Michał APOLINARSKI

Poznań University of Technology, Institute of Control and Information Engineering

doi:10.15199/48.2016.12.58

IDEA key schedule evaluation based on cluster analysis

Abstract*. One of the most important feature of the key schedule in block ciphers is that the generated round keys should be independent, because it affects the quality of the block cipher cryptanalysis. In this articles we present quality evaluation of bit sequences generated by IDEA block cipher's key schedule according of various values of bit rotation used in algorithm. Received results of statistical tests in conjunction with the cluster analysis (Wroclaw taxonomy – dendritic method), allowed to point optimal rotation value for given design criteria.*

Streszczenie. *Jedną z głównych cech jaką powinien posiadać algorytm generowania kluczy rundowych w szyfrze blokowym to generowanie niezależnych kluczy rundowych, ponieważ wpływa to na jakość kryptoanalizy szyfru blokowego. W tym artykule przedstawiono ocenę jakości generowanych sekwencji bitowych przez algorytm generowania kluczy rundowych szyfru blokowego IDEA przy zastosowaniu różnych wartości rotacji bitowych. Otrzymane wyniki testów statystycznych w połączeniu z analizą skupień metodą taksonomii wrocławskiej (metodą dendrytową) pozwoliło na wskazanie optymalnej wartości rotacji dla założonego kryterium projektowego. (**Ocena algorytmu generowaniu kluczy rundowych IDEA oparta na analizie skupień**)*

Keywords: key schedule, block ciphers, cluster analysis, Wroclaw taxonomy, statistical tests suit, NIST 800-22, IDEA block cipher, IDEA key schedule.
Słowa kluczowe: algorytmy generowania kluczy rundowych, klucze rundowe, szyfry blokowe, analiza skupień, taksonomii wrocławska, metoda dendrytowa, dendryt, testy statystyczne, NIST 800-22, szyfr blokowy IDEA.

Introduction

Difficulty of cipher cryptanalysis is connected with quality of used in block cipher round keys. If key schedule generates good, independent round keys (without statistical defects) then cryptanalysis is more difficult - needs more resources [2,3].

Block cipher IDEA (International Data Encryption Algorithm) [4] operates on 64-bit length blocks using a 128-bit length master key. The encryption process is carried out in a 8.5 rounds using the 52 round keys of length 16 bits generated as follows:

- master key is divided into eight 16-bit round keys,
- then master key is rotated by 25 bits to the left (circular shift by 25 bits),
- then master key is divided once again into eight 16-bit round keys and so on until 52 round keys are generated.

The result of key schedule algorithm are 52 keys with a length of 16-bits marked as follows:

$$k_1^{(1)} \dots k_6^{(1)}, k_1^{(2)} \dots k_6^{(2)}, \dots, k_1^{(8)} \dots k_6^{(8)}, k_1^{(9)} \dots k_4^{(9)}$$

The aim of this research was to test all available variants of cyclic shift (bit rotation) in IDEA key schedule and define best rotation. So for the purposes of this research IDEA's key schedule was parameterized in such way that the rotation value could be variable from 1 to 127 bits. Then statistical test (described in next chapter) was performed on generated sequences for each key schedule variant. Next step was combined best statistical results and define hypothetical best rotation. Then using cluster analyze (Wroclaw taksonomy – dendric method) we grouped the similar results and determined the nearest rotation values to the hypothetical best one.

Statistical tests description

In this chapter we present the results of chosen NIST 800-22 statistical tests performed on bit sequences generated by different variants of bit rotation in IDEA block cipher key schedule. Due to the fact that IDEA generates 52 round keys, but single key is only 16 bit length, which gives 832 bit of cryptographic material as a single test sequence. That's why only four test could be performed without interfering in algorithm conception, it was [1]:

- Frequency Test (F) - checks the frequency of occurrences of 1 and 0 in sequence and verifies whether they correspond to the random sequence (recommended length. sample n > 100).
- Block Frequency Test (BF) - counting frequencies of the different *m*-bit blocks in test sequence and checks to see if they appear at the same frequency (recommended length. sample n > 100).
- Cumulative Sums Test (CS) - checks whether the sum of the bits (e.g. 1 bit is one and bit 0 is equal to -1) across the binders are not too large or too small, which would mean too great a number 0 or 1 in different parts of the query sequence (the recommended length. sample n > 100).
- Runs Test (R) - counts strings of ones and zeros of different lengths in the sequence and checks if these numbers correspond to the random sequence (recommended length. sample n > 100) .

