Weights on affine subspaces and some other cryptographic characteristics of Boolean functions of 5 variables

Alekseev E.K.[1], Kushchinskaya L.A.[2]

Abstract

Recently one new key recovery method for a filter generator was proposed. It is based on so-called planar approximations of such a generator. This paper contains the numerical part of the research of the Boolean functions properties which allow to protect the generator against this method. The main theoretical part of this research is presented at the CTCrypt 2019 conference.

Keywords: Boolean functions, affine classification, nonlinearity, algebraic degree, planar approximations

1 Introduction

In [1] a new key recovery method for a filter generator (see the definition in the next section) was proposed. It uses a planar approximation — a concept introduced in the same reference. This is the name of a set of planes sequences (cosets of some linear subspaces). In this case, the planes from the same sequence should be images of a certain single plane with respect to different degrees of the linear transformation used in the generator. The key can be recovered the more efficiently, the closer the filter function to some constant on the planes included in the approximation is. The problem of constructing such approximations is generally nontrivial (several special cases are considered in [1]).

The method mentioned above is not applicable for a function balanced on all planes of all dimensions. Indeed, there is no suitable trajectory for such a function. However, the non-existence of even such a function, which is balanced on all planes of at least one dimension was proved in [2]. However, the balancedness of the filter function on all planes of all dimensions is still not a necessary condition for the resistance of the filter generator to the method mentioned above and it can be relaxed. This is because the efficiency of the method depends not on the presence of unbalanced planes, but on their number and on how close the filter function f on such planes is to some constant. So the resistance of the generator is directly affected by the distribution of the weight of the filter function on the planes of different dimensions. More precisely, only the deviations of the weight on the planes from the half of the cardinality of these planes are important. Of particular interest is the number of planes which the filter function is balanced on.

[1]CRYPTO-PRO LCC, alekseev@cryptopro.ru

[2]Lomonosov Moscow State University, Faculty of Computational Mathematics and Cybernetics, lyudmila.kuschinskaja@yandex.ru

This paper contains the numerical part of the research of the Boolean functions properties mentioned above. For all Boolean functions of 5 variables we present the values of the number of the planes which the functions is unbalanced on. Also we present all possible values of the deviations mentioned above for the balanced Boolean functions of 5 variables. The main theoretical part of this research is presented at the CTCrypt 2019 conference [2].

2 Notation and statements

Let $\mathbb{F}_2$ be a field of 2 elements. Let $V_n = \mathbb{F}_2^n$ be a linear space of dimension n on the field $\mathbb{F}_2$. The set $supp(x) = \{i \in \{0, \ldots, n-1\} \,|\, x_i = 1\}$ is called a carrier of the vector $x = (x_0, \ldots, x_{n-1}) \in V_n$. The fact that $L \subseteq V_n$ is a subspace of the space V_n is denoted as follows: $L < V_n$. A coset of the subspace of this space shall be called a *plane* or *affine subspace* of the space V_n, and its dimension is the dimension of this subspace. Planes of dimension $n-1$ of the space V_n are called hyperplanes.

Any mapping $f : V_n \to \mathbb{F}_2$ is called a *Boolean function* f of n variables. The set of all Boolean functions of n variables is denoted by $\mathcal{F}_n$. The *carrier* of the function $f \in \mathcal{F}_n$ is the set $1_f = \{x \in V_n \,|\, f(x) = 1\}$. *The weight* $\mathrm{wt}\,(f)$ of the Boolean function $f \in \mathcal{F}_n$ is the power of its carrier. The function $f \in \mathcal{F}_n$ is *balanced* if $\mathrm{wt}\,(f) = 2^{n-1}$. The distance $\mathrm{dist}\,(f, g)$ between $f \in \mathcal{F}_n$ and $g \in \mathcal{F}_n$ is the value of $\mathrm{wt}\,(f \oplus g)$. The algebraic degree $\deg\,(f)$ of the Boolean function $f \in \mathcal{F}_n$ is the number of variables in the longest term in its Algebraic Normal Form (Zhegalkin polynomial) [4].

For $u \in V_n$ and $a \in \mathbb{F}_2$ let $l_{u,a}$ be the affine function $l_{u,a}(x) = \langle x, u \rangle \oplus a$ of n variables, where $\langle x, u \rangle$ is the scalar product of vectors x and u. Let l_u be the linear function $l_{u,0^n}$. The set $\{l_u(x) \oplus b | u \in V_n, b \in \mathbb{F}_2\}$ of affine Boolean functions of n variables is denoted as $\mathcal{A}_n$. Nonlinearity $\mathrm{nl}\,(f)$ of the Boolean function $f \in \mathcal{F}_n$ is the Hamming distance to the set of all affine functions $\mathcal{A}_n$: $\mathrm{nl}\,(f) = \mathrm{dist}\,(f, \mathcal{A}_n) = \min\limits_{l \in \mathcal{A}_n} \mathrm{dist}\,(f, l)$.

