Tracing Bit Differences in Strings Transformed by Linear Quasigroups of Order 4

3 authors:

Marija Mihova
Ss. Cyril and Methodius University in Skopje

Maja Siljanoska
Ss. Cyril and Methodius University in Skopje

Smile Markovski
Ss. Cyril and Methodius University in Skopje

TRACING BIT DIFFERENCES IN STRINGS TRANSFORMED BY LINEAR QUASIGROUPS OF ORDER 4

Marija Mihova
Faculty of Computer Science and Engineering
Skopje, Macedonia

Maja Siljanoska
Faculty of Computer Science and Engineering
Skopje, Macedonia

Smile Markovski
Faculty of Computer Science and Engineering
Skopje, Macedonia

Abstract

Quasigroups are simple algebraic structures whose application in cryptography is increasing rapidly, however not all quasigroups are suitable for cryptographic purposes. In this paper we investigate how a change of one bit in an input binary string affects the strings obtained by applying E-transformation as a multilevel encryptor based on linear quasigroups of order 4. We define a Boolean presentation of quasigroups and we show that for quasigroups of order 4 their Boolean presentations are of degree at most 2. We also give some properties for linear quasigroups and show that using these properties the number of linear quasigroups of order 4 can be easily computed.

I. Introduction

Quasigroups are simple algebraic structures whose properties and especially their large number enable them to be applicable in many areas, including cryptography, coding theory, telecommunications etc. Even though their application in cryptography is increasing rapidly, not all quasigroups are suitable for cryptographic purposes.

The quasigroups of order 2^n can be represented as vector valued Boolean functions $f : \{0,1\}^{2n} \to \{0,1\}^n$ [1]. Using this representation, they can be classified as linear, semilinear and nonlinear quasigroups. Different quasigroup string transformations based on binary quasigroups have been defined for encryption and decryption, among them e-transformation and d-transformation, as defined in [3]. e-transformation is used as a single level encryption function, whereas multilevel encryption can be achieved by applying E-transformation as a composition of consecutive e-transformations. Based on such transformations several cryptographic primitives and codes have been designed, see [4], [5].

In this paper we analyse how a change of one bit in a given input binary string affects the binary strings obtained by applying E-transformation as a multilevel encryptor based on linear quasigroups of order 4. Our analysis shows that the changes in the transformed strings do not depend on the input binary string. Furthermore, a change of one bit in the input binary string which is encrypted using E-transformation results with presence of patterns in the encrypted strings. We also give some properties for linear quasigroups, using which we are able to easily compute the number of linear quasigroups of order 4.

II. Boolean presentations of quasigroups and the class of linear quasigroups

A quasigroup $(Q,*)$ is a groupoid satysfying the law

$$(\forall u,v \in Q)\,(\exists! x,y \in Q)\,(x*u = v \wedge u*y = v),$$

i.e. the equations $x*u=v, u*y=v$ have unique solutions x,y for each given $u,v\in Q$. If $(Q,*)$ is a quasigroup, then $*$ is called a quasigroup operation.

For any finite binary quasigroup $(Q,*)$ given by its multiplication table, a Latin square consisting of the matrix formed by the main body of the table can be associated, since each row and column of the matrix is a permutation of Q.

Let $(Q,*)$ be a finite quasigroup of order 2^n. Then the elements of Q can be represented in a one-to-one way by n-tuples of bits $(b_1,b_2,\ldots,b_n),\ b_i\in\{0,1\}$. If for $a,b,c\in Q$ we have $a*b=c$, then for the corresponding bit representations of a,b,c we have that

$$(a_1,a_2,\ldots,a_n)*(b_1,b_2,\ldots,b_n)=(c_1,c_2,\ldots,c_n),$$

where $c_i = c_i(a_1,a_2,\ldots,a_n,b_1,b_2,\ldots,b_n) : \{0,1\}^{2n} \to \{0,1\}$ are Boolean functions on $2n$ variables. Since the quasigroup operation $*$ is uniquely determined by the Boolean functions c_i, we say that the n-tuple $< c_1,c_2,\ldots,c_n >$ of Boolean functions is a Boolean presentation of the quasigroup $(Q,*)$.

Note that every Boolean function $f(x_1,\ldots,x_k)$ can be uniquely given in its algebraic normal form (ANF), i.e., as a polynomial in the Galois field $GF(2)$ as follows: $f(x_1,\ldots,x_k) = \sum\limits_{I\subseteq\{0,1\}^n} \alpha_I x^I$, where $\alpha_I\in\{0,1\}$ and $x^I = x_i x_j \ldots x_t$ for $I=\{i,j,\ldots,t\}$. A Boolean function is said to be of degree d if its ANF is of degree d.

