# CORRELATION MATRICES AND PROP RATIO TABLES FOR QUASIGROUPS OF ORDER 4

Aleksandra Mileva
Faculty of Informatics,
"Goce Delcev" University
Stip, Republic of Macedonia

Smile Markovski
Faculty of Natural Sciences and Mathematics,
"Ss. Cyril and Methodius" University
Skopje, Republic of Macedonia

## ABSTRACT

Two basic attacks of cryptographic primitives are the linear and the differential cryptanalysis. To fight these attacks, building blocks of cryptographic primitives must have some desirable properties. Prop ratio tables and correlation matrices are important tools for linear and differential cryptanalysis, hence one have to take care on resistance of these attack when designing of cryptographic primitives. In this paper we present the analysis of correlation matrices and prop ratio tables of quasigroups of order 4 as building blocks.

## I. INTRODUCTION

Most of the successful attacks on block ciphers are different variants of linear or differential cryptanalysis. These attacks are also applicable, more or less successfully, on stream ciphers and cryptographic hash functions.

*Linear cryptanalysis*, introduced by M. Matsui [1], exploits the high probability occurrences of linear expressions involving plaintext bits, ciphertext bits and/or sub-key bits of cipher. It is a known plaintext attack, because the attacker must have information on a random set of plaintexts and corresponding ciphertexts (but cannot select plaintexts he wants to). The basic idea of this attack is to approximate the operation of a portion of the cipher with an expression that is linear, where the linearity refers to a mod-2 bitwise operation (XOR). If the cipher has a tendency for expression that hold with high or low probability, this is an evidence that the cipher exhibits non-random behaviour. If some expression hold with probability 1, then it is a perfect representation of the linear relationship in the cipher, and if some expression hold with probability 0, then it is a perfect representation of the affine relationship in the cipher, so the cipher has a catastrophic weakness.

*Differential cryptanalysis*, introduced by E. Biham and A. Shamir [2], is a chosen plaintext attack/chosen ciphertext attack, because the attacker is able to choose pairs of plaintexts such that there is a specified difference $\Delta X$ between members of the pair. For any particular cipher, the plaintext pair difference must be carefully chosen, if the attack has to be successful. The attacker then trace a path of highly probable difference through all rounds of the cipher until the difference of the corresponding ciphertext pairs $\Delta Y$, termed a *differential characteristic*, has suitable value. The resulting pair of differences ($\Delta X$, $\Delta Y$) is called a *differential*. In an ideally randomizing cipher, the probability that a particular output difference $\Delta Y$ occurs given a particular input difference $\Delta X$ is $1/2^n$, where $n$ is the number of input bits. Statistics of the differentials can discover where the cipher exhibits non-random behaviour resulting with recovering of the encryption key. A difference can be defined in several ways: XOR difference with eXclusive OR (XOR) operation ([2]); modular difference with integer modular subtraction operation (X. Wang and H. Yu [3] for hash functions), etc. Statistical properties of differentials depend upon the nature of non-linear components of the cryptographic primitive, usually S-boxes, so they must be examined.

There are many generalisations of differential and linear attacks, like*: truncated and higher order differentials* (L. Knudsen [4]), *impossible differential cryptanalysis* (A. Shamir [5]), *boomerang attack* (D. Wagner [6]), *rectangle attack* (E. Biham and all [7]), *differential-linear cryptanalysis* (M. E. Hellman and S. K. Langford [8]), *non-linear cryptanalysis* (L. Knudsen and M. Robshaw [9]), *chosen plaintext linear cryptanalysis* (L. Knudsen and J. M. Mathiassen [10]) etc.

Because of the importance of the linear and the differential cryptanalysis, new designs are expected to be accompanied by evidence that the algorithms are resistant to them. For example, AES with underlying Rijndael ([11,12]) have been proven secure against those attacks. So, if someone chooses to use quasigroups as non-linear component of some cryptographic primitive, the first thing he/she has to do is examination of its resistance to those attacks. One can use correlation matrices and prop ratio tables as tools for this assignment.

## II. CORRELATION MATRICES

The correlation matrix of Boolean mappings is a useful concept, introduced by J. Daemen and all [13], in demonstrating and proving properties of Boolean functions and mappings. This is useful because most components of cryptographic primitives are Boolean mappings. The elements of the correlation matrices consist of the correlation coefficients associated with linear combinations of input bits and linear combinations of output bits. Linear cryptanalysis can be seen as the exploitation of correlations between linear combinations of bits of different intermediate encryption values in a block cipher calculation, so correlation matrices are therefore the natural representation for the description and understanding of the mechanisms of linear cryptanalysis.

A *Boolean function* $f$ is a function $f : Z_2^n \to Z_2$. A *Boolean mapping* or *vector-valued Boolean function* $h$ is a mapping $h : Z_2^n \to Z_2^m$ and it can be decomposed into $m$ component Boolean functions ($h_0$, $h_1$, ..., $h_{m-1}$).

**Definition 1.** The *correlation coefficient* associated with a pair of Boolean functions $f(a)$ and $g(a)$ is denoted by $C(f, g)$ and is given by

$$C(f, g) = 2P[f(a) = g(a)] - 1 \quad (1)$$

The correlation coefficient ranges between $-1$ and 1 and if it is different from 0, the functions are said to be *correlated*.

