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

Aripov Mersaid, Tuychiev Gulom

(Corresponding author: Gulom Tuychiev)

National University of Uzbekistan, Republic of Uzbekistan, Tashkent

(Email: mirsaidaripov@mail.ru, blasterjon@gmail.com)

(Received Aug. 12, 2015; revised and accepted Oct. 2, 2015)

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

1 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 [37]. Out of 15 submitted algorithms the Rijndael cipher by Daemen and Rijmen [22] was chosen to become the new Advanced Encryption Standard in November 2001 [15]. The Advanced Encryption Standard is a block cipher with a fixed block length of 128 bits. It supports three different 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 transformations occurring to the elements of the *State*. Each round consists in applying 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 MixColumns() 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*.

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.

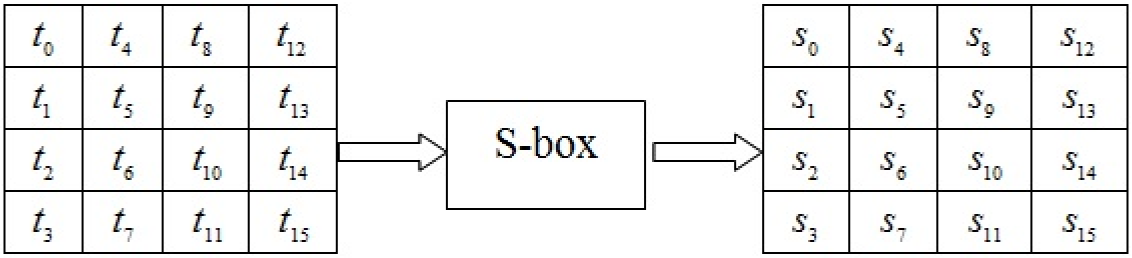

Figure 1: SubBytes() transformation

Similarly, the third and fourth rows are shifted by offsets of two and three respectively. Figure 2 illustrates the ShiftRows() transformation.

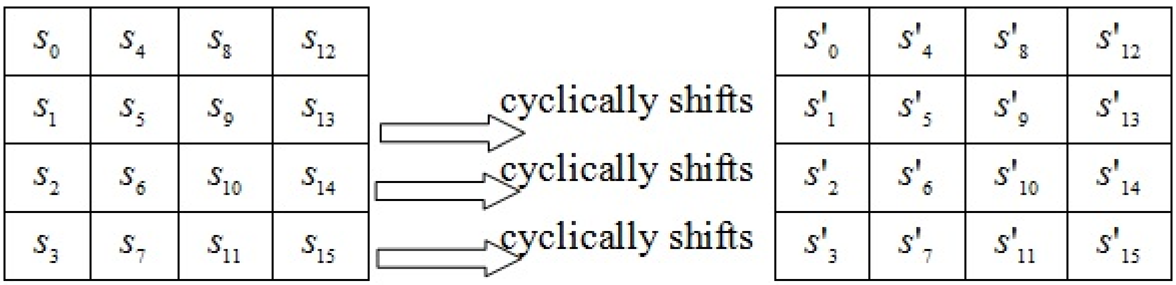

Figure 2: ShiftRows() transformation

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:

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

Figure 3 illustrates the MixColumns() transformation.

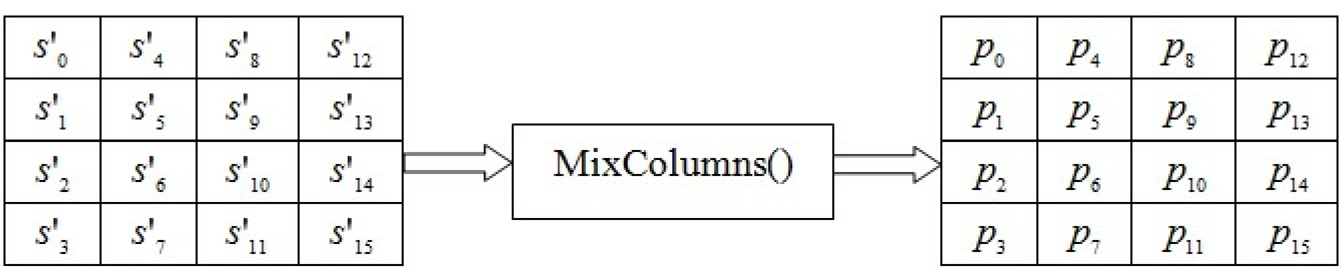

Figure 3: MixColumns() transformation

2 Analysis of AES, PES and IDEA

The first attack is a SQUARE attack suggested in [10] which uses 2^{128} - 2^{119} chosen plaintexts and 2^{120} encryptions. The second attack is a meet-in-the-middle attack proposed in [13] that requires 2^{32} chosen plaintexts and has a time complexity equivalent to almost 2128 encryptions. Recently, another attack on 7-round AES-128 was presented in [19]. 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 [3]. The resulting impossible differential 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 [3, 9, 10, 16, 19, 24]. The two most notable ones are the SQUARE attack on 8-round AES-192 presented in [10] 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 [24] 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 ¡ n ¡ 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 [3, 9, 10, 19, 24]. The best attack is the meet in the middle attack in [24] 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 [42] for the latest results on related-key impossible differential attacks on AES and to [17] for the latest results on related-key rectangle attacks on AES.