Given a Boolean presentation $< c_1,c_2,\ldots,c_n >$ of a quasigroup $(Q,*)$, for any fixed bits $\alpha_1,\alpha_2,\ldots,\alpha_n$ we have that $< c_1+\alpha_1, c_2+\alpha_2,\ldots,c_n+\alpha_n >$ is a Boolean presentation of a quasigroup, too. Let $(Q,\widetilde{*})$ denote a quasigroup of order 2^n with Boolean presentation $< c_1,c_2,\ldots,c_n >$ such that the free coefficient of each c_i is equal to 0. Then we say that $(Q,\widetilde{*})$ is in standard form.

Theorem 1: To each quasigroup $< c_1,c_2,\ldots,c_n >$ of order 2^n in standard form, 2^n-1 different quasigroups $< c_1+\alpha_1, c_2+\alpha_2,\ldots,c_n+\alpha_n >$ of order 2^n can be associated.

In the sequel we consider only quasigroups of order 4 and we represent the elements of those quasigroups by pairs (x,y)

of bits. Then their Boolean presentations are of form $< f, g >$ with ANF

$$\begin{aligned} f\left(a,b,c,d\right) =&\alpha_0 + \alpha_a a + \alpha_b b + \alpha_c c + \alpha_d d + \alpha_{ab} ab \\ &+ \alpha_{ac} ac + \alpha_{ad} ad + \alpha_{bc} bc + \alpha_{bd} bd \\ &+ \alpha_{cd} cd + \alpha_{abc} abc + \alpha_{abd} abd \\ &+ \alpha_{acd} acd + \alpha_{bcd} bcd + \alpha_{abcd} abcd, \end{aligned} \tag{1}$$

$$\begin{aligned} g\left(a,b,c,d\right) =&\beta_0 + \beta_a a + \beta_b b + \beta_c c + \beta_d d + \beta_{ab} ab \\ &+ \beta_{ac} ac + \beta_{ad} ad + \beta_{bc} bc + \beta_{bd} bd \\ &+ \beta_{cd} cd + \beta_{abc} abc + \beta_{abd} abd \\ &+ \beta_{acd} acd + \beta_{bcd} bcd + \beta_{abcd} abcd, \end{aligned} \tag{2}$$

where $\alpha_i, \beta_i \in \{0,1\}$ for each index i.

Theorem 2: Each quasigroup of order 4 has Boolean presentation $< f, g >$ with Boolean functions f, g of degree 2:

$$\begin{aligned} f(a,b,c,d) &= \alpha_0 + \alpha_a a + \alpha_b b + \alpha_c c + \alpha_d d \\ &\quad + \alpha_{ac} ac + \alpha_{ad} ad + \alpha_{bc} bc + \alpha_{bd} bd, \\ g(a,b,c,d) &= \beta_0 + \beta_a a + \beta_b b + \beta_c c + \beta_d d \\ &\quad + \beta_{ac} ac + \beta_{ad} ad + \beta_{bc} bc + \beta_{bd} bd. \end{aligned} \tag{3}$$

Proof: The algebraic normal forms of f and g given in (1) and (2) can be written in the following equivalent forms:

$$\begin{aligned} f\left(a,b,c,d\right) =& f_1\left(c,d\right) + a f_2\left(c,d\right) + b f_3\left(c,d\right) \\ &+ ab f_4\left(c,d\right), \end{aligned} \tag{4}$$

$$\begin{aligned} f\left(a,b,c,d\right) =& f_1^{'}\left(a,b\right) + c f_2^{'}\left(a,b\right) + d f_3^{'}\left(a,b\right) \\ &+ cd f_4^{'}\left(a,b\right), \end{aligned} \tag{5}$$

$$\begin{aligned} g\left(a,b,c,d\right) =& g_1\left(c,d\right) + a g_2\left(c,d\right) + b g_3\left(c,d\right) \\ &+ ab g_4\left(c,d\right), \end{aligned} \tag{6}$$

$$\begin{aligned} g\left(a,b,c,d\right) =& g_1^{'}\left(a,b\right) + c g_2^{'}\left(a,b\right) + d g_3^{'}\left(a,b\right) \\ &+ cd g_4^{'}\left(a,b\right), \end{aligned} \tag{7}$$

where $f_i, f_i', g_i, g_i' : \{0,1\}^2 \to \{0,1\}$ are Boolean functions, for each $i = 1,2,3,4$.

