Mathematical Society of the Republic of Moldova

Vladimir Andrunachievici Institute of Mathematics and Computer Science

Tiraspol State University

Information Society Development Institute

Proceedings IMCS-55

The Fifth Conference of Mathematical Society of the Republic of Moldova

dedicated to the 55th anniversary of the foundation of Vladimir Andrunachievici Institute of Mathematics and Computer Science

September 28 – October 1, 2019
Chisinau, Republic of Moldova, 2019

CZU [51+004](478)(082)
C 65

VLADIMIR ANDRUNACHIEVICI INSTITUTE OF MATHEMATICS AND COMPUTER SCIENCE
5, Academiei street, Chisinau, Republic of Moldova, MD 2028
Tel: (373 22) 72-59-82, Fax: (373 22) 73-80-27,
E-mail: imam@math.md
WEB address: http://www.math.md

Editors: Mitrofan Choban, Inga Titchiev.

Authors are fully responsible for the content of their papers.

Descrierea CIP a Camerei Naţionale a Cărţii

"Conference of Mathematical Society of the Republic of Moldova", (5 ; 2019 ; Chişinău). The Fifth Conference of Mathematical Society of the Republic of Moldova : dedicated to the 55th anniversary of the foundation of Vladimir Andrunachievici Institute of Mathematics and Computer Science, September 28 – October 1, 2019 Chisinau, Republic of Moldova : Proceedings IMCS-55 / ed.: Mitrofan Choban, Inga Titchiev. – Chişinău : Vladimir Andrunachievici Institute of Mathematics and Computer Science, 2019 (Tipogr. "Valinex"). – 346 p. : fig., tab.

Antetit.: Mathematical Vladimir Andrunachievici Inst. of Mathematics and Computer Science Soc. of the Rep. of Moldova, , Tiraspol State Univ. [et al.]. – Referinţe bibliogr. la sfârşitul art. – 150 ex.

ISBN 978-9975-68-378-4.

[51+004](478)(082)

ISBN 978-9975-68-378-4

This issue is supported by grant 19.00059.50.03A/MS, “IMCS-55 – The Fifth Conference of the Mathematical Society of Moldova – international conference dedicated to the 55th anniversary of the foundation of the Vladimir Andrunachievici Institute of Mathematics and Computer Science”.

Proceedings of the Fifth Conference of Mathematical Society of Moldova
IMCS-55, September 28 - October 1, 2019, Chisinau, Republic of Moldova

Investigation of Some Cryptographic Properties of the 8x8 S-boxes Created by Quasigroups

Aleksandra Stojanova, Dušan Bikov,
Aleksandra Mileva, Yunqing Xu

Abstract

We investigate several cryptographic properties in 8-bit S-boxes obtained by quasigroups of order 4 and 16 by different methods. The best produced S-boxes so far are regular and have algebraic degree 7, nonlinearity 98 (linearity 60), differential uniformity 8, and autocorrelation 88.

Keywords: Nonlinearity, differential uniformity.

1 Introduction

The main building blocks for obtaining confusion in all modern block ciphers are so called substitution boxes, or S-boxes. Designers of block ciphers very often choose S-boxes with special cryptographic properties, which means high nonlinearity (or low linearity), low differential uniformity, high algebraic degree, low autocorrelation and regularity (balance). The well known fact is that the bijective S-boxes are always regular. The AES S-box is the example of the best found 8x8 S-boxes, which is optimal with respect to most of the cryptographic properties (with algebraic degree 7, nonlinearity 112 (or linearity 32), differential uniformity 4, and autocorrelation 32).

Let $\mathbb{F}_2$ denote the Galois field with two elements, and let $\mathbb{F}_2^n$ denote the vector space of binary n-tuples over $\mathbb{F}_2$ with respect to addition $\oplus$ and scalar multiplication. An *$n-$ary Boolean function* is a function $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$. A *Boolean map* is a map $S : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$, $(m \geq 1)$. Every Boolean map S can be represented as: $S(x_1, \ldots, x_n) =$

$(f_1(x_1,\dots,x_n), f_2(x_1,\dots x_n),\dots,f_m(x_1,\dots,x_n))$. Each f_i can be represented in ANF as $f_i(x_1,x_2,\dots,x_n) = \bigoplus_{I\subseteq\{1,2,\dots,n\}} \alpha_I(\prod_{i\in I} x_i)$, where $\alpha_I \in \mathbb{F}_2$.

For all $\mathbf{x}\in\mathbb{F}_2^n$, the Walsh-Hadamard transform $W_f : \mathbb{F}_2^n \to \mathbb{R}$ of f is $W_f(\mathbf{x}) = \sum_{\mathbf{a}\in\mathbb{F}_2^n}(-1)^{f(\mathbf{a})\oplus\mathbf{a}\cdot\mathbf{x}}$, where $W_f(\mathbf{x})\in[-2^n,2^n]$ is known as a spectral Walsh coefficient, while the Autocorrelation transform of f is $ACT_f(\mathbf{x}) = \sum_{\mathbf{a}\in\mathbb{F}_2^n}(-1)^{f(\mathbf{a})\oplus f(\mathbf{a}\oplus\mathbf{x})}$, where $ACT_f(\mathbf{x})\in[-2^n,2^n]$ is known as a spectral autocorrelation coefficient. The *autocorrelation (absolute indicator)* of f is $AC(f) = \max\limits_{\mathbf{x}\in\mathbb{F}_2^n\setminus\mathbf{0}} |ACT_f(\mathbf{x})|$. The *nonlinearity* of a Boolean function f is defined as $NL(f) = 2^{n-1} - \frac{1}{2}\max\limits_{\mathbf{x}\in\mathbb{F}_2^n}|W_f(\mathbf{x})|$, while the *linearity* of f is defined as $L(f) = \max\limits_{\mathbf{x}\in\mathbb{F}_2^n}|W_f(\mathbf{x})|$. They are related by the equation $L(f) + 2NL(f) = 2^n$.

