RESEARCH ON THE CRITERIA FOR THE STRUCTURE OF THE USED IN THE IDA ALGORITHM P FUNCTION

Ivan Ivanov, Stella Vetova, Krasimira Ivanova, Kiril Aleksiev, Lubov Ilieva

Abstract: *The following paper presents some conducted extensive research on the cryptographic algorithm IDA, concerning one of the basic properties of the block algorithms "diffusion." The object of the studies is the criteria for the structure of the function P used in this algorithm.*

Keywords: *cryptography, cryptographic algorithm, P function, S matrix, IDA algorithm.*

ITHEA Keywords: *E.3 Data Encryption – cryptosystems; F. Theory of Computation: F.2 Analysis of Algorithms and Problem Complexity; K. Computing Milieux: K.7 The Computing Profession: K.7.3 Testing, Certification, and Licensing.*

Introduction

The purpose of the presented paper is the exploration of the used in the IDA algorithm criteria for the structure of the P function [Ivanov, 2014] in the following main tasks: (1) introduction of the criteria for the structure of the P function; (2) research on the structure of the P function on the base of the set criteria; (3) results analysis.

There are three criteria used in the process of development of the P function as follows [Stallings, 2013; Schneier, 2013; Sokolov & Shangin, 2002]:

1. The four output bits obtained as a result of the S matrix in the i-th loop should be distributed so that two of them might affect the middle bits of the i + 1 loop, and the other two bits to affect the final ones.
2. The four output bits of the S matrix in the next loop should affect the results of six different S matrices, and none of the pairs of these four output bits should not come to the input of any S matrix.
3. For the two S matrices, Si and Sk, if any of the output bits of the Si matrix in the next loop affects the middle bits of Sk, then none of the output bits of Sk, should affect the middle bits of Si.

Using the described three criteria the algorithm satisfies the requirement for the property "diffusion" [Katz & Lindell, 2014].

The structure of the P function

Besides its application for bits rearranging, the P function (P) is applied for the determination of the encryption function setting the values in Table 1. In the starting sequence, the conversion runs in the following order:

1. Bit with number sixteen takes first position;
2. Bit with number seven takes the second position;
3. Bit with number twenty takes the third position, etc.

Table 1. Conversion function (P)

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

Research on the structure of the P function in the IDA algorithm, on the base of the set criteria

The next research uses IDA algorithm with the following input data:

P=11110010 11100101 11101011 11100101 11110100 11101110 11101101 11101000

K=11101010 11101110 11110000 11100101 11101010 11110010 11101110 11110000 00100000 11101101 11100000 00100000 11110010 11100101 11101011 11100101 11101010 11101110 11101100 11110011 11101101 11101000 11101010 11100000 11110110 11101000 11101110 11101101 11101101 11101000 11110010 11100101

In S_{0R} = 00010001 00001111 11011111 00011101 01100001 00101011, the obtained result is:

S_1(in)=000100; 00 - line number, 0010 - column number, S_1(out)=13=1101;

S_2(in)=010000; 00 - line number, 1000 - column number, S_2(out)=9=1001;

S_3(in)=111111; 11 - line number, 1111 - column number, S_3(out)=12=1100;

S_4(in)=011111; 01 - line number, 1111 - column number, S_4(out)=9=1001;

S_5(in)=000111; 01 - line number, 0011 - column number, S_5(out)=12=1100;

S_6(in)=010110; 00 - line number, 1011 - column number, S_6(out)=4=0100;

S_7(in)=000100; 00 - line number, 0010 - column number, S_7(out)=2=0010;

S_8(in)=101011; 11 - line number, 0101 - column number, S_8(out)=10=1010;

These results represent the output sequences of the eight S matrices (boxes). The sequences are applied to the input of the conversion function P (Table 1).

$S_{0R,32}$ = 11011001 11001001 11000100 00101010

№	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
$S_{0R,32}$	1	1	0	1	1	0	0	1	1	1	0	0	1	0	0	1	1	1	0

№	20	21	22	23	24	25	26	27	28	29	30	31	32
$S_{0R,32}$	0	0	1	0	0	0	0	1	0	1	0	1	0

After applying the function P on $S_{0R,32}$, the obtained result P_{0R} is:

P_{0R} = 10001001 10001111 11000101 01001010

In order to continue to the second loop, it is necessary that the XOR-based adder should be used first on the base of $P_{0R,32}$ and K_4, to obtain R_0:

for $P_{0R,32}$ and K_4=11101010 11101110 11101100 11110011 the result is:

№	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
P_{0R}	1	0	0	0	1	0	0	1	1	0	0	0	1	1	1	1	1	1	0
K_4	1	1	1	0	1	0	1	0	1	1	1	0	1	1	1	0	1	1	1
R_0	0	1	1	0	0	0	1	1	0	1	1	0	0	0	0	1	0	0	1