Let c_x, d_x be given arbitrary values of c, d and let $f_i\left(c_x, d_x\right) = k_i$ and $g_i\left(c_x, d_x\right) = m_i$ for $i = 1,2,3,4$, where $k_i, m_i \in \{0,1\}$. Then, from (4) and (6) it follows that

$$\begin{aligned} f\left(a,b,c_x,d_x\right) &= k_1 + a k_2 + b k_3 + ab k_4, \\ g\left(a,b,c_x,d_x\right) &= m_1 + a m_2 + b m_3 + ab m_4. \end{aligned}$$

Let $x_i = f\left(a_i, b_i, c_x, d_x\right),\ y_i = g\left(a_i, b_i, c_x, d_x\right)$, for $i = 1,2,3,4$. There are four possible cases to consider:

$$\begin{aligned} (a_1,b_1) = (0,0) \quad &\Rightarrow \quad x_1 = k_1,\ y_1 = m_1, \\ (a_2,b_2) = (0,1) \quad &\Rightarrow \quad x_2 = k_1 + k_3,\ y_2 = m_1 + m_3, \\ (a_3,b_3) = (1,0) \quad &\Rightarrow \quad x_3 = k_1 + k_2,\ y_3 = m_1 + m_2, \\ (a_4,b_4) = (1,1) \quad &\Rightarrow \quad x_4 = k_1 + k_2 + k_3 + k_4, \\ &\qquad\ y_4 = m_1 + m_2 + m_3 + m_4. \end{aligned}$$

Since the elements $(x_1,y_1),(x_2,y_2),(x_3,y_3),(x_4,y_4)$ are from one column of the corresponding Latin square of the quasigroup (it is the column for (c_x,d_x)), we have that $\{(x_1,y_1),(x_2,y_2),(x_3,y_3),(x_4,y_4)\} = \{(0,0),(0,1),(1,0),(1,1)\}$. So, there are two 0s and two 1s among x_1,x_2,x_3,x_4 and there are two 0s and two 1s among y_1,y_2,y_3,y_4.

Case 1. Let $x_4 = 0$. Then there must be two 1s and one 0 among x_1,x_2,x_3, so $0 = x_1+x_2+x_3 = 0 = k_1+(k_1+k_3)+(k_1+k_2) = k_1+k_2+k_3$. Now, from the equality $x_4 = k_1+k_2+k_3+k_4$, by replacing $x_4 = 0$ and $k_1+k_2+k_3 = 0$, we get $k_4 = 0$.

Case 2. Let $x_4 = 1$. Then there must be two 0s and one 1 among x_1,x_2,x_3,so $1 = x_1+x_2+x_3 = k_1+(k_1+k_3)+(k_1+k_2) = k_1+k_2+k_3$. By replacing $x_4 = 1$ and $k_1+k_2+k_3 = 1$ in the equality $x_4 = k_1+k_2+k_3+k_4$, we get again $k_4 = 0$.

We conclude that $f_4\left(c_x,d_x\right) = k_4 = 0$. Since (c_x,d_x) was chosen arbitrarily, we have that $f_4\left(c,d\right) = 0$ for all $(c,d) \in Q$.

It can be shown in the same way that $g_4\left(c,d\right) = 0$, $f_4'\left(c,d\right) = 0$ and $g_4'\left(c,d\right) = 0$. This completes the proof of the theorem. ■

According to the degree of the polynomials f and g in the Boolean presentations $< f, g >$, the quasigroups of order 4 can be classified as follows:

1) *Linear quasigroups.* Both f and g are linear polynomials,

$$\begin{aligned} f(a,b,c,d) &= \alpha_0 + \alpha_a a + \alpha_b b + \alpha_c c + \alpha_d d, \\ g(a,b,c,d) &= \beta_0 + \beta_a a + \beta_b b + \beta_c c + \beta_d d. \end{aligned} \tag{8}$$

2) *Semilinear quasigroups.* One of the functions f or g is linear and the other is quadratic.
3) *Quadratic quasigroups.* Both f and g are quadratic polynomials.