A *selection vector* $w$ is a binary vector that selects all components $i$ of a vector that have $w_i = 1$. By $w^T a$ can be represented the linear combination of the components of a vector $a$ selected by $w$.

Let $\hat{f}(a)$ be a real-valued function defined by $\hat{f}(a) = (-1)^{f(a)}$, so in regards of a linear Boolean function, $w^T a$ becomes $(-1)^{w^T a}$. The bitwise sum of two Boolean functions corresponds to the bitwise product of their real-valued counterparts, i.e., $f(a) \hat{+} g(a) = \hat{f}(a)\hat{g}(a)$.

The *inner product* of real-valued functions is defined by,

$$\left\langle \hat{f}(a), \hat{g}(a) \right\rangle = \sum_a \hat{f}(a)\hat{g}(a) \quad (2)$$

It can easily be shown that

$$C(f, g) = 2^{-n} \left\langle \hat{f}(a), \hat{g}(a) \right\rangle$$

The real-valued functions corresponding to the linear Boolean functions form an orthogonal basis with respect to the defined inner product:

$$\left\langle (-1)^{u^T a}, (-1)^{v^T a} \right\rangle = 2^n \delta(u + v) \quad (3)$$

where $\delta(w)$ is the real-valued function equal to 1 if $w$ is the zero vector and 0 otherwise.

All correlation coefficients between linear combinations of input bits and that of output bits of the mapping $h$ can be arranged in a correlation $2^m \times 2^n$ – matrix $C^h$. The element $C_{uv}$ in the row $u$ and the column $v$ is equal to $C\left(u^T h(a), w^T a\right)$. The rows in this matrix can be interpreted as

$$(-1)^{u^T h(a)} = \sum_w C^h_{uw} (-1)^{w^T a} \quad (4)$$

In words, this means that the real-valued function corresponding to a linear combination of output bits can be written as a linear combination of the real-valued functions corresponding to a linear combination of input bits.

Correlation matrices can be applied to express correlations in iterated transformations, such as most block ciphers (see [13,14] for more information). Linear cryptanalysis are possible if there are predictable input-output correlations over all but a few rounds significantly larger than $2^{n/2}$, where n is the block length of the block ciphers [14]. An input-output correlation is composed of linear trails and, in order a crypto primitive to be resistant against this attack, a necessary condition is that there are no linear trails with correlation coefficients higher than $2^{n/2}$.

## III. PROP RATIO TABLES

Differential cryptanalysis exploits difference propagation and so, as a tool for its examination, one can uses $2^m \times 2^n$ prop ratio tables ([14]).

Let $a$ and $a^*$ be $n$-dimensional vectors with bitwise difference $a + a^* = a'$. Let $b = h(a)$, $b^* = h(a^*)$ and $b' = b + b^*$. Hence, the difference $a'$ propagates to the difference $b'$ through mapping $h$ and this can be represented by $(a' \dashv h \vdash b')$.

**Definition 2.** The *prop ratio* $R_p$ of a difference propagation $(a' \dashv h \vdash b')$ is given by

$$R_p(a' \dashv h \vdash b') = 2^{-n} \sum_a \delta\left(b' + h(a + a') + h(a)\right) \quad (5)$$

The prop ratio ranges between 0 and 1 and if a pair is chosen uniformly from the set of all pairs $(a, a^*)$ with $a + a^* = a'$, The equality $h(a) + h(a^*) = b'$ is true with some probability. It can be easily seen that $\sum_b R_p(a' \dashv h \vdash b') = 1$. If $R_p(a' \dashv h \vdash b') = 0$, the difference propagation $(a' \dashv h \vdash b')$ is called *invalid*. The input difference $a'$ and the output difference $b'$ are said to be *incompatible* through $h$. Difference propagation is composed of differential trails.

**Definition 3.** The *restriction weight* of a valid difference propagation $(a' \dashv h \vdash b')$ is the negative of the binary logarithm of the prop ratio, i.e.,

$$w_r(a' \dashv h \vdash b') = -\log_2 R_p(a' \dashv h \vdash b') \quad (6)$$

The restriction weight ranges between 0 and $n - 1$ and can be seen as the amount of information (in bits) that is restricted by $(a' \dashv h \vdash b')$ on $a$. If $h$ is linear, $w_r(a' \dashv h \vdash b') = 0$, so it can be seen that this difference propagation does not restrict or gives away information on $a$.

The correlation matrix and the prop ratio table of a mapping $h$ are connected through the following theorem (J. Daemen [14]).

**Theorem 1.** The table of prop ratios and the table containing the squared elements of the correlation matrix of a Boolean mapping $h$ are linked by,

$$R_p(a' \dashv h \vdash b') = 2^{-m} \sum_{u,w} (-1)^{w^T a' + u^T b'} C^2_{uw} \quad (7)$$

and, dually, by

$$C^2_{uw} = 2^{-n} \sum_{a',b'} (-1)^{w^T a' + u^T b'} R_p(a' \dashv h \vdash b') \quad (8)$$

Differential cryptanalysis attacks are possible if there are predictable difference propagations over all but a few rounds that have prop ratio significantly larger than $2^{1-n}$, where $n$ is the block length in the block ciphers [14]. To be resistant against this attack, necessary condition is that there are no differential trails with predicted prop ratio higher than $2^{1-n}$.