Let $\mathbb{N}_0$ be the set $\mathbb{N} \cup \{0\}$. A *filter generator* is a mapping from $\mathbb{N}_0 \times V_n$ to $\mathbb{F}_2$, which is determined by a non-degenerate linear mapping $A : V_n \to V_n$ and bt a balanced Boolean function $f \in \mathcal{F}_n$ called a *filter function* which assigns a number i and a vector $u^* \in V_n$ to the bit $z_i = f(A^i(u^*))$. The vector u^* is called a *key* or an *initial content* of the filter generator, and the sequence of bits $z_0, z_1, \ldots$ — *an output sequence* of the filter generator. The result of encrypting plaintext $x \in V_N$ based on the key $u^* \in V_n$ using a stream cipher based on the filter generator is the vector $y \in V_N$, such that $y_i = x_i \oplus z_i$ for any $i \in \{0, \ldots, N-1\}$. In other words, $y = x \oplus z$, where $z = (z_0, z_1, \ldots, z_{N-1}) \in V_N$ is the initial segment of length N of the output sequence of the filter generator.

Definition 2.1. *For any function $f \in \mathcal{F}_n$ a planar characteristic $\mathrm{pl}_d\,(f)$ of order d, $1 \leqslant d \leqslant n$, is the tuple of length $2^{d-1}+1$ whose w-th component is equal to the number of planes of dimension d on which the weight of the function f is equal to either $2^{d-1} - w$ or $2^{d-1} + w$ ($0 \leqslant w \leqslant 2^{d-1}$).*

Further we will say that a certain plane of the space V_n is f-balanced (f-unbalanced) for some function f if it is balanced (unbalanced) on this plane. If specifying a particular function f is not important or it is clear from the context which function f is in question, we will simply say about a balanced (unbalanced) plane.

The next section contains all possible values of the number of unbalanced planes for functions of 5 variables. And for balanced functions, the most interesting in terms of cryptography, all possible values of planar characteristics are given in Section 4. It was possible to obtain and present the indicated results in the convenient for analysis form because the planar characteristic is invariant relative to some generalization of the full affine group, namely, the group $\mathfrak{GA}(V_n)\mathfrak{H}_0$.

Let $\mathfrak{GA}(V_n)\mathfrak{H}_d$ be the set of a triples (A,b,h), where A is a nondegenerate $n \times n$-matrix over the field $\mathbb{F}_2$, $b \in V_n$, and h is a function from $\mathcal{F}_n$ such that $\deg(h) \leqslant d$. If $\alpha = (A,b,h) \in \mathfrak{GA}(V_n)\mathfrak{H}_d$, and $f \in \mathcal{F}_n$, then let f^α be a function of $\mathcal{F}_n$, such that $f^\alpha(x) = f(Ax \oplus b) \oplus h(x)$. Thus, each element of $\mathfrak{GA}(V_n)\mathfrak{H}_d$ corresponds to some transformation of the set $\mathcal{F}_n$. The set of such transformations is a group with respect to the superposition operation.

Statement 2.1. *[2] For any function $f \in \mathcal{F}_n$, any natural $d, 1 \leqslant d \leqslant n$, , and any element $\alpha \in \mathfrak{GA}(V_n)\mathfrak{H}_0$ the planar weight characteristics* $\mathrm{pl}_d(f)$ *and* $\mathrm{pl}_d(f^\alpha)$ *are equal.*

It is easy to see that the set $\mathcal{F}_n$ is split into the non-overlapping sets $\{f^\alpha \mid \alpha \in \mathfrak{GA}(V_n)\mathfrak{H}_d\}$ called equivalence classes with respect to $\mathfrak{GA}(V_n)\mathfrak{H}_d$ and denoted by $\{f\}_{\mathfrak{GA}(V_n)\mathfrak{H}_d}$. Any function from such a set is called a representative of this equivalence class (the entire equivalence class can be obtained using the action of elements of the group $\mathfrak{GA}(V_n)\mathfrak{H}_d$ on this function). The forming of the classification of the set $\mathcal{F}_n$ with respect to the group $\mathfrak{GA}(V_n)\mathfrak{H}_d$ is understood as the forming of a list that includes one representative of each existing equivalence classes. An example of such a classification can be found in [3].

