \neq m} \int_{R_\beta} Pr\left[r | \mathbf{s}_m\right] d\mathbf{r} \tag{8}$$

where Pr_m is the probability of each signal $\boldsymbol{s}_m \in \{\boldsymbol{s}_1, \boldsymbol{s}_2, \ldots, \boldsymbol{s}_N\}$.

Theorem 1 *The error probability of the DNA/AG cryptosystem over two algebraic curves, one Hyperelliptic curve H_yC over $GF(2^p)$ and a Hermitian curve H_eC over $GF((2^q)^2)$ is:*

$$P_e^{DNA/AG} = 2Q\left(\sqrt{\frac{2\left(\frac{|d|}{2qn}\right)\varepsilon_b}{N_0}}\right)\left[1 - \frac{1}{2}Q\left(\sqrt{\frac{2\left(\frac{|d|}{2qn}\right)\varepsilon_b}{N_0}}\right)\right] \tag{9}$$

where $Q(x) = \Pr\left[\aleph\left(\overline{m}, \sigma^2\right) > x\right]$ *and* $\aleph\left(\overline{m}, \sigma^2\right)$ *is the PDF of a Gaussian random variable with mean* $\overline{m}$ *and variance* σ^2.

Proof Using Eq. (8) with $M = 2$ we get,

$$P_e = \sum_{m=1}^{2} Pr_m \cdot \sum_{1 \le \widehat{m} \le 2;\, \widehat{m} \ne m} \int_{R_{\widehat{m}}} \Pr\left[\boldsymbol{r}\,|\boldsymbol{s}_m\right] d\boldsymbol{r} \tag{10}$$

Here, we use a pair of binary antipodal signals $s_1(t) = s(t)$ and $s_2(t) = -s(t)$, and their probabilities are $Pr_1 = p_r$ and $Pr_2 = 1 - p_r$, respectively.

When a Hyperelliptic curve over $GF\left(2^p\right)$ is used as source compression and a Hermitian curve over $GF\left(\left(2^q\right)^2\right)$ in the channel, the expression for P_e is modified depending on the compression rate $|d|/2qk$ and code channel rate $2qk/2qn$. Where $|d| = \delta_0$ is the bit length of binary data d, as depicted in Fig. 1. Therefore, the error probability is given as

$$\begin{aligned} P_e = p_r \int_{R_2} \Pr\left[r|s = \sqrt{\left(\frac{|d|}{2qk}\right)\left(\frac{2qk}{2qn}\right)\varepsilon_b}\right] dr, \\ + (1 - p_r)\int_{R_1} \Pr\left[r|s = -\sqrt{\left(\frac{|d|}{2qk}\right)\left(\frac{2qk}{2qn}\right)\varepsilon_b}\right] dr \end{aligned} \tag{11}$$

$$\begin{aligned} = p_r \int_{R_2} \Pr\left[r|s = \sqrt{\left(\frac{|d|}{2qn}\right)\varepsilon_b}\right] dr + (1 - p_r) \\ \int_{R_1} \Pr\left[r|s = -\sqrt{\left(\frac{|d|}{2qn}\right)\varepsilon_b}\right] dr \end{aligned} \tag{12}$$

To describe the decision regions in Eq. 12, the following threshold is used [29]

$$r_{th} = \frac{N_0}{4\sqrt{\left(\frac{|d|}{2qn}\right)\varepsilon_b}} \ln\left(\frac{1 - p_r}{p_r}\right), \tag{13}$$

hence, the error probability is given as

$$\begin{aligned} = p_r \int_{-\infty}^{r_{th}} \Pr\left[r|s = \sqrt{\left(\frac{|d|}{2qn}\right)\varepsilon_b}\right] dr + (1 - p_r) \\ \int_{r_{th}}^{\infty} \Pr\left[r|s = -\sqrt{\left(\frac{|d|}{2qn}\right)\varepsilon_b}\right] dr \end{aligned} \tag{14}$$

$$\begin{aligned} = p_r \Pr\left[\aleph\left(\sqrt{\left(\frac{|d|}{2qn}\right)\varepsilon_b}, \frac{N_0}{2}\right) < r_{th}\right] + (1 - p_r) \\ \Pr\left[\aleph\left(-\sqrt{\left(\frac{|d|}{2qn}\right)\varepsilon_b}, \frac{N_0}{2}\right) > r_{th}\right] \end{aligned} \tag{15}$$

$$= p_r Q\left(\frac{\sqrt{\left(\frac{|d|}{2qn}\right)\varepsilon_b} - r_{th}}{\sqrt{\frac{N_0}{2}}}\right) + (1 - p_r)\, Q\left(\frac{r_{th} + \sqrt{\left(\frac{|d|}{2qn}\right)\varepsilon_b}}{\sqrt{\frac{N_0}{2}}}\right) \tag{16}$$

In particular, if $p_r = \frac{1}{2}$, then $r_{th} = 0$, and

$$P_e = Q\left(\sqrt{\frac{2\left(\frac{|d|}{2qn}\right)\varepsilon_b}{N_0}}\right) \tag{17}$$