## IV. Prop Ratio Tables and Correlation Matrices of Quasigroups of Order 4

One can use quasigroups as non-linear building blocks of cryptographic primitives.

**Definition 4.** *A quasigroup* $(Q,*)$ is a groupoid (i.e., algebra with one binary operation * on the set $Q$) satisfying the law:

$$(\forall u,v \in Q)(\exists! x,y \in Q)(x*u = v \,\&\, u*y = v) \quad (9)$$

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

In this paper we examined the prop ratio tables and the correlation matrices of quasigroups of order 4. There are 576 different quasigroups of order 4 (we take $Q = Z_2^2$) and they can be ordered by lexicographic ordering (that corresponds to the rows of the main body of the multiplication table, taken upside down). Every quasigroup (Q, *) of order 4 can be represented as vector-valued Boolean function $h: Z_2^4 \to Z_2^2$ and for $(x_0, x_1)$, $(x_2, x_3)$ and $(y_0, y_1)$ in $Q = Z_2^2$, $h(x_0, x_1, x_2, x_3) = (x_0, x_1) * (x_2, x_3) = (y_0, y_1)$.

**Example 1.** The quasigroup of lexicographic order 113 is given by the next table

| * | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 3 | 1 | 2 |
| 1 | 3 | 0 | 2 | 1 |
| 2 | 1 | 2 | 0 | 3 |
| 3 | 2 | 1 | 3 | 0 |

and it has a prop ratio table given below (the input differences in integer representation are listed above and the output differences at the left)

| *h* | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 |
| 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 |
| 2 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 |
| 3 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 |

and a correlation matrix

| *h* | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| 2 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 |

There are 144 out of 576 quasigroups of order 4 that have a prop ratio table with all nontrivial difference propagations with prop ratio 1 and restriction weight of 0, and correlation matrix with every nonzero output selection vector correlated only to one input selection vector with correlation 1, as the quasigroup from Example 1. They correspond to the set of linear quasigroups in D. Gligoroski and all [15], and they are represented by their lexicographic order in the following list:

{1, 4, 11, 14, 21, 24, 26, 27, 37, 40, 43, 46, 51, 54, 57, 60, 70, 71, 77, 80, 82, 83, 92, 93, 100, 101, 110, 111, 113, 116, 126, 127, 132, 133, 138, 139, 146, 147, 157, 160, 163, 166, 169, 172, 179, 182, 189, 192, 196, 197, 203, 206, 212, 213, 222, 223, 228, 229, 234, 235, 243, 246, 252, 253, 259, 262, 269, 272, 274, 275, 284, 285, 292, 293, 302, 303, 305, 308, 315, 318, 324, 325, 331, 334, 342, 343, 348, 349, 354, 355, 364, 365, 371, 374, 380, 381, 385, 388, 395, 398, 405, 408, 411, 414, 417, 420, 430, 431, 438, 439, 444, 445, 450, 451, 461, 464, 466, 467, 476, 477, 484, 485, 494, 495, 497, 500, 506, 507, 517, 520, 523, 526, 531, 534, 537, 540, 550, 551, 553, 556, 563, 566, 573, 576}

Because of the nature of their prop ratio tables, their correlation matrices and their linearity, they should not be used as a non-linear building block of any cryptographic primitive.

**Example 2.** The quasigroup with lexicographic order 231 is given by the table

| * | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 0 |
| 1 | 2 | 3 | 0 | 1 |
| 2 | 0 | 1 | 2 | 3 |
| 3 | 3 | 0 | 1 | 2 |

and it has a prop ratio table

| *h* | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 0 | 0 | 0 | 0 | ½ | 0 | ½ | 0 | ½ | 0 | ½ | 0 | 0 | **1** | 0 |
| 1 | 0 | ½ | 0 | ½ | ½ | 0 | ½ | 0 | ½ | 0 | ½ | 0 | 0 | ½ | 0 | ½ |
| 2 | 0 | 0 | **1** | 0 | 0 | ½ | 0 | ½ | 0 | ½ | 0 | ½ | **1** | 0 | 0 | 0 |
| 3 | 0 | ½ | 0 | ½ | ½ | 0 | ½ | 0 | ½ | 0 | ½ | 0 | 0 | ½ | 0 | ½ |

One can see from this table that there are 3 nontrivial difference propagations with prop ratio 1 and restriction weight of 0. The input difference 0010 (=2) always propagates to output difference 10 (=2), 1000 (=12) always propagates to output difference 10 (=2) and the input difference 1110 (=14) always propagates to output difference 00 (=0). For example, the input difference 0010 is for the pairs: 0*0 = 1 and 0*2 = 3; 0*1 = 2 and 0*3 = 0; 1*0 = 2 and 1*2 = 0; 1*1 = 3 and 1*3 = 1; 2*0 = 0 and 2*2 = 2; 2*1 = 1 and 2*3 = 3; 3*0 = 3 and 3*2 = 1; and 3*1 = 0 and 3*3 = 2. Their output difference is 10.