At the end of this section we consider linear quasigroups. The standard form of a linear quasigroup $< f, g >$ is given by the functions

$$\begin{aligned} f(a,b,c,d) &= \alpha_a a + \alpha_b b + \alpha_c c + \alpha_d d, \\ g(a,b,c,d) &= \beta_a a + \beta_b b + \beta_c c + \beta_d d. \end{aligned} \tag{9}$$

By Theorem 1 we have that 3 other linear quasigroups of order 4 are associated to each standard one.

The Cayley table of a standard quasigroup $(Q, \widetilde{*})$ is shown in Fig. 1. *Note:* The row and the column for $(1,1)$ are intentionally left out due to space limitations, but their elements are simply sums of the other three elements in the corresponding row and column.

$\widetilde{*}$	$(0,0)$	$(0,1)$	$(1,0)$
$(0,0)$	$(0,0)$	(α_d, β_d)	(α_c, β_c)
$(0,1)$	(α_b, β_b)	$(\alpha_b + \alpha_d, \beta_b + \beta_d)$	$(\alpha_b + \alpha_c, \beta_b + \beta_c)$
$(1,0)$	(α_a, β_a)	$(\alpha_a + \alpha_d, \beta_a + \beta_d)$	$(\alpha_a + \alpha_c, \beta_a + \beta_c)$

Fig. 1. The Cayley table of $(Q, \widetilde{*})$

From the quasigroup properties of $(Q, \widetilde{*})$ it follows that there must be one 0 and two 1s among $\alpha_c, \alpha_d, \alpha_c + \alpha_d$ and one 0 and two 1s among $\beta_c, \beta_d, \beta_c + \beta_d$, which yields the following proposition:

Proposition 1: If we are given a linear quasigroup of order 4, then none of the following statements holds:

$(a)\quad \alpha_c = \alpha_d = 0$ or $\beta_c = \beta_d = 0$,

$(b)\quad \alpha_c = \beta_c = 0$ or $\alpha_d = \beta_d = 0$,

$(c)\quad (\alpha_c, \alpha_d) = (\beta_c, \beta_d)$.

The same is valid for $\alpha_a, \alpha_b, \beta_a, \beta_b$ as well.

Theorem 3: The number of linear quasigroups of order 4 is 144.

Proof: In a standard linear quasigroup of order 4 $(Q, \widetilde{*})$ we have $(0,0)\,\widetilde{*}\,(0,0) = (0,0)$. Then among $\alpha_c, \alpha_d, \alpha_c + \alpha_d$ there must be one 0 and two 1s, which can be chosen in $\binom{3}{1}$ different ways. Using Proposition 1, in those elements where the first bit is 0, the second bit must be 1, whereas in the elements where the first bit is 1, the second bit can be either 0 either 1, yielding 2 possible ways of choosing the second bit. Hence, the number of ways of choosing $\alpha_c, \alpha_d, \alpha_c + \alpha_d$ and $\beta_c, \beta_d, \beta_c + \beta_d$ is $\binom{3}{1} \cdot 2$. Similarly, $\alpha_a, \alpha_b, \alpha_a + \alpha_b$ and $\beta_a, \beta_b, \beta_a + \beta_b$ can be chosen in $\binom{3}{1} \cdot 2$ different ways as well.

Therefore, the number of standard linear quasigroups of order 4 is $(\binom{3}{1} \cdot 2)^2$ and since by Theorem 1 there are 3 other linear quasigroups associated to the standard one, the total number of linear quasigroups of order 4 will be $(\binom{3}{1} \cdot 2)^2 \cdot 4 = 144$. ∎

III. Quasigroup string transformations

Using quasigroups several quasigroup string transformations can be defined, see [2], [3]. Consider a quasigroup $(Q, *)$ of order 4 where $Q = \{0,1\}^2$ is given as a set of 2-bit elements. Let Q^+ be the set of all finite strings formed by the elements of Q. The elements of Q^+ will be denoted $x_1x_2x_3x_4...x_{2n-1}x_{2n}$ rather than $((x_1,x_2),(x_3,x_4),...,(x_{2n-1},x_{2n}))$, where $(x_i, x_{i+1}) \in Q$, $i = 1,3,5,...,2n-1$, for $n \geq 1$.