If an alphabet with four symbols is used, the modulation for this cryptosystem can be M-ary PSK with $M = 4$ or QPSK, hence the expression of the error probability depends on the compression factor of the source and also the reason code for symbols with two bits. Next, for $M = 4$, the probability of correct decision of a two-bit symbol can be calculated by the symmetry of the constellations. Figure 2 shows the decision regions R_1, R_2, R_3 and R_4 . The probability of the combined system is estimated from the probability of error of a symbol when transmitting $\boldsymbol{s}_1 = \left(\sqrt{\frac{2\left(\frac{|d|}{2qn}\right)\varepsilon_b}{N_0}}, 0\right)$. The vector at the receiver is given by $\boldsymbol{r} = (r_1, r_2) = \left(\sqrt{\frac{2\left(\frac{|d|}{2qn}\right)\varepsilon_b}{N_0}} + n_1, n_2\right)$, where n_1 and n_2 are two Gaussian noise. When there is no crosstalk for $M = 4$

$$P_c^{M=4} = (1 - P_e)^2 \tag{18}$$

where $P_c^{M=4}$ is the probability of correct decision of a two-bit symbol. When a Hyperelliptic curve over $GF\left(2^p\right)$ is used as source compression and a Hermitian curve over $GF\left(\left(2^q\right)^2\right)$ in the channel, the expression is modified depending on the compression rate $|d|/2qk$ and code channel rate $2qk/2qn$.

$$P_e^{M=4} = 1 - P_c^{M=4} = 1 - (1 - 2P_e + P_e^2) \tag{19}$$

$$= 2Q\left(\sqrt{\frac{2\left(\frac{|d|}{2qn}\right)\varepsilon_b}{N_0}}\right)\left[1 - \frac{1}{2}Q\left(\sqrt{\frac{2\left(\frac{|d|}{2qn}\right)\varepsilon_b}{N_0}}\right)\right] \tag{20}$$

Finally, $P_e^{DNA/AG} = P_e^{M=4}$. □

4.2 Security of the DNA/AG cryptographic system

In this subsection we will analyse the intractability of DNA/AG cryptosystem over an AWGN channel using the compression over $GF\left(2^p\right)$ and decoding problem over $GF\left(\left(2^q\right)^2\right)$ of the proposed cryptosystem.

The authors of [4] use the fact that the Three-Dimensional Matching problem is NP-complete, and they prove that the Coset Weights and Subspace Weights decision problems are reduced to Three-Dimensional Matching problem and then are NP-complete. Furthermore, the work done in [4] is extended by the work of Vardy [36]. In this work Vardy shows that the Minimun Distance problem over $GF\left(2^{\omega}\right)$ is NP-complete (Theorem 3 of [36]). In his work the Minimun Distance over $GF\left(2^{\omega}\right)$ problem is reduced to the Finite-Field Subset Sum problem, which is NP-complete. From Theorem 3 of Vardy [36], we obtain the following corollary.

Corollary 1 *For McEliece-Hermitian code the Minimum Distance over $GF\left(2^{\omega}\right)$ problem is NP-complete.*

Proof We use the Minimum Distance over $GF\left(2^{\omega}\right)$ problem of Vardy [36].

The matrix $\boldsymbol{H}$ is calculated as the parity check matrix of the McEliece-Hermitian code,

$$\boldsymbol{H} = \left[\boldsymbol{I}_{(n-k)} \vdots \boldsymbol{A}^{T}\right] \tag{21}$$

The generator matrix $\boldsymbol{G}$ is given by formula (6), and it was written in systematic form as

$$\boldsymbol{G} = \left[\boldsymbol{A} \vdots \boldsymbol{I}_{k}\right] \tag{22}$$

where $\boldsymbol{A}$ is a $k \times (n-k)$ matrix, $\boldsymbol{I}_{(n-k)}$ and $\boldsymbol{I}_{k}$ are identity matrices. Then, the McEliece-Hermitian Minimum Distance over $GF\left(2^{\omega}\right)$ problem given by:
For an integer $\omega > 0$, a $n \times (n-k)$ parity check matrix $\boldsymbol{H}$ over $GF\left(2^{\omega}\right)$, a $\varpi \in \mathbb{Z}$, $\varpi > 0$.
Is there a nonzero vector x of length n over $GF\left(2^{\omega}\right)$ such that $x\boldsymbol{H} = \boldsymbol{0}$ and $wt\left(x\right) \leq \varpi$? is an instance of Minimum Distance problem over $GF\left(2^{m}\right)$ of Vardy.
Therefore, the McEliece-Hermitian Minimum Distance problem over $GF\left(2^{\omega}\right)$ is NP-complete. □

On the other hand, four attacks that have been reported for the McEliece cryptosystem in the past twenty six years [3]. When boundaries are computed for small fields there is a small difference, which could indicate four different attacks, but when the simulation are for larger values of the fields such as those required in this paper, the asymptote is the same for the four attacks. Then, the last three attacks can be considered as a variation of the first proposed by Lee-Brickell 1988 attack [3].

The McEliece cryptosystem attacks reported by [3] only consider Goppa codes constructed over the Galois fields $GF\left(2^{\omega}\right)$, whereas we propose to use McEliece cryptosystem and Hermitian codes, that is, construct the generator matrix of the code using rational points on a Hermitian curve H_eC over $GF((2^q)^2)$, as shown in Sect. 3.

A survey of attacks against the McEliece cryptosystem is presented in [3] in which different work factors for classical information set decoding attacks are calculated. For example, at Information Set Decoding (ISD) algorithms the work factor (Lee-Brickell attack in [3]) is given by

$$W_{ISD} \sim k^{3} \frac{1}{\Pr\left\{\boldsymbol{Z}_{k} = \boldsymbol{0}\right\}} \tag{23}$$

where the vector $\boldsymbol{Z}_k$ is constructed using the first k components of the random error vector $\boldsymbol{Z}$, and

$$\Pr\left\{\boldsymbol{Z}_{k} = \boldsymbol{0}\right\} = \binom{n-t}{k} / \binom{n}{k} \tag{24}$$

is the probability of the first k components of vector $\boldsymbol{Z}$ are zero.

The results given in [3] were used to calculate the average work factor attacks, who consider $GF\left(2^{\omega}\right)$ with $9 \leq \omega \leq 14$. And we extrapolate the average work factor for $GF\left(2^{\omega}\right)$ with $15 \leq \omega \leq 41$.

