Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 15 Issue 4 Version 1.0 Year 2015
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

The Encryption Algorithm AES-RFWKIDEA32-1 based on Network RFWKIDEA32-1

By Gulom Tuychiev
National University of Uzbekistan, Uzbekistan

Abstract- In this article we developed a new block encryption algorithm based on network RFWKIDEA32-1 using of the transformations of the encryption algorithm AES, which is called AES-RFWKIDEA32-1. The block's length of this encryption algorithm is 256 bits, the number of rounds are 10, 12 and 14. The advantages of the encryption algorithms are that, when encryption and decryption process used the same algorithm. In addition, the encryption algorithm AES-RFWKIDEA32-1 encrypts faster than AES.

Keywords: advanced encryption standard, feystel network, lai-massey scheme, round function, round keys, output transformation, multiplica- tion, addition, multiplicative inverse, additive inverse.

GJCST-E Classification : C.2.1

The Encryption Algorithm AES-RFWKIDEA32-1 based on Network RFWKIDEA32-1

Gulom Tuychiev

Abstract- In this article we developed a new block encryption algorithm based on network RFWKIDEA32-1 using of the transformations of the encryption algorithm AES, which is called AES-RFWKIDEA32-1. The block's length of this encryption algorithm is 256 bits, the number of rounds are 10, 12 and 14. The advantages of the encryption algorithms are that, when encryption and decryption process used the same algorithm. In addition, the encryption algorithm AES-RFWKIDEA32-1 encrypts faster than AES.

Keywords: advanced encryption standard, feystel network, lai-massey scheme, round function, round keys, output transformation, multiplica- tion, addition, multiplicative inverse, additive inverse.

I. Introduction

In September 1997 the National Institute of Standards and Technology issued a public call for proposals for a new block cipher to succeed the Data Encryption Standard [41]. Out of 15 submitted algorithms the Rijndael cipher by Daemen and Rijmen [13] was chosen to become the new Advanced Encryption Standard in November 2001 [28]. The Advanced Encryption Standard is a block cipher with a fixed block length of 128 bits. It supports three diferent key lengths: 128 bits, 192 bits, and 256 bits. Encrypting a 128-bit block means transforming it in n rounds into a 128-bit output block. The number of rounds n depends on the key length: n =10 for 128-bit keys, n =12 for 192-bit keys, and n=14 for 256-bit keys. The 16-byte input block (t_0, t_1, . . . , t_{15}) which is transformed during encryption is usually written as a 4x4 byte matrix, the called AES State.

t_0	t_4	t_8	t_{12}
t_1	t_5	t_9	t_{13}
t_2	t_6	t_{10}	t_{14}
t_3	t_7	t_{11}	t_{15}

The structure of each round of AES can be reduced to four basic transfor-mations occurring to the elements of the State. Each round consists in applying

a) Lecture Notes in Computer Science: Authors' Instructions

successively to the State the SubBytes(), ShiftRows(), MixColumns() and AddRoundKey() transformations. The first round does the same with an extra AddRoundKey() at the beginning whereas the last round excludes the Mix-Columns() transformation.

The SubBytes() transformation is a nonlinear byte substitution that operates independently on each byte of the State using a substitution table (S-box). Figure 1 illustrates the SubBytes() transformation on the State.

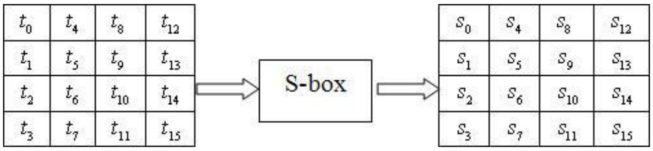
t_0 t_4 t_8 t_{12}
t_1 t_5 t_9 t_{13}
t_2 t_6 t_{10} t_{14}
t_3 t_7 t_{11} t_{15}
S-box
s_0 s_4 s_8 s_{12}
s_1 s_5 s_9 s_{13}
s_2 s_6 s_{10} s_{14}
s_3 s_7 s_{11} s_{15}

Figure 1: SubBytes() transformation

In the ShiftRows() transformation operates on the rows of the State; it cyclically shifts the bytes in each row by a certain offset. For AES, the first row is left unchanged. Each byte of the second row is shifted one to the left. Similarly, the third and fourth rows are shifted by offsets of two and three respectively. Figure 2 illustrates the ShiftRows() transformation.

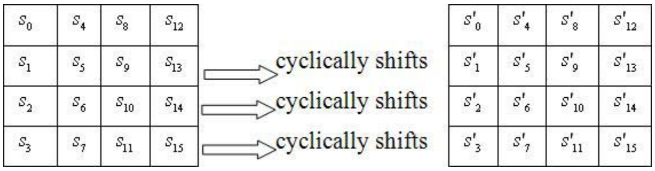
s_0 s_4 s_8 s_{12}
s_1 s_5 s_9 s_{13}
s_2 s_6 s_{10} s_{14}
s_3 s_7 s_{11} s_{15}
cyclically shifts
cyclically shifts
cyclically shifts
s'_0 s'_4 s'_8 s'_{12}
s'_1 s'_5 s'_9 s'_{13}
s'_2 s'_6 s'_{10} s'_{14}
s'_3 s'_7 s'_{11} s'_{15}

Figure 2 : ShiftRows() transformation

The MixColumns() transformation operates on the State column-by-column, treating each column as a four-term polynomial. The columns are considered as polynomials over GF(2^8) and multiplied modulo x^4 +1 with a fixed polynomial a(x), given by a(x) = $3x^2 + x^2 + x + 2$. Let p = a(x) $\otimes s'$:

$$\begin{bmatrix} p_{4i} \\ p_{4i+1} \\ p_{4i+2} \\ p_{4i+3} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s'_{4i} \\ s'_{4i+1} \\ s'_{4i+2} \\ s'_{4i+3} \end{bmatrix}, \ i = \overline{0...3}$$

As a result of this multiplication, the four bytes in a column are replaced by the following:

Figure 3 . illustrates the MixColumns() transformation

$$y_{4i} = (\{02\} \bullet s'_{4i}) \oplus (\{03\} \bullet s'_{4i+1}) \oplus s'_{4i+2} \oplus s'_{4i+3}$$

$$y_{4i+1} = s'_{4i} \oplus (\{02\} \bullet s'_{4i+1}) \oplus (\{03\} \bullet s'_{4i+2}) \oplus s'_{4i+3}$$

$$y_{4i+2} = s'_{4i} \oplus s'_{4i+1} \oplus (\{02\} \bullet s'_{4i+2}) \oplus (\{03\} \bullet s'_{4i+3})$$

$$y_{4i+4} = (\{03\} \bullet s'_{4i}) \oplus s'_{4i+1} \oplus s'_{4i+2} \oplus (\{02\} \bullet s'_{4i+3}).$$

Author: National University of Uzbekistan, Republic of Uzbekistan, Tashkent. e-mail: blasterjon@gmail.com

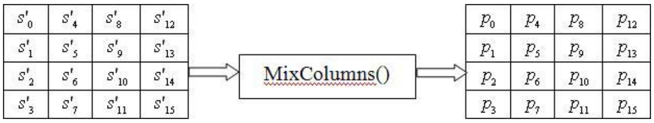

Figure 3 : MixColumns() transformation

II. Analysis of aes, pes and Idea

The first attack is a SQUARE attack suggested in [15] which uses $2^{128} - 2^{119}$ chosen plaintexts and 2120 encryptions. The second attack is a meet-in-the- middle attack proposed in [16] that requires 2^{32} chosen plaintexts and has a time complexity equivalent to almost 2^{128} encryptions. Recently, another at- tack on 7-round AES-128 was presented in [1]. The new attack is an impossible differential attack that requires $2^{117:5}$ chosen plaintexts and has a running time of 2^{121} encryptions. Similar results, but with better attack algorithms and lower complexities were reported in [42]. The resulting impossible diferential attack on 7-round AES-192 has a data complexity of 292 chosen plaintexts and time complexity of 2^{162} encryptions, while the attack on AES-256 uses $2^{116:5}$ chosen plaintexts and running time of $2^{247:5}$ encryptions.