For each $(a,b) \in Q$ we define a transformation $e_{*,(a,b)} : Q^+ \to Q^+$ based on the quasigroup operation $*$ with leader $(a,b) \in Q$ as follows:

Let $(x_i, x_{i+1}) \in Q$ for $i = 1,3,..,2n-1$, i.e., $\gamma = x_1x_2x_3x_4...x_{2n-1}x_{2n}$ is a given string from Q^+. Then

$$\begin{aligned} e_{*,(a,b)}(\gamma) &= e_{*,(a,b)}(x_1x_2x_3x_4...x_{2n-1}x_{2n}) \\ &= x'_1x'_2x'_3x'_4...x'_{2n-1}x'_{2n}\ , \end{aligned} \tag{10}$$

where

$$(x'_1, x'_2) = (a,b) * (x_1, x_2)$$
$$(x'_i, x'_{i+1}) = (x'_{i-2}, x'_{i-1}) * (x_i, x_{i+1})\ ,\ i = 3,...,2n-1\ .$$

The function $e_{*,(a,b)}$ is called e-transformation of Q^+ based on the quasigroup operation $*$ with leader $l = (a,b) \in Q$, and its graphical representation is shown on Fig. 2. (It is used as an encryption function for designing cryptographic primitives such as stream ciphers, block ciphers, hash functions, pseudo random number generators, etc.)

Consecutive e-transformations based on $*$ can be applied on a given string formed by the elements of Q, as a composition of e-transformations using the same or different leaders for each transformation. This composition of k mappings

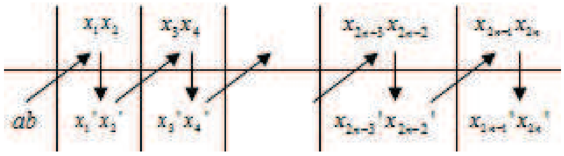

Fig. 2. Graphical representation of e-transformation

$E_k = e_{*,l_1} \circ e_{*,l_2} \circ \cdots \circ e_{*,l_k}$, where $l_i \in Q, i = 1,\ldots,k$, are the k leaders (not necessarily distinct), is said to be E-transformation of Q^+. These multiple levels of mapping ensure lower resemblance of the output string to that of the input string. (In applications, this makes it harder to decrypt the data.)

Let $\gamma = x_1x_2x_3x_4...x_{2n-1}x_{2n} \in Q^+$ be a given input binary string. In our analysis we will consider E-transformations in which an arbitrary leader is used for each of the transformation levels, as presented graphically on Fig. 3:

$$\begin{aligned} E_1(\gamma) &= e_{*,(a,b)}(\gamma) = x'_1x'_2...x'_{2n-1}x'_{2n} \\ E_2(\gamma) &= e_{*,(c,d)}(E_1(\gamma)) = x''_1x''_2...x''_{2n-1}x''_{2n} \\ E_3(\gamma) &= e_{*,(r,s)}(E_2(\gamma)) = x'''_1x'''_2...x'''_{2n-1}x'''_{2n} \quad \text{etc.} \end{aligned}$$

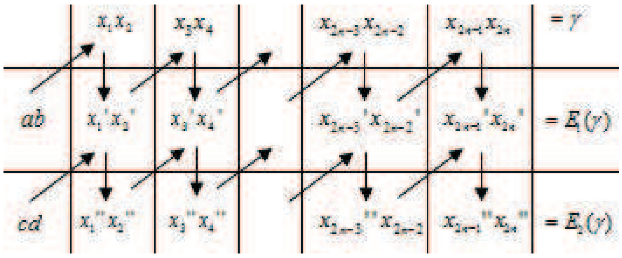

Fig. 3. Graphical representation of E-transformation

IV. Bit changes in the quasigroup operands and their effect on the quasigroup operation result

Let γ be an input binary string. In order to investigate how a change of one bit in γ affects the encrypted strings $E(\gamma)$, we first analyze how the bit changes in the quasigroup operands affect the result of the quasigroup operation $*$.

Let $(a,b), (x,y) \in Q$. Then from Theorem 2 we have

$$(a,b) * (x,y) = (f(a,b,x,y), g(a,b,x,y)), \tag{11}$$

where $< f, g >$ is the Boolean presentation of the quasigroup $(Q, *)$. The Boolean functions f and g are given by the equalities (3).

Now, let $\Delta a, \Delta b, \Delta x, \Delta y \in \{0,1\}$ be the potential bit changes in a, b, x, y, respectively. A value $\Delta z = 1$ denotes that a change in the value of z certainly occurs, whereas a value $\Delta z = 0$ denotes that there is no change at all in the value of z.