The next section provides a classification of Boolean functions of 5 variables with respect to the group $\mathfrak{GA}(V_5)\mathfrak{H}_0$. For each of these functions the values of parameters are given, which coincide for all functions from the corresponding equivalence class. They are the power of the equivalence class, the algebraic degree, the nonlinearity and the number of unbalanced planes of dimensions $4,3,2,1$. From the definition of the group $\mathfrak{GA}(V_n)\mathfrak{H}_0$ it follows that the same equivalence class contains the same number of functions of weight w and $2^n - w$. Therefore, the entire classification is divided into 17 tables, each of which includes equivalence classes containing functions whose weight is equal to w or $2^5 - w$ for $w = 0, 1, \ldots, 16$. The tables show global and local numbering. The minimum and maximum values in the columns containing the numbers of unbalanced planes of various dimensions are in bold. The representative function itself is specified in the form of a truth table written in hexadecimal notation. The function values are written in the lexicographical order of its input arguments from left to right:

$$f(00000)f(00001)f(00010)\ldots f(11101)f(11110)f(11111).$$

For example, the function $f = 80018003$ takes the value 1 only on vectors $(00000), (01111), (10000), (11110), (11111)$.

3 Quantities of unbalanced planes

Functions of the weight of 0 and 32

№	$№_{\text{local}}$	f	$\lvert\{f\}_{\mathfrak{GA}(V_5)\mathfrak{H}_0}\rvert$	$\deg(f)$	$\mathrm{nl}(f)$	4	3	2	1
1	1	00000000	2	0	0	62	620	1240	496

Functions of the weight of 1 and 31

№	$№_{\text{local}}$	f	$\lvert\{f\}_{\mathfrak{GA}(V_5)\mathfrak{H}_0}\rvert$	$\deg(f)$	$\mathrm{nl}(f)$	4	3	2	1
2	1	00000001	64	5	1	62	620	1240	465

Functions of the weight of 2 and 30

№	$№_{\text{local}}$	f	$\lvert\{f\}_{\mathfrak{GA}(V_5)\mathfrak{H}_0}\rvert$	$\deg(f)$	$\mathrm{nl}(f)$	4	3	2	1
3	1	00000003	992	4	2	62	620	1225	436

Functions of the weight of 3 and 29

№	$№_{\text{local}}$	f	$\lvert\{f\}_{\mathfrak{GA}(V_5)\mathfrak{H}_0}\rvert$	$\deg(f)$	$\mathrm{nl}(f)$	4	3	2	1
4	1	00000007	9920	5	3	62	620	1198	409

Functions of the weight of 4 and 28

№	$№_{\text{local}}$	f	$\lvert\{f\}_{\mathfrak{GA}(V_5)\mathfrak{H}_0}\rvert$	$\deg(f)$	$\mathrm{nl}(f)$	4	3	2	1
5	1	0000000F	2480	3	4	62	613	1156	384
6	2	00000017	69440	4	4	62	619	1162	384

Functions of the weight of 5 and 27

№	$№_{\text{local}}$	f	$\lvert\{f\}_{\mathfrak{GA}(V_5)\mathfrak{H}_0}\rvert$	$\deg(f)$	$\mathrm{nl}(f)$	4	3	2	1
7	1	0000001F	69440	5	5	62	614	1114	361
8	2	00000117	333312	5	5	62	615	1120	361

Functions of the weight of 6 and 26

№	№$_{\text{local}}$	f	$\lvert\{f\}_{\mathfrak{GA}(V_5)\mathfrak{H}_0}\rvert$	deg (f)	nl (f)	4	3	2	1
9	1	0000003F	34720	4	6	**62**	**602**	**1057**	340
10	2	0000011F	833280	4	6	**62**	**609**	1069	340
11	3	00000356	55552	3	6	**62**	605	**1075**	340
12	4	00010117	888832	4	6	**62**	605	**1075**	340

Functions of the weight of 7 and 25

№	№$_{\text{local}}$	f	$\lvert\{f\}_{\mathfrak{GA}(V_5)\mathfrak{H}_0}\rvert$	deg (f)	nl (f)	4	3	2	1
13	1	0000007F	9920	5	7	**62**	**578**	**988**	321
14	2	0000013F	833280	5	7	**62**	597	1012	321
15	3	00000357	555520	5	7	**62**	**603**	1018	321
16	4	0001011F	4444160	5	7	**62**	594	1024	321
17	5	00010356	888832	5	7	**62**	585	**1030**	321

Functions of the weight of 8 and 24

№	№$_{\text{local}}$	f	$\lvert\{f\}_{\mathfrak{GA}(V_5)\mathfrak{H}_0}\rvert$	deg (f)	nl (f)	4	3	2	1
18	1	000000FF	1240	2	8	**59**	**536**	**904**	304
19	2	0000017F	238080	4	8	61	578	946	304
20	3	0000033F	104160	3	8	61	574	952	304
21	4	0000035F	1249920	4	8	61	**590**	958	304
22	5	0001013F	6666240	4	8	**62**	577	970	304
23	6	00010357	8888320	4	8	**62**	578	976	304
24	7	00030355	555520	3	8	**62**	578	976	304
25	8	00030356	3333120	4	8	**62**	564	**982**	304