There are several attacks on AES-192 [1, 14, 15, 24, 29, 42]. The two most no-table ones are the SQUARE attack on 8-round AES-192 presented in [15] that requires almost the entire code book and has a running time of 2^{188} encryptions and the meet in the middle attack on 7-round AES-192 in [14] that requires 2^{34+n} chosen plaintexts and has a running time of 2^{208}-^{n} + 2^{82+n} encryptions. Legitimate values for n in the meet in the middle attack on AES-192 are 94 i n i 17, thus, the minimal data complexity is 2^{51} chosen plaintexts (with time complexity equivalent to exhaustive search), and the minimal time complexity is 2^{146} (with data complexity of 2^{97} chosen plaintexts). AES-256 is analyzed in [1,14, 15, 24, 42]. The best attack is the meet in the middle attack in [14] which uses 2^{32} chosen plaintexts and has a total running time of 2^{209} encryptions. Finally, we would like to note the existence of many related-key attacks on AES-192 and AES-256. As the main issue of this paper is not related-key attacks, and as we deal with the single key model, we do not elaborate on the matter here, but the reader is referred to [43] for the latest results on related-key impossible di_er-ential attacks on AES and to [20] for the latest results on related-key rectangle attacks on AES.

The strength of AES with respect to impossible di_erentials was challenged several times. The first attack of this kind is a 5-round attack presented in [4]. This attack is improved in [11] to a 6-round attack. In [29], an impossible differential attack on 7-round AES-192 and AES-256 is presented. The latter attack uses 2^{92} chosen plaintexts (or $2^{92:5}$ chosen plaintexts for AES-256) and has a running time of 2186 encryptions (or $2^{250:5}$ encryptions for AES-256). The tim 4 Lecture Notes in Computer Science: Authors' Instructions for AES-192. In [1] a new 7-round impossible diferential attack was presented. The new attack uses a diferent impossible diferential, which is of the same general type as the one used in previous attacks (but has a slightly diferent structure). Using the new impossible diferential leads to an attack that requires $2^{117:5}$ chosen plaintexts and has a running time of 2^{121} encryptions. This attack was later improved in [2, 42] to use $2^{115:5}$ chosen plaintexts with time complexity of 2^{119} encryptions.

The last application of impossible diferential cryptanalysis to AES was the extension of the 7-round attack from [1] to 8-round AES-256 in [42]. The extended attack has a data complexity of 2116:5 chosen plaintexts and time com-plexity of $2^{247:5}$ encryption. We note that there were three more claimed impossible diferential attacks on AES in [8{10]. However, as all these attacks are awed [7]. In paper [25] present a new attack on 7-round AES-128, a new attack on 7-round AES-192, and two attacks on 8-round AES-256. The attacks are based on the attacks proposed in [1, 29] but use additional techniques, including the early abort technique and key schedule considerations.

The best attack we present on 8-round AES-256 requires $2^{89:1}$ chosen plain-texts and has a time complexity of $2^{129:7}$ memory accesses. These results are significantly better than any previously published impossible diferential attack on AES. We summarize results along with previously known results in Table 1.

Table 1: A Summary of the Attacks on AES

Number of rounds	complexity		Attack type
	Data (CP)	Time	
AES-128			
7	2^{128} - 2^{119}	2^{120}	Square [15]
7	$2^{117.5}$	2^{121}	Impossible Differential [15]
7	$2^{117.5}$	2^{119}	Impossible Differential [2, 42]
7	2^{32}	2^{128}	Meet in the middle [16]
7	$2^{112.2}$	$2^{117.2}$ MA	Impossible Differential [25]
AES-192			
7	2^{32}	2^{184}	Square [24]
7	19*2^{32}	2^{155}	Square [15]
7	2^{92}	$2^{186.2}$	Impossible Differential [29]
7	$2^{115.5}$	2^{119}	Impossible Differential [42]
7	2^{92}	2^{162}	Impossible Differential [42]
7	2^{34+n}	$2^{208-n} + 2^{82+n}$	Meet in the middle [14]
8	$2128 - 2119$	2^{188}	Square [15]
7	$2^{113.8}$	$2^{118.8}$ MA	Impossible Differential [25]
7	$2^{91.2}$	$2^{139.2}$	Impossible Differential [25]
AES-256			
7	2^{32}	2^{200}	Square [24]
7	21*2^{32}	2^{172}	Square [15]
7	$2^{92.5}$	$2^{250.5}$	Impossible Differential [29]
7	2^{32}	2^{208}	Meet in the middle [14]
7	2^{34+n}	$2^{208-n} + 2^{82+n}$	Meet in the middle [14]
7	$2^{115.5}$	2^{119}	Impossible Differential [42]
8	$2^{116.5}$	$2^{247.5}$	Impossible Differential [42]
8	$2^{128} - 2119$	2^{204}	Square [15]
8	2^{32}	2^{209}	Meet in the middle [14]
7	$2^{113.8}$	$2^{118.8}$ MA	Impossible Differential [25]
7	2^{92}	2^{163} MA	Impossible Differential [25]
8	$2^{111.1}$	$2^{227.8}$ MA	Impossible Differential [25]
8	$2^{89.1}$	$2^{229.7}$ MA	Impossible Differential [25]

The Proposed Encryption Standard (PES) is a 64-bit block cipher, using a 128-bit key, designed by Lai and Massey in 1990 (see [22]) and was a predecessor to IDEA (International Data Encryption Algorithm) [21]. IDEA was originally called IPES (Improved PES). PES iterates eight rounds plus an output trans- formation. The cryptanalysis of PES and IDEA presented on Table 2 and Table 3.

