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

Gulom Tuychiev[1]

[1] National University of Uzbekistan,

Received: 10 February 2015 Accepted: 3 March 2015 Published: 15 March 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 AESRFWKIDEA32- 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.

Index terms— advanced encryption standard, feystel network, lai-massey scheme, round function, round keys, output transformation, multiplica- tion, addition, multi

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 o_set. 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 o_sets of two and three respectively. Figure 2 illustrates the 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) As a result of this multiplication, the four bytes in a column are replaced by the following: ? ? ? ? ? ? ? ? s_{4i} s_{4i+1} s_{4i+2} s_{4i+3} ? ? ? ? , i = 0...3 $y_{4i} = (\{02\} ? s_{4i}) ? (\{03\} ? s_{4i+1}) ? s_{4i+2} ? s_{4i+3}$ $y_{4i+1} = s_{4i} ? (\{02\} ? s_{4i+1}) ? (\{03\} ? s_{4i+2}) ? s_{4i+3}$ $y_{4i+2} = s_{4i} ? s_{4i+1} ? (\{02\} ? s_{4i+2}) ? (\{03\} ? s_{4i+3})$ $y_{4i+4} = (\{03\} ? s_{4i}) ? s_{4i+1} ? s_{4i+2} ? (\{02\} ? s_{4i+3})$.

1 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 7round AES-128 was presented in **??**1]. The new attack is an impossible diferential 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, **??**9,42]. 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 diferential 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] 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 **??**. Table **??**: A Summary of the Attacks on AES iterates eight rounds plus an output trans-formation. The cryptanalysis of PES and IDEA presented on Table 2 and Table 3. 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.

2 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?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 . The S-box SubBytes() transformation shown in Table **??** 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 **??** : 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 , and performs the following steps: 1. subblocks summed by XOR respectively with round key K 32n+32 , K 32n+33 , ..., K 32n+63: 2. subblocks 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: X 0 0 , X 1 0 , . . . , X 31 0 X 0 0 , X 1 0 , . . . , X 31 0 X j 0 = X j 0 ? K 32n+32+j , j = 0...31. X 0 0 , X 1 0 , . . . , X 31 0 t 0 = (X 0 i?1 + K 32(i?1)) ? (X 16 i?1 ? K 32(i?1)+16), t 1 = (X 1 i?1 ? K 32(i?1)+1) ? (X 17 i?1 + K 32(i?1)+17), t 2 = (X 2 i?1 + K 32(i?1)+2) ? (X 18 i?1 ? K 32(i?1)+18), t 3 = (X 3 i?1 ? K 32(i?1)+3) ? (X 19 i?1 + K 32(i?1)+19), t 4 = (X 4 i?1 + K 32(i?1)+4) ? (X 20 i?1 ? K 32(i?1)+20), t 5 = (X 5 i?1 ? K 32(i?1)+5) ? (X 21 i?1 + K 32(i?1)+21), t 6 = (X 6 i?1 + K 32(i?1)+6) ? (X 22 i?1 ? K 32(i?1)+22), t 7 = (X 7 i?1 ? K 32(i?1)+7) ? (X 23 i?1 + K 32(i?1)+23), t 8 = (X 8 i?1 + K 32(i?1)+8) ? (X 24 i?1 ? K 32(i?1)+24), t 9 = (X 9 i?1 ? K 32(i?1)+9) ? (X 25 i?1 + K 32(i?1)+25), t 10 = (X 10 i?1 + K 32(i?1)+10) ? (X 26 i?1 ? K 32(i?1)+26), t 11 = (X 11 i?1 ? K 32(i?1)+11) ? (X 27 i?1 + K 32(i?1)+27),

3 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 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 1024) bits is divided into 8-bit round keys Lenght 8, here K = . Then we calculate When generating a round keys + 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 = SubBytes SubBytes(RotWord8 Rcon[imod8] otherwise = SubBytes . After each round key generation the value is cyclic shift to the left by 1 bit.