We have perform mentioned four statistical test for each type o rotation from 1 to 127 bits. To perform all fifteen statistical test length of single tested sequence should be at least 10^6 bit length.

For testing purpose we have generated 1000 pseudorandom 128-bit length master keys that were input to our parameterized key schedule algorithm. The output was 127 files (one file for each of the variants of rotation). Each file was a sequence of 1000 bits streams of 832 bits (52 x 16 bits round keys) - a single sequence was delivered from concatenating 52 round keys. Those 127 system files served as an input for NIST 800-22 statistical suit.

Results of statistical tests

The result of tests was 127 sets of data shown in table 1. The values shown in the table represent the proportion of samples that meet the individual tests (the best results were marked in bold). In the last three rows are set highest value ratio, which defined hypothetical best rotation according to our criterion (it can be counted as 128th test result), the average value of the results x_j *as:*

$$x_j = \frac{\sum_{1}^{128} x_{ij}}{128}$$

where: x_{ij} – test result, x_j – avg. test result, , and i = 1…128, j = 1…5
and standard deviation s_j as:

$$s_j = \sqrt{\frac{\sum_{1}^{128}(x_{ij} - x_j)^2}{127}}$$

where: s_j – standard deviation, x_{ij} – test result, x_j – avg. test result, , and i = 1…128, j = 1…5