Theorem 2 *The proposed DNA/AG cryptosystem has a work factor given by*

$$W_{ISD} \sim \Gamma \cdot \frac{k^{3}}{\Pr\left\{\boldsymbol{Z}_{k} = \boldsymbol{0}\right\}} \tag{25}$$

Proof The proposed DNA/AG cryptosystem is based on the McEliece cryptosystem, where generator matrix $\boldsymbol{G}$ is constructed using rational points on a Hermitian curve H_eC over a Galois field $GF\left(\left(2^{q}\right)^{2}\right)$ (refer to Eq. 6). Since the generator matrix $\boldsymbol{G}$ is constructed using n rational points chosen from a total of N_r [13], the attack must consider Γ possible choices for generator matrix, where Γ can be calculated as combinations $\Gamma = C_{n}^{N_r} = \frac{N_r!}{(N_r-n)!n!}$ or permutations $\Gamma = P_{n}^{N_r} = \frac{N_r!}{(N_r-n)!}$. This increases the complexity of the attack because it should be considered that each user will use a different collection of n rational points from among all those possible collections. Then, the work factor is amplified by Γ as shown in Eq. 25.

The security of the proposed algorithm is guaranteed by Theorem 3, and its proof is based on the intractability of decoding problem.

Theorem 3 *The DNA/AG Minimum Distance problem based on the combination of two algebraic curves, one Hyperelliptic curve H_yC over $GF(2^p)$ and a Hermitian curve H_eC over $GF((2^q)^2)$ is NP-complete, where $p > 2q$.*

Proof Assuming that F_{pr} and E_{pr} have been removed, the combination of both curves is performed through the following relationships:

$$\text{For data compression} \quad n \cdot (2q) < 5 \cdot p \tag{26}$$

$$\text{For divisor addressing} \quad k \cdot (2q) \sim \lceil \log_2 \boldsymbol{K} \rceil \tag{27}$$

where, n, k and q are parameters of McEleice Hermitian code constructed over the Hermitian curve H_eC over $GF((2^q)^2)$. Further, the order of Jacobian $\boldsymbol{K} = \left(\sqrt{2^p}+1\right)^{2g}$ and p are parameters of the Hyperelliptic curve H_yC over $GF(2^p)$ (see [19] for details about these relationships). In particular, the parameters p and q should be chosen so that $p > 2q$.

Then, the Hyperelliptic curve H_yC over $GF(2^p)$ determines the choice of the Hermitian curve H_eC over $GF((2^q)^2)$. Therefore, we use the Corollary 1 to conclude that the Minimum Distance based on the combination of two algebraic curves, one Hyperelliptic curve H_yC over $GF(2^p)$ and a Hermitian curve H_eC over $GF((2^q)^2)$ problem is NP-complete □

5 Discussion of results

Figure 1 shows the system description of the DNA/AG cryptosystem which is described in detail in Sect. 3, that uses the F_{pr} and E_{pr} keys plus the combination of two algebraic curves, a Hyperelliptic curve over $GF(2^p)$ to produce compression, and a Hermitian curve to encrypt over a field $GF((2^q)^2)$ using the decoding problem. By combination we mean that the design parameters of each curve define the parameters of the other curve and vice-versa. Also that can not be splinted as three boxes since they are protected by the pair F_{pr} and E_{pr}.

The Data compression process is introduced by the Hyperelliptic curve over $GF(2^p)$ and the Divisor addressing mapping Ψ, which are combined with a Hermitian curve over a field $GF((2^q)^2)$, where $p > 2q$. The encryption process uses an algebraic geometric code constructed on a Hermitian curve over a field $GF((2^q)^2)$. Figures 1 and 2 also describe the process of modulation and demodulation over an AWGN channel, since the alphabet has four DNA symbols with a diversity of two bits, we use uncoded QPSK modulation as a reference to evaluate the performance. Since each element in $GF(64) = GF(2^6)$ comprises 6 bits then 3 QPSK symbols, x_1, x_2 and x_3 are needed to transmit the finite field element. Therefore, the probability of receiving a finite field element y in $GF(64)$ given that we transmitted a finite field element $c \in GF(64)$ can be found by first expressing c in binary form. Each pair of bits in c, b_1 , b_2 and b_3, are mapped to 3 QPSK symbols and the probability can be determined by finding the product of the 3 QPSK probabilities $\Pr(r_1|b_1)$, $\Pr(r_2|b_2)$ and $\Pr(r_3|b_3)$. For example,

$$\begin{aligned}\Pr(y\ |c = \alpha^6) = \Pr(y|c = 000011) = \Pr(r_1|\ b_1 = 00)\\ \Pr(r_2|b_2 = 00)\Pr(r_3|b_3 = 11)\end{aligned} \tag{28}$$

At the R_x side, the decryption process solves a system of equations to calculate the coefficients of a polynomial. To locate the position of the errors, we use the roots of this polynomial evaluated at each of the points on the Hermitian curve; later we calculate error values using the inverse discrete Fourier transform. By knowing the positions and values of the errors, we add them to the received codeword and get an estimation of the cursor for the reduced divisor. The Data decompression process uses Ψ^{-1} to extract the original data. Finally the keys F_{pr} and E_{pr} are removed.

Above descriptions are very interesting because they introduce reduction in memory usage and spectrum efficiency at the R_x of Fig. 1. Additionally the combination of a Hyperelliptic curve with a Hermitian code inside F_{pr} and E_{pr}, produces gain in terms of data transmission. Inserting the F_{pr} and E_{pr} primers in the transmitter side T_x has a constant computational cost, as in the receiver side R_x. The real challenge is to evaluate the computational cost of the compression and encryption of the data in the carrier S_c.