Decryption round keys are computed on the basis of encryption round keys and decryption roundt 12 = (X 12 i?1 + K 32(i?1)+12) ? (X 28 i?1 ? K 32(i?1)+28), t 13 = (X 13 i?1 ? K 32(i?1)+13) ? (X 29 i?1 + K 32(i?1)+29), t 14 = (X 14 i?1 + K 32(i?1)+14) ? (X 30 i?1 ? K 32(i?1)+30), t 15 = (X 15 i?1 ? K 32(i?1)+15) ? (X 31 i?1 + K 32(i?1)+31), , i = 1. X 0 i?1 , X 1 i?1 , . . . , X 31 i?1 , i.. X j i?1 = X j i?1 ?y 15? j , X j+16 i?1 = X j+16 i?1 ?y 15?j , j = 0...15, i = 1. X j i?1 and X 31?j i?1 , j = 1... 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. X 0 n , X 1 n , . . . , X 31 n . X 0 n+1 = X 0 n + K 32n , X 1 n+1 = X 30 n ? K 32n+1 , X 2 n+1 = X 29 n + K 32n+2 , X 3 n+1 = X 28 n ? K 32n+3 , X 4 n+1 = X 27 n + K 32n+4 , X 5 n+1 = X 26 n ? K 32n+5 , X 6 n+1 = X 25 n + K 32n+6 , X 7 n+1 = X 24 n ? K 32n+7 , X 8 n+1 = X 23 n + K 32n+8 , X 9 n+1 = X 22 n ? K 32n+9 , X 10 n+1 = X 21 n + K 32n+10 , X 11 n+1 = X 20 n ? K 32n+11 , X 12 n+1 = X 19 n + K 32n+12 , X 13 n+1 = X 18 n ? K 32n+13 , X 14 n+1 = X 17 n + K 32n+14 , X 15 n+1 = X 16 n ? K 32n+15 , X 16 n+1 = X 15 n ? K 32n+16 , X 17 n+1 = X 14 n + K 32n+17 , X 18 n+1 = X 13 n ? K 32n+18 , X 19 n+1 = X 12 n + K 32n+19 , X 20 n+1 = X 11 n ? K 32n+20 , X 21 n+1 = X 10 n + K 32n+21 , X 22 n+1 = X 9 n ? K 32n+22 , X 23 n+1 = X 8 n + K 32n+23 , X 24 n+1 = X 7 n ? K 32n+24 , X 25 n+1 = X 6 n + K 32n+25 , X 26 n+1 = X 5 n ? K 32n+26 , X 27 n+1 = X 4 n + K 32n+27 , X 28 n+1 = X 3 n ? K 32n+28 , X 29 n+1 = X 2 n + K 32n+29 , X 30 n+1 = X 1 n ? K 32n+30 , X 31 n+1 = X 31 n + K 32n+31 , K d i K c i ? l ? K c 0 , K c 1 ,..., K c Lenght?1 , = l/ ? {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 K L = K c 0 ?K c 1 ?...?K c Lenght? 1 . If K L = 0 then K L is chosen as 0xC5, i.e. K L = 0xC5. K c i , i = Lenght...32n K c i (K c i?Lenght+1) ? K c i?Lenght)) ? ?K L K c i (K c i?Lenght)?SubBytes(K c i?Lenght+1)? K L K L

keys of the output transformation associate with of encryption round keys as follows: 8. subblocks are summed to XOR with the roundkey 31. As ciphertext plaintext X receives the combined 16-bit subblocks X 0 n+1 , X 1 n+1 , . . . , X 31 n+1 key K 32n+64 , K 32n+65 , . . . , K 32n+95 : X j n+1 = X j n+1 ? K 32n+64+j , j = 0... X 0 n+1 ||X 1 n+1 ||...||X 31 n+1 . (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 Global Journal) = (?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:(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).

Decryption round keys of the first 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 , 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 = 2...n

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

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 = 0...31.

IV.

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 = 256, resistance to diferential cryptanal ysis = 256, strict avalanche criterion SAC = 8, bit independence criterion BIC = 8.? = 32 ? = 4/

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.