The strength of AES with respect to impossible differentials was challenged several times. The first attack of this kind is a 5-round attack presented in [5]. This attack is improved in [7] to a 6-round attack. In [16], 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 2^{186} encryptions (or $2^{250.5}$ encryptions for AES-256). The time complexity of the latter attack was improved in [3] to 2^{162} encryptions for AES-192. In [19] a new 7-round impossible differential attack was presented. The new attack uses a different impossible differential, which is of the same general type as the one used in previous attacks (but has a slightly different structure). Using the new impossible differential 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 [3, 20] to use $2^{115.5}$ chosen plaintexts with time complexity of 2^{119} encryptions.

The last application of impossible differential cryptanalysis to AES was the extension of the 7-round attack from [19] to 8-round AES-256 in [3]. The extended attack has a data complexity of $2^{116.5}$ chosen plaintexts and time complexity of $2^{247.5}$ encryption. We note that there were three more claimed impossible differential attacks on AES in [40, 41, 43]. However, as all these attacks are flawed [2]. In paper [6] 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 [16, 19] 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 plaintexts and has a time complexity of $2^{129.7}$ memory accesses. These results are significantly better than any previously published impossible differential attack on AES. We summarize results along with previously known results in Table 1.

The Proposed Encryption Standard (PES) is a 64-bit block cipher, using a 128-bit key, designed by Lai and Massey in 1990 (see [11]) and was a predecessor to IDEA (International Data Encryption Algorithm) [8]. IDEA was originally called IPES (Improved PES). PES iterates eight rounds plus an output transformation. The cryptanalysis of PES and IDEA presented on Table 2 and Table 3.

On the basis of encryption algorithm IDEA and Lai-Massey scheme developed the networks IDEA32-1 and RFWKIDEA32-1, consisting from one round function [27, 36]. 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(), AddRoundKey() AES encryption algorithm as a round function networks IDEA8-1 [28], RFWKIDEA8-1 [28], PES8-1 [29], RFWKPES8-1 [30], IDEA16-1 [26], created encryption algorithms AES-IDEA8-1 [33], AES-RFWKIDEA8-1 [35], AES-PES8-1 [34], AES-RFWKPES8-1 [31], AES-IDEA16-1 [32].

In this paper developed block encryption algorithm AES-RFWKIDEA32-1 based network RFWKIDEA32-1 [36] 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.

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 [10]
7	$2^{117.5}$	2^{121}	Impossible Differential [10]
7	$2^{117.5}$	2^{119}	Impossible Differential [20, 3]
7	2^{32}	2^{128}	Meet in the middle [13]
7	$2^{112.2}$	$2^{117.2}$ MA	Impossible Differential [6]
AES-192			
7	2^{32}	2^{184}	Square [9]
7	$19 \cdot 2^{32}$	2^{155}	Square [10]
7	2^{92}	$2^{186.2}$	Impossible Differential [16]
7	$2^{115.5}$	2^{119}	Impossible Differential [3]
7	2^{92}	2^{162}	Impossible Differential [3]
7	2^{34+n}	$2^{208-n} + 2^{82+n}$	Meet in the middle [24]
8	$2^{128} - 2^{119}$	2^{188}	Square [10]
7	$2^{113.8}$	$2^{118.8}$ MA	Impossible Differential [6]
7	$2^{91.2}$	$2^{139.2}$	Impossible Differential [6]
AES-256			
7	2^{32}	2^{200}	Square [9]
7	$21 \cdot 2^{32}$	2^{172}	Square [10]
7	$2^{92.5}$	$2^{250.5}$	Impossible Differential [16]
7	2^{32}	2^{208}	Meet in the middle [24]
7	2^{34+n}	$2^{208-n} + 2^{82+n}$	Meet in the middle [24]
7	$2^{115.5}$	2^{119}	Impossible Differential [3]
8	$2^{116.5}$	$2^{247.5}$	Impossible Differential [3]
8	$2^{128} - 2^{119}$	2^{204}	Square [10]
8	2^{32}	2^{209}	Meet in the middle [24]
7	$2^{113.8}$	$2^{118.8}$ MA	Impossible Differential [6]
7	2^{92}	2^{163} MA	Impossible Differential [6]
8	$2^{111.1}$	$2^{227.8}$ MA	Impossible Differential [6]
8	$2^{89.1}$	$2^{229.7}$ MA	Impossible Differential [6]

Table 2: A summary of the attacks on IDEA

Attack Type	Year	Attacked Rounds	Key Bits round	Chosen Plaintext	Time
Differential [12]	1993	2	32	2^{10}	2^{42}
Differential [38]	1993	2.5	32	2^{10}	2^{32}
Differential [12]	1993	2.5	96	2^{10}	2^{106}
Related-Key Differential [39]	1996	3	32	6	$6 \cdot 2^{32}$
Differential-Linear [21]	1996	3	32	2^{30}	2^{44}
Differential [1]	1996	3	32	2^{30}	$0.75 \cdot 2^{44}$
Truncated Differential [23, 21]	1997	3.5	48	2^{56}	2^{67}
Miss-in-the-middle [25]	1998	3.5	64	$2^{38.5}$	2^{53}
Miss-in-the-middle [25]	1998	4	69	2^{37}	2^{70}
Related-Key Differential-Linear [4]	1998	4	15	38.3	-
Miss-in-the-Middle [25]	1998	4.5	80	2^{64}	2^{112}
Square attack [18]	2000	2.5	77	$3 \cdot 2^{16}$	$2^{63} + 2^{47}$
Square attack [18]	2000	2.5	31	2^{32}	2^{62}
Square [18]	2000	2.5	31	2^{48}	2^{79}
Related-Key Square [18]	2001	2.5	32	2	2^{41}

Table 3: A summary of the attacks on PES

Attack Type	Year	Attacked Rounds	Key Bits round	Chosen Plaintext	Time
Differential [14]	1991	7	96	2^{64}	2^{160}
Square [18]	2000	2.5	31	2^{17}	2^{47}
Square [18]	2001	2.5	31	2^{32}	2^{63}
Related-Key Square [18]	2001	2.5	32	2	241

3 The Encryption Algorithm AES-RFWKIDEA32-1

3.1 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 of 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 $K_{32(i-1)}$, $K_{32(i-1)+1}$, ..., $K_{32(i-1)+31}$,, $i=\overline{1...n+1}$ 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 MixColumns() transformation we obtain 8-bits subblocks y_0, y_1, ..., y_{15}, where $y_0{=}p_0$, $y_1{=}p_1$, ..., $y_{15}{=}p_{15}$.

