ANALYZING THE CRYPTOGRAPHIC PROPERTIES OF THE BOOLEAN REPRESENTATION OF QUASIGROUPS OF ORDER 4

Vesna Dimitrova Zlatka Trajcheska Marija Petkovska
Faculty of Computer Science and Engineering
"Ss. Cyril and Methodius" University,
Skopje, Macedonia

ABSTRACT

The advancement of cryptology includes various types of mathematical disciplines. Quasigroups are algebraic structures that are fit for cryptographic use and their cryptographic properties are intriguing. Looking into these properties we can classify the quasigroups based on different criteria and sort out the ones with best attributes for encryption and resistance to attacks. The Boolean representations of quasigroups allow us to find out more about their cryptographic properties. In this paper we will use those representations to analyze some of their properties and compare the results with previous research. The scope of this research are quasigroups of order 4.

I. INTRODUCTION

The quasigroups are plain algebraic structures which are suitable for cryptographic and coding purposes due to their large, exponentially growing number, and also their specific properties. Formally, a groupoid $(Q, *)$, where * is binary operation, is called a quasigroup if it satisfies:

$$(\forall\, a, b \in Q)(\exists!\, x, y \in Q)(x * a = b \wedge a * y = b) \qquad (1)$$

In this paper we are interested only in the quasigroups of order 4. We use lexicographic ordering [2] of the quasigroups of order 4. This is done by representing the quasigroup as a string of length n^2 which is obtained by concatenation of its rows. Then, these strings are ordered lexicographically and thus we acquire the ordering of quasigroups.

Another important issue that should be discussed before we pass to the main results of this paper is the Boolean representations of the quasigroups. Actually, we use the approach of representing the quasigroups as Boolean functions [2]. A Boolean function of n variables is defined as a function $f : \mathbb{F}_2^n \to \mathbb{F}_2$, where $\mathbb{F}_2 = \{0, 1\}$ is a two-element field [2][6]. Each Boolean function can be uniquely presented in its Algebraic Normal Form (ANF) [2][6], as a polynomial of n variables over the field $\mathbb{F}_2$ that has degree less or equal than 1 in each single variable, i.e.:

$$f(x_1, x_2, ..., x_n) = \sum_{I \subseteq \{1,...,n\}} a_I x^I \qquad (2)$$

where

$$x^I = \prod_{i \in I} x_i, x^{\emptyset} = 1 \; and \; a_I \in \{0, 1\}.$$

Every quasigroup $(Q, *)$ of order 2^n can be represented as a vector valued Boolean function $f : \{0, 1\}^{2n} \to \{0, 1\}^n$. The elements $x \in Q$ can be considered as binary vectors $x = (x_1, ..., x_n) \in \{0, 1\}^n$. Now, we represent the quasigroup in the following way: $\forall x, y \in Q$ we have that

$$x * y \equiv f(x_1, ..., x_{2n}) = (f_1(x_1, ..., x_{2n}), ..., f_n(x_1, ..., x_{2n}))$$

where

$$x = (x_1, x_2, ..., x_n), y = (x_{n+1}, x_{n+2}, ..., x_{2n})$$

and

$$f_i : \{0, 1\}^{2n} \to \{0, 1\}$$

are the Boolean function components of the previously defined f [2].

Because here we are considering only the quasigroups of order 4, it is clear that their Boolean representations will be composed of 2 Boolean functions, each with 4 arguments. For each quasigroup we will analyze the cryptographic properties of both Boolean functions.

There is a classification of quasigroups by their Boolean representations that is already presented in previous research (see [2]) that we will use for comparison with the new results. In this classification the quasigroups are categorized as linear or non-linear by Boolean representations. A quasigroup is called linear by Boolean representation if and only if all functions f_i for $i = 1, 2, ..., n$ are linear polynomials. On the other hand, a quasigroup is called non-linear by Boolean representation if there exist function f_i for some $i = 1, 2, ..., n$ which is not linear. There is also a specific subset of the non-linear quasigroups that are called pure non-linear quasigroups by Boolean representations. In these quasigroups all components are non-linear Boolean functions.