The DNA/AG cryptosystem can be implemented using look-up tables or a method running in memory based on the exponential representation of the elements in the Galois field and operate in a binary computer and vice versa. In order to make a fair comparison of the complexity of using pairs of bits in polynomial notation representing the Adenine $(A) = 0$, Thymine $(T) = 1$, Cytosine $(C) = \alpha$ and Guanine $(G) = \alpha^2$ in a DNA sequence.

Figure 3 shows the shifts distribution of the DNA/AG scheme without look-up table. In the case that the hops in Algorithm 1 are not activated, a 75 % of the energy is concentrated in one or two hops. But if the jumps are activated, a drastic reduction of energy for more than two hops is achieved. This reduction in energy introduce less complexity for all operations and all fields. Figure 4 shows a gain of 50 % in terms of memory usage and execution time by the DNA/AG cryptosystem without look up tables compared to the DNA/AG cryptosystem with look up tables.

Assuming that each bit has a probability of 0.5, being 0 or 1, then Algorithm 1 performs jumps equivalent to the amount of bits 0, which are in a ω-bit binary array. Then it is expected that the gain of Algorithm 1 against an algorithm that use lookup table remains in the same tendency for $\omega > 41$. A suitable gain for almost the entire range of ω can be found, examples of these are: $\frac{(62-30)\cdot 100}{62} = 52\,\%$ for $\omega = 6$, and $\frac{(2199023255550-1099511953471)}{2199023255550} = 50\,\%$ for $\omega = 41$. This means that independently of the value of ω, the computational power required will always be reduced by approximately 50 %.

There are two other algorithms that get the binary portrayal from the exponential representation of an element in a Galois field $GF(2^\omega)$. One uses a sequential search using a look-up table, wheras the other implements calculation in memory

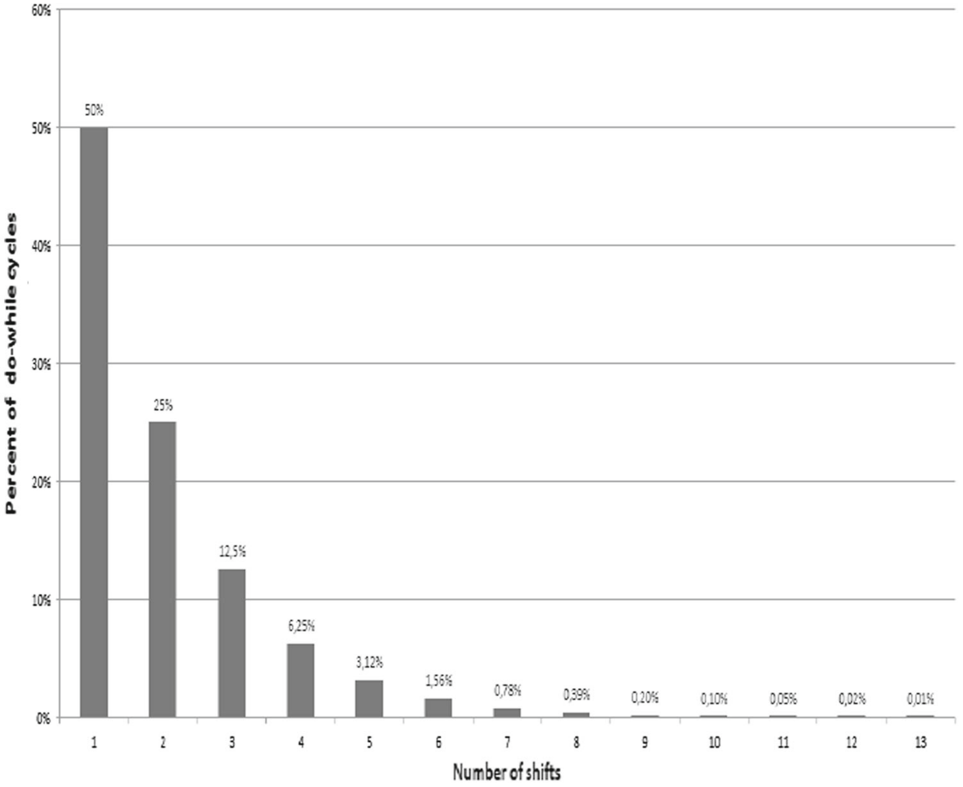

Fig. 3 Shifts distribution of DNA/AG without look-up table for $\alpha^{2^{\omega}-2} \in GF(2^{\omega})$