The correlation matrix for this quasigroup is

| *h* | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | **-1** | 0 | 0 |
| 2 | 0 | 0 | 0 | 0 | 0 | 0 | ½ | ½ | 0 | 0 | -½ | ½ | 0 | 0 | 0 | 0 |
| 3 | 0 | 0 | 0 | 0 | 0 | 0 | -½ | ½ | 0 | 0 | -½ | -½ | 0 | 0 | 0 | 0 |

One can see that there exists a nonzero output selection vector (01) that is correlated only to one input selection vector

(1101) with correlation -1. This means that the second bit $y_1$ of the output can be represented by affine function from the input bits, i.e., $y_1 = 1 \oplus x_0 \oplus x_1 \oplus x_3$.

There are 432 out of 576 quasigroups of order 4 that have prop ratio table with 3 nontrivial difference propagations with prop ratio 1 and restriction weight of 0. Other nontrivial difference propagations are with prop ratio ½ and restriction weight of 1. They correspond to the set of nonlinear quasigroups in [15].

216 quasigroups of this set have correlation matrix with one nonzero output selection vector that is correlated only to one input selection vector with correlation -1, as quasigroup from Example 2, and they are represented in the following list:
{149, 150, 151, 152, 153, 154, 158, 159, 161, 162, 164, 165, 173, 174, 175, 176, 177, 178, 180, 181, 185, 186, 190, 191, 193, 194, 199, 200, 204, 205, 207, 208, 209, 210, 211, 214, 217, 218, 219, 220, 227, 230, 231, 232, 233, 236, 237, 238, 241, 242, 247, 248, 249, 250, 251, 254, 260, 261, 263, 264, 265, 266, 268, 273, 276, 277, 278, 283, 287, 288, 289, 290, 295, 296, 298, 301, 304, 306, 307, 311, 313, 314, 319, 320, 321, 322, 326, 332, 333, 335, 336, 337, 338, 339, 340, 347, 350, 351, 352, 353, 356, 357, 358, 361, 362, 367, 368, 372, 373, 375, 376, 377, 378, 379, 382, 389, 390, 391, 392, 393, 394, 396, 397, 403, 404, 406, 407, 409, 410, 415, 416, 418, 419, 421, 422, 427, 428, 429, 432, 433, 434, 435, 436, 443, 446, 447, 448, 449, 452, 455, 456, 457, 458, 459, 460, 465, 468, 471, 472, 475, 478, 479, 480, 481, 482, 487, 488, 491, 492, 493, 496, 498, 499, 501, 502, 509, 510, 511, 512, 515, 516, 518, 519, 521, 522, 524, 525, 529, 530, 535, 536, 538, 539, 541, 542, 547, 548, 549, 552, 557, 558, 559, 560, 561, 562, 564, 565, 571, 572, 574, 575}.

The others 216 quasigroups of this set of 432 nonlinear quasigroups have correlation matrix with one nonzero output selection vector that is correlated only to one input selection vector with correlation 1, as quasigroup from Example 3, and they are represented in the following list:
{2, 3, 5, 6, 7, 8, 9, 10, 12, 13, 15, 16, 17, 18, 19, 20, 22, 23, 25, 28, 29, 30, 31, 32, 33, 34, 35, 36, 38, 39, 41, 42, 44, 45, 47, 48, 49, 50, 52, 53, 55, 56, 58, 59, 61, 62, 63, 64, 65, 66, 67, 68, 69, 72, 73, 74, 75, 76, 78, 79, 81, 84, 85, 86, 87, 88, 89, 90, 91, 94, 95, 96, 97, 98, 99, 102, 103, 104, 105, 106, 107, 108, 109, 112, 114, 115, 117, 118, 119, 120, 121, 122, 123, 124, 125, 128, 129, 130, 131, 134, 135, 136, 137, 140, 141, 142, 143, 144, 145, 148, 155, 156, 167, 168, 170, 171, 183, 184, 187, 188, 195, 198, 201, 202, 215, 216, 221, 224, 225, 226, 239, 240, 244, 245, 255, 256, 257, 258, 270, 271, 279, 280, 281, 282, 291, 294, 299, 300, 309, 310, 316, 317, 327, 328, 329, 330, 341, 344, 345, 346, 359, 360, 363, 366, 369, 370, 383, 384, 386, 387, 399, 400, 401, 402, 412, 413, 423, 424, 425, 426, 437, 440, 441, 442, 453, 454, 462, 463, 469, 470, 473, 474, 483, 486, 489, 490, 503, 504, 505, 508, 513, 514, 527, 528, 532, 533, 543, 544, 545, 546, 554, 555, 567, 568, 569, 570}.