The S-box SubBytes() transformation shown in Table 4 and is the only nonlinear 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 4: 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, ..., X_0^{31}, and performs the following steps:

1) Subblocks X_0^0, X_0^1, ..., X_0^{31} summed by XOR respectively with round keys 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, ..., X_0^{31} multiplied and summed respectively with the round keys $K_{32(i-1)}$, $K_{32(i-1)+1}$,

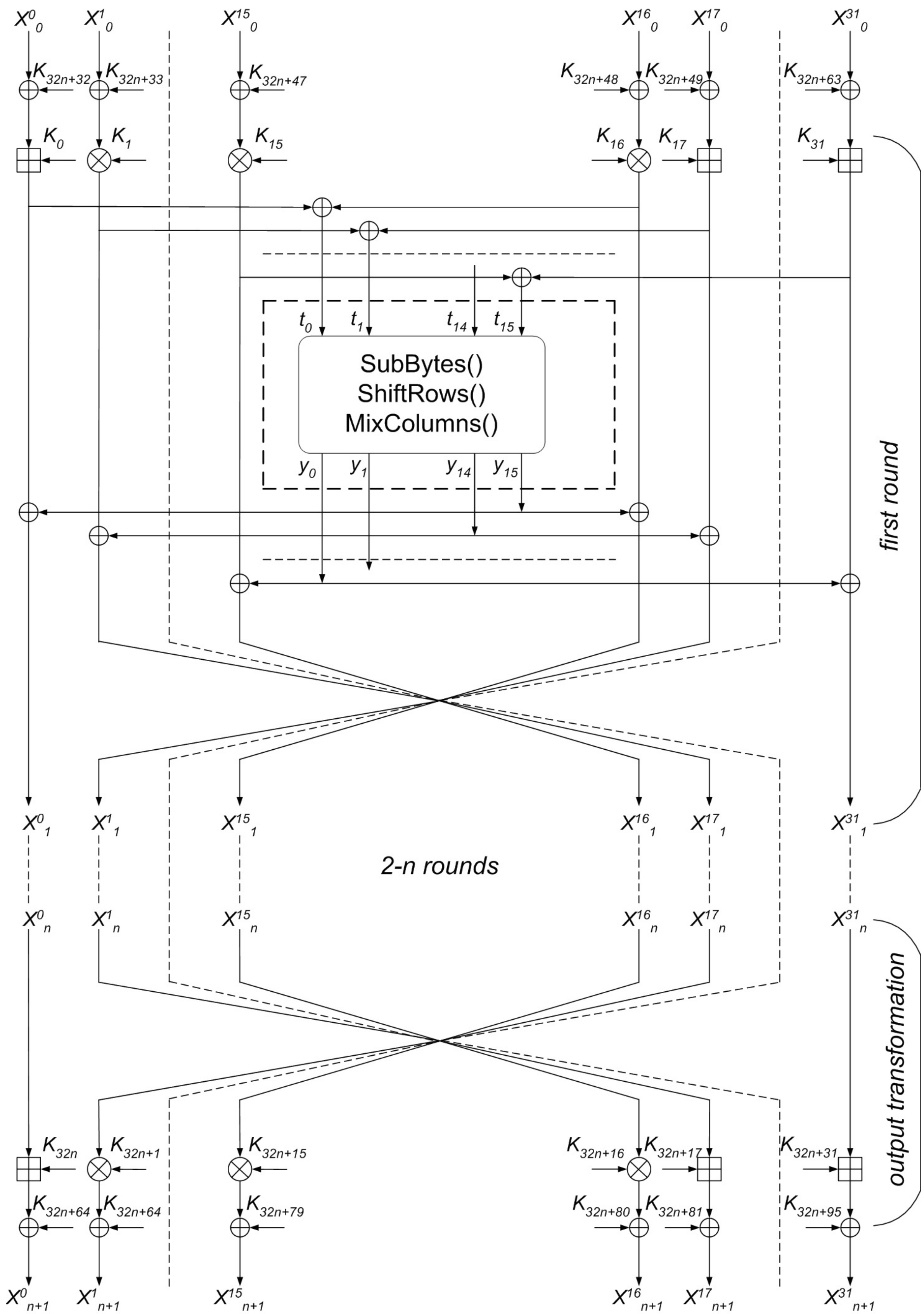

Figure 4: The scheme n-rounded encryption algorithm AES-RFWKIDEA32-1

..., $K_{32(i-1)+31}$ and calculated 8-bit subblocks $t_0, t_1, \ldots, t_{15}$. This step can be represented as follows:

$$\begin{aligned}
t_0 &= (X_{i-1}^0 + K_{32(i-1)}) \oplus (X_{i-1}^{16} \cdot K_{32(i-1)+16}),\\
t_1 &= (X_{i-1}^1 \cdot K_{32(i-1)+1}) \oplus (X_{i-1}^{17} + K_{32(i-1)+17}),\\
t_2 &= (X_{i-1}^2 + K_{32(i-1)+2}) \oplus (X_{i-1}^{18} \cdot K_{32(i-1)+18}),\\
t_3 &= (X_{i-1}^3 \cdot K_{32(i-1)+3}) \oplus (X_{i-1}^{19} + K_{32(i-1)+19}),\\
t_4 &= (X_{i-1}^4 + K_{32(i-1)+4}) \oplus (X_{i-1}^{20} \cdot K_{32(i-1)+20}),\\
t_5 &= (X_{i-1}^5 \cdot K_{32(i-1)+5}) \oplus (X_{i-1}^{21} + K_{32(i-1)+21}),\\
t_6 &= (X_{i-1}^6 + K_{32(i-1)+6}) \oplus (X_{i-1}^{22} \cdot K_{32(i-1)+22}),\\
t_7 &= (X_{i-1}^7 \cdot K_{32(i-1)+7}) \oplus (X_{i-1}^{23} + K_{32(i-1)+23}),\\
t_8 &= (X_{i-1}^8 + K_{32(i-1)+8}) \oplus (X_{i-1}^{24} \cdot K_{32(i-1)+24}),\\
t_9 &= (X_{i-1}^9 \cdot K_{32(i-1)+9}) \oplus (X_{i-1}^{25} + K_{32(i-1)+25}),\\
t_{10} &= (X_{i-1}^{10} + K_{32(i-1)+10}) \oplus (X_{i-1}^{26} \cdot K_{32(i-1)+26}),\\
t_{11} &= (X_{i-1}^{11} \cdot K_{32(i-1)+11}) \oplus (X_{i-1}^{27} + K_{32(i-1)+27}),\\
t_{12} &= (X_{i-1}^{12} + K_{32(i-1)+12}) \oplus (X_{i-1}^{28} \cdot K_{32(i-1)+28}),\\
t_{13} &= (X_{i-1}^{13} \cdot K_{32(i-1)+13}) \oplus (X_{i-1}^{29} + K_{32(i-1)+29}),\\
t_{14} &= (X_{i-1}^{14} + K_{32(i-1)+14}) \oplus (X_{i-1}^{30} \cdot K_{32(i-1)+30}),\\
t_{15} &= (X_{i-1}^{15} \cdot K_{32(i-1)+15}) \oplus (X_{i-1}^{31} + K_{32(i-1)+31}), i = 1.
\end{aligned}$$

3) Performed SubBytes(), ShiftRows(), MixColumns() transformation. Output subblocks of the round function of the encryption algorithm are $y_0, y_1, \ldots, y_{31}$.

4) Subblocks $y_0, y_1, \ldots, y_{31}$ are summed to XOR with subblocks $X_{i-1}^0, X_{i-1}^1, \ldots, X_{i-1}^{31}$, i.. $X_{i-1}^j = X_{i-1}^j \oplus y_{15-j}$, $X_{i-1}^{j+16} = X_{i-1}^{j+16} \oplus y_{15-j}$, $j = \overline{0...15}$, $i = 1$.

5) At the end of the round subblocks X_{i-1}^j and X_{i-1}^{31-j}, $j = \overline{1...15}$ swapped, i.., $X_i^0 = X_{i-1}^0$, $X_i^1 = X_{i-1}^{30}$, $X_i^2 = X_{i-1}^{29}$, $X_i^3 = X_{i-1}^{28}$, $X_i^4 = X_{i-1}^{27}$, $X_i^5 = X_{i-1}^{26}$, $X_i^6 = X_{i-1}^{25}$, $X_i^7 = X_{i-1}^{24}$, $X_i^8 = X_{i-1}^{23}$, $X_i^9 = X_{i-1}^{22}$, $X_i^{10} = X_{i-1}^{21}$, $X_i^{11} = X_{i-1}^{20}$, $X_i^{12} = X_{i-1}^{19}$, $X_i^{13} = X_{i-1}^{18}$, $X_i^{14} = X_{i-1}^{17}$, $X_i^{15} = X_{i-1}^{16}$, $X_i^{16} = X_{i-1}^{15}$, $X_i^{17} = X_{i-1}^{14}$, $X_i^{18} = X_{i-1}^{13}$, $X_i^{19} = X_{i-1}^{12}$, $X_i^{20} = X_{i-1}^{11}$, $X_i^{21} = X_{i-1}^{10}$, $X_i^{22} = X_{i-1}^{9}$, $X_i^{23} = X_{i-1}^{8}$, $X_i^{24} = X_{i-1}^{7}$, $X_i^{25} = X_{i-1}^{6}$, $X_i^{26} = X_{i-1}^{5}$, $X_i^{27} = X_{i-1}^{4}$, $X_i^{28} = X_{i-1}^{3}$, $X_i^{29} = X_{i-1}^{2}$, $X_i^{30} = X_{i-1}^{1}$, $X_i^{31} = X_{i-1}^{31}$, $i = 1$.

6) Repeating steps 2-5 n times, i.e., $i = \overline{2...n}$ obtain subblocks $X_n^0, X_n^1, \ldots, X_n^{31}$.