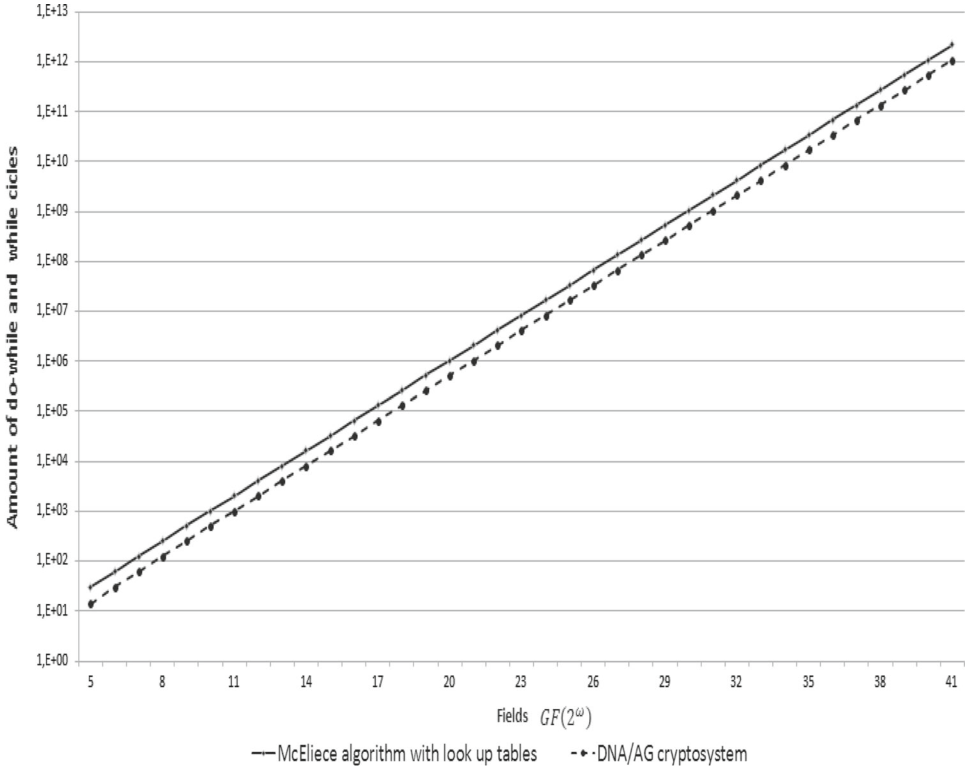

Fig. 4 Comparison between DNA/AG implementation and McEliece with look up table

without a look-up table. The experimental results for these other algorithms are similar to those presented in Figs. 3 and 4; therefore, the discussion will not be repeated.

In previous work we have simulated performance curves for different codes using algebraic curves, such as Elliptic, Hyperelliptic, and Hermitian curves over Galois fields.

Algorithm 1 : Element Generator without look up table.

Input: $a = \left(a_{p-1}, \ldots, a_1, a_0\right)$ where $a_i \in \{0, 1\}$, P_{prim} = a primitive polynomial for $GF\left(2^{\omega}\right)$.
Output: $e \in \mathbb{N}$

```
$aux \leftarrow countzero\,(a)$ ;
for ($lsb = 0 \rightarrow \omega - 1$)
    if ($a_{lsb} == 1$) then
        $break$;
if ($aux == \omega - 1$) then
    $e \leftarrow lsb$;
else
    $s \leftarrow lsb$;
    $e \leftarrow \omega + lsb$;
    $c \leftarrow a$;
    $k \leftarrow 0$;
    do
        $c \leftarrow c >> s$;
        $e \leftarrow e + k$;
        $c \leftarrow c \oplus P_{prim}$;
        for ($j = 0 \rightarrow length\,(c) - 1$)
            if $\left(c_j == \omega - 1\right)$ then
                $s \leftarrow j$;
                $k \leftarrow j$;
                $break$;
    while ($countzero\,(c) < length\,(c) - 1$)
return $e$;
```

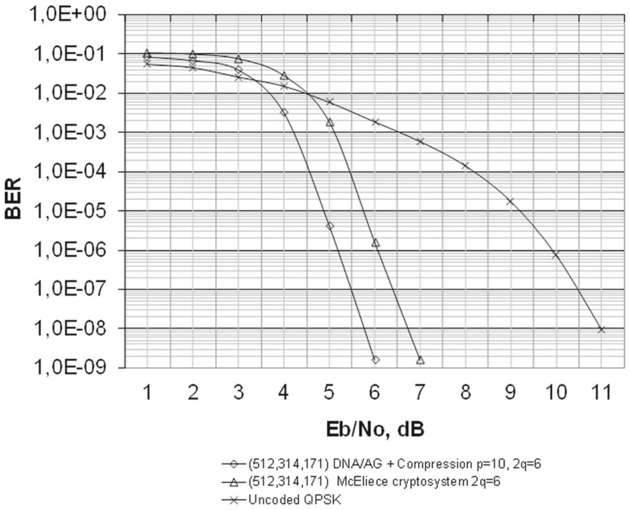

Fig. 5 Performance of data transmission of the DNA/AG cryptosystem, McEliece cryptosystem, and uncoded QPSK over an AWGN channel

Also, in previous papers we have explored the use of reduced divisors for compression, but with other cryptographic schemes, such as the Diffie Hellman and ElGamal schemes which are based on the discrete logarithm problem.

Figure 5 compares the performance of the proposed cryptosystem in terms of bit error rate (BER) and signal-to-noise ratio (SNR), after selecting the Galois fields $GF(2^p)$ and $GF((2^q)^2)$. In Fig. 5 Performance of data transmission of the DNA/AG cryptosystem, we compare uncoded QPSK, (512, 314, 171) McEliece code, and (512, 314, 171) DNA/AG cryptosystem schemes. As an example, for a BER = 1 E-06, a gain of 5 dB is achieved by the (512, 314, 171) DNA/AG cryptosystem scheme compared to that of the uncoded QPSK systems. Whereas a gain of about 1.0 dB is achieved by the (512, 314, 171) DNA/AG cryptosystem compared to that of the (512, 314, 171) McEliece code for a BER of 1 E-06, over an AWGN Channel.

Hermitian codes have been compared with Reed Solomon codes in the same circumstances, and naturally Hermitian codes always outperform the Reed Solomon codes because they have greater length and longer minimum Hamming distance. Additionally, a Hermitian code over a small field can have a similar performance to a Reed solomon code built on a larger field [5,8,9]. Therefore, safer cryptosystems can be constructed using smaller fields and lower power consumption.

The compression generated by the Hyperelliptic curve in Fig. 5 introduces approximately the same gain because less symbols are transmitted in the channel with less energy per bit. This is because the same Hyperelliptic curve is used to compress data and to generate the channel code, with fewer symbols to reconstitute the original data. With the combination described above the proposed DNA/AG cryptosystem resists the attacks described in [3] because the work factor for such attacks is increased in proportion to the number $\Gamma = C_n^{N_r}$ or $\Gamma = P_n^{N_r}$ of possible choices for the generator matrix of the Hermitian code. It also resists the attack reported in [11] because there is no linear relationship between the original information and the information encoded with the Hermitian code. One of the newest attacks to the McEliece cryptosystem found in literature is based on Error Correcting Pair [11]. This attack can not be applied to DNA/AG cryptosystem because the data is protected by F_p and E_p, encoded by Table 1 and by the reduced divisor of the Hyperelliptic curve. From the construction of Vardy over $GF(2^{\omega})$, the Theorem 3 was generated with the purpose of ensuring the safety of DNA/AG cryptosystem, for $p > 2q$.