Table 1. Results of NIST 800-22 tests

rotation by	F	BF	CS (forw.)	CS (rev.)	R
1	0,691	0,894	0,708	0,715	0,610
2	0,690	0,890	0,709	0,704	**0,622**
3	0,690	0,900	0,707	0,706	0,603
4	0,684	0,899	0,709	0,704	0,603
5	0,690	0,901	0,720	0,710	0,593
6	0,696	0,911	**0,722**	0,710	0,597
7	0,700	0,917	0,718	0,720	0,593
8	0,702	0,915	0,714	0,716	0,601
9	0,700	0,913	0,708	0,714	0,595
10	0,692	0,913	0,714	0,702	0,594
11	0,682	0,907	0,709	0,703	0,601
12	0,692	0,907	0,705	0,696	0,600
13	0,690	0,915	0,712	0,704	0,584
14	0,691	0,905	0,706	0,699	0,598
15	0,688	0,913	0,702	0,698	0,594
16	0,684	0,913	0,708	0,706	0,604
17	0,684	0,917	0,702	0,704	0,604
18	0,681	0,917	0,704	0,699	0,604
19	0,686	0,913	0,702	0,702	0,600
20	0,691	0,922	0,702	0,704	0,598
21	0,691	0,922	0,704	0,709	0,611
22	0,689	0,919	0,712	0,707	0,600
23	0,684	0,914	0,716	0,706	0,612
24	0,692	0,915	0,710	0,706	0,616
25	0,686	0,915	0,704	0,698	0,603
26	0,684	0,917	0,708	0,704	0,603
27	0,694	0,919	0,710	0,712	0,599
28	0,700	0,913	**0,722**	0,714	0,601
29	**0,704**	0,913	0,714	0,716	0,592
30	0,700	0,913	0,710	0,712	0,593
31	0,688	0,917	0,712	0,704	0,594
32	0,688	0,909	0,708	0,700	0,591
33	0,684	0,909	0,711	0,699	0,597
34	0,688	0,909	0,710	0,701	0,592
35	0,685	0,909	0,708	0,701	0,596
36	0,685	**0,923**	0,700	0,697	0,603
37	0,674	0,915	0,706	0,700	0,604
38	0,690	0,915	0,700	0,698	0,608
39	0,683	0,919	0,706	0,695	0,602
40	0,680	0,917	0,700	0,700	0,600
41	0,692	0,921	0,702	0,706	0,603
42	0,685	0,922	0,710	0,705	0,604
43	0,685	0,921	0,708	0,701	0,608
44	0,693	0,917	0,714	0,715	0,614
45	0,692	0,919	0,714	0,704	0,604
46	0,690	0,912	0,704	0,706	0,612
47	0,684	0,913	0,710	0,704	0,603
48	0,688	0,915	0,710	0,710	0,599
49	0,696	0,915	0,718	0,714	0,601
50	0,694	0,911	0,716	0,718	0,599
51	0,700	0,911	0,708	0,714	0,603
52	0,694	0,913	0,712	0,706	0,595
53	0,688	0,909	0,708	0,700	0,595
54	0,686	0,913	0,713	0,703	0,607
55	0,688	0,911	0,708	0,703	0,588
56	0,687	0,911	0,714	0,702	0,592
57	0,687	0,919	0,704	0,699	0,600
58	0,686	0,917	0,704	0,704	0,600
59	0,688	0,911	0,700	0,702	0,612
60	0,684	0,903	0,702	0,706	0,594
61	0,682	0,893	0,702	0,699	0,596
62	0,692	0,894	0,706	0,708	0,616
63	0,691	0,889	0,706	0,707	0,615
64	0,699	0,886	0,708	0,711	0,618
65	0,691	0,894	0,708	0,715	0,604
66	0,690	0,890	0,707	0,704	0,617
67	0,690	0,900	0,705	0,706	0,603
68	0,684	0,899	0,709	0,704	0,603
69	0,690	0,901	0,720	0,710	0,603
70	0,696	0,911	0,718	0,710	0,597
71	0,700	0,917	0,716	**0,720**	0,605
72	0,702	0,915	0,712	0,716	0,602
73	0,700	0,913	0,704	0,714	0,594
74	0,692	0,913	0,712	0,702	0,604
75	0,682	0,907	0,705	0,703	0,605
76	0,692	0,907	0,701	0,696	0,598
77	0,690	0,915	0,706	0,704	0,584
78	0,691	0,905	0,704	0,699	0,600
79	0,688	0,913	0,702	0,700	0,594
80	0,684	0,913	0,706	0,706	0,598
81	0,684	0,917	0,700	0,704	0,604
82	0,681	0,917	0,702	0,699	0,596
83	0,686	0,913	0,698	0,702	0,601
84	0,691	0,922	0,696	0,704	0,594
85	0,691	0,922	0,698	0,709	0,613
86	0,689	0,919	0,708	0,707	0,604
87	0,684	0,914	0,712	0,706	0,613
88	0,692	0,915	0,710	0,706	0,607
89	0,686	0,915	0,704	0,698	0,602
90	0,684	0,917	0,712	0,704	0,595
91	0,694	0,919	0,710	0,712	0,595
92	0,700	0,913	0,720	0,714	0,595
93	**0,704**	0,913	0,714	0,716	0,591
94	0,700	0,913	0,710	0,712	0,596
95	0,688	0,917	0,712	0,704	0,592
96	0,688	0,909	0,704	0,700	0,593
97	0,684	0,909	0,709	0,699	0,588
98	0,688	0,909	0,710	0,701	0,582
99	0,685	0,909	0,706	0,701	0,595
100	0,685	**0,923**	0,700	0,697	0,600
101	0,674	0,915	0,704	0,700	0,598
102	0,690	0,915	0,702	0,698	0,606
103	0,683	0,919	0,704	0,695	0,604
104	0,680	0,917	0,700	0,700	0,596
105	0,692	0,921	0,704	0,706	0,607
106	0,685	0,922	0,708	0,705	0,601
107	0,685	0,921	0,706	0,701	0,604
108	0,693	0,917	0,712	0,715	0,612
109	0,692	0,919	0,712	0,704	0,605
110	0,690	0,912	0,702	0,706	0,606
111	0,684	0,913	0,712	0,704	0,603
112	0,688	0,915	0,716	0,710	0,597
113	0,696	0,915	**0,722**	0,714	0,601
114	0,694	0,911	0,720	0,718	0,607
115	0,700	0,911	0,712	0,714	0,597
116	0,694	0,913	0,714	0,706	0,598
117	0,688	0,909	0,706	0,700	0,596
118	0,686	0,913	0,713	0,703	0,601
119	0,688	0,911	0,708	0,703	0,590
120	0,687	0,911	0,712	0,702	0,588
121	0,687	0,919	0,704	0,699	0,597
122	0,686	0,917	0,706	0,704	0,596
123	0,688	0,911	0,704	0,702	0,601
124	0,684	0,903	0,706	0,706	0,606
125	0,682	0,893	0,704	0,699	0,602
126	0,692	0,894	0,708	0,708	0,610
127	0,691	0,889	0,708	0,707	0,601
128 - MAX	**0,7040**	**0,9230**	**0,722**	**0,720**	**0,622**
AVG	0,689477	0,911695	0,708391	0,705430	0,600875
standard deviation	0,005934	0,008127	0,005672	0,005964	0,007470