Table 2: A Summary of the Attacks on IDEA

Attack Type	Year	Attacked Rounds	Key Bits round	Chosen Plaintext	Time
Differential [26]	1993	2	32	210	242
Differential [12]	1993	2.5	32	210	232
Differential [26]	1993	2.5	96	210	2106
Related-Key Differential [18]	1996	3	32	6	6 * 232
Differential-Linear [6]	1996	3	32	230	244
Differential [5]	1996	3	32	230	0.75 * 244
Truncated Differential [19, 6]	1997	3.5	48	256	267
Miss-in-the-middle [3]	1998	3.5	64	238.5	253
Miss-in-the-middle [3]	1998	4	69	237	270

Related-Key Differential-Linear [17]	1998	4	15	38.3	-
Miss-in-the-Middle [3]	1998	4.5	80	264	2112
Square attack [27]	2000	2.5	77	3 * 216	262 + 247
Square attack [27]	2000	2.5	31	232	262
Square [27]	2000	2.5	31	248	279
Related-Key Square [27]	2001	2.5	32	2	241

Table 3 : A Summary of the Attacks on PES

Attack Type	Year	Attacked Rounds	Key Bits round	Chosen Plaintext	Time
Differential [23]	1991	7	96	264	2160
Square [27]	2000	2.5	31	217	247
Square [27]	2001	2.5	31	232	263
Related-Key Square [27]	2001	2.5	32	2	241

On the basis of encryption algorithm IDEAnd scheme Lai-Massey developed the networks IDEA32-1 and RFWKIDEA32-1, consisting from one round function [30, 31]. In the networks IDEA32-1 and RFWKIDEA32-1, similarly as in the Feistel network, when it encryption and decryption using the same algorithm. In the networks used one round function having 16 input and output blocks and as the round function can use any transformation.

Using transformation SubBytes(), ShiftRows(), MixColumns(), AddRound-Key() AES encryption algorithm as a round function networks IDEA8-1 [32], RFWKIDEA8-1 [32], PES8-1 [33], RFWKPES8-1 [34], IDEA16-1 [35], created encryption algorithms AES-IDEA8-1 [36], AES-RFWKIDEA8-1 [37], AES-PES8-1 [38], AES-RFWKPES8-1 [39], AES-IDEA16-1 [40].

In this paper developed block encryption algorithm AES-RFWKIDEA32-1 based network RFWKIDEA32-1 using transformation of the encryption algorithm AES. The length of block of the encryption algorithms is 256 bits, the number of rounds n equal to 10, 12, 14 and the length of key is variable from 256 bits to 1024 bits in steps 128 bits, i.e., key length is equal to 256, 384, 512,640, 768, 896 and 1024 bits.

III. The Encryption Algorithm AES-Rfwkidea32-1

a) *The structure of the encryption algorithm AES-RFWKIDEA32- 1*

In the encryption algorithm AES-RFWKIDEA32-1 as the round function used SubBytes(), ShiftRows(), MixColumns() transformation encryption algorithm AES. The scheme n-rounded encryption algorithm AES-RFWKIDEA32-1 shown in Figure 4, and the length of subblocks X^0, X^1, ..., X^{31}, length of round keys $K_{32(i-1)}$, $K_{32(i-1)+1}$, ..., $K_{32(i-1)+31}$,, $i = 1 \ldots n + 1$ and K_{32n+32}, K_{32n+33}, ..., K_{32n+95} are equal to 8-bits.

Consider the round function of the encryption algorithm AES-RFWKIDEA32-1. Initially 32-bit subblocks t_0, t_1, ... , t_{15} are written into the State array and are executed the above transformations SubBytes(), ShiftRows(), MixColumns(). After the AddRoundKey() transformation we obtain 8-bits subblocks y_0, y_1, ..., y_{15}.

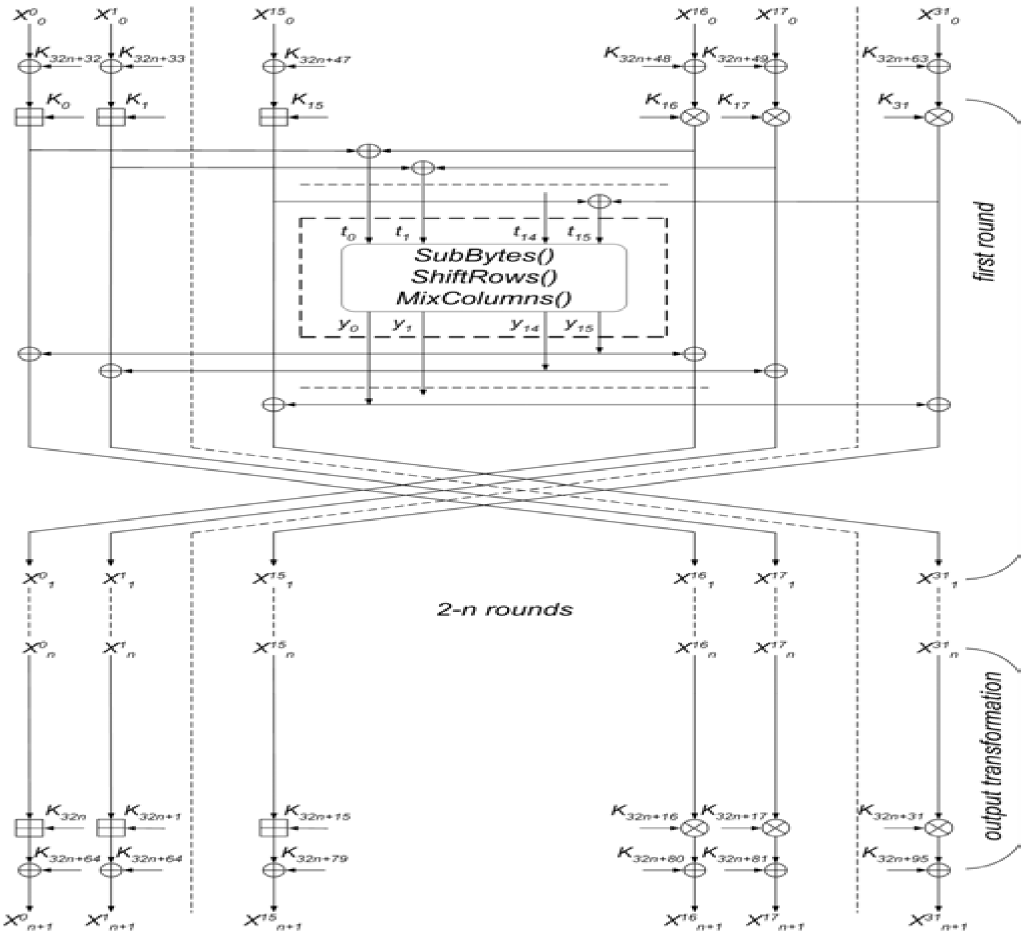

Figure 4: The scheme n-rounded encryption algorithm AES-RFWKIDEA32-1

The S-box SubBytes() transformation shown in Table 1 and is the only non-linear transformation. The length of the input and output blocks S-box is eight bits. For example, if the input value the S-box is equal to 0xE7, then the output value is equal 0x79, i.e. selected elements of intersection row 0xE and column 0x7.