5 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. [1] [2]

Figure 1: Introductionn

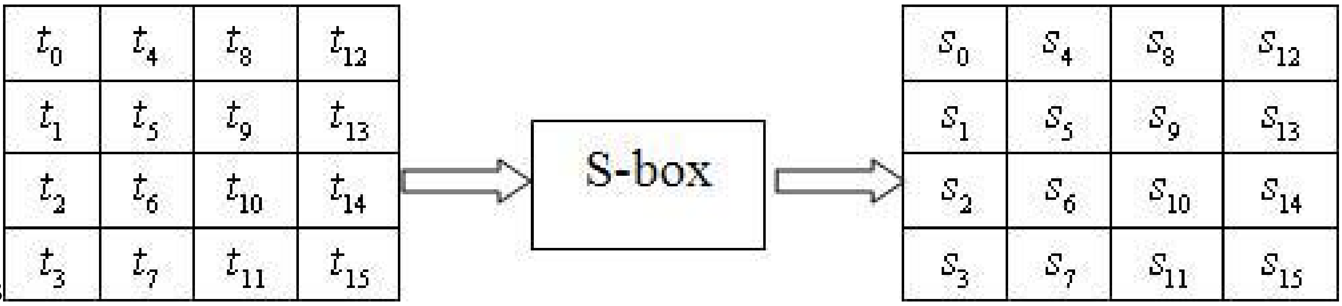
3


Figure 2: Figure 3 .

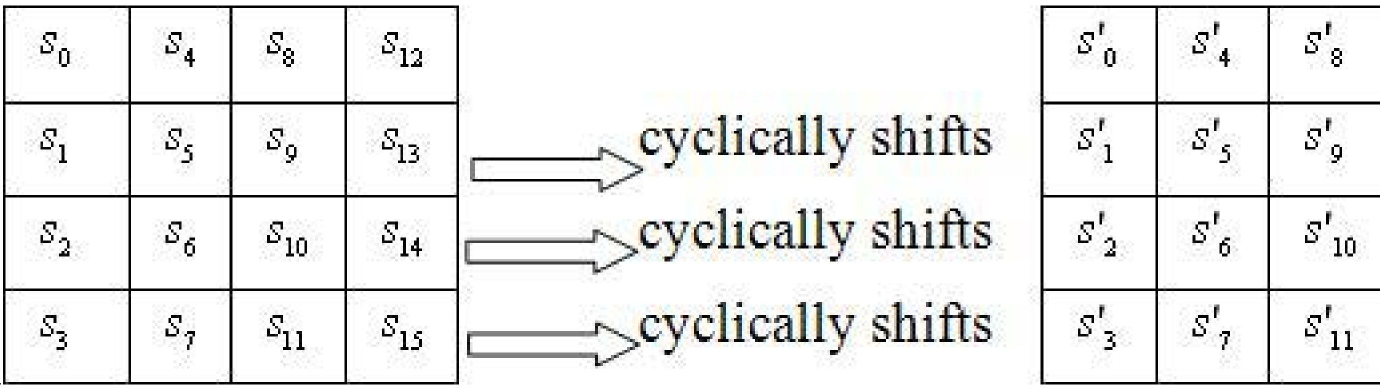
1


Figure 3: Figure 1 :

2

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}

Figure 4: Figure 2 :

3

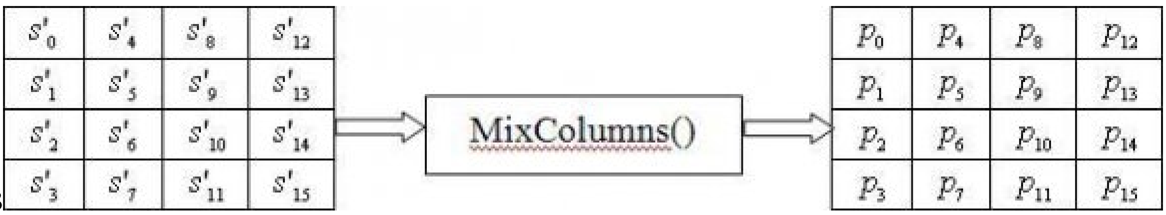


Figure 5: Figure 3 :