The charts show a histogram for each test. Figure 1 shows frequency test results of the bit rate for which the highest value (0.7040) was obtained with a rotation by 29 or 93 bits.

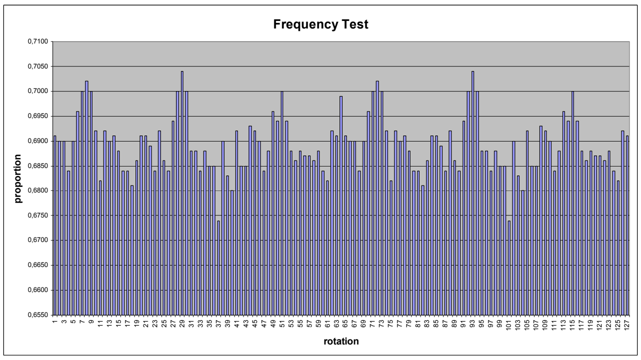

Fig.1. Frequency Test histogram

In the block frequency test (fig. 2) highest ratio value (0.923) was obtained with a rotation of 36 or 100 bits.

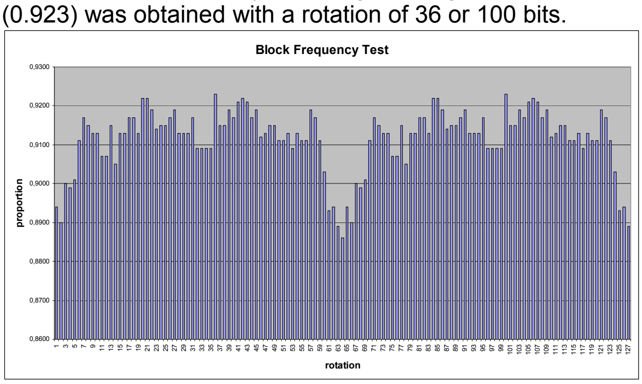

Fig.2. Block Frequency Test histogram

In the cumulative sums test for the version of "forward" the highest value ratio (0.722) obtained with a rotation of 6, 28, 113 bits.

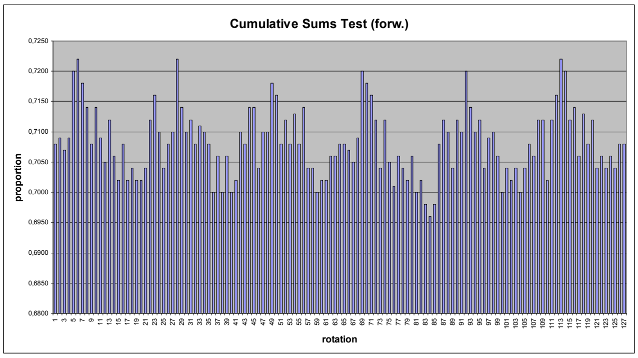

Fig.3. Cumulative Sums Test (forward) histogram

While the version of the "reverse" the highest value ratio (0.7200) obtained with a rotation of 71 bits.