Let us denote

$$\begin{aligned} h_f &= f(a + \Delta a, b + \Delta b, x + \Delta x, y + \Delta y)\,, \\ h_g &= g(a + \Delta a, b + \Delta b, x + \Delta x, y + \Delta y)\,. \end{aligned} \tag{12}$$

Then we have

$$\begin{aligned} h_f = &\alpha_0 + \alpha_a (a + \Delta a) + \alpha_b (b + \Delta b) \\ &+ \alpha_x (x + \Delta x) + \alpha_y (y + \Delta y) \\ &+ \alpha_{ax} (a + \Delta a) (x + \Delta x) \\ &+ \alpha_{ay} (a + \Delta a) (y + \Delta y) \\ &+ \alpha_{bx} (b + \Delta b) (x + \Delta x) \\ &+ \alpha_{by} (b + \Delta b) (y + \Delta y) \\ = &f (a, b, x, y) + \Delta f, \end{aligned} \tag{13}$$

and, similarly,

$$h_g = g (a, b, x, y) + \Delta g, \tag{14}$$

where $\Delta f, \Delta g$ are Boolean functions given by

$$\begin{aligned} \Delta f = &\alpha_a \Delta a + \alpha_b \Delta b + \alpha_x \Delta x + \alpha_y \Delta y \\ &+ \alpha_{ax} (a\Delta x + x\Delta a + \Delta a\Delta x) \\ &+ \alpha_{ay} (a\Delta y + y\Delta a + \Delta a\Delta y) \\ &+ \alpha_{bx} (b\Delta x + x\Delta b + \Delta b\Delta x) \\ &+ \alpha_{by} (b\Delta y + y\Delta b + \Delta b\Delta y), \end{aligned} \tag{15}$$

$$\begin{aligned} \Delta g = &\beta_a \Delta a + \beta_b \Delta b + \beta_x \Delta x + \beta_y \Delta y \\ &+ \beta_{ax} (a\Delta x + x\Delta a + \Delta a\Delta x) \\ &+ \beta_{ay} (a\Delta y + y\Delta a + \Delta a\Delta y) \\ &+ \beta_{bx} (b\Delta x + x\Delta b + \Delta b\Delta x) \\ &+ \beta_{by} (b\Delta y + y\Delta b + \Delta b\Delta y). \end{aligned} \tag{16}$$

Therefore, using (13) and (14), we have

$$\begin{aligned} (h_f, h_g) &= (a + \Delta a, b + \Delta b) * (x + \Delta x, y + \Delta y) \\ &= (f (a, b, x, y) + \Delta f,\ g (a, b, x, y) + \Delta g) \\ &= (f (a, b, x, y), g (a, b, x, y)) + (\Delta f, \Delta g) \\ &= (a, b) * (x, y) + \Delta_{(a,b)*(x,y)}\ . \end{aligned} \tag{17}$$

If $(Q, *)$ is a linear quasigroup, then its Boolean presentation $< f, g >$ is given by the equalities (8) and therefore we get

$$\begin{aligned} \Delta f &= \alpha_a \Delta a + \alpha_b \Delta b + \alpha_x \Delta x + \alpha_y \Delta y, \\ \Delta g &= \beta_a \Delta a + \beta_b \Delta b + \beta_x \Delta x + \beta_y \Delta y. \end{aligned} \tag{18}$$

Thus, the changes in the result of the quasigroup operation which occur due to bit changes in the quasigroup operands take the following form

$$\begin{aligned} \Delta_{(a,b)*(x,y)} = &(\alpha_a \Delta a + \alpha_b \Delta b + \alpha_x \Delta x + \alpha_y \Delta y, \\ &\beta_a \Delta a + \beta_b \Delta b + \beta_x \Delta x + \beta_y \Delta y)\ . \end{aligned} \tag{19}$$

It can be noticed from (19) that

$$\Delta_{(a,b)*(x,y)} = (\Delta a, \Delta b) * (\Delta x, \Delta y) - (\alpha_0, \beta_0),$$

hence for each linear quasigroup operation $*$, a quasigroup operation in standard form over the bit changes

$$\Delta_{(a,b)*(x,y)} = (\Delta a, \Delta b) \widetilde{*} (\Delta x, \Delta y)$$

is obtained.

Therefore, the next theorem clearly holds.

Theorem 4: Let $(Q, *)$ be a linear quasigroup of order 4. If bit changes occur in the initial quasigroup operands, then the changes in the result of the quasigroup operation $*$ do not depend on the operands, they depend only on the actual bit changes in the operands as well as the definition of the quasigroup operation.

This theorem indicates that the linear quasigroups of order 4 obviously have no real practical value for cryptographic purposes.