№	20	21	22	23	24	25	26	27	28	29	30	31	32
P_{0R}	0	0	1	0	1	0	1	0	0	1	0	1	0
K_4	0	1	1	0	0	1	1	1	1	0	0	1	1
R_0	0	1	0	0	1	1	0	1	1	1	0	0	1

R_0 = 01100011 01100001 00101001 10111001

Second loop

Since at each next loop the left and the right parts replace, the right sequence R_0 leaves labeled L_1:

L_1 = 01100011 01100001 00101001 10111001

№	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
L_1	0	1	1	0	0	0	1	1	0	1	1	0	0	0	0	1	0	0	1

№	20	21	22	23	24	25	26	27	28	29	30	31	32
L_1	0	1	0	0	1	1	0	1	1	1	0	0	1

This sequence goes through the expansion function E. The result is the sequence E_{1L} [Ivanov et al., 2014]:

E_{1L} = 10110000 01101011 00000010 10010101 00111101 11110010

Then, addition using XOR-based adder on the base of E_{1L} and K_5 is applied to obtain S_{1L}:

Exclusive OR of the sequences E_{1L} and K_5:

№	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
E_{1L}	1	0	1	1	0	0	0	0	0	1	1	0	1	0	1	1	0	0	0
K_5	1	1	1	0	1	1	0	1	1	1	1	0	1	0	0	0	1	1	1
S_{1L}	0	1	0	1	1	1	0	1	1	0	0	0	0	0	1	1	1	1	1

№	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
E_{1L}	0	0	0	1	0	1	0	0	1	0	1	0	1	0	0	1	1
K_5	0	1	0	1	0	1	1	1	0	0	0	0	0	1	1	1	1
S_{1L}	0	1	0	0	0	0	1	1	1	0	1	0	1	1	1	0	0

№	37	38	39	40	41	42	43	44	45	46	47	48
E_{1L}	1	1	0	1	1	1	1	1	0	0	1	0
K_5	0	1	1	0	1	1	1	0	1	0	0	0
S_{1L}	1	0	1	1	0	0	0	1	1	0	1	0

S_{1L} = 01011101 10000011 11101000 01110101 11001011 00011010

The sequences of S_{1L} are submitted to the inputs of the eight S boxes:

S_1(in)= 010111; 01 - line number, 1011 – column number, S_1(out)=11=1011;

S_2(in)= 011000; 00 - line number, 1100 - column number, S_2(out)=12=1100;

S_3(in)= 001111; 01 - line number, 0111 - column number, S_3(out)=10=1010;

S_4(in)= 101000; 10 - line number, 0100 - column number, S_4(out)=12=1100;

S_5(in)= 011101; 01 - line number, 1110 - column number, S_5(out)=8=1000;

S_6(in)= 011100; 00 - line number, 1110 - column number, S_6(out)=5=0101;

S_7(in)= 101100; 10 - line number, 0110 - column number, S_7(out)=7=0111;

S_8(in)= 011010; 00 - line number, 1101 - column number, S_8(out)=0=0000;

The obtained results represent the output sequences of the eight S matrices (boxes). These sequences are applied to the input of the conversion function P (Table 1).

$S_{1L,32}$ = 10111100 10101100 10000101 01110000

№	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
$S_{1L,32}$	1	0	1	1	1	1	0	0	1	0	1	0	1	1	0	0	1	0	0

№	20	21	22	23	24	25	26	27	28	29	30	31	32
$S_{1L,32}$	0	0	1	0	1	0	1	1	1	0	0	0	0

After applying the P function on $S_{1L,32}$, the obtained result P_{1L} is:

P_{1L} = 00000011 10011000 00110111 01011110

To continue to the third loop, it is necessary to go through the XOR-based adder on the base of $P_{1L,32}$ and K_7 to receive L_1:

For $P_{1L,32}$ and K_7 = 11001011 11010101 11100101 11011101 the result is:

№	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
P_{1L}	0	0	0	0	0	0	1	1	1	0	0	1	1	0	0	0	0	0	1
K_7	1	1	0	0	1	0	1	1	1	1	0	1	0	1	0	1	1	1	1
L_1	1	1	0	0	1	0	0	0	0	1	0	0	1	1	0	1	1	1	0

№	20	21	22	23	24	25	26	27	28	29	30	31	32
P_{1L}	1	0	1	1	1	0	1	0	1	1	1	1	0
K_7	0	0	1	0	1	1	1	0	1	1	1	0	1
L_1	1	0	0	1	0	1	0	0	0	0	0	1	1

L_1 = 11001000 01001101 11010010 10000011

Research results

Results on the base of criteria 1

Taking into consideration the performed research work, the following results are obtained: in $S_{0R,32}$ = 11011001 11001001 11000100 00101010, the result is P_{0R} = 10001001 10001111 11000101 01001010, and in $S_{1L,32}$ = 10111100 10101100 10000101 01110000 the result is P_{1L} = 00000011 10011000 00110111 01011110. These results indicate that this criterion is one hundred percent satisfied. This comes from the fact that the distribution of the four separate output bits obtained as a result of the S matrix is such that two of them affect the middle bits of the i + 1 loop, and the other two affect the final ones.