7) In output transformation round keys are multiplied and summed into subblocks, i.e. $X_{n+1}^0 = X_n^0 + K_{32n}$, $X_{n+1}^1 = X_n^{30} \cdot K_{32n+1}$, $X_{n+1}^2 = X_n^{29} + K_{32n+2}$, $X_{n+1}^3 = X_n^{28} \cdot K_{32n+3}$, $X_{n+1}^4 = X_n^{27} + K_{32n+4}$, $X_{n+1}^5 = X_n^{26} \cdot K_{32n+5}$, $X_{n+1}^6 = X_n^{25} + K_{32n+6}$, $X_{n+1}^7 = X_n^{24} \cdot K_{32n+7}$, $X_{n+1}^8 = X_n^{23} + K_{32n+8}$, $X_{n+1}^9 = X_n^{22} \cdot K_{32n+9}$, $X_{n+1}^{10} = X_n^{21} + K_{32n+10}$, $X_{n+1}^{11} = X_n^{20} \cdot K_{32n+11}$, $X_{n+1}^{12} = X_n^{19} + K_{32n+12}$, $X_{n+1}^{13} = X_n^{18} \cdot K_{32n+13}$, $X_{n+1}^{14} = X_n^{17} + K_{32n+14}$, $X_{n+1}^{15} = X_n^{16} \cdot K_{32n+15}$, $X_{n+1}^{16} = X_n^{15} \cdot K_{32n+16}$, $X_{n+1}^{17} = X_n^{14} + K_{32n+17}$, $X_{n+1}^{18} = X_n^{13} \cdot K_{32n+18}$, $X_{n+1}^{19} = X_n^{12} + K_{32n+19}$, $X_{n+1}^{20} = X_n^{11} \cdot K_{32n+20}$, $X_{n+1}^{21} = X_n^{10} + K_{32n+21}$, $X_{n+1}^{22} = X_n^{9} \cdot K_{32n+22}$, $X_{n+1}^{23} = X_n^{8} + K_{32n+23}$, $X_{n+1}^{24} = X_n^{7} \cdot K_{32n+24}$, $X_{n+1}^{25} = X_n^{6} + K_{32n+25}$, $X_{n+1}^{26} = X_n^{5} \cdot K_{32n+26}$, $X_{n+1}^{27} = X_n^{4} + K_{32n+27}$, $X_{n+1}^{28} = X_n^{3} \cdot K_{32n+28}$, $X_{n+1}^{29} = X_n^{2} + K_{32n+29}$, $X_{n+1}^{30} = X_n^{1} \cdot K_{32n+30}$, $X_{n+1}^{31} = X_n^{31} + K_{32n+31}$;

8) Subblocks $X_{n+1}^0, X_{n+1}^1, \ldots, X_{n+1}^{31}$ are summed to XOR with the round key $K_{32n+64}, K_{32n+65}, \ldots, K_{32n+95}$: $X_{n+1}^j = X_{n+1}^j \oplus K_{32n+64+j}$, $j = \overline{0...31}$. As ciphertext plaintext X receives the combined 16-bit subblocks $X_{n+1}^0 || X_{n+1}^1 || ... || X_{n+1}^{31}$.

3.2 Key Generation of the Encryption Algorithm AES-RFWKIDEA32-1

In n-rounded encryption algorithm AES-RFWKIDEA32-1 in each round we applied sixteen (32) round keys of the 8-bit and output transformation thirty two round keys of the 8-bit. In addition, before the first round and after the output transformation we used thirty two 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_i^c instead of K_i, while decryption used decryption round keys K_i^d. 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 keys K_0^c, K_1^c,..., $K_{Lenght-1}^c$, $Lenght = l/8$, here $K = \{k_0, k_1, ..., k_{l-1}\}$, $K_0^c = \{k_0, k_1, ..., k_7\}$, $K_1^c = \{k_8, k_9, ..., k_{15}\}$,..., $K_{Lenght-1}^c = \{k_{l-8}, k_{l-7}, ..., k_{l-1}\}$ and $K = K_0^c || K_1^c ||...|| K_{Lenght-1}^c$. Then we calculate $K_L = K_0^c \oplus K_1^c \oplus ... \oplus K_{Lenght-1}^c$. If $K_L = 0$ then K_L is chosen as 0xC5, i.e. $K_L = 0xC5$. When generating a round keys K_i^c, $i = \overline{Lenght...32n + 95}$, we used transformation *SubBytes()* and *RotWord8()*, here *SubBytes()*-is transformation 8-bit subblock 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 computed as $K_i^c = SubBytes(K_{i-Lenght+1}^c) \oplus SubBytes(RotWord8(K_{i-Lenght}^c)) \oplus Rcon[imod8] \oplus K_L$, otherwise $K_i^c = SubBytes(K_{i-Lenght}^c) \oplus SubBytes(K_{i-Lenght+1}^c) \oplus K_L$. 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 encryption round keys as follows:

$$\begin{aligned}
& (K_{32n}^d, K_{32n+1}^d, K_{32n+2}^d, K_{32n+3}^d, K_{32n+4}^d, K_{32n+5}^d, K_{32n+6}^d, K_{32n+7}^d, K_{32n+8}^d, K_{32n+9}^d, K_{32n+10}^d, K_{32n+11}^d, \\
& \quad K_{32n+12}^d, K_{32n+13}^d, K_{32n+14}^d, K_{32n+15}^d, K_{32n+16}^d, K_{32n+17}^d, K_{32n+18}^d, K_{32n+19}^d, K_{32n+20}^d, K_{32n+21}^d, K_{32n+22}^d, \\
& \quad K_{32n+23}^d, K_{32n+24}^d, K_{32n+25}^d, K_{32n+26}^d, K_{32n+27}^d, K_{32n+28}^d, K_{32n+29}^d, K_{32n+30}^d, K_{32n+31}^d) \\
= & (-K_0^c, (K_1^c)^{-1}, -K_2^c, (K_3^c)^{-1}, -K_4^c, (K_5^c)^{-1}, -K_6^c, (K_7^c)^{-1}, -K_8^c, (K_9^c)^{-1}, -K_{10}^c, (K_{11}^c)^{-1}, \\
& \quad -K_{12}^c, (K_{13}^c)^{-1}, -K_{14}^c, (K_{15}^c)^{-1}, (K_{16}^c)^{-1}, -K_{17}^c, (K_{18}^c)^{-1}, -K_{19}^c, (K_{20}^c)^{-1}, -K_{21}^c, (K_{22}^c)^{-1}, -K_{23}^c, (K_{24}^c)^{-1}, \\
& \quad -K_{25}^c, (K_{26}^c)^{-1}, -K_{27}^c, (K_{28}^c)^{-1}, -K_{29}^c, (K_{30}^c)^{-1}, -K_{31}^c).
\end{aligned}$$