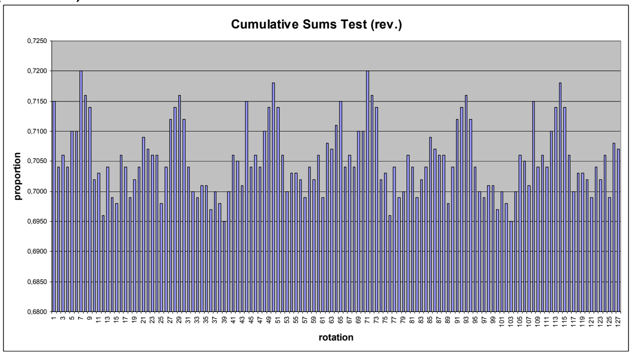

Fig.4. Cumulative Sums Test (reverse) histogram

In the runs test (fig. 5) the highest ratio value (0.622) was obtained with a rotation of 2 bits.

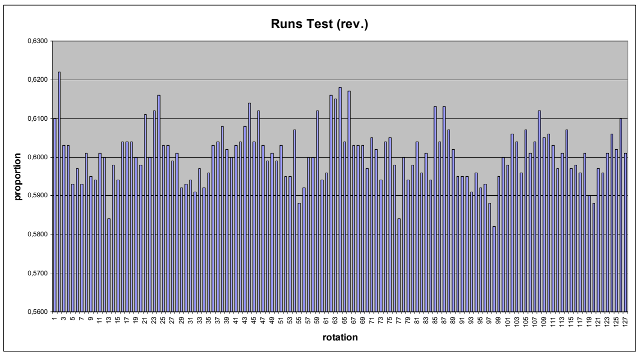

Fig.5. Runs Test histogram

The next step was to prepare standardized values of tests (see table 2):

$$y_{ij} = \frac{(x_{ij} - x_j)}{s_j}$$

where: x_{ij} – test result, x_j – avg. test result, s_j – standard deviation, and i = 1…128, j = 1…5