II. ANALYSIS OF THE CRYPTOGRAPHIC PROPERTIES

The Boolean functions have certain properties that are important of cryptological aspect. Thus it is necessary to determine how they are reflected on the quasigroups using their Boolean representations, or in other words, determine which quasigroups have the best cryptographic properties.

In this research we use the Boolean representations of quasigroups in Algebraic Normal Form. Besides that, we use the *boolfun* package [5], which is a convenient open source software that evaluates the cryptographic properties of Boolean functions. It is a package for the R language (a free software language and software environment for statistical computing and graphics).

For the time being, we analyzed several cryptographic properties

balance, correlation immunity and resiliency. The results will be presented further in this paper.

A. Algebraic immunity

In order to understand what is algebraic immunity we first need to define the term annihilator in $\mathcal{B}_n$ (the set of all Boolean functions that have n arguments). Namely, an annihilator of $f \in \mathcal{B}_n$ is a function $g \in \mathcal{B}_n$ such that $f(\overline{x}) \cdot g(\overline{x}) = 0$ for each $\overline{x} \in \mathbb{F}_2^n$. Now, the algebraic immunity of a Boolean function f, or $AI(f)$ is the smallest value of d such that $f(\overline{x})$ or $1 \oplus f(\overline{x})$ has a non-zero annihilator of degree d. [5][9]
The algebraic immunity is an indicator of the resistance to algebraic attacks for given Boolean function. It is proven [1] that $AI(f) \leq \lceil n/2 \rceil$, where $\lceil m \rceil$ is the smallest integer equal to or bigger than m. This means that the best result that we could get in the examination of the algebraic immunity of the quasigroups is 2. Since each quasigroup is represented by two Boolean functions f_1 and f_2, we will consider the algebraic immunity of each quasigroup as a pair $(AI(f_1), AI(f_2))$. This means that the best result we can get is $(2, 2)$ and the worst $(1, 1)$.
Figure 1 shows the distribution of quasigroups based on their algebraic immunity.

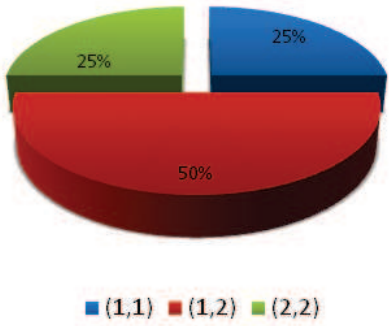

Figure 1: The distribution of quasigroups based on their algebraic immunity

B. Nonlinearity

The nonlinearity in this context (as a property of Boolean functions) is not the same with the nonlinearity by Boolean representation that was mentioned before, as a criteria for classification of the quasigroups. The term nonlinearity of a Boolean function in this subsection should be considered as follows [4].
Firstly, we need to define the term affine Boolean function. An affine Boolean function $h \in \mathcal{B}_n$ is a Boolean function in the form of:

$$h(x_1, x_2, ..., x_n) = \alpha_0 \oplus \alpha_1 x_1 \oplus \cdots \oplus \alpha_n x_n$$

where $\alpha_i \in \{0, 1\}$ for $i = 0, 1, ..., n$. The set of affine Boolean functions with n arguments is denoted by $\mathcal{A}_n$.
Now, the distance between two Boolean functions $f, g \in \mathcal{B}_n$ is defined as $d(f, g) = |\{x \mid f(x) \neq g(x)\}|$.
The nonlinearity of f (denoted by $NL(f)$) is the minimal distance between f and any $h \in \mathcal{A}_n$ [4][7]. It is proven that: we can get maximum $(6, 6)$ for nonlinearity of the Boolean representations of the quasigroups of order 4. However, the maximal nonlinearity that appears in the results is 4. This means that there is not a perfect nonlinear Boolean function among the Boolean representations.
Figure 2 shows the distribution of quasigroups based on their nonlinearity.