Functions of the weight of 9 and 23

№	№$_{\text{local}}$	f	$\lvert\{f\}_{\mathfrak{GA}(V_5)\mathfrak{H}_0}\rvert$	deg (f)	nl (f)	4	3	2	1
26	1	000001FF	29760	5	7	**60**	550	**868**	289
27	2	0000037F	833280	5	7	**62**	569	892	289
28	3	00000777	555520	5	7	**62**	**575**	898	289
29	4	0001017F	1904640	5	9	**60**	557	910	289
30	5	0001033F	1666560	5	9	61	548	916	289
31	6	0001035F	19998720	5	9	61	559	922	289
32	7	00030357	13332480	5	9	**62**	555	928	289
33	8	00030567	13332480	5	9	**62**	551	**934**	289
34	9	00031556	4444160	5	9	**62**	**536**	**934**	289

Functions of the weight of 10 and 22

№	$№_{\text{local}}$	f	$\lvert\{f\}_{\mathfrak{GU}(V_5)\mathfrak{H}_0}\rvert$	$\deg(f)$	$\mathrm{nl}(f)$	4	3	2	1
35	1	000003FF	104160	4	6	60	542	**817**	276
36	2	0000077F	833280	4	6	**62**	**549**	829	276
37	3	0000177E	55552	3	6	**62**	545	835	276
38	4	000101FF	238080	4	8	61	536	841	276
39	5	0001037F	13332480	4	8	61	535	865	276
40	6	00010777	8888320	4	8	**62**	536	871	276
41	7	0003033F	166656	4	10	**57**	500	865	276
42	8	0003035F	9999360	4	10	59	527	877	276
43	9	0003056F	3333120	3	10	59	533	883	276
44	10	00030577	39997440	4	10	60	533	883	276
45	11	00031557	4444160	4	10	59	532	877	276
46	12	0003155B	39997440	4	10	61	524	889	276
47	13	00035556	634880	3	10	59	508	883	276
48	14	0003555A	1666560	4	10	61	**494**	889	276
49	15	00071356	5332992	4	10	**62**	530	**895**	276

Functions of the weight of 11 and 21

№	$№_{\text{local}}$	f	$\lvert\{f\}_{\mathfrak{GU}(V_5)\mathfrak{H}_0}\rvert$	$\deg(f)$	$\mathrm{nl}(f)$	4	3	2	1
50	1	000007FF	208320	5	5	60	514	**754**	265
51	2	0000177F	333312	5	5	**62**	**515**	760	265
52	3	000103FF	1666560	5	7	61	512	802	265
53	4	0001077F	13332480	5	7	60	509	814	265
54	5	0001177E	888832	5	7	**62**	500	820	265
55	6	0003037F	3333120	5	9	59	491	826	265
56	7	0003057F	19998720	5	9	61	507	832	265
57	8	00030777	26664960	5	9	58	503	838	265
58	9	0003155F	39997440	5	9	58	508	838	265
59	10	0003156F	39997440	5	9	60	504	844	265
60	11	00035557	634880	5	9	**62**	**515**	820	265
61	12	0003555B	13332480	5	9	60	494	844	265
62	13	0007133D	19998720	5	11	**57**	490	850	265
63	14	00071357	63995904	5	11	**57**	505	850	265
64	15	0007333C	333312	5	11	**57**	**430**	850	265
65	16	00073356	13332480	5	11	59	506	**856**	265

Functions of the weight of 12 and 20

№	№$_{\text{local}}$	f	$\lvert\{f\}_{\mathfrak{GA}(V_5)\mathfrak{H}_0}\rvert$	$\deg(f)$	$\mathrm{nl}(f)$	4	3	2	1
66	1	00000FFF	17360	3	4	56	461	**676**	256
67	2	000017FF	208320	4	4	**60**	467	682	256
68	3	000107FF	3333120	4	6	59	479	754	256
69	4	0001177F	5332992	4	6	57	475	760	256
70	5	000303FF	416640	3	8	55	457	772	256
71	6	000305FF	2499840	4	8	59	483	778	256
72	7	0003077F	19998720	4	8	59	470	790	256
73	8	0003157F	53329920	4	8	57	481	796	256
74	9	0003177D	6666240	3	8	51	481	796	256
75	10	0003177E	6666240	4	8	55	467	802	256
76	11	0003555F	6666240	4	8	59	**490**	790	256
77	12	0003556F	19998720	4	8	55	477	802	256
78	13	00070777	4444160	4	10	59	467	802	256
79	14	0007133F	9999360	4	10	59	477	802	256
80	15	0007135F	79994880	4	10	57	483	808	256
81	16	0007137D	79994880	4	10	55	474	814	256
82	17	0007333D	6666240	4	10	55	449	814	256
83	18	00073357	79994880	4	10	55	479	814	256
84	19	00073567	53329920	4	10	53	485	820	256
85	20	000F333C	27776	2	12	**47**	**335**	820	256
86	21	000F3355	1666560	3	12	**47**	455	820	256
87	22	000F3356	4999680	4	12	51	481	**826**	256
88	23	00171B56	5332992	3	12	**47**	485	820	256