The McEliece cryptosystem has keys that can be considered matrices, but still can be compared with the RSA and DH algorithms. In [19] the authors developed a model to compare and to analyse security using two algebraic curves equivalent to the proposed cryptosystem. This model allowed to compare the benefit introduced by an elliptic and a hyperelliptic curves with respect to RSA. For the same level of security, the keys exchange that use algebraic curves with the DLP, are much smaller than those using the factorization of large numbers into the prime factors problem used to implement RSA. In reference [10], it is shown that the problem of decoding algebraic curves using Reed Solomon is at least as much or as hard the DLP. In this way we can compare the

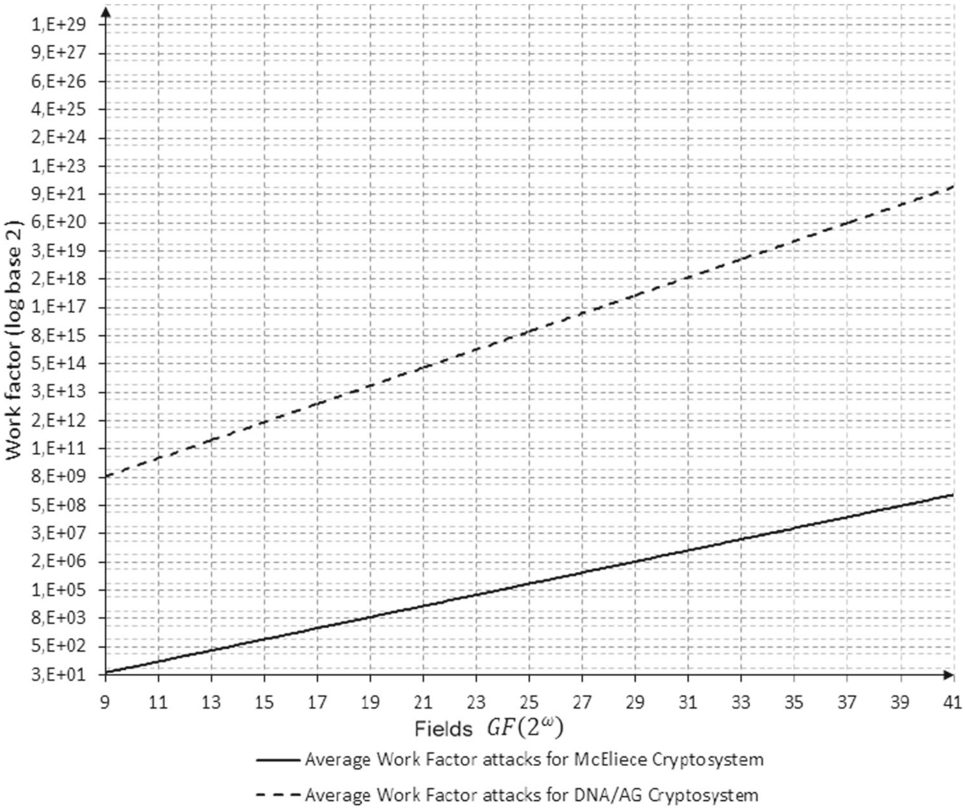

Fig. 6 Comparison of the Work factor of attacks for DNA/AG Cryptosystem and McEliece Cryptosystem

RSA, DH, and McEliece cryptosystems for the same level of security expressed in terms of the time that it takes to break the cryptosystem. In this paper the linear code was replaced by a Hermitian code. Hermitian algebraic curves are characterized by having more points, divisors, and more reduced divisors than those generated by the Reed Solomon, elliptical, and hyper elliptic curves. Therefore, Hermitian curves can be used for designing more resistant codes capable of resisting severe attacks on the keys. Hence, the decoding process using the proposed systems offers more strength compared to DH and RSA algorithms.

In the previous sections the choice of Galois fields $GF(2^p)$ and $GF((2^q)^2)$ has been conditioned, according to $p > 2q$. This condition is necessary to ensure the compression and security. The security is achieved through the use of the Hermitian code. Figure 6 shows a comparison obtained by simulations that evidence the increase of the work factor of the attacks on the DNA/AG cryptosystem compared with the attacks on the traditional McEliece Cryptosystem. In particular, the work factor of the attacks on the DNA/AG cryptosystem is increased by the factor Γ, as described by the expression given by (25) in Sect. 4.2, for example and the DNA/AG cryptosystem outperform McElieces security level in a $3.75E + 12\,\%$ for $\omega = 25$.

6 Conclusions

This paper presents a new DNA/AG cryptosystem that uses a combination of DNA with a pair of ForwardPrimer and EndPrimer markers, and two algebraic curves over different Galois fields. The security of this cryptosystem is based on the use of DNA encoding, a compression process, and coding using a Hermitian code. Because the proposed DNA/AG cryptosystem does not use look up tables, it reduces by 50 % the use of memory and computational time when it is compared with the McEliece algorithm, which implements look up tables and sequential search. The proposed cryptosystem was evaluated in terms of BER to evaluate the gain of the transmitted data assuming an AWGN channel. The performance of the proposed (512, 314, 171) DNA/AG cryptosystem scheme was compared with the (512, 314, 171) McEliece code, and uncoded QPSK. For a BER = 1 E-06, a gain of 5 dB is achieved by the (512,314,171) DNA/AG cryptosystem scheme compared to that of the uncoded QPSK systems. Whereas a gain of about 1.0 dB is achieved by the (512,314,171) DNA/AG cryptosystem compared to that of the (512,314,171) McEliece code for a BER= 1 E-06. Further, the proposed DNA/AG algorithm outperformed the security level of McEliece algorithm by $3.75E + 12\,\%$ for $\omega = 25$.