V. Tracing Bit Changes in Strings Encrypted by Linear Quasigroups of Order 4

Using the results acquired in the previous sections, we can now describe how a change of one bit in a given input binary string affects the binary strings obtained by consecutive encryption of the input string using E-transformation based on linear quasigroups of order 4.

Theorem 5: Let $(Q, *)$ be a linear quasigroup of order 4 and let $\gamma \in Q^+$ be a given input binary string which is to be encrypted using E-transformation as a multilevel encryptor. Let us assume that there is a change of one bit in the first 2-bit element of γ. Then, the resulting sequence of changes in the encrypted string in each level of encryption is of the form $sp...p$, where s and p are binary sequences with length $|s|$ and $|p|$, respectively. Moreover, if the k-th level of sequence of changes has the form $sp...p$, then the sequence of changes in the $k+1$-th level of encryption will have the form $s'p'...p'$, where $|s'| \leq |s| + 6\,|p|$, and $|p'| = i\,|p|$, for $i = 2, 4, 6, 8$.

Proof: Before the change of one bit occurs in the first 2-bit element of the binary string $\gamma = x_1 x_2 ... x_{2n-1} x_{2n}$, the sequence of changes is $\Delta\gamma = \underbrace{0000...00}_{2n}$. After a change of one bit in (x_1, x_2), the first 2-bit element of $\Delta\gamma$ will be $(\Delta x_1, \Delta x_2) = (0, 1)$ or $(\Delta x_1, \Delta x_2) = (1, 0)$. In the first level of encryption we apply e-transformation with an arbitrary leader $(a, b) \in Q$, no bit change happens in the leader, so $(\Delta a, \Delta b) = (0, 0)$. However, a $(\Delta a_1, \Delta b_1) \neq (0, 0)$ exists such that $(0, 0) * (\Delta x_1, \Delta x_2) \equiv (\Delta a_1, \Delta b_1) * (0, 0)$, therefore for $k = 1$ we can consider a starting sequence of changes $\Delta\gamma = \underbrace{0000...00}_{2n}$ and a leader $(\Delta a_1, \Delta b_1) \neq (0, 0)$:

$$E_1 (\Delta\gamma) = e_{*,(\Delta a_1, \Delta b_1)} (\Delta\gamma) = \Delta x_1' \Delta x_2' ... \Delta x_{2n-1}' \Delta x_{2n}'\ ,$$

Since $(\Delta a_1, \Delta b_1) \neq (0, 0)$, none of the 2-bit elements in the encrypted string $E_1 (\Delta\gamma)$ can equal $(0, 0)$.

Therefore, there are several possible cases to consider:

1) If $(\Delta x_3', \Delta x_4') = (\Delta x_1', \Delta x_2')$, then we get the pattern $p = \Delta x_1' \Delta x_2'$, so $|p| = 2$ and $|s| = 0$. This implies that the string $E_1 (\Delta\gamma)$ has the form $p...p$, where $|p| = 2$.
2) If $(\Delta x_3', \Delta x_4') \neq (\Delta x_1', \Delta x_2')$, then:
   a) If $(\Delta x_5', \Delta x_6') = (x_1', x_2')$, then we get the pattern $p = \Delta x_1' \Delta x_2' \Delta x_3' \Delta x_4'$, so $|p| = 4$ and $|s| = 0$. Hence, $E_1 (\Delta\gamma)$ has the form $p...p$, where $|p| = 4$.
   b) If $(\Delta x_5', \Delta x_6') = (\Delta x_3', \Delta x_4')$, then we get the pattern $p = \Delta x_3' \Delta x_4'$, i.e. $|p| = 2$. Before the pattern occurs there is a sequence $s = \Delta x_1' \Delta x_2'$ with length 2.

(

Therefore, $E_1(\Delta\gamma)$ gets the form $sp...p$, where $|s| = 2$ and $|p| = 2$.