Results on the base of criteria 2

On the base of the performed research work, the following results are obtained: in $S_{0R,32}$ = 11011001 11001001 11000100 00101010, the result is P_{0R} = 10001001 10001111 11000101 01001010, and in $S_{1L,32}$ = 10111100 10101100 10000101 01110000 the result is P_{1L} = 00000011 10011000 00110111 01011110. These results indicate that this criterion is one hundred percent satisfied. The reason is that the four output bits of the S matrix in the next loop, affect the results of six different matrices S and no pair of these four output bits comes to the input of the S matrix.

Results on the base of criteria 3

The performance of the research work produces the following results: in $S_{0R,32}$ = 11011001 11001001 11000100 00101010, the result is P_{0R} = 10001001 10001111 11000101 01001010, and in $S_{1L,32}$ = 10111100 10101100 10000101 01110000 the result is P_{1L} = 00000011 10011000 00110111 01011110. These results indicate that this criterion is one hundred percent satisfied. This comes from the fact that for any two S matrices, S_i and S_k, if any of the output bits of the S_i matrix in the next loop affect the middle bits of S_k, then no output bit of S_k, affects the middle bit of S_i.

Conclusion

The described research work and obtained results lead to the following three conclusions:

1. The set criteria for the P function used in the IDA algorithm are one hundred percent satisfied;
2. One of the basic properties of the block algorithms called “diffusion” is realized. This means that if there is a key and two clear texts which differ by only one bit, the produced encrypted texts are totally different. Therefore, each bit of the ciphertext depends on all the bits of the clear text;
3. High degree of protection against differential cryptographic analysis is applied.

Acknowledgements

The paper is published with partial financial support from the "Scientific Research Fund" of University of Telecommunications and Posts, Sofia, Bulgaria, by the research project “Methods for development and estimation of cipher functions in block encryption algorithms”.

Bibliography

[Ivanov et al., 2014] Ivanov I, Arnaudov R, Dikov D, Stanchev G, Patent application 111513: Method for increasing data security in storage and during information transmission in special purpose telemetry systems, Bulgarian patent office, Official Bulletin, Issue 12, pp.14, Dec 2014.

[Katz & Lindell, 2014] Katz J., Lindell Y. Introduction to Modern Cryptography, Second Edition (Chapman & Hall/CRC Cryptography and Network Security Series), CRC Press, 2014.

[Schneier, 2013] Schneier B., Appliet Cryptography Protocols, Algorithms, and Source Code in C, Wiley, 2013.

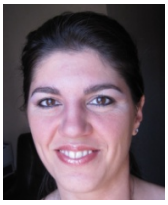
[Sokolov & Shangin, 2002] Sokolov V., Shangin F. Information protection distributed corporate networks and systems. DMK Press, Moskva, 2002.

[Stallings, 2013] Stallings W. Cryptography and Network Security: Principles and Practice (6th Edition), Hardcover, 2013.

Authors' Information

Ivan Ivanov *– Assist. Prof. PhD; University of Telecommunications and Posts, Sofia, Bulgaria; e-mail: i.ivanov@utp.bg;*

Major Fields of Scientific Research: Information and Network Security, Cryptographic Methods and Algorithms, Cyber security.



Stella Vetova *– Scientific Researcher, e-mail: vetova.bas@gmail.com;*

Major Fields of Scientific Research: Databases and security, Artificial Intelligence, Computer networks.

Krassimira Ivanova *- Assoc. prof. Dr.; University of Telecommunications and Posts, Sofia, Bulgaria; Institute of Mathematics and Informatics, BAS, Bulgaria;*
e-mail: krasy78@mail.bg;
Major Fields of Scientific Research: Software Engineering, Business Informatics, Data Mining, Multidimensional multi-layer data structures in self-structured systems

Kiril Aleksiev *– Assoc. Prof. PhD; University of Telecommunications and Posts, Sofia, Bulgaria; e-mail: kiril.m.alexiev@gmail.com;*
Major Fields of Scientific Research: Information Technology, Computer networks, Project management.

Lubov Ilieva *– Assoc. Prof. PhD; University of Telecommunications and Posts, Sofia, Bulgaria; e-mail: l.ilieva@utp.bg;*
Major Fields of Scientific Research: Psychology, Philosophy, Social Psychology, Business communications, Management Communicational Skills.