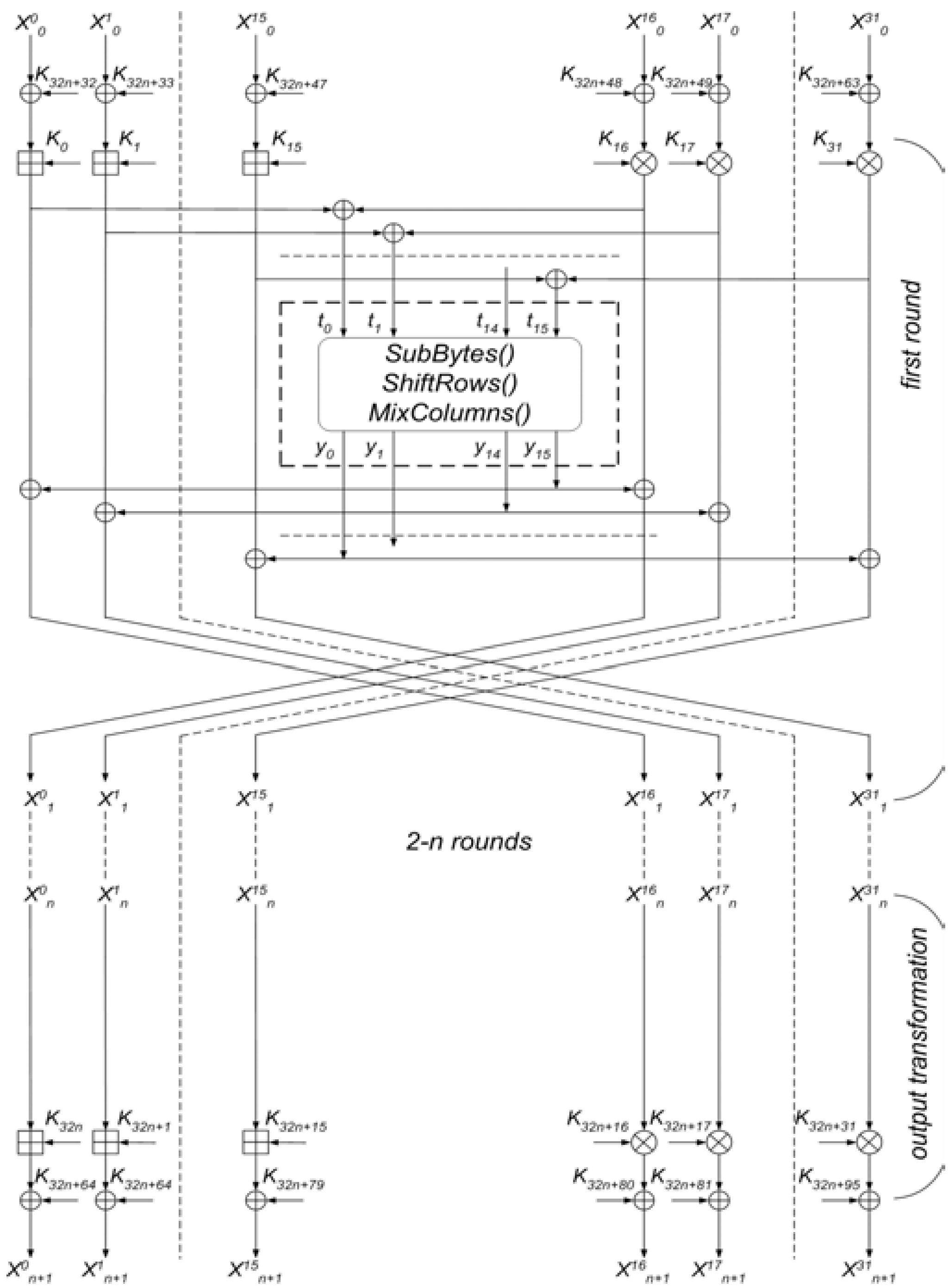

SubBytes()
ShiftRows()
MixColumns()
first round
2-n rounds
output transformation

Figure 6:

2

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	

Figure 7: Table 2 :

3

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

Figure 8: Table 3 :

[Chen J. Personal communications (2008)] , *Chen J. Personal communications* August 2008.

[Demirci and Selcuk ()] 'A Meet-in-the-Middle Attack on 8-Round AES // proceedings of Fast Software Encryption 15'. H Demirci , A Selcuk . Lecture Notes in Computer Science 2008. Springer. 5806 p. 116126.