Functions of the weight of 13 and 19

№	№$_{\text{local}}$	f	$\lvert\{f\}_{\mathfrak{GA}(V_5)\mathfrak{H}_0}\rvert$	deg (f)	nl (f)	4	3	2	1
89	1	00001FFF	69440	5	3	56	400	**598**	249
90	2	00010FFF	277760	5	5	**59**	436	694	249
91	3	000117FF	3333120	5	5	53	437	700	249
92	4	000307FF	4999680	5	7	57	434	742	249
93	5	000315FF	6666240	5	7	51	455	748	249
94	6	0003177F	26664960	5	7	54	446	754	249
95	7	0003557F	13332480	5	7	54	461	754	249
96	8	0003567F	13332480	5	7	48	452	760	249
97	9	0007077F	4444160	5	9	56	427	760	249
98	10	0007137F	79994880	5	9	53	454	772	249
99	11	00071777	53329920	5	9	56	455	778	249
100	12	0007177E	17776640	5	9	50	436	784	249
101	13	0007333F	3333120	5	9	**59**	453	766	249
102	14	0007335F	39997440	5	9	56	460	778	249
103	15	00073377	19998720	5	9	53	**469**	772	249
104	16	0007337D	39997440	5	9	50	446	784	249
105	17	0007356F	13332480	5	9	50	456	784	249
106	18	00073577	159989760	5	9	50	461	784	249
107	19	000F333D	555520	5	11	53	**392**	790	249
108	20	000F3357	19998720	5	11	53	452	790	249
109	21	000F3567	13332480	5	11	**47**	468	**796**	249
110	22	0017173D	13332480	5	11	53	442	790	249
111	23	00171B3D	39997440	5	11	**47**	463	**796**	249
112	24	00171B57	106659840	5	11	53	462	790	249

Functions of the weight of 14 and 18

№	№$_{\text{local}}$	f	$\lvert\{f\}_{\mathfrak{GL}(V_5)\mathfrak{H}_0}\rvert$	$\deg(f)$	$\mathrm{nl}(f)$	4	3	2	1
113	1	00003FFF	14880	4	2	48	**312**	**505**	244
114	2	00011FFF	1111040	4	4	47	389	637	244
115	3	00030FFF	416640	4	6	51	384	697	244
116	4	000317FF	9999360	4	6	49	411	709	244
117	5	000355FF	1666560	4	6	49	431	709	244
118	6	000356FF	1666560	3	6	**33**	427	715	244
119	7	0003577F	13332480	4	6	48	427	715	244
120	8	000707FF	1666560	4	8	49	378	721	244
121	9	000713FF	9999360	4	8	47	425	733	244
122	10	0007177F	53329920	4	8	49	422	745	244
123	11	0007337F	39997440	4	8	49	437	745	244
124	12	0007357F	79994880	4	8	48	438	751	244
125	13	00073777	53329920	4	8	48	448	751	244
126	14	0007377D	53329920	4	8	47	434	757	244
127	15	000F1777	13332480	4	10	51	434	757	244
128	16	000F177E	4444160	3	10	35	410	763	244
129	17	000F333F	277760	4	10	**53**	422	745	244
130	18	000F335F	9999360	4	10	51	449	757	244
131	19	000F337D	4999680	4	10	49	416	769	244
132	20	000F356F	3333120	3	10	35	**455**	763	244
133	21	000F3577	39997440	4	10	49	446	769	244
134	22	0017173F	19998720	4	10	51	429	757	244
135	23	0017177E	6666240	4	10	49	396	769	244
136	24	00171B3F	19998720	3	10	35	445	763	244
137	25	00171B5F	159989760	4	10	50	445	763	244
138	26	00171B7D	79994880	4	10	49	436	769	244
139	27	00171F3D	159989760	4	10	49	441	769	244
140	28	00173D3D	13332480	4	10	50	**455**	763	244
141	29	00173D5B	79994880	4	10	48	452	775	244
142	30	011717BC	6666240	4	12	47	443	**781**	244