c) If $(\Delta x'_5, \Delta x'_6) \neq (\Delta x'_1, \Delta x'_2)$ and $(\Delta x'_5, \Delta x'_6) \neq (\Delta x'_3, \Delta x'_4)$, then
   i) If $(\Delta x'_7, \Delta x'_8) = (\Delta x'_1, \Delta x'_2)$, then we obtain the pattern $p = \Delta x'_1 \Delta x'_2 \Delta x'_3 \Delta x'_4 \Delta x'_5 \Delta x'_6$, so $|p| = 6$ and $|s| = 0$. Therefore, the encrypted string $E_1(\Delta\gamma)$ has the form $p...p$, where $|p| = 6$.
   ii) If $(\Delta x'_7, \Delta x'_8) = (\Delta x'_3, \Delta x'_4)$, then after the sequence $s = \Delta x'_1 \Delta x'_2$ of length 2, we get a pattern $p = \Delta x'_3 \Delta x'_4 \Delta x'_5 \Delta x'_6$ of length 4. This means that $E_1(\Delta\gamma)$ takes the form $sp...p$, where $|s| = 2$ and $|p| = 4$.
   iii) If $(\Delta x'_7, \Delta x'_8) = (\Delta x'_5, \Delta x'_6)$, then the encrypted string consists a sequence $s = \Delta x'_1 \Delta x'_2 \Delta x'_3 \Delta x'_4$ and afterwards a repeating pattern $p = \Delta x'_5 \Delta x'_6$. Therefore, the $E_1(\Delta\gamma)$ gets the form $sp...p$, where $|s| = 4$ and $|p| = 2$.

The above analysis yields that for $k = 1$, the string $E_1(\Delta\gamma)$ obtained when applying e-transformation as a single level encryptor over the input sequence of changes $\Delta\gamma$ is of form $sp...p$, where $|s| = 0, 2, 4$ and $|p| = 2, 4, 6$.

For $k > 1$, an arbitrary leader is used without any bit changes, thus the consecutive e-transformations of the initial sequence of changes $\Delta\gamma$ are applied for a leader $(0, 0)$:

$$E_k(\Delta\gamma) = e_{*,(0,0)}(E_{k-1}(\Delta\gamma)), \text{ for } k > 1 \ .$$

Let us assume that the statement in the theorem holds for k, $k > 1$, i.e. $E_k(\Delta\gamma)$ has the form $s_k p_k ... p_k$, where $|s_k| \leq |s_{k-1}| + 6|p_{k-1}|$ and $|p_k| = i|p_{k-1}|$, for $i = 2, 4, 6, 8$. Then for $k+1$ we will get that $E_{k+1}(\Delta\gamma) = s_{k+1} p_{k+1} ... p_{k+1}$, where $|s_{k+1}| \leq |s_k| + 6|p_k|$ and $|p_{k+1}| = i|p_k|$ for $i = 2, 4, 6, 8$. This result can be obtained in a similar way as before for $k = 1$, the only difference being that here $(0, 0)$ might occur as a 2-bit element of $E_k(\Delta\gamma)$. ■

Following this theorem, we are able to predict how the change of one bit in a given input binary string will affect the strings transformed by linear quasigroups of order 4. The bit change in the input string causes occurence of patterns with known form and length in the transformed strings, asserting the conclusion that the linear quasigroups are not suitable for cryprographic purposes in practical applications.

VI. Conclusions and future work

In this paper we investigated how a change of one bit in a given input binary string affects the strings obtained by applying E-transformation based on linear quasigroups of order 4. Our investigation showed that patterns with known form and length occur, making the linear quasigroups not suitable for cryptographic purposes. In addition, we also described some properties for linear quasigroups of order 4 and using them we were able to easily compute their number.

The ideas presented in this paper can be further extended for exploiting the properies of semilinear and quadratic quasigroups of order 4, as well as for their generalization on quasigroups of order 2^n.

References

[1] D. Gligoroski, V. Dimitrova, S. Markovski, *Quasigroups as Boolean Functions, Their Equation Systems and Gröbner Bases*, In: Sala, M., Mora, T., Perret, L., Sakata, S., Traverso, C. (eds.), Gröbner Bases, Coding, and Cryptography, pp. 415-420, Springer, Heidelberg, 2009

[2] S. Markovski, D. Gligoroski, V. Bakeva, *Quasigroup String Processing: Part 1*, Contributions, Section of Mathematical and Technical Sciences, pp. 13-28, Macedonian Academy of Sciences and Arts, XX 1-2, 1999

[3] S. Markovski, *Quasigroup String Processing and Applications in Cryptography*, In: 1st International Conference of Mathematics and Informatics for Industry, pp. 278-289, Thessaloniki, Greece, 2003

[4] D. Gligoroski, S. Markovski, *Quasigroup Transformations and Their Cryptographic Potentials*, talk at EIDMA Cryptography Working Group, Utrecht, The Netherlands, October 10, 2003

[5] A. Mileva, *Cryptographic Primitives and Their Applications*, PhD Thesis, Ss. Cyril and Methodius University, Skopje, Macedonia, 2010