[Chen et al. ()] 'A New Method for Impossib le Di_erential cryptanalysis of 8-Round'. J Chen , Y Hu , Y Wei . *Lecture Notes in Computer Science: Authors' Instructions 13*, 2006. 11 p. . Adanced Encryption Standard // Wuhan Univeristy Journan of NationalSciences

[Chen et al. ()] 'A New Method for Impossible Di_erential Cryptanalysis of 7-round Advanced Encryption Standard'. J Chen , Y Hu , Y Wei . *Proceedings of International Conference on Communications, Circuits and Systems Proceedings*, (International Conference on Communications, Circuits and Systems Proceedings) 2006. 2006. IEEE. 3 p. .

[Bahrak and Reza ()] *A Novel Impossible Di_erential Cryptanalysis of AES // proceedings of the Western European Workshop on Research in Cryptology*, B Bahrak , A M Reza . 2007. 2007. Bochum, Germany.

[Lai and Massey ()] 'A Proposal for a New Block Encryption Standard // Advances in Cryptology'. X Lai , J L Massey . *LNCS* I.B. Damgard (ed.) 1990. Springer-Verlag. 90 p. 389404.

[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 {Tashkent*, G N Tuychiev . 2014.

[Tuychiev ()] *About networks IDEA328, IDEA324, IDEA322, IDEA321, created on the basis of network IDEA3216 // Infocommunications: Networks Technologies-Solutions*, G N Tuychiev . 2014. Tashkent. p. 4550.

[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, {Tashkent*, G N Tuychiev . 2014. 3 p. .

[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*, G N Tuychiev . 2012. 2014. Tashkent. II p. .

[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*, G N Tuychiev . 2012. 2014. Tashkent. 2 p. .

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

[Lucks ()] 'Attacking Seven Rounds of Rijndael under 192-bit and 256-bit Keys // proceedings of the Third AES Candidate Conference (AES3)'. S Lucks . *Journal of Information Technology* 2000. 2015. 3 (1) p. .

[Borst et al. ()] J Borst , L Knudsen , V Rijmen . *Advances in Cryptology, Eurocrypt97, LNCS 1233, W. Fumy*, 1997. Springer-Verlag. p. 113.

[Daemen et al. (1993)] *Cryptanalysis of 2.5 Rounds of IDEA (Extended Abstract) // Department of Electrical Engineering*, J Daemen , R Govaerts , J Vandewalle . 93/1. Mar. 1993. p. 16. (Technical Report)

[Biham and Keller ()] *Cryptanalysis of Reduced Variants of Rijndael // unpublished manuscript*, E Biham , N Keller . 1999.

[Borst] *Di_erential-Linear Cryptanalysis of IDEA // Department of Electrical Engineering*, J Borst . 96/2. (Technical Report) (14 pages)

[Ferguson et al.] N Ferguson , J Kelsey , S Lucks , B Schneier , M Stay , D Wagner , D Whiting . *Cryptanalysis of Rijndael // proceedings of Fast Software The Encryption Algorithm AES-RFWKIDEA32-1 based on Network*, p. .

[Gilbert and Minier ()] H Gilbert , M Minier . *Rijndael // proceedings of the Third AES Candidate Conference (AES3)*, (New York, USA) 2000. p. 230241.

[Hawkes ()] P Hawkes . *Di_erential-LinearWeak Key Classes of IDEA // Advances in Cryptology,Eurocrypt98, LNCS 1403, K. Nyberg*, 1998. Springer-Verlag. p. 112126.

[Bahrak and Reza ()] 'Impossible Di_erential Attack on Seven-Round AES-128'. B Bahrak , A M Reza . *IET Information Security journal* 2008. 2 (2) p. 2832. (IET)

[Chen et al. ()] 'Impossible di_erential cryptanalysis of Advanced Encryption Standard'. J Chen , Y Hu , Y Zhang . *Science in China Series F: Information Sciences* 2007. Springer-Verlag. 50 (3) p. 342350.

[Cheon et al. ()] 'Improved Impossible Di_erential Cryptanalysis of Rijndael and Crypton // proceedings of Information Security and Cryptology ICISC'. J Cheon , M Kim , K Kim , J-Y Lee , S Kang . Lecture Notes in Computer Science 2001. 2002. Springer. 2288 p. 3949.