Table 1 : The S-box of encryption algorithm AES-RFWKIDEA32-1

	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xA	0xB	0xC	0xD	0xE	0xF
0x0	0x87	0x1C	0x05	0x06	0x13	0x86	0x84	0xC9	0x3F	0xEF	0x85	0xA6	0x10	0x41	0xA2	0x15
0x1	0xD2	0xF3	0xCA	0x0C	0x12	0x4E	0xC5	0x1B	0xA8	0x59	0xB3	0xA0	0x78	0xB9	0x17	0xDB
0x2	0x21	0x08	0x63	0xB5	0x35	0x24	0x01	0xD8	0x3D	0xA9	0x89	0x0B	0x0F	0x5A	0x2F	0x6D
0x3	0xFD	0xC1	0xA7	0xC3	0x7E	0x71	0xED	0x72	0xE5	0x77	0xFB	0x93	0x82	0xA5	0x33	0x0D
0x4	0xEE	0xE3	0xBC	0x76	0x66	0x94	0x56	0xBB	0x57	0x26	0x51	0x23	0xAE	0x83	0xA4	0xF9
0x5	0x47	0x4B	0xFF	0x88	0xBF	0x18	0x2B	0x46	0x96	0xC2	0x30	0x2E	0xD6	0xDC	0x5E	0xC0
0x6	0x5B	0x80	0xB2	0x02	0xC7	0xCC	0x27	0xE9	0xCD	0x0A	0xF7	0x04	0x5F	0x3C	0x60	0xBA
0x7	0x4F	0xA3	0xDF	0xE0	0x73	0x68	0x3E	0x09	0x38	0x31	0x52	0xAF	0x7F	0x00	0x03	0x53
0x8	0xC8	0xFC	0x67	0x98	0x44	0x61	0xDD	0x65	0xD9	0xA1	0x14	0x2C	0x9D	0x4C	0x6E	0x07
0x9	0x9F	0xEB	0xC4	0x58	0xB7	0xB6	0x7B	0xFA	0xD5	0x90	0x3A	0x7D	0x50	0x54	0xE6	0x42
0xA	0x9B	0x37	0x36	0xF6	0xCE	0xF5	0xBD	0x5C	0xD3	0x43	0xB8	0x97	0x6B	0x69	0x99	0x0E
0xB	0x81	0xDA	0x25	0x8C	0xE8	0x49	0xD4	0xAA	0x9C	0x55	0x19	0x92	0x8D	0x16	0xB0	0xFE
0xC	0x32	0x1E	0xAD	0xB4	0x7C	0xB1	0x39	0xD1	0x9A	0x48	0x1D	0x64	0xC6	0x28	0xE2	0xF2
0xD	0x1F	0x34	0x29	0x95	0xDE	0xE7	0x11	0xF4	0x8F	0x2D	0x45	0x2A	0xF1	0xCB	0x6C	0x70
0xE	0x8B	0x1A	0x7A	0x6F	0x8E	0x4A	0xF0	0x79	0x62	0x74	0xE1	0x8A	0xD0	0x4D	0xBE	0x40
0xF	0xF8	0xAB	0xEA	0xEC	0x20	0x91	0xD7	0x9E	0xCF	0x6A	0xAC	0xE4	0x3B	0x5D	0x22	0x75

Consider the encryption process of encryption algorithm AES-RFWKIDEA32-1. Initially the 256-bit plaintext X partitioned into subblocks of 8-bits $X_0^0, X_0^1, \ldots, X_0^{31}$, and performs the following steps:

1. subblocks $X_0^0, X_0^1, \ldots, X_0^{31}$ summed by XOR respectively with round key K_{32n+32}, K_{32n+33}, ..., $K_{32n+63:}$

$$X_0^j = X_0^j \oplus K_{32n+32+j},\ j = \overline{0...31}.$$

2. subblocks $X_0^0, X_0^1, \ldots, X_0^{31}$ multiplied and summed respectively with the round keys $K_{32(i-1)}$, $K_{32(i-1)+1}$, . . . , $K_{32(i-1)+31}$ and calculated 8-bit sub- blocks t_0, t_1, . . . , t_{15}. This step can be represented as follows:

$$t_0 = (X_{i-1}^0 + K_{32(i-1)}) \oplus (X_{i-1}^{16} \cdot K_{32(i-1)+16}),$$
$$t_1 = (X_{i-1}^1 \cdot K_{32(i-1)+1}) \oplus (X_{i-1}^{17} + K_{32(i-1)+17}),$$
$$t_2 = (X_{i-1}^2 + K_{32(i-1)+2}) \oplus (X_{i-1}^{18} \cdot K_{32(i-1)+18}),$$
$$t_3 = (X_{i-1}^3 \cdot K_{32(i-1)+3}) \oplus (X_{i-1}^{19} + K_{32(i-1)+19}),$$
$$t_4 = (X_{i-1}^4 + K_{32(i-1)+4}) \oplus (X_{i-1}^{20} \cdot K_{32(i-1)+20}),$$
$$t_5 = (X_{i-1}^5 \cdot K_{32(i-1)+5}) \oplus (X_{i-1}^{21} + K_{32(i-1)+21}),$$
$$t_6 = (X_{i-1}^6 + K_{32(i-1)+6}) \oplus (X_{i-1}^{22} \cdot K_{32(i-1)+22}),$$
$$t_7 = (X_{i-1}^7 \cdot K_{32(i-1)+7}) \oplus (X_{i-1}^{23} + K_{32(i-1)+23}),$$
$$t_8 = (X_{i-1}^8 + K_{32(i-1)+8}) \oplus (X_{i-1}^{24} \cdot K_{32(i-1)+24}),$$
$$t_9 = (X_{i-1}^9 \cdot K_{32(i-1)+9}) \oplus (X_{i-1}^{25} + K_{32(i-1)+25}),$$
$$t_{10} = (X_{i-1}^{10} + K_{32(i-1)+10}) \oplus (X_{i-1}^{26} \cdot K_{32(i-1)+26}),$$
$$t_{11} = (X_{i-1}^{11} \cdot K_{32(i-1)+11}) \oplus (X_{i-1}^{27} + K_{32(i-1)+27}),$$

$$t_{12} = (X^{12}_{i-1} + K_{32(i-1)+12}) \oplus (X^{28}_{i-1} \cdot K_{32(i-1)+28}),$$
$$t_{13} = (X^{13}_{i-1} \cdot K_{32(i-1)+13}) \oplus (X^{29}_{i-1} + K_{32(i-1)+29}),$$
$$t_{14} = (X^{14}_{i-1} + K_{32(i-1)+14}) \oplus (X^{30}_{i-1} \cdot K_{32(i-1)+30}),$$
$$t_{15} = (X^{15}_{i-1} \cdot K_{32(i-1)+15}) \oplus (X^{31}_{i-1} + K_{32(i-1)+31}),\ , i = 1.$$

3. performed SubBytes(), ShiftRows(), MixColumns() transformation. Output subblocks of the round function of the encryption algorithm are y$_0$, y$_1$, . . . ,y$_{31}$.

4. subblocks y$_0$, y$_1$, . . . , y$_{31}$ are summed to XOR with subblocks $X^0_{i-1}, X^1_{i-1}, \dots, X^{31}_{i-1}$, i.. $X^j_{i-1} = X^j_{i-1} \oplus y_{15-j}$, $X^{j+16}_{i-1} = X^{j+16}_{i-1} \oplus y_{15-j}$, $j = \overline{0...15}$, $i = 1$.