**Example 3.** The quasigroup with lexicographic order 109 is given by the table

| * | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 3 | 1 | 2 |
| 1 | 2 | 1 | 3 | 0 |
| 2 | 1 | 0 | 2 | 3 |
| 3 | 3 | 2 | 0 | 1 |

and it has a prop ratio table

| *h* | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | **1** | 0 | ½ | ½ | 0 | 0 | ½ | ½ | 0 |
| 1 | 0 | ½ | ½ | 0 | 0 | ½ | ½ | 0 | ½ | 0 | 0 | ½ | ½ | 0 | 0 | ½ |
| 2 | 0 | 0 | 0 | **1** | **1** | 0 | 0 | 0 | 0 | ½ | ½ | 0 | 0 | ½ | ½ | 0 |
| 3 | 0 | ½ | ½ | 0 | 0 | ½ | ½ | 0 | ½ | 0 | 0 | ½ | ½ | 0 | 0 | ½ |

and a correlation matrix

| *h* | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | **1** | 0 | 0 | 0 | 0 |
| 2 | 0 | 0 | 0 | 0 | 0 | ½ | ½ | 0 | 0 | 0 | 0 | 0 | 0 | ½ | -½ | 0 |
| 3 | 0 | 0 | 0 | 0 | 0 | -½ | ½ | 0 | 0 | 0 | 0 | 0 | 0 | ½ | ½ | 0 |

One can see that there exists nonzero output selection vector (01) that is correlated only to one input selection vector (1011) with correlation 1. This means that the second bit $y_1$ of output can be represented by linear function from the input bits, i.e., $y_1 = x_0 \oplus x_2 \oplus x_3$.

From viewpoint of the linear and the differential cryptanalysis, even those nonlinear quasigroups can be exploited for an attack if they are used only once. Namely, they do not fulfil the necessary condition for linear and differential cryptanalysis resistance: for prop ratio table the maximal prop ratio for every column, except the first one, should be ½, and for correlation matrix the maximal correlation coefficient for every row, except the first one, should be ½.

These weaknesses can be outperformed and resistance to those attacks can be gained by usage of quasigroup transformations, for example, e-transformations (see [16] and [17]). The usage of higher order quasigroups gives also better performances in respect of resistance to linear and differential attacks. It can be seen from Example 4, where we have presented the prop ratio table and the correlation matrix of random quasigroup of order 8. A quasigroup of order 8 can be represented as vector-valued Boolean function $h : Z_2^6 \to Z_2^3$.

**Example 4.** We examined the quasigroup of order 8, given by the table

| * | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| 0 | 5 | 2 | 4 | 6 | 1 | 7 | 0 | 3 |
| 1 | 6 | 0 | 7 | 5 | 3 | 1 | 4 | 2 |
| 2 | 2 | 7 | 1 | 4 | 0 | 6 | 3 | 5 |
| 3 | 7 | 4 | 0 | 1 | 2 | 3 | 5 | 6 |
| 4 | 3 | 1 | 6 | 0 | 7 | 5 | 2 | 4 |
| 5 | 1 | 3 | 5 | 2 | 4 | 0 | 6 | 7 |
| 6 | 0 | 5 | 2 | 3 | 6 | 4 | 7 | 1 |
| 7 | 4 | 6 | 3 | 7 | 5 | 2 | 1 | 0 |

and it has prop ratio table with maximum prop ratio 11/32 (without first column) and is not smaller than $2^{1-3} = 1/4$. Any nontrivial difference propagation is with prop ratio smaller or equal to 11/32 (Appendix A).

The correlation matrix has maximum correlation coefficient ½ (without first row) and is not smaller than $2^{-3/2} \approx 0.3536$. Any nonzero output selection vector is correlated with minimum 26 up to maximum 37 input selection vectors with correlation coefficient at most ½ (Appendix A).

## V. Conclusion

Two basic attacks of cryptographic primitives, especially of block ciphers, are the linear and the differential cryptanalysis; consequently, the new designs are expected to be accompanied by evidence that they are resistant to them. One can use as tools the prop ratio tables and the correlation matrices for examining of the non-linear parts of the cryptographic primitives. If someone decides to use quasigroups of order 4, he/she must consider their prop ratio tables and correlation matrices. There are 144 out from 576 quasigroups of order 4 that have linear properties, evident by their prop ratio tables and correlation matrices. The other 432 quasigroups have nonlinear properties, but if applied only once they still do not fulfil the necessary condition for linear and differential cryptanalysis resistance.

By using quasigroup transformations, for example, e-transformations, and quasigroups of higher order (or both), these weaknesses can be outperformed.

## References


[1] M. Matsui, "Linear Cryptanalysis Method for DES Cipher", *Advances in Cryptology, EUROCRYPT 1993*, pp. 386-397, 1993.

[2] E. Biham and A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystems", *Advances in Cryptology, EUROCRYPT 1990*, pp. 2-21, 1990.

[3] X. Wang, and H. Yu, "How to break MD5 and Other Hash Functions", *Advances in Cryptology – EUROCRYPT 2005, LNCS 3494*, Springer-Verlag, pp. 19-35, 2005

[4] L. Knudsen, "Truncated and Higher Order Differentials", *Fast Software Encryption 1994,* Springer-Verlag, pp. 196-211, 1994

[5] A. Shamir, "Impossible differential attacks", *CRYPTO 1998*, rump session, 1998

[6] D. Wagner, "The Boomerang Attack", *Fast Software Encryption 1999, LNCS 1636,* pp. 156-, 1999

[7] E. Biham, O. Dunkelman, N. Keller, "The Rectangle Attack, Rectangling the Serpent", *EUROCRYPT 2001, LNCS 2045*, Springer-Verlag, pp. 340-, 2001