Table 2. Array of standardized values

rotation by	Y1	Y2	Y3	Y4	Y5
1	0,2567	-2,1772	-0,0689	1,6047	1,2216
2	0,0882	-2,6694	0,1074	-0,2397	2,8281
3	0,0882	-1,4390	-0,2452	0,0956	0,2845
4	-0,9229	-1,5620	0,1074	-0,2397	0,2845
5	0,0882	-1,3159	2,0466	0,7663	-1,0543
6	1,0993	-0,0856	2,3992	0,7663	-0,5188
7	1,7734	0,6527	1,6940	2,4430	-1,0543
8	2,1105	0,4066	0,9889	1,7723	0,0167
9	1,7734	0,1605	-0,0689	1,4370	-0,7865
10	0,4253	0,1605	0,9889	-0,5751	-0,9204
11	-1,2600	-0,5777	0,1074	-0,4074	0,0167
12	0,4253	-0,5777	-0,5977	-1,5811	-0,1171
13	0,0882	0,4066	0,6363	-0,2397	-2,2592
14	0,2567	-0,8238	-0,4214	-1,0781	-0,3849
15	-0,2488	0,1605	-1,1266	-1,2457	-0,9204
16	-0,9229	0,1605	-0,0689	0,0956	0,4184
17	-0,9229	0,6527	-1,1266	-0,2397	0,4184
18	-1,4285	0,6527	-0,7740	-1,0781	0,4184
19	-0,5859	0,1605	-1,1266	-0,5751	-0,1171
20	0,2567	1,2679	-1,1266	-0,2397	-0,3849
21	0,2567	1,2679	-0,7740	0,5986	1,3555
22	-0,0803	0,8988	0,6363	0,2633	-0,1171
23	-0,9229	0,2836	1,3415	0,0956	1,4894
24	0,4253	0,4066	0,2837	0,0956	2,0249
25	-0,5859	0,4066	-0,7740	-1,2457	0,2845
26	-0,9229	0,6527	-0,0689	-0,2397	0,2845
27	0,7623	0,8988	0,2837	1,1017	-0,2510
28	1,7734	0,1605	2,3992	1,4370	0,0167
29	2,4475	0,1605	0,9889	1,7723	-1,1881
30	1,7734	0,1605	0,2837	1,1017	-1,0543
31	-0,2488	0,6527	0,6363	-0,2397	-0,9204
32	-0,2488	-0,3316	-0,0689	-0,9104	-1,3220
33	-0,9229	-0,3316	0,4600	-1,0781	-0,5188
34	-0,2488	-0,3316	0,2837	-0,7427	-1,1881
35	-0,7544	-0,3316	-0,0689	-0,7427	-0,6526
36	-0,7544	1,3909	-1,4792	-1,4134	0,2845
37	-2,6081	0,4066	-0,4214	-0,9104	0,4184
38	0,0882	0,4066	-1,4792	-1,2457	0,9539
39	-1,0914	0,8988	-0,4214	-1,7488	0,1506
40	-1,5970	0,6527	-1,4792	-0,9104	-0,1171
41	0,4253	1,1448	-1,1266	0,0956	0,2845
42	-0,7544	1,2679	0,2837	-0,0720	0,4184
43	-0,7544	1,1448	-0,0689	-0,7427	0,9539
44	0,5938	0,6527	0,9889	1,6047	1,7571
45	0,4253	0,8988	0,9889	-0,2397	0,4184
46	0,0882	0,0375	-0,7740	0,0956	1,4894
47	-0,9229	0,1605	0,2837	-0,2397	0,2845
48	-0,2488	0,4066	0,2837	0,7663	-0,2510
49	1,0993	0,4066	1,6940	1,4370	0,0167
50	0,7623	-0,0856	1,3415	2,1077	-0,2510
51	1,7734	-0,0856	-0,0689	1,4370	0,2845
52	0,7623	0,1605	0,6363	0,0956	-0,7865
53	-0,2488	-0,3316	-0,0689	-0,9104	-0,7865
54	-0,5859	0,1605	0,8126	-0,4074	0,8200
55	-0,2488	-0,0856	-0,0689	-0,4074	-1,7236
56	-0,4174	-0,0856	0,9889	-0,5751	-1,1881
57	-0,4174	0,8988	-0,7740	-1,0781	-0,1171
58	-0,5859	0,6527	-0,7740	-0,2397	-0,1171
59	-0,2488	-0,0856	-1,4792	-0,5751	1,4894
60	-0,9229	-1,0699	-1,1266	0,0956	-0,9204
61	-1,2600	-2,3003	-1,1266	-1,0781	-0,6526
62	0,4253	-2,1772	-0,4214	0,4310	2,0249
63	0,2567	-2,7924	-0,4214	0,2633	1,8910
64	1,6049	-3,1615	-0,0689	0,9340	2,2926
65	0,2567	-2,1772	-0,0689	1,6047	0,4184
66	0,0882	-2,6694	-0,2452	-0,2397	2,1587
67	0,0882	-1,4390	-0,5977	0,0956	0,2845
68	-0,9229	-1,5620	0,1074	-0,2397	0,2845
69	0,0882	-1,3159	2,0466	0,7663	0,2845
70	1,0993	-0,0856	1,6940	0,7663	-0,5188
71	1,7734	0,6527	1,3415	2,4430	0,5522
72	2,1105	0,4066	0,6363	1,7723	0,1506
73	1,7734	0,1605	-0,7740	1,4370	-0,9204
74	0,4253	0,1605	0,6363	-0,5751	0,4184
75	-1,2600	-0,5777	-0,5977	-0,4074	0,5522
76	0,4253	-0,5777	-1,3029	-1,5811	-0,3849
77	0,0882	0,4066	-0,4214	-0,2397	-2,2592
78	0,2567	-0,8238	-0,7740	-1,0781	-0,1171
79	-0,2488	0,1605	-1,1266	-0,9104	-0,9204
80	-0,9229	0,1605	-0,4214	0,0956	-0,3849
81	-0,9229	0,6527	-1,4792	-0,2397	0,4184
82	-1,4285	0,6527	-1,1266	-1,0781	-0,6526
83	-0,5859	0,1605	-1,8318	-0,5751	0,0167
84	0,2567	1,2679	-2,1843	-0,2397	-0,9204
85	0,2567	1,2679	-1,8318	0,5986	1,6232
86	-0,0803	0,8988	-0,0689	0,2633	0,4184
87	-0,9229	0,2836	0,6363	0,0956	1,6232
88	0,4253	0,4066	0,2837	0,0956	0,8200
89	-0,5859	0,4066	-0,7740	-1,2457	0,1506
90	-0,9229	0,6527	0,6363	-0,2397	-0,7865
91	0,7623	0,8988	0,2837	1,1017	-0,7865
92	1,7734	0,1605	2,0466	1,4370	-0,7865
93	2,4475	0,1605	0,9889	1,7723	-1,3220
94	1,7734	0,1605	0,2837	1,1017	-0,6526
95	-0,2488	0,6527	0,6363	-0,2397	-1,1881
96	-0,2488	-0,3316	-0,7740	-0,9104	-1,0543
97	-0,9229	-0,3316	0,1074	-1,0781	-1,7236
98	-0,2488	-0,3316	0,2837	-0,7427	-2,5269
99	-0,7544	-0,3316	-0,4214	-0,7427	-0,7865
100	-0,7544	1,3909	-1,4792	-1,4134	-0,1171
101	-2,6081	0,4066	-0,7740	-0,9104	-0,3849
102	0,0882	0,4066	-1,1266	-1,2457	0,6861
103	-1,0914	0,8988	-0,7740	-1,7488	0,4184
104	-1,5970	0,6527	-1,4792	-0,9104	-0,6526
105	0,4253	1,1448	-0,7740	0,0956	0,8200
106	-0,7544	1,2679	-0,0689	-0,0720	0,0167
107	-0,7544	1,1448	-0,4214	-0,7427	0,4184
108	0,5938	0,6527	0,6363	1,6047	1,4894