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

$$\begin{aligned}
& (K_{320}^d, K_{321}^d, K_{322}^d, K_{323}^d, K_{324}^d, K_{325}^d, K_{326}^d, K_{327}^d, K_{328}^d, K_{329}^d, K_{330}^d, K_{331}^d, K_{332}^d, K_{333}^d, K_{334}^d, K_{335}^d, K_{336}^d, \\
& \quad K_{337}^d, K_{338}^d, K_{339}^d, K_{340}^d, K_{341}^d, K_{342}^d, K_{343}^d, K_{344}^d, K_{345}^d, K_{346}^d, K_{347}^d, K_{348}^d, K_{349}^d, K_{350}^d, K_{351}^d) \\
= & (-K_0^c, (K_1^c)^{-1}, -K_2^c, (K_3^c)^{-1}, -K_4^c, (K_5^c)^{-1}, -K_6^c, (K_7^c)^{-1}, -K_8^c, (K_9^c)^{-1}, -K_{10}^c, (K_{11}^c)^{-1}, -K_{12}^c, \\
& \quad (K_{13}^c)^{-1}, -K_{14}^c, (K_{15}^c)^{-1}, (K_{16}^c)^{-1}, \\
& \quad -K_{17}^c, (K_{18}^c)^{-1}, -K_{19}^c, (K_{20}^c)^{-1}, -K_{21}^c, (K_{22}^c)^{-1}, -K_{23}^c, (K_{24}^c)^{-1}, \\
& \quad -K_{25}^c, (K_{26}^c)^{-1}, -K_{27}^c, (K_{28}^c)^{-1}, -K_{29}^c, (K_{30}^c)^{-1}, -K_{31}^c).
\end{aligned}$$

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

$$\begin{aligned}
& (K_0^d, K_1^d, K_2^d, K_3^d, K_4^d, K_5^d, K_6^d, K_7^d, K_8^d, K_9^d, K_{10}^d, K_{11}^d, K_{12}^d, K_{13}^d, K_{14}^d, K_{15}^d, K_{16}^d, K_{17}^d, K_{18}^d, K_{19}^d, K_{20}^d, K_{21}^d, \\
& \quad K_{22}^d, K_{23}^d, K_{24}^d, K_{25}^d, K_{26}^d, K_{27}^d, K_{28}^d, K_{29}^d, K_{30}^d, K_{31}^d) \\
= & (-K_{32n}^c, (K_{32n+1}^c)^{-1}, -K_{32n+2}^c, (K_{32n+3}^c)^{-1}, -K_{32n+4}^c, (K_{32n+5}^c)^{-1}, -K_{32n+6}^c, (K_{32n+7}^c)^{-1}, -K_{32n+8}^c, \\
& \quad (K_{32n+9}^c)^{-1}, -K_{32n+10}^c, (K_{32n+11}^c)^{-1}, -K_{32n+12}^c, (K_{32n+13}^c)^{-1}, -K_{32n+14}^c, (K_{32n+15}^c)^{-1}, (K_{32n+16}^c)^{-1}, \\
& \quad -K_{32n+17}^c, (K_{32n+18}^c)^{-1}, -K_{32n+19}^c, (K_{32n+20}^c)^{-1}, -K_{32n+21}^c, (K_{32n+22}^c)^{-1}, -K_{32n+23}^c, (K_{32n+24}^c)^{-1}, \\
& \quad -K_{32n+25}^c, (K_{32n+26}^c)^{-1}, -K_{32n+27}^c, (K_{32n+28}^c)^{-1}, -K_{32n+29}^c, (K_{32n+30}^c)^{-1}, -K_{32n+31}^c).
\end{aligned}$$