Functions of the weight of 15 and 17

№	$№_{\text{local}}$	f	$\lvert\{f\}_{\mathfrak{GL}(V_5)\mathfrak{H}_0}\rvert$	$\deg(f)$	$\mathrm{nl}(f)$	4	3	2	1
143	1	00007FFF	1984	5	1	**32**	**200**	**400**	241
144	2	00013FFF	238080	5	3	39	333	568	241
145	3	00031FFF	1666560	5	5	39	369	664	241
146	4	000357FF	6666240	5	5	43	395	670	241
147	5	00070FFF	277760	5	7	35	308	688	241
148	6	000717FF	13332480	5	7	41	387	712	241
149	7	000733FF	4999680	5	7	41	407	712	241
150	8	000735FF	9999360	5	7	45	413	718	241
151	9	0007377F	79994880	5	7	44	419	724	241
152	10	00077777	4444160	5	7	44	434	724	241
153	11	0007777B	13332480	5	7	48	425	730	241
154	12	000F177F	13332480	5	9	42	405	730	241
155	13	000F337F	4999680	5	9	41	426	736	241
156	14	000F357F	19998720	5	9	45	437	742	241
157	15	000F3777	13332480	5	9	44	**443**	748	241
158	16	000F377D	13332480	5	9	48	424	754	241
159	17	0017177F	13332480	5	9	41	396	736	241
160	18	00171B7F	79994880	5	9	45	422	742	241
161	19	00171F3F	79994880	5	9	45	432	742	241
162	20	00171F77	159989760	5	9	44	428	748	241
163	21	00171F7E	53329920	5	9	48	414	754	241
164	22	00173D3F	79994880	5	9	44	438	748	241
165	23	00173D5F	159989760	5	9	48	434	754	241
166	24	00173D7E	39997440	5	9	48	439	754	241
167	25	001F373D	13332480	5	11	47	425	760	241
168	26	001F3757	106659840	5	11	47	440	760	241
169	27	0117177E	888832	5	11	47	335	760	241
170	28	011717BD	39997440	5	11	47	415	760	241
171	29	01171BD7	63995904	5	11	47	435	760	241
172	30	01171BFC	39997440	5	11	**51**	441	**766**	241

Functions of the weight of 16

№	$№_{\text{local}}$	f	$\lvert\{f\}_{\mathfrak{GA}(V_5)\mathfrak{H}_0}\rvert$	deg (f)	nl (f)	4	3	2	1
173	1	0000FFFF	62	1	0	**2**	**60**	**280**	240
174	2	00017FFF	15872	4	2	32	270	**490**	240
175	3	00033FFF	59520	3	4	16	326	616	240
176	4	00035FFF	833280	4	4	40	362	622	240
177	5	00071FFF	555520	4	6	32	342	682	240
178	6	000737FF	9999360	4	6	40	394	694	240
179	7	0007777F	8888320	4	6	44	410	700	240
180	8	000F0FFF	8680	2	8	**8**	**204**	664	240
181	9	000F17FF	1666560	4	8	36	366	706	240
182	10	000F33FF	312480	3	8	20	402	712	240
183	11	000F35FF	1249920	4	8	44	418	718	240
184	12	000F377F	9999360	4	8	42	425	730	240
185	13	000F7777	555520	3	8	26	**446**	736	240
186	14	000F777B	1666560	4	8	50	432	742	240
187	15	001717FF	833280	3	8	20	362	712	240
188	16	00171BFF	4999680	4	8	44	398	718	240
189	17	00171F7F	53329920	4	8	42	410	730	240
190	18	00173D7F	39997440	4	8	46	426	736	240
191	19	00173F3F	9999360	4	8	42	425	730	240
192	20	00173F5F	39997440	4	8	46	426	736	240
193	21	00173F7D	9999360	3	8	26	426	736	240
194	22	00173F7E	19998720	4	8	50	422	742	240
195	23	00177E7E	1666560	4	8	50	432	742	240
196	24	001F1F77	13332480	4	10	40	422	742	240
197	25	001F373F	9999360	4	10	40	432	742	240
198	26	001F375F	79994880	4	10	44	438	748	240
199	27	001F377D	39997440	4	10	48	429	754	240
200	28	0117177F	444416	4	10	32	360	730	240
201	29	011717BF	19998720	4	10	40	412	742	240
202	30	011717FE	6666240	4	10	48	384	754	240
203	31	01171BDF	53329920	4	10	44	428	748	240
204	32	01171BFD	79994880	4	10	48	424	754	240
205	33	01171FF6	39997440	4	10	48	429	754	240
206	34	01173DED	31997952	4	10	52	440	760	240
207	35	011F377C	1666560	3	12	32	400	760	240
208	36	011F37BC	1666560	4	12	**56**	436	**766**	240
209	37	011F37D6	5332992	3	12	32	440	760	240
210	38	033F566A	27776	2	12	32	240	760	240