Acknowledgements The authors acknowledge the financial support of the 'Center for multidisciplinary research on signal processing' (Project Conicyt/ACT1120), Project USACH/Dicyt No 061413SG, and V.R.I.D.T./U.C.N. Antofagasta.

References

1. Adleman, L. M. (1994). Molecular computation of solutions to combinatorial problems. *Science-AAAS*, *266*(5187), 1021–1023.
2. Aich, A.,& Sen, A., et al. (2015). Deoxyribonucleic Acid (DNA) for a Shared Secret Key Cryptosystem with Diffie Hellman Key sharing technique. In: *Third International Conference on Computer, Communication, Control and Information Technology (C3IT)*, 2015, pp. 1 – 6.
3. Baldi, M. (2014). QC-LDPC code-based cryptography. New York: SpringerBriefs in Electrical and Computer Engineering. ISBN 978-3-319-02556-8.
4. Berlekamp, E. R. R., McEliece, J., & van Tilborg, H. C. (1978). On the inherent intractability of certain coding problems. *IEEE Transactions on Information Theory*, *IT–24*, 384–386.
5. Carrasco, R., & Johnston, M. (2008). *Non-binary error control coding for wireless communication and data storage*. New York: Wiley.
6. Chang, W. L. (2012). Fast Parallel DNA-Based Algorithms for Molecular Computation: Quadratic Congruence and Factoring Integers. *IEEE Transactions on Nano Bioscience*, *11*(1), 62–69.
7. Chang, W. L., Guo, Ho M., & Guo, M. (2005). Fast Parallel Molecular Algorithms for DNA-Based Computation: Factoring Integers. *IEEE Transactions on Nano Bioscience*, *4*(2), 149–163.
8. Chen, L., Carrasco, R., & Johnston, M. (2008) Reduced complexity interpolation for list decoding hermitian codes. IEEE Transactions on Wireless Communications, *7*, (11) , art. no. 4684611 , pp. 4353–4361.
9. Chen, L., Carrasco, R., & Johnston, M. (2009). Soft-decision list decoding of hermitian codes. *IEEE Transactions on Communications*, *57*(8), 2169–2176.
10. Cheng, Q., & Wan, D. (2004). On the list and bounded distance decodibility of ReedSolomon codes. In *Proceedings of the 45th Annual IEEE Symposium on Foundations of Computer Science*, 2004, pp. 335-341.
11. Couvreur, A., Marquez-Corbella, I., & Pellikaan, R. (Jul 2014). 'A polynomial time attack against algebraic geometry code based public key cryptosystems'. *IEEE International Symposium on Information Theory (ISIT)*, Honolulu HI, USA, pp.1446–1450.
12. Fulton, W. (1969). *Algebraic Curves. An introduction to Algebraic Geometry*. N.Y.: W.A. Benjamin, Inc.
13. Garcia, A. (2005). On Curves over Finite Fields. *Seminaires & Congres Societe Mathematique de France*, *11*, 75–110.
14. Gupta, S., Jain, A. (Mar 2015)'Efficient Image Encryption Algorithm Using DNA Approach'. *2nd International Conference on Computing for Sustainable Global Development (INDIACom)*, New Delhi, India, pp. 726–731.
15. Ho, M., Shih, Y. (2008). Fast Parallel Bio-Molecular Logic Computing Algorithms of Discrete Logarithm. In *8th IEEE International Conference on BioInformatics and BioEngineering*, 2008, pp. 1 - 6.
16. Hoholdt, T., & Pellikaan, R. (1995). On the decoding of algebraic-geometric codes. *IEEE Transactions on Information Theory*, *IT–41*(6), 1589–1614.
17. Hungerford, T. W. (2012) Abstract Algebra, an Introduction. 3 edn. Brooks Cole, 1986, (2012)
18. Hurt, N. E. (2003). *Many rational points. Coding theory and algebraic geometry*. Dordrecht: Springer Science+BusinessMedia Dordrecht. ISBN 978-90-481-6496-7.
19. Jiron, I., Soto, I., Carrasco, R., & Becerra, N. (2006). Hyperelliptic curves encryption combined with block codes for Gaussian channel. *Int. J. Commun. Syst*, *19*, 809–830.
20. Justesen, J., Arsen, J. L., et al. (1989). Construction and Decoding of a Class of Algebraic Geometry Codes. *IEEE Transactions on Information Theory*, *35*(4), 811–821.
21. Justesen, J., Larsen, K. J., et al. (1992). Fast Decoding of Codes from Algebraic Plane Curves. *IEEE Transactions on Information Theory*, *38*(1), 111–119.
22. Kari, L., Seki, S., & Sosk, P. (2012). *DNA Computing - Foundations and Implications, Handbook of Natural Computing*. Berlin: Springer, Berlin Heidelberg.
23. Koblitz, N. (1998). *Algebraic aspect of cryptography, algorithms and computation in mathematics* (Vol. 3). Berlin: Springer. ISBN 3-540-63446-0.
24. Kumar, M., Iqbal, A., & Kumar, P. (2016). A new RGB image encryption algorithm based on DNA encoding and elliptic curve DiffiHellman cryptography. *Signal Processing*, *125*, 187–202.
25. Kumar Kaundal, A., & Verma, A. K. (2015). Extending Feistel structure to DNA Cryptography. *Journal of Discrete Mathematical Sciences and Cryptography*, *18*(4), 349–362.
26. Lin, S.,& Costello,D. (2004). *Error control coding. Fundamentals and applications* (2nd ed.). Englewood Cliffs, NJ: Prentice-Hall. ISBN-10:0130426725.
27. Ontiveros, B., Soto, I., & Carrasco, R. (2006). Construction of an elliptic curve over finite fields to combine with convolutional code for cryptography. *IEE Proceedings: Circuits Devices and Systems*, *153*(4), 299–306.
28. Paar, Ch., & Pelzl, J. (2010). *Understanding Cryptography. A Textbook for Students and Practioners*. Berlin: Springer-Verlag, Berlin Heidelberg.
29. Proakis, J. G., & Masoud, S. (2008). *Digital communications* (5th ed.). New York: McGraw-Hill. ISBN 9780072957167.
30. Saranya M. R., Arun, K., Mohan, K., Anusudha, K. (Feb 2015) 'Algorithm for Enhanced Image Security Using DNA and Genetic Algorithm'. *IEEE International Conference on Signal Processing, Informatics, Communication and Energy Systems (SPICES)*, Kerala, India, pp. 1–5.
31. Schneier, B. (1996). *Applied cryptography: Protocols, algorithms, and source codes in C* (2nd ed.). New York: Wiley. ISBN-10:0471117099.
32. Singh, A., Singh, R. (Mar 2015) 'Information Hiding Techniques Based on DNA Inconsistency: An Overview'. *2nd International Conference on Computing for Sustainable Global Development (INDIACom)*, New Delhi, India, pp. 2068–2072.
33. Soto, I., Jiron, I., Valencia, A., & Carrasco, R. (2015). Secure DNA data compression using algebraic curves. *Electronics Letters*, *51*(18), 1466–1468.
34. Stichtenoth, H. (1988). A Note on Hermitian Codes Over $GF(q^2)$. *IEEE Transactions on Information Theory*, *34*(5), 1345–1348.
35. Valencia, C., Soto, I., & Carrasco, R. (2007). Secure data compression with sphere packing. *Electronics Letters*, *43*(23), 1298–1300.
36. Vardy, A. (1997). The Intractability of Computing the Minimum Distance of a Code. *IEEE Transactions on Information Theory*, *43*(6), 1757–1766.