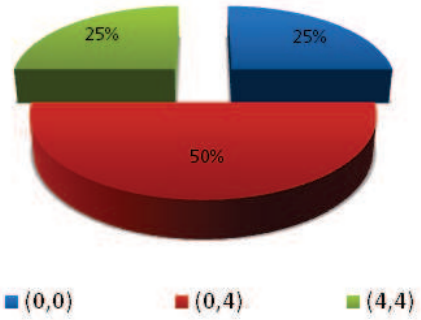

Figure 2: The distribution of quasigroups based on their nonlinearity

C. Balance, correlation immunity and resiliency

A Boolean function is balanced if its truth table contains as many zeros as ones. In our case, all quasigroups of order 4 are balanced.
Correlation immunity is a property of Boolean functions that is an indicator of their resistance to correlation attacks. A Boolean function is correlation immune of order m, if the distribution of its truth table is unaltered while fixing any m inputs [3]. The matter of finding the best quasigroups based on their Boolean representations for cryptographic purposes is impossible without making a compromise between the correlation immunity and the algebraic degree (the maximum number of variables in a monomial with non-zero coefficient) of the Boolean function (which implies its nonlinearity). Namely, a proposition introduced by Thomas Siegenthaler (see [8] and [3]) states that if f is a Boolean function defined on $\mathbb{F}_2^n$ with algebraic degree d and order of correlation immunity m, then $d + m \leq n$ with $m < n$.
Figure 3 shows the distribution of quasigroups based on their correlation immunity order.

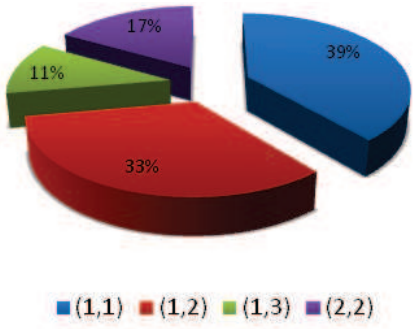

Figure 3: The distribution of quasigroups based on their correlation immunity order

balance and correlation immunity. A function $f \in \mathcal{B}_n$ is m-resilient if f is balanced and its correlation immunity order is m [5]. It is related to the number of input bits that do not give statistical information about the output bit. Since all of the Boolean representations of the quasigroups of order 4 are balanced, this means that if the Boolean function has correlation immunity order m then it is m-resilient. In other words, the distribution of quasigroups based on their resiliency matches the distribution of quasigroups based on their correlation immunity order.

Table 1 presents the classification of quasigroups based on their correlation immunity order.