5. at the end of the round subblocks X^j_{i-1} and X^{31-j}_{i-1}, $j = \overline{1...\quad}$ 15 swapped, i..,

$$X^0_i = X^0_{i-1},\ X^1_i = X^{30}_{i-1},\ X^2_i = X^{29}_{i-1},\ X^3_i = X^{28}_{i-1},$$
$$X^3_i = X^{27}_{i-1},\ X^5_i = X^{26}_{i-1},\ X^6_i = X^{25}_{i-1},\ X^7_i = X^{24}_{i-1},$$
$$X^8_i = X^{23}_{i-1},\ X^9_i = X^{22}_{i-1},\ X^{10}_i = X^{21}_{i-1},\ X^{11}_i = X^{20}_{i-1},$$
$$X^{12}_i = X^{19}_{i-1},\ X^{13}_i = X^{18}_{i-1},\ X^{14}_i = X^{17}_{i-1},\ X^{15}_i = X^{16}_{i-1},$$
$$X^{16}_i = X^{15}_{i-1},\ X^{17}_i = X^{14}_{i-1},\ X^{18}_i = X^{13}_{i-1},\ X^{19}_i = X^{12}_{i-1},$$
$$X^{20}_i = X^{11}_{i-1},\ X^{21}_i = X^{10}_{i-1},\ X^{22}_i = X^{9}_{i-1},\ X^{23}_i = X^{8}_{i-1},$$
$$X^{24}_i = X^{7}_{i-1},\ X^{25}_i = X^{6}_{i-1},\ X^{26}_i = X^{5}_{i-1},\ X^{27}_i = X^{4}_{i-1},$$
$$X^{28}_i = X^{3}_{i-1},\ X^{29}_i = X^{2}_{i-1},\ X^{30}_i = X^{1}_{i-1},\ X^{31}_i = X^{31}_{i-1},$$
$$i = 1.$$

6. repeating steps 2-5 n times, i.e., i = 2...n obtain subblocks $X^0_n,\ X^1_n,\ \dots, X^{31}_n$.

7. in output transformation round keys are multiplied and summed into sub-blocks, i.e.

$$X^0_{n+1} = X^0_n + K_{32n},\ X^1_{n+1} = X^{30}_n \cdot K_{32n+1},$$
$$X^2_{n+1} = X^{29}_n + K_{32n+2},\ X^3_{n+1} = X^{28}_n \cdot K_{32n+3},$$
$$X^4_{n+1} = X^{27}_n + K_{32n+4},\ X^5_{n+1} = X^{26}_n \cdot K_{32n+5},$$
$$X^6_{n+1} = X^{25}_n + K_{32n+6},\ X^7_{n+1} = X^{24}_n \cdot K_{32n+7},$$
$$X^8_{n+1} = X^{23}_n + K_{32n+8},\ X^9_{n+1} = X^{22}_n \cdot K_{32n+9},$$
$$X^{10}_{n+1} = X^{21}_n + K_{32n+10},\ X^{11}_{n+1} = X^{20}_n \cdot K_{32n+11},$$
$$X^{12}_{n+1} = X^{19}_n + K_{32n+12},\ X^{13}_{n+1} = X^{18}_n \cdot K_{32n+13},$$
$$X^{14}_{n+1} = X^{17}_n + K_{32n+14},\ X^{15}_{n+1} = X^{16}_n \cdot K_{32n+15},$$
$$X^{16}_{n+1} = X^{15}_n \cdot K_{32n+16},\ X^{17}_{n+1} = X^{14}_n + K_{32n+17},$$
$$X^{18}_{n+1} = X^{13}_n \cdot K_{32n+18},\ X^{19}_{n+1} = X^{12}_n + K_{32n+19},$$
$$X^{20}_{n+1} = X^{11}_n \cdot K_{32n+20},\ X^{21}_{n+1} = X^{10}_n + K_{32n+21},$$
$$X^{22}_{n+1} = X^{9}_n \cdot K_{32n+22},\ X^{23}_{n+1} = X^{8}_n + K_{32n+23},$$
$$X^{24}_{n+1} = X^{7}_n \cdot K_{32n+24},\ X^{25}_{n+1} = X^{6}_n + K_{32n+25},$$
$$X^{26}_{n+1} = X^{5}_n \cdot K_{32n+26},\ X^{27}_{n+1} = X^{4}_n + K_{32n+27},$$
$$X^{28}_{n+1} = X^{3}_n \cdot K_{32n+28},\ X^{29}_{n+1} = X^{2}_n + K_{32n+29},$$
$$X^{30}_{n+1} = X^{1}_n \cdot K_{32n+30},\ X^{31}_{n+1} = X^{31}_n + K_{32n+31},$$

8. subblocks $X^0_{n+1},\ X^1_{n+1},\ \dots,\ X^{31}_{n+1}$ are summed
K K
to XOR with the roundkey $\underline{\text{key}}$ $_{32n+64}$, $_{32n+65}$, $\dots$, K_{32n+95}: $X^j_{n+1} = X^j_{n+1} \oplus K_{32n+64+j}$, $j = 0...$ 31. As ciphertext plaintext X receives the combined 16-bit subblocks $X^0_{n+1}||X^1_{n+1}||...||X^{31}_{n+1}$.

b) *Key generation of the encryption algorithm AES-RFWKIDEA32-1*

In n-round encryption algorithm AES-RFWKIDEA32-1 in each round we applied sixteen (32) round keys of the 8-bit and output transformation sixteen (32) round keys of the 8-bit. In addition, before the first round and after the output transformation we used sixteen (32) round keys of 8-bits. Total number of 8-bit round keys is equal to 32n+96. In Figure 4 encryption used encryption round keys K^c_i instead of K$_i$, while decryption used decryption round keys K^d_i . If n=10 then need 416 to generate round keys, if n=12, you need to generate 480 round keys and if n=14 need 544 to generate round keys.

When generating round keys like the AES encryption algorithm uses an array Rcon: Rcon=[0x01, 0x02, 0x04, 0x08, 0x10, 0x20, 0x40, 0x80].

The key encryption algorithm K of length l (256 $\leq l \leq$1024) bits is divided into 8-bit round keysK^c_0, K^c_1 ,..., $K^c{}_{Lenght-1}$, Lenght $= l/$ 8, her$\underline{\text{e}}$ K $= \{k_0, k_1, ..., k_{l-1}\}$, $K^c_0 = \{k_0, k_1, ..., k_7\}$, $K^c_1 = \{k_8, k_9, ..., k_{15}\}$,..., $K^c_{Lenght-1} = \{k_{l-8}, k_{l-7}, ..., k_{l-1}\}$ and $K = K^c_0||\ K^c_1||...||K^c_{Lenght-1}$. Then we calculate $K_L = K^c_0 \oplus K^c_1 \oplus ... \oplus K^c_{Lenght-1}$. If $K_L = 0$ then K_L is chosen as 0xC5, i.e. $K_L = $ 0xC5.