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

$$\begin{aligned}
& (K_{32(i-1)}^d, K_{32(i-1)+1}^d, K_{32(i-1)+2}^d, K_{32(i-1)+3}^d, K_{32(i-1)+4}^d, K_{32(i-1)+5}^d, K_{32(i-1)+6}^d, K_{32(i-1)+7}^d, K_{32(i-1)+8}^d, \\
& \quad K_{32(i-1)+9}^d, K_{32(i-1)+10}^d, K_{32(i-1)+11}^d, K_{32(i-1)+12}^d, K_{32(i-1)+13}^d, K_{32(i-1)+14}^d, K_{32(i-1)+15}^d, K_{32(i-1)+16}^d, \\
& \quad K_{32(i-1)+17}^d, K_{32(i-1)+18}^d, K_{32(i-1)+19}^d, K_{32(i-1)+20}^d, K_{32(i-1)+21}^d, K_{32(i-1)+22}^d, K_{32(i-1)+23}^d, K_{32(i-1)+24}^d, \\
& \quad K_{32(i-1)+25}^d, K_{32(i-1)+26}^d, K_{32(i-1)+27}^d, K_{32(i-1)+28}^d, K_{32(i-1)+29}^d, K_{32(i-1)+30}^d, K_{32(i-1)+31}^d) \\
= & (-K_{32(n-i+1)}^c, (K_{32(n-i+1)+30}^c)^{-1}, -K_{32(n-i+1)+29}^c, (K_{32(n-i+1)+28}^c)^{-1}, -K_{32(n-i+1)+27}^c, (K_{32(n-i+1)+26}^c)^{-1}, \\
& \quad -K_{32(n-i+1)+25}^c, (K_{32(n-i+1)+24}^c)^{-1}, -K_{32(n-i+1)+23}^c, (K_{32(n-i+1)+22}^c)^{-1}, -K_{32(n-i+1)+21}^c, \\
& \quad (K_{32(n-i+1)+20}^c)^{-1}, -K_{32(n-i+1)+19}^c, (K_{32(n-i+1)+18}^c)^{-1}, -K_{32(n-i+1)+17}^c, (K_{32(n-i+1)+16}^c)^{-1}, \\
& \quad (K_{32(n-i+1)+15}^c)^{-1}, -K_{32(n-i+1)+14}^c, (K_{32(n-i+1)+13}^c)^{-1}, -K_{32(n-i+1)+12}^c, (K_{32(n-i+1)+11}^c)^{-1}, \\
& \quad -K_{32(n-i+1)+10}^c, (K_{32(n-i+1)+9}^c)^{-1}, -K_{32(n-i+1)+8}^c, (K_{32(n-i+1)+7}^c)^{-1}, -K_{32(n-i+1)+6}^c, (K_{32(n-i+1)+5}^c)^{-1}, \\
& \quad -K_{32(n-i+1)+4}^c, (K_{32(n-i+1)+3}^c)^{-1}, -K_{32(n-i+1)+2}^c, (K_{32(n-i+1)+1}^c)^{-1}, -K_{32(n-i+1)+31}^c), i = \overline{2...n}
\end{aligned}$$

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

4 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 $\lambda = 32/256$, resistance to differential cryptanalysis $\delta = 4/256$, 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, $NL = 112$, $\lambda = 32/256$, $\delta = 4/256$, SAC= BIC=8.

5 Conclusions

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

References

[1] J. Borst, "Differential-linear cryptanalysis of idea," *Department of Electrical Engineering, ESATCOSIC Technical Report 96/2, 14 pages.*

[2] J. Chen, "Personal communications," august 2008.

[3] D. Feng, W. Zhang, W. Wu, "New results on impossible differential cryptanalysis of reduced AES," in *Proceedings of ICISC 2007*, LNCS 4817, pp. 239–250, 2007.

[4] P. Hawkes, "Differential-linear weak key classes of idea," in *Advances in Cryptology (Eurocrypt98)*, LNCS 1403, pp. 112–126, Springer, 1998.

[5] N. Keller, E. Biham, "Cryptanalysis of reduced variants of rijndael," *unpublished manuscript*, 1999.

[6] N. Keller, J. Kim, J. Lu, O. Dunkelman, "New impossible differential attacks on AES," in *Indocrypt 2008*, LNCS 5365, pp. 279–293, Springer, 2008.

[7] K. Kim, J. Y. Lee, S. Kang, J. Cheon, M. Kim, "Improved impossible differential cryptanalysis of rijndael and crypton," in *Proceedings of Information Security and Cryptology (ICISC'01)*, LNCS 2288, pp. 39–49, Springer, 2002.

[8] X. Lai, "On the design and security of block ciphers," *Doctoral Theses, Hartung-Gorre*, 1992.

[9] S. Lucks, "Attacking seven rounds of rijndael under 192-bit and 256-bit keys," in *Proceedings of the Third AES Candidate Conference (AES3)*, pp. 215–229, 2000.

[10] S. Lucks, B. Schneier, M. Stay, D. Wagner, D. Whiting, N. Ferguson, J. Kelsey, "Improved cryptanalysis of rijndael," in *Proceedings of Fast Software Encryption 7*, LNCS 1978, pp. 213–230, Springer, 2001.

[11] J. L. Massey, X. Lai, "A proposal for a new block encryption standard," in *Advances in Cryptology (Eurocrypt90)*, LNCS 473, pp. 389–404, Springer, 1990.

[12] W. Meier, "On the security of the idea block cipher," in *Advances in Cryptology (Eurocrypt93)*, LNCS 765, pp. 371–385, Springer, 1994.

[13] M. Minier, H. Gilbert, "A collision attack on 7 rounds of rijndael," in *Proceedings of the Third AES Candidate Conference (AES3)*, pp. 230–241, 2000.

[14] S. Murphy, X. Lai, J. L. Massey, "Markov ciphers and differential cryptanalysis," in *Advances in Cryptology (Eurocrypt91)*, LNCS 547, pp. 17–38, Springer, 1991.

[15] National Institute of Standards and Technology. Announcing the Advanced Encryption Standard (AES), "Federal information processing standards publication 197," 2001. (`http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf`)

[16] R. Ch W. Phan, "Impossible differential cryptanalysis of 7-round advanced encryption standard (AES)," *Information Processing Letters*, vol. 91, no. 1, pp. 33–38, 2004.

[17] B. Preneel, J. Kim, S. Hong, "Related-key rectangle attacks on reduced AES-192 and AES-256," in *Proceedings of Fast Software Encryption 14*, LNCS 4593, pp. 225–241, Springer, 2007.