109	0,4253	0,8988	0,6363	-0,2397	0,5522
110	0,0882	0,0375	-1,1266	0,0956	0,6861
111	-0,9229	0,1605	0,6363	-0,2397	0,2845
112	-0,2488	0,4066	1,3415	0,7663	-0,5188
113	1,0993	0,4066	2,3992	1,4370	0,0167
114	0,7623	-0,0856	2,0466	2,1077	0,8200
115	1,7734	-0,0856	0,6363	1,4370	-0,5188
116	0,7623	0,1605	0,9889	0,0956	-0,3849
117	-0,2488	-0,3316	-0,4214	-0,9104	-0,6526
118	-0,5859	0,1605	0,8126	-0,4074	0,0167
119	-0,2488	-0,0856	-0,0689	-0,4074	-1,4559
120	-0,4174	-0,0856	0,6363	-0,5751	-1,7236
121	-0,4174	0,8988	-0,7740	-1,0781	-0,5188
122	-0,5859	0,6527	-0,4214	-0,2397	-0,6526
123	-0,2488	-0,0856	-0,7740	-0,5751	0,0167
124	-0,9229	-1,0699	-0,4214	0,0956	0,6861
125	-1,2600	-2,3003	-0,7740	-1,0781	0,1506
126	0,4253	-2,1772	-0,0689	0,4310	1,2216
127	0,2567	-2,7924	-0,0689	0,2633	0,0167
128 hypothetical rotation	**2,4475**	**1,3909**	**2,3992**	**2,4430**	**2,8281**