Table 1: Classification of quasigroups by correlation immunity order

CI	Quasigroups
(1,1)	1, 2, 3, 5, 7, 9, 11, 12, 13, 15, 18, 19, 25, 28, 32, 34, 35, 44, 45, 47, 49, 51, 52, 53, 55, 57, 58, 59, 61, 63, 65, 68, 74, 75, 81, 84, 88, 91, 94, 96, 99, 102, 104, 105, 108, 114, 115, 117, 121, 124, 131, 134, 136, 137, 140, 144, 145, 148, 149, 155, 158, 159, 162, 167, 170, 171, 172, 174, 176, 178, 183, 185, 187, 189, 190, 191, 195, 198, 199, 201, 204, 205, 210, 215, 218, 219, 227, 230, 232, 233, 236, 238, 242, 244, 245, 246, 248, 250, 255, 257, 259, 260, 261, 263, 265, 268, 273, 276, 278, 283, 286, 288, 289, 291, 294, 299, 301, 304, 309, 312, 314, 316, 317, 318, 320, 322, 327, 329, 331, 332, 333, 335, 339, 341, 344, 345, 347, 350, 358, 359, 362, 367, 372, 373, 376, 378, 379, 382, 386, 387, 388, 390, 392, 394, 399, 401, 403, 405, 406, 407, 410, 415, 418, 419, 422, 428, 429, 432, 433, 437, 440, 441, 443, 446, 453, 456, 460, 462, 463, 469, 472, 473, 475, 478, 481, 483, 486, 489, 493, 496, 502, 503, 509, 512, 514, 516, 518, 519, 520, 522, 524, 525, 526, 528, 530, 532, 533, 542, 543, 545, 549, 552, 558, 559, 562, 564, 565, 566, 568, 570, 572, 574, 575, 576
(1,2)	4, 6, 8, 10, 14, 16, 17, 20, 21, 22, 23, 24, 26, 29, 31, 33, 37, 38, 50, 54, 56, 60, 62, 64, 66, 67, 69, 70, 71, 72, 73, 77, 78, 82, 85, 87, 97, 100, 103, 107, 109, 110, 123, 125, 126, 129, 132, 135, 147, 150, 152, 161, 163, 164, 169, 173, 175, 177, 179, 180, 181, 182, 184, 186, 188, 192, 194, 197, 200, 209, 211, 212, 220, 223, 224, 234, 237, 239, 241, 243, 247, 249, 251, 252, 253, 254, 256, 258, 262, 264, 266, 271, 272, 281, 284, 287, 290, 293, 296, 305, 306, 311, 313, 315, 319, 321, 323, 324, 325, 326, 328, 330, 334, 336, 338, 340, 343, 353, 354, 357, 365, 366, 368, 377, 380, 383, 385, 389, 391, 393, 395, 396, 397, 398, 400, 402, 404, 408, 413, 414, 416, 425, 427, 430, 442, 445, 448, 451, 452, 454, 467, 468, 470, 474, 477, 480, 490, 492, 495, 499, 500, 504, 505, 506, 507, 508, 510, 511, 513, 515, 517, 521, 523, 527, 539, 540, 544, 546, 548, 551, 553, 554, 555, 556, 557, 560, 561, 563, 567, 569, 571, 573
(1,3)	27, 30, 41, 43, 83, 86, 90, 93, 98, 101, 113, 119, 130, 133, 139, 142, 146, 151, 153, 157, 193, 196, 203, 207, 226, 229, 235, 240, 275, 280, 282, 285, 292, 295, 297, 302, 337, 342, 348, 351, 370, 374, 381, 384, 420, 424, 426, 431, 435, 438, 444, 447, 458, 464, 476, 479, 484, 487, 491, 494, 534, 536, 547, 550
(2,2)	36, 39, 40, 42, 46, 48, 76, 79, 80, 89, 92, 95, 106, 111, 112, 116, 118, 120, 122, 127, 128, 138, 141, 143, 154, 156, 160, 165, 166, 168, 202, 206, 208, 213, 214, 216, 217, 221, 222, 225, 228, 231, 267, 269, 270, 274, 277, 279, 298, 300, 303, 307, 308, 310, 346, 349, 352, 355, 356, 360, 361, 363, 364, 369, 371, 375, 409, 411, 412, 417, 421, 423, 434, 436, 439, 449, 450, 455, 457, 459, 461, 465, 466, 471, 482, 485, 488, 497, 498, 501, 529, 531, 535, 537, 538, 541

OTHER QUASIGROUPS PROPERTIES

Our interest is to compare the results that we obtained considering the algebraic immunity, nonlinearity, balance, correlation immunity and resiliency with results of previous research. In fact, we want to compare the classification of quasigroups based on the mentioned properties with the nonlinearity by Boolean representation (see [2]). The purpose of this is to analyze if there is a match between the classifications and to sort out the quasigroups with best attributes.