When generating a round keys K^c_i, $i = \overline{Lenght...32n+}$ 95, we used transforma- tion SubBytes() and RotWord8(), here SubBytes()-is transformation 8-bit sub-block into S-box and RotWord8()-cyclic shift to the left of 1 bit of the 8-bit subblock. When the condition imod3 = 1 is true, then the round keys are com- puted as $K^c_i =$ SubBytes $(K^c_{i-Lenght+1}) \oplus$ SubBytes(RotWord8 $K^c_{i-Lenght})) \oplus$ Rcon[imod8]$\oplus K_L$ otherwise $K^c_i =$ SubBytes $(K^c_{i-Lenght}) \oplus SubBytes(K^c_{i-Lenght+1}) \oplus K_L$. After each round key generation the value K_L is cyclic shift to the left by 1 bit.

Decryption round keys are computed on the basis of encryption round keys and decryption round keys of the output transformation associate with of en- cryption round keys as follows:

$$(K^d_{32n}, K^d_{32n+1}, K^d_{32n+2}, K^d_{32n+3}, K^d_{32n+4}, K^d_{32n+5}, K^d_{32n+6}, K^d_{32n+7},$$
$$K^d_{32n+8}, K^d_{32n+9}, K^d_{32n+10}, K^d_{32n+11}, K^d_{32n+12}, K^d_{32n+13}, K^d_{32n+14}, K^d_{32n+15},$$
$$K^d_{32n+16}, K^d_{32n+17}, K^d_{32n+18}, K^d_{32n+19}, K^d_{32n+20}, K^d_{32n+21}, K^d_{32n+22},$$
$$K^d_{32n+23}, K^d_{32n+24}, K^d_{32n+25}, K^d_{32n+26}, K^d_{32n+27}, K^d_{32n+28}, K^d_{32n+29},$$
$$K^d_{32n+30}, K^d_{32n+31}) = (-K^c_0, (K^c_1)^{-1}, -K^c_2, (K^c_3)^{-1}, -K^c_4, (K^c_5)^{-1},$$
$$-K^c_6, (K^c_7)^{-1}, -K^c_8, (K^c_9)^{-1}, -K^c_{10}, (K^c_{11})^{-1}, -K^c_{12}, (K^c_{13})^{-1}, -K^c_{14},$$
$$(K^c_{15})^{-1}, (K^c_{16})^{-1}, -K^c_{17}, (K^c_{18})^{-1}, -K^c_{19}, (K^c_{20})^{-1}, -K^c_{21}, (K^c_{22})^{-1},$$
$$-K^c_{23}, (K^c_{24})^{-1}, -K^c_{25}, (K^c_{26})^{-1}, -K^c_{27}, (K^c_{28})^{-1}, -K^c_{29}, (K^c_{30})^{-1}, -K^c_{31}).$$

$$(K^d_{320}, K^d_{321}, K^d_{322}, K^d_{323}, K^d_{324}, K^d_{325}, K^d_{326}, K^d_{327}, K^d_{328}, K^d_{329}, K^d_{330}, K^d_{331},$$
$$K^d_{332}, K^d_{333}, K^d_{334}, K^d_{335}, K^d_{336}, K^d_{337}, K^d_{338}, K^d_{339}, K^d_{340}, K^d_{341}, K^d_{342}, K^d_{343},$$
$$K^d_{344}, K^d_{345}, K^d_{346}, K^d_{347}, K^d_{348}, K^d_{349}, K^d_{350}, K^d_{351}) = (-K^c_0, (K^c_1)^{-1}, -K^c_2,$$
$$(K^c_3)^{-1}, -K^c_4, (K^c_5)^{-1}, -K^c_6, (K^c_7)^{-1}, -K^c_8, (K^c_9)^{-1}, -K^c_{10}, (K^c_{11})^{-1}, -K^c_{12},$$
$$(K^c_{13})^{-1}, -K^c_{14}, (K^c_{15})^{-1}, (K^c_{16})^{-1}, -K^c_{17}, (K^c_{18})^{-1}, -K^c_{19}, (K^c_{20})^{-1},$$
$$-K^c_{21}, (K^c_{22})^{-1}, -K^c_{23}, (K^c_{24})^{-1}, -K^c_{25}, (K^c_{26})^{-1}, -K^c_{27}, (K^c_{28})^{-1}, -K^c_{29},$$
$$(K^c_{30})^{-1}, -K^c_{31}).$$

For example, if the number of rounds is 10 the formula is as follows:

Decryption round keys of the first round associates with the encryption round keys as follows:

$$(K^d_0, K^d_1, K^d_2, K^d_3, K^d_4, K^d_5, K^d_6, K^d_7, K^d_8, K^d_9, K^d_{10}, K^d_{11}, K^d_{12}, K^d_{13}, K^d_{14}, K^d_{15},$$
$$K^d_{16}, K^d_{17}, K^d_{18}, K^d_{19}, K^d_{20}, K^d_{21}, K^d_{22}, K^d_{23}, K^d_{24}, K^d_{25}, K^d_{26}, K^d_{27}, K^d_{28}, K^d_{29}, K^d_{30},$$
$$K^d_{31}) = (-K^c_{32n}, (K^c_{32n+1})^{-1}, -K^c_{32n+2}, (K^c_{32n+3})^{-1}, -K^c_{32n+4}, (K^c_{32n+5})^{-1}$$
$$-K^c_{32n+6}, (K^c_{32n+7})^{-1}, -K^c_{32n+8}, (K^c_{32n+9})^{-1}, -K^c_{32n+10}, (K^c_{32n+11})^{-1},$$
$$-K^c_{32n+12}, (K^c_{32n+13})^{-1}, -K^c_{32n+14}, (K^c_{32n+15})^{-1}, (K^c_{32n+16})^{-1}, -K^c_{32n+17},$$
$$(K^c_{32n+18})^{-1}, -K^c_{32n+19}, (K^c_{32n+20})^{-1}, -K^c_{32n+21}, (K^c_{32n+22})^{-1}, -K^c_{32n+23},$$
$$(K^c_{32n+24})^{-1}, -K^c_{32n+25}, (K^c_{32n+26})^{-1}, -K^c_{32n+27}, (K^c_{32n+28})^{-1}, -K^c_{32n+29},$$
$$(K^c_{32n+30})^{-1}, -K^c_{32n+31}).$$