[8] M. E. Hellman and S. K. Langford, "Differential-linear cryptanalysis", *Advances in Cryptology – CRYPTO 1994, LNCS 839*, Springer-Verlag, pp. 26-39, 1994

[9] L. Knudsen and M. Robshaw, "Non-linear approximations in linear cryptanalysis", *Advances in Cryptology – EUROCRYPT 1996, LNCS 1070*, Springer-Verlag, pp. 224-236, 1996

[10] L. Knudsen and J. M. Mathiassen, "A chosen plaintext linear attack on DES", *Fast Software Encryption, 7th International Workshop, NewYork, USA,* Springer-Verlag, 2000

[11] J. Daemen and V. Rijmen, "The Wide Trail Design Strategy", *Cryptography and Coding 2001, LNCS 2260,* Springer-Verlag, pp. 222-238, 2001

[12] J. Daemen and V. Rijmen , "The Design of Rijndael: AES – The Advances Encryption Standard", Springer-Verlag, 2002

[13] J. Daemen, R. Govaerts, J. Vandewalle, "Correlation matrices", *Fast Software Encryption 1994, LNCS 1008,* Springer-Verlag, pp. 275-285, 1995

[14] J. Daemen, "Cipher and Hash Function Design. Strategies based on Linear and Differential Cryptanalysis", *PhD thesis, Katholieke Universiteit Leuven,* March 1995

[15] D. Gligoroski, V. Dimitrova, S. Markovski, "Classification of Quasigroups as Boolean Functions, their Algebraic Complexity and Application of Gröbner Bases in Solving Systems of Quasigroup Equations", *Invited short-note for RISC Book Series*, *"Groebner, Coding, and Cryptography"*, Ed. M. Sala, Springer, 2007

[16] A. Mileva and S. Markovski, "*Correlation matrices and prop ratio tables for quasigroup transformations*" (to be printed)

[17] S. Markovski, D. Gligoroski, V. Bakeva, "*Quasigroup string processing: part 1*", Contributions, Sec. Math. Tech. Sci., MANU, XX 1-2 (1999), pp. 13- 28


## Appendix A

The prop ratio table of Example 4:

| *h* | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1/4 | 1/16 | 3/16 | 3/32 | 5/32 | 3/32 | 5/32 | 0 | 1/8 | 5/32 | 5/32 | 5/32 |
| 1 | 0 | 5/32 | 1/4 | 1/32 | 5/32 | 1/16 | 7/32 | 1/8 | 1/8 | 5/32 | 1/16 | 3/32 | 1/32 | 1/4 | 5/32 | 1/8 | 1/4 | 1/16 | 3/16 | 1/16 | 1/8 |
| 2 | 0 | 1/4 | 3/32 | 1/32 | 1/8 | 1/8 | 9/32 | 3/32 | 3/16 | 1/16 | 7/32 | 1/32 | 1/8 | 3/16 | 3/32 | 3/32 | 3/32 | 5/32 | 1/8 | 1/8 | 1/16 |
| 3 | 0 | 3/32 | 5/32 | 5/16 | 3/32 | 3/16 | 0 | 5/32 | 5/16 | 1/32 | 5/32 | 3/16 | 1/8 | 1/32 | 5/32 | 0 | 3/32 | 5/32 | 1/32 | 7/32 | 5/32 |
| 4 | 0 | 1/16 | 1/8 | 1/16 | 7/32 | 7/32 | 5/32 | 5/32 | 1/8 | 3/16 | 1/16 | 1/8 | 5/32 | 5/32 | 1/32 | 5/32 | 5/32 | 0 | 5/32 | 3/16 | 3/16 |
| 5 | 0 | 3/32 | 3/16 | 5/32 | 1/4 | 1/32 | 3/16 | 3/32 | 1/8 | 5/32 | 1/8 | 5/32 | 1/32 | 1/8 | 3/32 | 3/16 | 7/32 | 1/8 | 1/8 | 1/32 | 5/32 |
| 6 | 0 | 1/4 | 1/32 | 7/32 | 1/32 | 7/32 | 1/16 | 3/16 | 1/8 | 1/16 | 7/32 | 3/32 | 3/16 | 1/16 | 3/32 | 5/32 | 1/16 | 5/32 | 3/16 | 5/32 | 1/32 |
| 7 | 0 | 3/32 | 5/32 | 3/16 | 1/8 | 5/32 | 3/32 | 3/16 | 0 | 3/32 | 3/32 | 1/8 | 1/4 | 1/32 | 9/32 | 1/8 | 1/8 | 7/32 | 1/32 | 1/16 | 1/8 |

| | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | 41 | 42 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1/32 | 1/4 | 1/8 | 0 | 1/8 | 5/32 | 5/32 | 1/8 | 3/16 | 1/32 | 7/32 | 0 | 3/16 | 3/32 | 1/32 | 3/32 | **11/32** | 1/8 | 1/8 | 0 | 1/16 | 7/32 |
| 1 | 1/8 | 1/16 | 1/8 | 1/8 | 3/16 | 1/16 | 3/16 | 1/8 | 3/16 | 1/16 | 1/16 | 1/16 | 1/8 | 3/32 | 3/32 | 3/16 | 1/16 | 2/32 | 9/32 | 3/16 | 1/16 | 3/32 |
| 2 | 3/16 | 3/32 | 5/32 | 3/32 | 3/32 | 1/8 | 5/16 | 1/16 | 1/16 | 7/32 | 1/32 | 9/32 | 1/8 | 3/32 | 1/16 | 1/4 | 1/32 | 1/16 | 3/32 | 5/32 | 1/16 | 3/32 |

| | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 3 | 3/32 | 5/32 | 3/32 | 3/32 | 3/32 | 5/32 | 1/32 | 3/16 | 1/8 | 1/8 | 3/16 | 5/32 | 1/16 | 7/32 | 1/16 | 3/32 | 1/16 | 7/32 | 1/8 | 1/32 | 5/16 | 3/32 |
| 4 | 3/32 | 1/8 | 3/32 | 5/32 | 1/16 | 5/32 | 1/8 | 1/8 | 3/32 | 1/16 | 7/32 | 3/32 | 3/16 | 1/8 | 9/32 | 1/32 | 1/8 | 1/16 | 3/32 | 7/32 | 1/8 | 1/8 |
| 5 | 3/16 | 1/16 | 3/32 | 3/32 | 1/4 | 1/8 | 1/32 | 1/16 | 7/32 | 5/32 | 1/16 | 1/32 | 1/8 | 1/16 | 9/32 | 1/16 | 5/32 | 5/32 | 1/8 | 5/32 | 1/16 | 3/16 |
| 6 | 1/8 | 5/32 | 1/8 | 1/8 | 5/32 | 1/8 | 1/32 | 3/16 | 3/32 | 1/4 | 1/32 | 3/16 | 1/16 | 1/8 | 1/16 | 1/4 | 1/8 | 1/8 | 1/16 | 1/8 | 3/16 | 1/16 |
| 7 | 5/32 | 3/32 | 3/16 | 5/16 | 1/32 | 3/32 | 1/8 | 1/8 | 1/32 | 3/32 | 3/16 | 3/16 | 1/8 | 3/16 | 1/8 | 1/32 | 3/32 | 5/32 | 3/32 | 1/8 | 1/8 | 1/8 |

| | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 50 | 51 | 52 | 53 | 54 | 55 | 56 | 57 | 58 | 59 | 60 | 61 | 62 | 63 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 5/32 | 1/4 | 1/16 | 7/32 | 1/32 | 0 | 1/8 | 1/16 | 3/16 | 1/8 | 1/16 | 3/16 | 1/4 | 0 | 1/8 | 1/4 | 1/8 | 5/32 | 5/32 | 3/32 | 3/32 |
| 1 | 5/32 | 3/16 | 1/16 | 3/32 | 5/32 | 1/8 | 5/32 | 5/32 | 3/16 | 1/32 | 3/16 | 1/8 | 1/32 | 1/8 | 3/32 | 3/32 | 3/16 | 5/32 | 1/16 | 3/16 | 3/32 |
| 2 | 0 | 3/16 | 7/32 | 0 | 9/32 | 1/8 | 5/32 | 3/16 | 3/32 | 1/8 | 1/32 | 1/8 | 5/32 | 1/16 | 3/32 | 1/16 | **11/32** | 1/16 | 5/32 | 1/8 | 3/32 |
| 3 | 1/16 | 0 | 5/32 | 3/16 | 5/32 | 3/16 | 1/16 | 3/32 | 3/32 | 7/32 | 5/32 | 1/8 | 1/16 | 1/8 | 3/16 | 3/32 | 1/32 | 1/8 | 3/16 | 1/32 | 7/32 |
| 4 | 3/32 | 3/32 | 1/8 | 1/8 | 3/32 | 1/16 | 1/4 | 5/32 | 3/32 | 1/16 | 1/8 | 5/32 | 3/32 | 3/16 | 1/8 | 3/32 | 1/32 | 1/8 | 1/16 | 9/32 | 3/32 |
| 5 | 3/32 | 5/32 | 1/16 | 3/16 | 3/32 | 1/8 | 3/32 | 1/16 | 5/32 | 5/32 | 3/16 | 1/32 | 3/16 | 1/4 | 3/32 | 1/8 | 3/32 | 1/8 | 1/32 | 1/8 | 5/32 |
| 6 | 3/16 | 1/32 | 7/32 | 3/32 | 3/32 | 3/16 | 1/32 | 5/32 | 1/8 | 1/8 | 1/32 | 5/32 | 3/16 | 3/16 | 3/32 | 3/32 | 1/8 | 5/32 | 1/8 | 1/16 | 5/32 |
| 7 | 1/4 | 3/32 | 3/32 | 3/32 | 3/32 | 3/16 | 1/8 | 1/8 | 1/16 | 5/32 | 7/32 | 3/32 | 1/32 | 1/16 | 3/16 | 3/16 | 1/16 | 3/32 | 7/32 | 3/32 | 3/32 |