Table 2: Classification of quasigroups by algebraic immunity, nonlinearity and nonlinearity by Boolean representation

Class	Quasigroups
AI (1,1) NL (0,0) linear by Bool. repr.	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
AI (1,2) NL (0,4) nonlinear by Bool. repr.	2, 3, 5, 6, 12, 13, 15, 16, 17, 18, 19, 20, 25, 28, 29, 30, 35, 36, 38, 39, 41, 42, 47, 48, 52, 53, 55, 56, 58, 59, 61, 62, 65, 66, 67, 68, 75, 76, 78, 79, 81, 84, 85, 86, 89, 90, 95, 96, 97, 98, 99, 102, 105, 106, 109, 112, 117, 118, 119, 120, 121, 122, 125, 128, 129, 130, 131, 134, 141, 142, 143, 144, 145, 148, 151, 152, 153, 154, 155, 156, 164, 165, 167, 168, 170, 171, 175, 176, 177, 178, 183, 184, 187, 188, 190, 191, 193, 194, 195, 198, 201, 202, 207, 208, 211, 214, 215, 216, 217, 218, 221, 224, 225, 226, 231, 232, 233, 236, 239, 240, 244, 245, 247, 248, 249, 250, 255, 256, 257, 258, 260, 261, 267, 268, 270, 271, 277, 278, 279, 280, 281, 282, 283, 286, 291, 294, 295, 296, 297, 298, 299, 300, 306, 307, 309, 310, 316, 317, 319, 320, 321, 322, 327, 328, 329, 330, 332, 333, 337, 338, 341, 344, 345, 346, 351, 352, 353, 356, 359, 360, 361, 362, 363, 366, 369, 370, 375, 376, 379, 382, 383, 384, 386, 387, 389, 390, 393, 394, 399, 400, 401, 402, 406, 407, 409, 410, 412, 413, 421, 422, 423, 424, 425, 426, 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
AI (2,2) NL (4,4) pure nonlinear by Bool. repr.	7, 8, 9, 10, 22, 23, 31, 32, 33, 34, 44, 45, 49, 50, 63, 64, 69, 72, 73, 74, 87, 88, 91, 94, 103, 104, 107, 108, 114, 115, 123, 124, 135, 136, 137, 140, 149, 150, 158, 159, 161, 162, 173, 174, 180, 181, 185, 186, 199, 200, 204, 205, 209, 210, 219, 220, 227, 230, 237, 238, 241, 242, 251, 254, 263, 264, 265, 266, 273, 276, 287, 288, 289, 290, 301, 304, 311, 312, 313, 314, 323, 326, 335, 336, 339, 340, 347, 350, 357, 358, 367, 368, 372, 373, 377, 378, 391, 392, 396, 397, 403, 404, 415, 416, 418, 419, 427, 428, 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

A. Algebraic immunity, nonlinearity and nonlinearity by Boolean representation

These three classifications match perfectly and this is presented in Table 2. Actually, all the quasigroups that are linear by Boolean representations also have algebraic immunity (1,1)

Boolean representations also have algebraic immunity (1,2) or (2,1) and nonlinearity (0,4) or (4,0). Finally, all the quasigroups that are pure nonlinear by Boolean representations also have algebraic immunity (2,2) and nonlinearity (4,4).

B. Algebraic immunity, nonlinearity and nonlinearity by Boolean representation opposed to balance, correlation immunity and resiliency

It is important to compare the results of the classification presented in Table 1 with the one presented in Table 2. As we mentioned before compromise between nonlinearity and correlation immunity is inevitable. Also, we can say that the most important is the specific context of application of quasigroups, since the mentioned properties are almost inverse, so the question of selecting the best quasigroups for cryptographic purposes depends on the requirements we want it to fulfill. In other words, if we want resistance to algebraic attacks, we should use the pure non-linear quasigroups by Boolean representations, but they are the worst for resistance to correlation attacks. If we want resistance to correlation attacks, we should use the linear quasigroups, but they are the worst for resistance to algebraic attacks. We could use nonlinear quasigroups by Boolean representations, because they are not the worst for nonlinearity or correlation immunity, but they are not good enough for both resistance to algebraic attacks and resistance to correlation attacks.