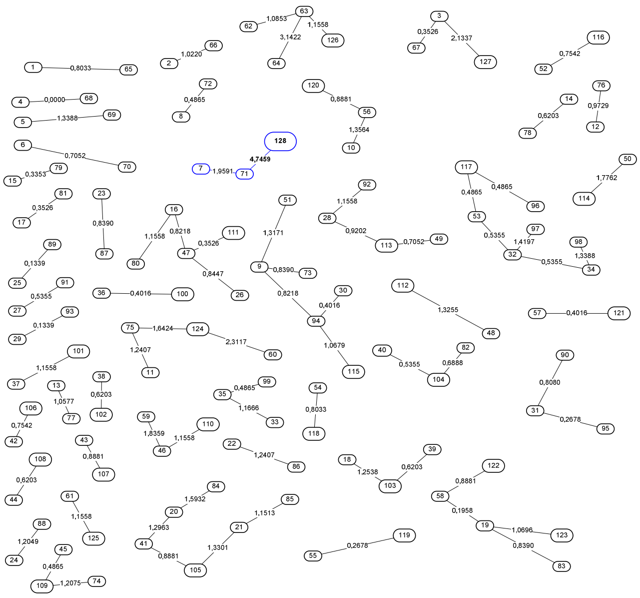

Fig.6. Level-1 dendrite

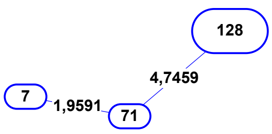

Fig.7. Cluster that include hypothetical solution

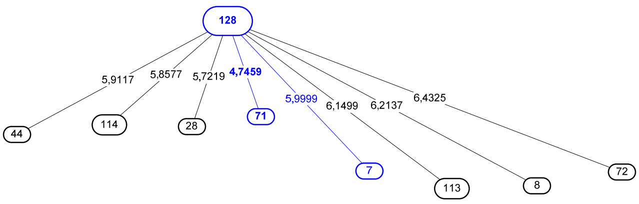

Fig.8. Eight most similar rotation values to the hypothetical best solution

Cluster analysis

The results obtained in the experiment and presented in the previous section hypothetically determined the best rotation in key schedule that gives the highest percentage of samples that meet the tests. The next step was to determine which of existing (possible) rotation is most similar (is the nearest solution) to the hypothetical element. For this purpose we used dendric method (Wroclaw-taxonomy). Algorithm of building dendrite is as follow:

1. determinate stochastic distance matrix of taxonomy (we used as measure of distance Manhattan distance):

$$d_m(x, y) = \sum |x_k - y_k|$$

where k= 1..n

2. determinate the value of the smallest distance within the taxonomic data for individual objects,
3. assume that every object is the tip of the dendrite, a rate of similarity to the ligament, and then joining together objects coming indicated by the distance in the second step,
4. if the resulting dendrite is inconsistent (has several parts), repeat steps 1-3 until you have a consistent graph (search for each vertex subgraph another similarity index value which will allow to join fragments of dendrite.

In our research we could omitted step 4 because from the point of view in adopted criterion for assessing the quality of rotation interesting were the nearest solutions to hypothetical rotation.

Figure 6 shows the level-1 dendrite constructed based on a matrix of similarities (its shape, localization of vertex, length of branches are random, the most important is value of similarity). Vertex 128 is marked as a hypothetical optimal solution.

Figure 7 shows a fragment of cluster from the constructed 1-degree dendrite, which build consisted dendrite with hypothetical best solution, its rotation by 71 and by 7 bits.

Figure 8 shows the eight rotations values relative similar to the hypothetical, but most of those values are more similar to other elements and build level-1 dendrite with them not with hypothetical solution its 28, 114, 44, 113, 8, 72.

Conclusions

By the conducted research we have performed statistical tests for all available rotation variant and designate a set of solution most similar to hypothetical best rotation due to statistical criteria. We indicated rotation by 71 and by 7 bits to the left as the rotation nearest to the hypothetical rotation.

Presented methodology of evaluating key schedule by combining statistical tests and cluster analysis can be performed most widely during designing process of building new cryptographic algorithms or during modifying existing. Using Wroclaw taxonomy we can find solution that meet our criteria and are nearest to the hypothetical best solution.

Acknowledgements. This research has been supported by Polish Ministry of Science and Higher Education under grant 04/45/DSPB/0136 and 04/45/DSMK/0160

***Authors**: mgr inż. Michał Apolinarski, Politechnika Poznańska, Instytut Automatyki i Inżynierii Informatycznej, ul. Piotrowo 3a, 60-965 Poznań, e-mail: michal.apolinarski@put.poznan.pl*

REFERENCES

[1] "A Statistical Test Suite for Random and Pseudorandom Number Generators for Crypto-graphic Applications", NIST Special Publication 800-22, revision 2, 2008.
[2] Biham E., "New types of cryptanalytic attacks using related keys", workshop on the theory and application of cryptographic techniques on Advances in cryptology, p.398-409, Janu-ary 1994, Lofthus, Norway
[3] Biham E., Shamir A., "Differential Cryptanalysis of the Data Encryption Standard", Springer-Verlag, New York, 1993.
[4] Lai X., Massey J., Murphy S., "Markov Ciphers and Di erential Cryptanalysis" Advances in Cryptology, CRYPTO '91, Springer-Verlag, 1991, pp. 17-38.