[18] B. Preneel, J. Vandewalle, Y. Kim, J. Nakahara, P. S. L. M. Barreto, "Square attacks on reduced-round pes and idea block ciphers," in *23rd Symposium on Information Theory*, pp. 187–195, 2002.

[19] A. M. Reza, B. Bahrak, "A novel impossible differential cryptanalysis of AES," in *Proceedings of the Western European Workshop on Research in Cryptology 2007*, 2007.

[20] A. M. Reza, B. Bahrak, "Impossible differential attack on seven-round AES-128," *IET Information Security Journal*, vol. 2, no. 2, pp. 28–32, 2008.

[21] V. Rijmen, J. Borst, L. Knudsen, "Two attacks on reduced idea (extended abstract)," in *Advances in Cryptology (Eurocrypt97)*, LNCS 1233, pp. 1–13, Springer, 1997.

[22] V. Rijmen, J. Daeman, "AES proposal: Rijndael, version 2," 1999. (`http://csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf`)

[23] V. Rijmen, L. R. Knudsen, "Truncated differentials of idea," *Department of Electrical Engineering, ESATCOSIC Technical Report 97/1.*

[24] A. Selcuk, H. Demirci, "A meet-in-the-middle attack on 8-round AES," in *Proceedings of Fast Software Encryption 15*, LNCS 5806, pp. 116–126, Springer, 2008.

[25] A. Shamir, E. Biham, A. Biryukov, "Miss-in-the-middle attacks on idea, khufu and khafre," in *6th Fast Software Encryption Workshop*, LNCS 1636, pp. 124–138, Springer, 1999.

[26] G. N. Tuychiev, "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*, 2014.

[27] G. N. Tuychiev, "About networks idea328, idea324, idea322, idea321, created on the basis of network idea3216," *Infocommunications: NetworksTechnologiesSolutions*, vol. 30, no. 2, pp. 45–50, 2014.

[28] G. N. Tuychiev, "About networks idea8-2, idea8-1 and rfwkidea8-4, rfwkidea8-2, rfwkidea8-1 developed on the basis of network idea8-4," *Uzbek mathematical journal*, no. 3, pp. 104–118, 2014.

[29] G. N. Tuychiev, "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 2014*, vol. 2, pp. 28–32, 2014.

[30] G. N. Tuychiev, "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 2014* , vol. 2, pp. 32–36, 2014.

[31] G. N. Tuychiev, "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*, vol. 3, no. 6, pp. 31–34, 2014.

[32] G. N. Tuychiev, "New encryption algorithm based on network idea16-1 using of the transformation of the encryption algorithm AES," *IPASJ International Journal of Information Technology*, vol. 3, pp. 6–12, 2015.

[33] G. N. Tuychiev, "New encryption algorithm based on network idea8-1 using of the transformation of the encryption algorithm AES," *IPASJ International Journal of Computer Science*, vol. 3, pp. 1–6, 2015.

[34] G. N. Tuychiev, "New encryption algorithm based on network pes8-1 using of the transformations of the encryption algorithm AES," *International Journal of Multidisciplinary in Cryptology and Information Security*, vol. 4, no. 1, pp. 1–5, 2015.

[35] G. N. Tuychiev, "New encryption algorithm based on network rfwkidea8-1 using transformation of AES encryption algorithm," *International Journal of Computer Networks and Communications Security*, vol. 2, no. 3, pp. 43–47, 2015.

[36] G. N. Tuychiev, "To the networks rfwkidea3216, rfwkidea328, rfwkidea324, rfwkidea322 and rfwkidea321, based on the network idea3216," *International Journal on Cryptography and Information Security (IJCIS)*, vol. 5, no. 1, pp. 9–20, 2015.

[37] U. S. Department of Commerce/National Institute of Standards and Technology. Data Encryption Standard (DES), "Federal information processing standards publication 46-3," 1979. (`http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf`)

[38] J. Vandewalle, J. Daemen, R. Govaerts, "Cryptanalysis of 2.5 rounds of IDEA (extended abstract)," *Department of Electrical Engineering, ESATCOSIC Technical Report 93/1*, pp. 1–6, 1993.

[39] D. Wagner, J. Kelsey, B. Schneier, "Key-schedule cryptanalysis of idea, g-des,gost, safer and triple-des," in *Advances in Cryptology (Crypto96)*, LNCS 1109, pp. 237–251, Springer, 1996.

[40] Y. Wei, J. Chen, Y. Hu, "A new method for impossib le differential cryptanalysis of 8-round adanced encryption standard," *Wuhan Univeristy Journan of National Sciences*, vol. 11, no. 6, pp. 1559–1562, 2006.

[41] Y. Wei, J. Chen, Y. Hu, "A new method for impossible differential cryptanalysis of 7-round advanced encryption standard," in *Proceedings of IEEE International Conference on Communications, Circuits and Systems Proceedings 2006*, vol. 3, pp. 1577–1579, 2006.

[42] L. Zhang, D. Feng, W. Zhang, W. Wu, "Improved related-key impossible differential attacks on reduced-round AES-192," in *Proceedings of Selected Areas in Cryptography 2006*, LNCS 4356, pp. 15–27, Springer, 2007.

[43] Y. Zhang, J. Chen, Y. Hu, "Impossible differential cryptanalysis of advanced encryption standard," *Science in China Series F: Information Sciences*, vol. 50, no. 3, pp. 342–350, 2007.

Aripov Mersaid Doctor of Phys. Math. Science, Professor of National University of Uzbekistan.

Tuychiev Gulom candidate technical Sciences (Ph.D.), National University of Uzbekistan.