Likewise, the decryption round keys of the second, third and n{round associates with the encryption round keys as follows:

$$(K^d_{32(i-1)}, K^d_{32(i-1)+1}, K^d_{32(i-1)+2}, K^d_{32(i-1)+3}, K^d_{32(i-1)+4}, K^d_{32(i-1)+5}, \qquad ,$$
$$K^d_{32(i-1)+6}, K^d_{32(i-1)+7}, K^d_{32(i-1)+8}, K^d_{32(i-1)+9}, K^d_{32(i-1)+10}, K^d_{32(i-1)+11},$$
$$K^d_{32(i-1)+12}, K^d_{32(i-1)+13}, K^d_{32(i-1)+14}, K^d_{32(i-1)+15}, K^d_{32(i-1)+16}, K^d_{32(i-1)+17},$$
$$K^d_{32(i-1)+18}, K^d_{32(i-1)+19}, K^d_{32(i-1)+20}, K^d_{32(i-1)+21}, K^d_{32(i-1)+22}, K^d_{32(i-1)+23},$$
$$K^d_{32(i-1)+24}, K^d_{32(i-1)+25}, K^d_{32(i-1)+26}, K^d_{32(i-1)+27}, K^d_{32(i-1)+28}, K^d_{32(i-1)+29},$$
$$K^d_{32(i-1)+30}, K^d_{32(i-1)+31}) = (-K^c_{32(n-i+1)}, (K^c_{32(n-i+1)+30})^{-1}, -K^c_{32(n-i+1)+29},$$
$$(K^c_{32(n-i+1)+28})^{-1}, -K^c_{32(n-i+1)+27}, (K^c_{32(n-i+1)+26})^{-1}, -K^c_{32(n-i+1)+25},$$
$$(K^c_{32(n-i+1)+24})^{-1}, -K^c_{32(n-i+1)+23}, (K^c_{32(n-i+1)+22})^{-1}, -K^c_{32(n-i+1)+21},$$
$$(K^c_{32(n-i+1)+20})^{-1}, -K^c_{32(n-i+1)+19}, (K^c_{32(n-i+1)+18})^{-1}, -K^c_{32(n-i+1)+17},$$
$$(K^c_{32(n-i+1)+16})^{-1}, (K^c_{32(n-i+1)+15})^{-1}, -K^c_{32(n-i+1)+14}, (K^c_{32(n-i+1)+13})^{-1},$$
$$-K^c_{32(n-i+1)+12}, (K^c_{32(n-i+1)+11})^{-1}, -K^c_{32(n-i+1)+10}, (K^c_{32(n-i+1)+9})^{-1},$$
$$-K^c_{32(n-i+1)+8}, (K^c_{32(n-i+1)+7})^{-1}, -K^c_{32(n-i+1)+6}, (K^c_{32(n-i+1)+5})^{-1},$$
$$-K^c_{32(n-i+1)+4}, (K^c_{32(n-i+1)+3})^{-1}, -K^c_{32(n-i+1)+2}, (K^c_{32(n-i+1)+1})^{-1},$$
$$-K^c_{32(n-i+1)+31}), \ i = \overline{2...n}$$

Decryption round keys applied to the _rst round and after the output transformation associated with the encryption round keys as follows: $K^d_{32n+32+\ j}$=$K^c_{32n+64+j}$, $K^d_{32n+64+j} = K^c_{32n+32+j}$, $j = \overline{0...31}$.

IV. Results

Using the transformations SubBytes(), ShiftRows(), MixColumns() of the encryption algorithm AES as the round function network RFWKIDEA32-1 we developed encryption algorithm AES-RFWKIDEA32-1. In the algorithm, the number of rounds of encryption and key's length is variable and the user can select the number of rounds and the key's length in dependence of the degree of secrecy of information and speed encryption.

As in the encryption algorithms based on the Feistel network, the advantages of the encryption algorithm AES-RFWKIDEA32-1 are that, when encryption and decryption process used the same algorithm. In the encryption algorithm AES-RFWKIDEA32-1 in decryption process encryption round keys are used in reverse order, thus on the basis of operations necessary to compute the inverse. For example, if the round key is multiplied by the subblock, while decryption is is necessary to calculate the multiplicative inverse, if summarized, it is necessary to calculate the additive inverse.

It is known that the resistance of AES encryption algorithm is closely associated with resistance S-box, applied in the algorithm. In the S-box's encryption algorithm AES algebraic degree of nonlinearity deg = 7, nonlinearity NL = 112, resistance to linear cryptanalysis λ= 32= 256, resistance to diferential cryptanal ysis δ = = $4/256$, strict avalanche criterion SAC = 8, bit independence criterion BIC = 8.

In the encryption algorithm AES-RFWKIDEA32-1 resistance S-box is equal to resistance S-box's encryption algorithm AES, i.e., deg = 7, NL = 112, _ = 32=256, _ = 4=256, SAC= BIC=8.

V. Conclusions

It is known that as a network-based algorithms Feystel the resistance algorithm based on network RFWKIDEA32-1 closely associated with resistance round function. Therefore, selecting the transformations SubBytes(), ShiftRows(), Mix-Columns() of the encryption algorithm AES, based on round function network RFWKIDEA32-1 we developed relatively resistant encryption algorithm.

References Références Referencias

1. Bahrak B., Reza A.M. A Novel Impossible Di_erential Cryptanalysis of AES // proceedings of the Western European Workshop on Research in Cryptology 2007, Bochum, Germany, 2007.
2. Bahrak B., Reza A.M. Impossible Di_erential Attack on Seven-Round AES-128 // IET Information Security journal, Vol. 2, Number 2, pp. 2832, IET, 2008.
3. Biham E., Biryukov A., Shamir A.. Miss-in-the-Middle Attacks on IDEA, Khufu and Khafre // 6th Fast Software Encryption Workshop, LNCS 1636, L.R. Knud-sen,Ed., Springer-Verlag, 1999, pp. 124138.
4. Biham E., Keller N. Cryptanalysis of Reduced Variants of Rijndael // unpublished manuscript, 1999.
5. Borst J. Di_erential-Linear Cryptanalysis of IDEA // Department of Electrical Engineering, ESATCOSIC Technical Report 96/2, 14 pages.
6. Borst J., Knudsen L., Rijmen V. Two Attacks on Reduced IDEA (extended abstract) // Advances in Cryptology, Eurocrypt97, LNCS 1233, W. Fumy, Ed.,Springer-Verlag, 1997, pp. 113.
7. Chen J. Personal communications, August 2008.
8. Chen J., Hu Y., Wei Y. A New Method for Impossible Di_erential Cryptanalysis of 7-round Advanced Encryption Standard // Proceedings of International Conference on Communications, Circuits and Systems Proceedings 2006, Vol. 3, pp. 1577-1579, IEEE, 2006.
9. Chen J., Hu Y., Wei Y. A New Method for Impossib le Di_erential cryptanalysis of 8-Round Adanced Encryption Standard // Wuhan Univeristy Journan of NationalSciences, vol. 11, number 6, pp. 1559-1562, 2006. Lecture Notes in Computer Science: Authors' Instructions 13\
10. Chen J., Hu Y., Zhang Y. Impossible di_erential cryptanalysis of Advanced Encryption Standard // Science in China Series F: Information Sciences, vol. 50, number 3, pp. 342350, Springer-Verlag, 2007.
11. Cheon J., Kim M., Kim K., Lee J-Y., Kang S. Improved Impossible Di_erential Cryptanalysis of Rijndael and Crypton // proceedings of Information Security and Cryptology ICISC 2001, Lecture Notes in Computer Science 2288,pp. 3949, Springer, 2002.
12. Daemen J., Govaerts R. , J. Vandewalle. Cryptanalysis of 2.5 Rounds of IDEA (Extended Abstract) // Department of Electrical Engineering, ESATCOSIC Technical Report 93/1, Mar. 1993, pp. 16.
13. Daeman J., Rijmen V. AES proposal: Rijndael, version 2, 1999. http://csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf
14. Demirci H, Selcuk A. A Meet-in-the-Middle Attack on 8-Round AES // proceedings of Fast Software Encryption 15, Lecture Notes in Computer Science 5806,pp. 116126, Springer, 2008.
15. Ferguson N., Kelsey J., Lucks S., Schneier B., Stay M., Wagner D., Whiting D. Improved Cryptanalysis of Rijndael // proceedings of Fast Software Encryption 7, Lecture Notes in Computer Science 1978, pp. 213230, Springer_Verlag, 2001.
16. Gilbert H., Minier M. A collision attack on 7 rounds of Rijndael // proceedings of the Third AES Candidate Conference (AES3), pp. 230241, New York, USA, 2000.
17. Hawkes P. Di_erential-LinearWeak Key Classes of IDEA // Advances in Cryptology,Eurocrypt98, LNCS 1403, K. Nyberg, Ed., Springer-Verlag, 1998, pp. 112126.
18. Kelsey J., Schneier B., Wagner D. Key-Schedule Cryptanalysis of IDEA, GDES,GOST, SAFER and Triple-DES // Advances in Cryptology, Crypto96, LNCS 1109,N. Koblitz, Ed., Springer-Verlag, 1996, pp. 237251.
19. Knudsen L.R., Rijmen V. Truncated Di_erentials of IDEA // Department of Electrical Engineering, ESATCOSIC Technical Report 97/1.
20. Kim J., Hong S., Preneel B. Related-Key Rectangle Attacks on Reduced AES-192 and AES-256 // Proceedings of Fast Software Encryption 14, Lecture Notes in Computer Science 4593, pp. 225241, Springer-Verlag, 2007.
21. Lai X. On the Design and Security of Block Ciphers // Hartung-Gorre Verlag, Konstanz, 1992.
22. Lai X., Massey J.L. A Proposal for a New Block Encryption Standard // Advances in Cryptology, Eurocrypt90, LNCS 473, I.B. Damgard, Ed., Springer-Verlag, 1990, pp. 389404.
23. Lai X., Massey J.L., Murphy S. Markov Ciphers and Di_erential Cryptanalysis // Advances in Cryptology, Eurocrypt91, LNCS 547, D.W. Davies, Ed., Springer-Verlag, 1991, pp. 1738.