The correlation matrix of Example 4:

| *h* | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1/8 | -1/8 | 0 | 1/8 | 0 | -1/4 | 1/8 | 0 | 0 | -3/8 | -1/8 | 0 |
| 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | -1/8 | 0 | 1/8 | 0 | 1/8 | 0 | -1/8 | 0 | 0 | 1/8 | -1/8 | 0 |
| 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | -1/8 | 1/8 | -1/8 | -1/8 | 0 | 1/4 | 0 | 0 | 0 | 0 | -1/4 |
| 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1/4 | -1/8 | 1/8 | 1/8 | -1/8 | 1/4 | 0 | 0 | -1/4 | 1/4 | 0 | 0 |
| 5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1/8 | 1/4 | -1/8 | 0 | -1/8 | 1/4 | 1/8 | 0 | -1/4 | -1/8 | -1/8 | 0 |
| 6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1/8 | 1/8 | 0 | -1/8 | -1/4 | -1/4 | -1/8 | 0 | 0 | 1/8 | -1/8 | 0 |
| 7 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1/4 | 0 | 0 | 0 | 1/4 | 0 | 0 | 0 | 0 | 1/4 |

| | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | 41 | 42 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | -1/4 | 1/8 | 1/8 | 0 | -1/8 | -1/4 | -1/8 | 1/8 | 0 | 1/8 | -1/4 | 0 | 0 | 0 | 0 | 1/8 | -1/8 | 1/8 | -1/8 | 0 | -1/8 | 1/8 |
| 2 | 0 | -1/8 | 1/8 | 0 | 1/8 | -1/8 | 0 | 0 | -1/8 | 1/8 | 0 | 0 | 1/8 | -1/4 | -1/8 | 1/8 | -1/4 | -1/8 | 0 | 0 | **1/2** | 0 |
| 3 | 0 | 0 | -1/4 | 0 | 0 | -1/8 | 1/8 | 1/8 | 3/8 | 0 | 0 | 0 | 1/8 | 0 | -3/8 | 0 | -1/8 | 0 | -1/8 | 0 | -1/8 | -1/8 |
| 4 | -1/4 | 1/4 | 0 | 0 | 0 | -1/8 | -1/8 | -1/8 | -1/8 | 0 | 0 | 0 | 1/8 | 1/8 | 0 | -1/4 | -1/8 | -1/8 | -1/4 | 0 | 1/8 | 0 |
| 5 | 0 | -1/8 | 1/8 | 0 | 1/8 | 1/8 | 0 | -1/4 | -1/8 | -1/8 | 1/4 | 0 | 1/8 | 1/8 | 0 | 1/8 | 0 | 1/4 | -1/8 | 0 | -1/4 | 1/8 |
| 6 | 0 | -1/8 | 1/8 | 0 | -1/8 | -1/4 | 1/8 | 1/8 | -1/4 | -1/8 | 0 | 0 | 0 | 1/8 | -1/8 | 1/8 | 1/8 | -1/4 | 0 | 0 | -1/8 | 0 |
| 7 | 0 | 0 | 1/4 | 0 | 0 | -1/4 | 0 | 0 | 1/4 | 0 | 0 | 0 | 0 | -1/8 | 1/8 | -1/4 | 0 | 1/8 | 1/8 | 0 | 0 | -1/8 |

| | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 50 | 51 | 52 | 53 | 54 | 55 | 56 | 57 | 58 | 59 | 60 | 61 | 62 | 63 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 0 | -1/8 | -1/8 | 1/4 | 0 | 0 | 1/8 | -1/8 | 1/8 | 1/8 | 1/4 | 0 | 0 | 1/8 | 0 | -1/8 | 0 | -1/8 | -1/4 | -1/8 |
| 2 | 1/4 | -1/8 | 1/8 | -1/8 | -1/8 | 0 | 1/8 | 1/8 | 0 | -1/8 | 0 | 1/4 | 1/8 | 0 | 1/4 | 1/8 | -1/8 | 1/8 | 1/8 | 0 | 0 |
| 3 | 0 | -1/8 | 0 | 0 | -1/8 | 0 | 1/8 | -1/4 | -1/8 | 0 | 1/8 | 0 | 1/8 | 0 | -1/8 | 1/8 | -1/4 | -1/8 | 1/4 | 0 | 1/8 |
| 4 | -1/8 | -1/8 | 0 | 1/8 | 0 | 0 | -1/8 | -1/8 | 0 | -1/4 | 1/8 | 1/8 | -1/4 | 0 | -1/8 | 0 | 1/8 | 1/8 | 0 | -1/8 | 0 |
| 5 | 1/8 | -1/8 | 1/8 | 0 | 0 | 0 | -1/8 | 0 | -1/8 | 1/8 | 0 | 1/8 | 0 | 0 | 1/4 | 0 | -1/4 | 1/8 | 1/8 | 1/8 | 1/8 |
| 6 | -1/8 | -1/4 | -1/8 | 0 | 1/8 | 0 | 0 | 0 | 0 | -1/8 | -1/8 | 1/8 | 1/8 | 0 | 1/8 | -1/8 | 1/4 | -1/4 | 1/8 | 1/8 | 1/4 |
| 7 | -1/8 | -1/4 | 0 | 1/8 | -1/8 | 0 | 0 | 1/8 | 3/8 | 1/4 | -1/4 | 1/8 | -1/8 | 0 | 0 | -1/8 | -1/8 | 0 | 0 | 1/8 | 1/8 |