[Zhang et al. ()] 'Improved Related-Key Impossible Di_erential Attacks on Reduced-Round AES-192 // Proceedings of Selected Areas in Cryptography'. W Zhang , W Wu , L Zhang , Dengguo Feng . *Computer Science: Authors' Instructions 15*, Lecture Notes in Computer Science 2006. 2007. Springer-Verlag. 4356 p. 1527.

[Kelsey et al. (ed.) ()] J Kelsey , B Schneier , D Wagner , Key-Schedule Cryptanalysis Of , Idea , Gost Gdes , Triple-Des / . *Advances in Cryptology, Crypto96, LNCS 1109*, N Koblitz (ed.) 1996. Springer-Verlag. p. 237251.

[Lai et al. ()] X Lai , J L Massey , S Murphy . *Markov Ciphers and Di_erential Cryptanalysis // Advances in Cryptology, Eurocrypt91*, D W Davies (ed.) 1991. Springer-Verlag. 547 p. 1738.

[Lu et al.] J Lu , O Dunkelman , N Keller , J Kim . *New Impossible Di_erential Attacks on AES*,

[Biham et al. ()] 'Miss-in-the-Middle Attacks on IDEA'. E Biham , A Biryukov , A Shamir . *Khufu and Khafre // 6th Fast Software Encryption Workshop*, L R Knud-Sen (ed.) 1999. Springer-Verlag. 1636 p. 124138.

[Tuychiev] *New encryption algorithm based on network IDEA16-1 using of the transformation of the encryption algorithm AES // IPASJ International The Encryption Algorithm AES-RFWKIDEA32-1 based on Network*, G Tuychiev . p. .

[Tuychiev ()] 'New encryption algorithm based on network IDEA8-1 using of the transformation of the encryption algorithm AES'. G Tuychiev . *IPASJ International Journal of Computer Science* 2015. 3 (1) p. .

[Tuychiev ()] *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*, G Tuychiev . 2015. 4 p. .

[Tuychiev ()] 'New encryption algorithm based on network RFWKIDEA8-1 using transformation of AES encryption algorithm'. G Tuychiev . *International Journal of Computer Networks and Communications Security* 2015. 3 (2) p. .

[Tuychiev ()] 'New encryption algorithm based on network RFWKPES8-1 using of the transformations of the encryption algorithm AES'. G Tuychiev . *International Journal of Multidisciplinary in Cryptology and Information Security* 2014. 3 p. .

[Zhang et al. ()] 'New Results on Impossible Di_erential Cryptanalysis of Reduced AES // proceedings of ICISC'. W Zhang , W Wu , D Feng . Lecture Notes in Computer Science 2007. 2007. Springer-Verlag. 4817 p. 239250.

[Lai ()] *On the Design and Security of Block Ciphers // Hartung-Gorre Verlag*, X Lai . 1992. Konstanz.

[Meier ()] 'On the Security of the IDEA Block Cipher // Advances in Cryptology'. W Meier . *LNCS* T. Helleseth (ed.) 1994. Springer-Verlag. 93 p. 371385.

[Kim et al. ()] 'Related-Key Rectangle Attacks on Reduced AES-192 and AES-256 // Proceedings of Fast Software Encryption 14'. J Kim , S Hong , B Preneel . Lecture Notes in Computer Science 2007. Springer-Verlag. 4593 p. 225241.

[Nakahara et al. ()] 'SQUARE Attacks on Reduced-Round PES and IDEA Block Ciphers. 28. National Institute of Standards and Technology'. J Nakahara , S L M Paulo , Barreto , B Preneel , J Vandewalle , Y Kim . `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*, 2001. 2004. Elsevier. 91 p. . (Federal Information Processing Standards Pub-14 Lecture Notes in Computer Science: Authors' Instructions lication 197)

[Tuychiev (2015)] 'To the networks RFWKIDEA3216, RFWKIDEA328, RFWKIDEA324, RFWKIDEA322 and RFWKIDEA321, based on the net-work IDEA3216'. G Tuychiev . *International Journal on Cryptography and Information Security (IJCIS)* March 2015. 5 (1) p. .

[Knudsen and Rijmen] *Truncated Di_erentials of IDEA // Department of Electrical Engineering*, L R Knudsen , V Rijmen . 97/1. (Technical Report)