For Boolean map S we have the following definitions [2, 3]:

- Algebraic degree: $deg(S) = \max\limits_{i\in\{1,2,\dots,m\}}\{deg(f_i)\}$
- Nonlinearity: $NL(S) = \min\limits_{\mathbf{v}\in\mathbb{F}_2^m\setminus\{\mathbf{0}\}} NL(\mathbf{v}\cdot S)$
- Linarity: $L(S) = \max\limits_{\mathbf{v}\in\mathbb{F}_2^m\setminus\{\mathbf{0}\}} L(\mathbf{v}\cdot S)$
- Autocorrelation: $AC(S) = \max\limits_{\mathbf{v}\in\mathbb{F}_2^m\setminus\{\mathbf{0}\}} AC(\mathbf{v}\cdot S)$
- Differential uniformity: $\Delta(S) = \max\limits_{\mathbf{u}\in\mathbb{F}_2^n\setminus\{\mathbf{0}\},\mathbf{v}\in\mathbb{F}_2^m} |\{\mathbf{x}\in\mathbb{F}_2^n | S(\mathbf{x})\oplus S(\mathbf{x}\oplus\mathbf{u}) = \mathbf{v}\}|$

2 Main Results

Mihajloska and Gligoroski [1] constructed optimal 4x4 S-boxes from quasigroups of order 4, by using four e quasigroup transformations, alternating in normal and reverse mode (in a sense that they apply the string in reverse order – *oe*). We investigate several cryptographic properties of the 8x8 S-boxes obtained by similar constructions with quasigroups of order 4 and 16. In some of the constructions we combine quasigroup transformations with the addition of 2-, 4-, or 8-bit constants.

Method 1 – alternate use of e and oe transformations generated by quasigroups of order 4, like in [1]. Part of the results are given in Table 1, where $n$eoe type means that there are total of n quasigroup transformations.

Table 1. Method 1 – part of the results

Type	NL(S)	L(S)	$\Delta(S)$	AC(S)	deg(S)	No. of S
4eoe	64	128	24	256	7	192
8eoe	98	60	10	88,96,64	7	3360
10eoe	98	60	10	88	7	27392
12eoe	98	60	8 10	96 88	7	≥ 714 ≥ 84281

Method 2 – combination of e and oe transformations, with addition of 2-bit, 4-bit or 8-bit constants (some results in Table 2).

Table 2. Method 2 – part of the results

Type	NL(S)	L(S)	$\Delta(S)$	AC(S)	deg(S)	No. of S
1e_add2	0	256	256	256	4	4608
1e_add4	0	256	128	256	4	2816
1e_add8	4 32	248 192	132 164	256	7	6144 1536
1oe_add8	0	256	132	256	7	6144
2e_add2_oe_add2	0	256	128	256	6	98304
2e_add4_oe_add4	64	128	96	256	6	3072
4eoe_add2	64	128	24	256	7	768
4eoe_add8	88	80	24	160	7	16

Method 3 – as Method 1 and 2, but with one randomly generated shapeless quasigroup of order 16 (Fig. 1).

The best produced 8x8 S-box is obtained by 6 e quasigroup transformations, alternating in normal and reverse mode, from the quasigroup of order 16, with consecutive leaders (0, 3, 5, 3, 0, 0).

References

[1] H. Mihajloska, D. Gligoroski. *Construction of Optimal 4-bit S-boxes by Quasigroups of Order 4*. SECURWARE 2012, 2012.

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

Figure 1. Shapeless quasigroup of order 16.

Table 3. Method 3 – part of the results

Type	NL(S)	L(S)	$\Delta(S)$	AC(S)	deg(S)	No. of S
1e_add2	32	192	34	256	6	64
1e_add4	32 64	192 128	34 44	256	6	64 8
1e_add8	64	128	26	232-248	7	20
2e_add4_oe_add4	96 98	64 60	10 12,14	88 96-104	7	100 65536
2e_add8_oe	98	60	10	88	7	11
4eoe	98 94-90	60 68-76	10-12 8	88 96-112	7	15 5
6eoe	98	60	8	88 104	7	1 2

[2] K. Nyberg. *Perfect nonlinear S-boxes.* In: Davies, D.W. (Ed.) Eurocrypt 1991. LNCS, vol. 547, pp. 378–385. Springer, 1991.

[3] K. Nyberg. *S-boxes and round functions with controllable linearity and differential uniformity.* In: Preneel, B. (Ed.), FSE 1995. LNCS, vol. 1008, pp. 111–130. Springer Berlin Heidelberg, 1995.

Aleksandra Stojanova[1], Dušan Bikov[1], Aleksandra Mileva[1], Yunqing Xu[2]

[1]University Goce Delchev in Shtip, Republic of N. Macedonia
E–mails: {aleksandra.stojanova, dusan.bikov, aleksandra.mileva}@ugd.edu.mk

[2]Ningbo University, Peoples Republic of China
E–mail: xuyunqing@nbu.edu.cn