Figure 4 shows the distribution of quasigroups based on their correlation immunity opposed to their nonlinearity.

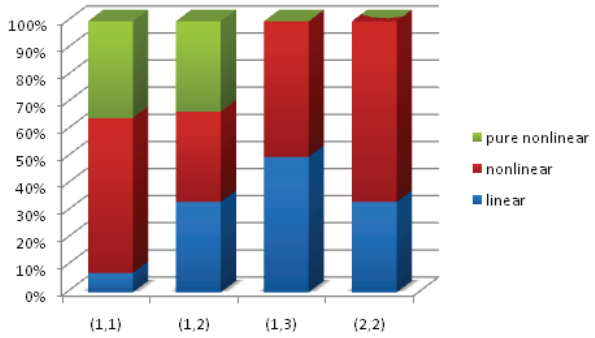

Figure 4: The distribution of quasigroups based on their correlation immunity opposed to their nonlinearity

IV. Conclusion

In this paper we have presented new properties of quasigroups relevant for cryptology using their Boolean representation. We have made two classifications: based on the algebraic immunity, nonlinearity and nonlinearity by Boolean representation on one hand and based on balance, correlation immunity and resiliency on the other hand.

To sum up, some of the quasigroups of order 4 have some good cryptographic properties, but none of them has perfect cryptographic properties. None of the Boolean functions of the Boolean representations of quasigroups has maximal which is expected since all of the Boolean representations of quasigroups are actually balanced Boolean functions, so they can't have maximal nonlinearity.

The quasigroups are good for application in cryptographic primitives, but not on their own. Their application should not be straight forward, but improved so that the cryptographic primitive they are applied in has higher nonlinearity, or higher correlation immunity, or it is prone to different types of attacks in general.

References

[1] Nicolas Courtois and Willi Meier, *Algebraic Attacks on Stream Ciphers with Linear Feedback*, Advances in Cryptology - Eurocrypt03, volume 2656 of Lecture Notes in Computer Science, pages 345359, Springer-Verlag, Berlin, Heidelberg, New York, 2003

[2] Vesna Dimitrova, *Quasigroup Processed Strings, their Boolean Representations and Application in Cryptography and Coding Theory*, PhD Thesis, Ss. Cyril and Methodius University, Skopje, Macedonia, 2010

[3] Baha Güçlü Dündar, *Cryptographic Properties of some Highly Nonlinear Balanced Boolean Functions*, Master's Degree Thesis, The Graduate School of Applied Mathematics, The Middle East Technical University, Ankara, Turkey, 2006

[4] Shouichi Hirose and Katsuo Ikeda *Nonlinearity Criteria of Boolean Functions*, KUIS Technical Report, KUIS-94-0002, 1994

[5] Frédéric Lafitte, *The boolfun Package : Cryptographic Properties of Boolean Functions*, 2012

[6] Klaus Pommerening, *Fourier Analysis of Boolean Maps*, A Tutorial, Mainz, 2005

[7] An Braeken, *Cryptographic Properties of Boolean Functions and S-Boxes*, PhD Thesis, Katholieke Universiteit Leuven, Leuven, Belgium, 2006

[8] Thomas Siegenthaler, *Correlation-immunity of nonlinear combining functions for cryptographic applications*, IEEE Transactions on Information Theory IT-30, pages 776780, 1984

[9] Xian-Mo Zhang and Josef Pieprzyk, Yuliang Zheng, *On Algebraic Immunity and Annihilators*, Information Security and Cryptology - ICISC 2006 volume 4296 of Lecture Notes in Computer Science, pages 65-80, Springer-Verlag, Berlin, Heidelberg 2006