4 Planar characteristics of balanced functions

Functions of the weight of 16 and their planar characteristics

№	f	dim	0	1	2	3	4	5	6	7	8
1	0000FFFF	1	256	240	-	-	-	-	-	-	-
		2	960	0	280	-	-	-	-	-	-
		3	560	0	0	0	60	-	-	-	-
		4	60	0	0	0	0	0	0	0	2
2	00017FFF	1	256	240	-	-	-	-	-	-	-
		2	750	280	210	-	-	-	-	-	-
		3	350	210	0	30	30	-	-	-	-
		4	30	30	0	0	0	0	0	2	0
3	00033FFF	1	256	240	-	-	-	-	-	-	-
		2	624	448	168	-	-	-	-	-	-
		3	294	224	56	32	14	-	-	-	-
		4	46	0	14	0	0	0	2	0	0
4	00035FFF	1	256	240	-	-	-	-	-	-	-
		2	618	456	166	-	-	-	-	-	-
		3	258	272	44	32	14	-	-	-	-
		4	22	32	6	0	0	0	2	0	0
5	00071FFF	1	256	240	-	-	-	-	-	-	-
		2	558	536	146	-	-	-	-	-	-
		3	278	210	96	30	6	-	-	-	-
		4	30	24	0	6	0	2	0	0	0
6	000737FF	1	256	240	-	-	-	-	-	-	-
		2	546	552	142	-	-	-	-	-	-
		3	226	276	84	28	6	-	-	-	-
		4	22	28	8	2	0	2	0	0	0
7	0007777F	1	256	240	-	-	-	-	-	-	-
		2	540	560	140	-	-	-	-	-	-
		3	210	294	84	26	6	-	-	-	-
		4	18	30	12	0	0	2	0	0	0
8	000F0FFF	1	256	240	-	-	-	-	-	-	-
		2	576	512	152	-	-	-	-	-	-
		3	416	0	192	0	12	-	-	-	-
		4	54	0	0	0	8	0	0	0	0
9	000F17FF	1	256	240	-	-	-	-	-	-	-
		2	534	568	138	-	-	-	-	-	-
		3	254	222	120	18	6	-	-	-	-
		4	26	28	0	4	4	0	0	0	0
10	000F33FF	1	256	240	-	-	-	-	-	-	-
		2	528	576	136	-	-	-	-	-	-

Continued on the next page

Functions of the weight of 16 and their planar characteristics

№	f	dim	0	1	2	3	4	5	6	7	8
		3	218	256	136	0	10	-	-	-	-
		4	42	0	16	0	4	0	0	0	0
11	000F35FF	1	256	240	-	-	-	-	-	-	-
		2	522	584	134	-	-	-	-	-	-
		3	202	288	108	16	6	-	-	-	-
		4	18	32	8	0	4	0	0	0	0
12	000F377F	1	256	240	-	-	-	-	-	-	-
		2	510	600	130	-	-	-	-	-	-
		3	195	290	116	14	5	-	-	-	-
		4	20	28	8	4	2	0	0	0	0
13	000F7777	1	256	240	-	-	-	-	-	-	-
		2	504	608	128	-	-	-	-	-	-
		3	174	312	120	8	6	-	-	-	-
		4	36	0	24	0	2	0	0	0	0
14	000F777B	1	256	240	-	-	-	-	-	-	-
		2	498	616	126	-	-	-	-	-	-
		3	188	292	124	12	4	-	-	-	-
		4	12	32	16	0	2	0	0	0	0
15	001717FF	1	256	240	-	-	-	-	-	-	-
		2	528	576	136	-	-	-	-	-	-
		3	258	224	104	32	2	-	-	-	-
		4	42	0	16	0	4	0	0	0	0
16	00171BFF	1	256	240	-	-	-	-	-	-	-
		2	522	584	134	-	-	-	-	-	-
		3	222	272	92	32	2	-	-	-	-
		4	18	32	8	0	4	0	0	0	0
17	00171F7F	1	256	240	-	-	-	-	-	-	-
		2	510	600	130	-	-	-	-	-	-
		3	210	278	104	26	2	-	-	-	-
		4	20	28	8	4	2	0	0	0	0
18	00173D7F	1	256	240	-	-	-	-	-	-	-
		2	504	608	128	-	-	-	-	-	-
		3	194	296	104	24	2	-	-	-	-
		4	16	30	12	2	2	0	0	0	0
19	00173F3F	1	256	240	-	-	-	-	-	-	-
		2	510	600	130	-	-	-	-	-	-
		3	195	290	116	14	5	-	-	-	-
		4	20	28	8	4	2	0	0	0	0
20	00173F5F	1	256	240	-	-	-	-	-	-	-
		2	504	608	128	-	-	-	-	-	-