24. Lucks S. Attacking Seven Rounds of Rijndael under 192-bit and 256-bit Keys // proceedings of the Third AES Candidate Conference (AES3), pp. 215229, New York, USA, 2000.
25. Lu J., Dunkelman O., Keller N., Kim J. New Impossible Di_erential Attacks on AES
26. Meier W. On the Security of the IDEA Block Cipher // Advances in Cryptology,Eurocrypt93, LNCS 765, T. Helleseth, Ed., Springer-Verlag, 1994, pp. 371385.
27. Nakahara J., Paulo S.L.M. Barreto, Preneel B., Vandewalle J., Kim Y. SQUARE Attacks on Reduced-Round PES and IDEA Block Ciphers.
28. National Institute of Standards and Technology. Announcing the Advanced Encryption Standard (AES), 2001. Federal Information Processing Standards Pub-14 Lecture Notes in Computer Science: Authors' Instructions lication 197. http:// csrc.nist.gov/publications/fips/fips197/fips-197.pdf
29. Phan R. Ch-W. Impossible Di_erential Cryptanalysis of 7-round Advanced Encryption Standard (AES) // Information Processing Letters, Vol. 91, Number 1, pp. 33-38, Elsevier, 2004.
30. Tuychiev G.N. About networks IDEA328, IDEA324, IDEA322, IDEA321, created on the basis of network IDEA3216 // Infocommunications: Networks Technologies- Solutions. Tashkent, 2014. 2 (30), pp. 4550.
31. Tuychiev G.N. To the networks RFWKIDEA3216, RFWKIDEA328, RFWKIDEA324, RFWKIDEA322 and RFWKIDEA321, based on the net- work IDEA3216 // International Journal on Cryptography and Information Security (IJCIS), Vol. 5, No. 1, March 2015, pp. 9-20
32. Tuychiev G.N. About networks IDEA8-2, IDEA8-1 and RFWKIDEA8-4, RFWKIDEA8-2, RFWKIDEA8-1 developed on the basis of network IDEA8-4 // Uzbek mathematical journal, {Tashkent, 2014, 3, pp. 104{118
33. Tuychiev G.N. About networks PES8-2 and PES8-1, developed on the basis of network PES8-4 // Transactions of the international scientific conference Modern problems of applied mathematics and information technologies {Al {Khorezmiy 2012, Volume II, { Tashkent, 2014, pp. 28{32.
34. Tuychiev G.N. About networks RFWKPES8{4, RFWKPES8{2, RFWKPES8{1, developed on the basis of network PES8{4 // Transactions of the international scientific conference Modern problems of applied mathematics and information technologies {Al {Khorezmiy 2012, Volume 2, { Tashkent, 2014, pp. 32{36
35. Tuychiev G.N. About networks IDEA16{4, IDEA16{2, IDEA16{1, created on the basis of network IDEA16{8 // Compilation of theses and reports republican seminar Information security in the sphere communication and information. Problems and their solutions {Tashkent, 2014
36. Tuychiev G. New encryption algorithm based on network IDEA8-1 using of the transformation of the encryption algorithm AES // IPASJ International Journal of Computer Science, 2015, Volume 3, Issue 1, pp. 1-6
37. Tuychiev G. New encryption algorithm based on network RFWKIDEA8-1 using transformation of AES encryption algorithm // International Journal of Computer Networks and Communications Security, 2015, Vol. 3, NO. 2, pp. 43-47
38. Tuychiev G. New encryption algorithm based on network PES8-1 using of the transformations of the encryption algorithm AES // International Journal of Mul-tidisciplinary in Cryptology and Information Security, 2015, vol.4., 1, pp. 1-5
39. Tuychiev G. New encryption algorithm based on network RFWKPES8-1 using of the transformations of the encryption algorithm AES // International Journal of Multidisciplinary in Cryptology and Information Security, 2014, vol.3., 6, pp. 31-34
40. Tuychiev G. New encryption algorithm based on network IDEA16-1 using of the transformation of the encryption algorithm AES // IPASJ International Journal of Information Technology, 2015, Volume 3, Issue 1, pp. 6-12
41. U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology. Data Encryption Standard (DES), 1979. Federal Information Pro-cessing Standards Publication 46-3, http:// csrc.nist.gov/publications/fips/fips46-3/fips 46- .pdf
42. Zhang W., Wu W., Feng D. New Results on Impossible Di_erential Cryptanalysis of Reduced AES // proceedings of ICISC 2007, Lecture Notes in Computer Science 4817, pp. 239250, Springer-Verlag, 2007.
43. Lecture Notes in Computer Science: Authors' Instructions 15 Zhang W., Wu W., Zhang L. Dengguo Feng, Improved Related-Key Impossible Di_erential Attacks on Reduced-Round AES-192 // Proceedings of Selected Areas in Cryptography 2006, Lecture Notes in Computer Science 4356, pp. 1527, Springer-Verlag, 2007.

Global Journals Inc. (US) Guidelines Handbook 2015

www.GlobalJournals.org