Ivan Jiron received his BSc Degree in Mathematics and MS in Science in Mathematic from Católica del Norte University, in 1989 and 1993, respectively. From 1997 to 1999 he studied computing engineer at the University of Santiago de Chile. In 2006 he obtained the Ph.D degree in engineering sciences from the University of Santiago de Chile. He is currently with the Católica del Norte University as an Associate Professor in the Mathematics Department, Faculty of Science. His main research interests include algebraic curves, signal processing, information security, and coding theory.

I. Soto was born in Punta Arenas, Chile. He received an Engineering degree from the University of Santiago of Chile in 1982, the degree of Master of Engineering University Federico Santa Maria in 1990 and the degree of PhD at the University of Staffordshire, UK. in 1997, respectively. He has taught in the departments of Computer Science, Industrial Engineering and Electrical Engineering at the University of Santiago of Chile, currently he is professor of telecommunications and signal processing at Electrical Engineering department. He has worked in wireless networking and security. Professor Ismael Soto has been National Director and member of the Institute of Electrical and Electronic Engineers, and member of International Speech Communication Association. His main research interests are information security, signal processing, coding, and equalization.

Cesar A. Azurdia-Meza received the B.Sc. degree in electrical engineering from Universidad del Valle de Guatemala, Guatemala in 2005, and the M.Sc. degree in electrical engineering from Linnaeus University, Sweden in 2009. In 2013 he obtained the Ph.D degree in Electronics and Radio Engineering, Kyung Hee University, Republic of Korea. He joined the Department of Electrical Engineering, University of Chile as an Assistant Professor in August 2013. He has served as Technical Program Committee (TPC) member for multiple conferences, as well as a reviewer in journals such as IEEE Communications Letter, IEEE Transactions on Wireless Communications, Wireless Personal Communications, and EURASIP Journal on Advances in Signal Processing. Dr. Azurdia is an IEEE and IEICE Communications Society Member. His research interests include topics such as Nyquist's ISI criterion, OFDM-based systems, SC-FDMA, visible light communication systems, 5G & beyond enabling technologies, and signal processing techniques for communication systems.

A. Valencia is a Mechanical Engineer from the Universidad de Chile in 1985 and holds the degree of Doktor-Ingenieur granted by the Ruhr-Universität Bochum in Germany in 1992. He has worked as an academic in the Department of Mechanical Engineering, Universidad de Chile from 1987 to date, conducting a series of research projects and technology transfer. The main areas of specialization are computational fluid dynamics CFD, analysis of the interaction between structures FSI, heat transfer, energy, computational biomechanics, and conversion processes of copper. He has experience in teaching, project management and university administration. He has participated in several CONICYT projects. He has participated also in several outreach projects. He has 52 paper's ISI, has guided about 74 engineering thesis and 9 master's thesis.

R. Carrasco was awarded a BSc Honours Degree from the University of Santiago, Chile in 1969. In 1980 he received a PhD from the University of Newcastle upon Tyne, UK. His research as a PhD candidate focused on implementing digital filters using several processors. He was awarded the IEE Heaviside Premium in 1982 for his work in multiprocessors systems. He is a fellow of the IEE (FIEE) and is a Chartered Engineer (CEng). He is an emeritus Professor in The School of Electrical, Electronic and Computer Engineering, Newcastle University. His principal research interests are digital signal processing algorithms for data communications systems, network communications systems, mobile communication, channel coding, and MIMO systems.