Continued on the next page

Functions of the weight of 16 and their planar characteristics

№	f	dim	0	1	2	3	4	5	6	7	8
		3	194	296	104	24	2	-	-	-	-
		4	16	30	12	2	2	0	0	0	0
21	00173F7D	1	256	240	-	-	-	-	-	-	-
		2	504	608	128	-	-	-	-	-	-
		3	194	296	104	24	2	-	-	-	-
		4	36	0	24	0	2	0	0	0	0
22	00173F7E	1	256	240	-	-	-	-	-	-	-
		2	498	616	126	-	-	-	-	-	-
		3	198	284	116	20	2	-	-	-	-
		4	12	32	16	0	2	0	0	0	0
23	00177E7E	1	256	240	-	-	-	-	-	-	-
		2	498	616	126	-	-	-	-	-	-
		3	188	292	124	12	4	-	-	-	-
		4	12	32	16	0	2	0	0	0	0
24	001F1F77	1	256	240	-	-	-	-	-	-	-
		2	498	616	126	-	-	-	-	-	-
		3	198	284	116	20	2	-	-	-	-
		4	22	24	8	8	0	0	0	0	0
25	001F373F	1	256	240	-	-	-	-	-	-	-
		2	498	616	126	-	-	-	-	-	-
		3	188	292	124	12	4	-	-	-	-
		4	22	24	8	8	0	0	0	0	0
26	001F375F	1	256	240	-	-	-	-	-	-	-
		2	492	624	124	-	-	-	-	-	-
		3	182	302	116	18	2	-	-	-	-
		4	18	26	12	6	0	0	0	0	0
27	001F377D	1	256	240	-	-	-	-	-	-	-
		2	486	632	122	-	-	-	-	-	-
		3	191	286	124	18	1	-	-	-	-
		4	14	28	16	4	0	0	0	0	0
28	0117177F	1	256	240	-	-	-	-	-	-	-
		2	510	600	130	-	-	-	-	-	-
		3	260	210	120	30	0	-	-	-	-
		4	30	20	12	0	0	0	0	0	0
29	011717BF	1	256	240	-	-	-	-	-	-	-
		2	498	616	126	-	-	-	-	-	-
		3	208	276	108	28	0	-	-	-	-
		4	22	24	8	8	0	0	0	0	0
30	011717FE	1	256	240	-	-	-	-	-	-	-
		2	486	632	122	-	-	-	-	-	-

Continued on the next page

Functions of the weight of 16 and their planar characteristics

№	f	dim	0	1	2	3	4	5	6	7	8
		3	236	122	144	18	0	-	-	-	-
		4	14	28	16	4	0	0	0	0	0
31	01171BDF	1	256	240	-	-	-	-	-	-	-
		2	492	624	124	-	-	-	-	-	-
		3	192	294	108	26	0	-	-	-	-
		4	18	26	12	6	0	0	0	0	0
32	01171BFD	1	256	240	-	-	-	-	-	-	-
		2	486	632	122	-	-	-	-	-	-
		3	196	282	120	22	0	-	-	-	-
		4	14	28	16	4	0	0	0	0	0
33	01171FF6	1	256	240	-	-	-	-	-	-	-
		2	486	632	122	-	-	-	-	-	-
		3	191	286	124	18	1	-	-	-	-
		4	14	28	16	4	0	0	0	0	0
34	01173DED	1	256	240	-	-	-	-	-	-	-
		2	480	640	120	-	-	-	-	-	-
		3	180	300	120	20	0	-	-	-	-
		4	10	30	20	2	0	0	0	0	0
35	011F377C	1	256	240	-	-	-	-	-	-	-
		2	480	640	120	-	-	-	-	-	-
		3	220	240	144	16	0	-	-	-	-
		4	30	32	0	0	0	0	0	0	0
36	011F37BC	1	256	240	-	-	-	-	-	-	-
		2	474	648	118	-	-	-	-	-	-
		3	184	288	132	16	0	-	-	-	-
		4	6	32	24	0	0	0	0	0	0
37	011F37D6	1	256	240	-	-	-	-	-	-	-
		2	480	640	120	-	-	-	-	-	-
		3	180	300	120	20	0	-	-	-	-
		4	30	32	0	0	0	0	0	0	0
38	033F566A	1	256	240	-	-	-	-	-	-	-
		2	480	640	120	-	-	-	-	-	-
		3	380	240	0	0	0	-	-	-	-
		4	30	32	0	0	0	0	0	0	0

5 Conclusion

The results presented in this paper and in [2] mainly relate to the properties of the Boolean functions. At the same time, this study does not demonstrate the application of these results to obtain applied cryptographic propositions about the resistance of the filter generator. This is the main issue that the authors intend to make the main topic of their further research.

The authors thank Liliya Akhmetzyanova and Stanislav Smyshlyaev for their valuable comments regarding the English version of the article.

References

[1] Alekseev E., Kuschinskaya L. (2019). «Generalization of one method of a filter generator key recovery». Discrete Mathematics and Applications, 29(2), pp. 69-87. Retrieved 16 May. 2019, from doi:10.1515/dma-2019-0008.

[2] Alekseev E., Kuschinskaya L. «On the Properties of Boolean Functions Related to Planar Approximation of the Filter Generator». 8th Workshop on Current Trends in Cryptology (CTCrypt 2019), Pre-proceedings, 2019.

[3] Strazdin I.E., Affine classification of Boolean functions of five variables, Automat. Control Comput. Sci. 9 (1975), 1–7.

[4] Cusick T.W., Stanica P. «Cryptographic Boolean Functions and Applications». Academic Press, San Diego, 2009.