Mathematical Problems of Computer Science 42, 97-106, 2014.

Design and Cryptanalysis of a New Encryption Algorithm SAFER-256

Gurgen H. Khachatrian, Melsik K. Kyureghyan and Knarik M. Kyuregyan

American University of Armenia
Institute for Informatics and Automation Problems of NAS RA
e-mail: gurgenkh@aua.am, melsik@ipia.sci.am, knarikyuregyan@gmail.com

Abstract

In this paper a new encryption algorithm of SAFER family named SAFER-256 is introduced. SAFER-256 is a 256 bit size block cipher with a 256 bit size user-selected key. Security of the new algorithm against differential analysis attack is also presented.

Keywords: Cipher, Round, Shuffling, Encryption, Decryption, Differential cryptanalysis, Effective weight.

1. Introduction

SAFER+ is one of the block ciphers of SAFER family proposed by Prof. James Massey together with Prof. Gurgen Khachatrian and Dr. Melsik Kureghyan. It is a 128 bit block size encryption algorithm with three different user-selected-key lengths, namely 128, 192 and 256. SAFER+ was submitted as a candidate for the Advanced Encryption Standard (AES) [2] and was subsequently adopted for use in the challenge/response entity authentication scheme in the Bluetooth protocol for wireless communications [5]. In this paper we propose a new 256 bit size block cipher named SAFER-256 with a 256 bit size user-selected-key. The structure of this algorithm is built based on the modified algorithm of SAFER+. The reason of presenting a new cipher is twofold. Firstly almost all existing and well known ciphers are 128 bit block ciphers and although they have options for the key size of 256 bits they do not really provide 256 bit security because of collision attacks on 128 bit block size which is not the case when the block size is 256. Secondly as we will show later in the paper the proceesing speed for the new cipher will be the same compared with analogous modifyied SAFER+ algorithm.

The paper is organized as follows: In section 2 an algorithm specification for SAFER-256 is given, section 3 represents results of differential anylsis for SAFER-256, section 4 is implementation aspects of SAFER-256 and the conclusion of the paper is in section 5.

2. SAFER-256 Algorithm Specification

SAFER-256 is a 256 bit block cipher. In Fig. 1 the encryption structure of the SAFER-256 algorithm is introduced. The 32-byte plaintext block passes through $r = 6$ rounds of encryption

for 256 bit key. In each round of encryption two subkeys are used. These round subkeys $(K_1, K_2, \dots, K_{2r+1})$ are determined from the user-selected key K according to the key schedule of SAFER+ [2]. The last subkey K_{2r+1} is "added" to the block produced by the r rounds of encryption in the manner that the bytes $1, 2, 3, 4, 9, 10, 11, 12, 17, 18, 19, 20, 25, 26, 27, 28$ are added together bit-by-bit modulo two (the bitwise "exclusive-or" operation) while the bytes $5, 6, 7, 8, 13, 14, 15, 16, 21, 22, 23, 24, 29, 30, 31, 32$ are added together modulo 256 ("byte addition"). This "addition" of round subkey K_{2r+1} constitutes the *output transformation* for encryption and produces the ciphertext block of 32-bytes.

The input for decryption is the ciphertext block of 32-bytes. The decryption begins with the *input transformation* that undoes the *output transformation* in the encryption process. At first the round subkey K_{2r+1} is "subtracted" from the ciphertext block in the manner that the round subkey bytes $1, 2, 3, 4, 9, 10, 11, 12, 17, 18, 19, 20, 25, 26, 27, 28$ are added together bit-by-bit modulo two to the corresponding ciphertext bytes while the round subkey bytes $5, 6, 7, 8, 13, 14, 15, 16, 21, 22, 23, 24, 29, 30, 31, 32$ are subtracted modulo 256 from the corresponding ciphertext bytes. The result of this "subtraction" is the same 32-byte block as was produced from the r rounds of encryption before the output transformation was applied. This block then passes through the r rounds of decryption, the round i of which undoes the round $r - i + 1$ of encryption, where $i = 1,2, \dots, r$. After the round r we obtain a plaintext block. Note that the round keys for decryption are the same as those for encryption but are used in reverse order.

2.1 SAFER-256 Encryption Round

The SAFER-256 round schema is given in Fig. 2. The first operation within the round i, $1 \le i \le r$, is the "addition" of the round subkey K_{2i-1} to the 16-byte round input in the manner that the bytes $1, 2, 3, 4, 9, 10, 11, 12, 17, 18, 19, 20, 25, 26, 27, 28$ are added together bit-by-bit modulo two while the bytes $5, 6, 7, 8, 13, 14, 15, 16, 21, 22, 23, 24, 29, 30, 31, 32$ are added together modulo 256. The 32-byte result of this "addition" is then processed by *a nonlinear layer* in the manner that the value x of byte j is converted to $45^x mod\ 257$ for bytes $j = 1, 2, 3, 4, 9, 10, 11, 12, 17, 18, 19, 20, 25, 26, 27, 28$ (with the convention that when $x = 128$, then $45^{128} mod\ 257 = 256$ is represented by 0), while the value x of byte j is converted to $\log_{45} x$ for bytes $j = 5, 6, 7, 8, 13, 14, 15, 16, 21, 22, 23, 24, 29, 30, 31, 32$ (with the convention that when $x = 0$, then the output $\log_{45} 0$ is represented by 128). The round key K_{2i} is then "added" to the output of the *nonlinear layer* in the manner that the bytes $5, 6, 7, 8, 13, 14, 15, 16, 21, 22, 23, 24, 29, 30, 31, 32$ are added together bit-by-bit modulo two, while the bytes $1, 2, 3, 4, 9, 10, 11, 12, 17, 18, 19, 20, 25, 26, 27, 28$ are added together modulo 256. The 16-byte result of this "addition"

$$x = [x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}, x_{12}, x_{13}, x_{14}, x_{15}, x_{16}, x_{17}, x_{18}, x_{19}, x_{20}, x_{21}, x_{22}, x_{23}, x_{24}, x_{25}, x_{26}, x_{27}, x_{28}, x_{29}, x_{30}, x_{31}, x_{32}]$$

is then postmultiplied by the matrix M modulo 256 to give the 32-byte round output

$$y = [y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8, y_9, y_{10}, y_{11}, y_{12}, y_{13}, y_{14}, y_{15}, y_{16}, y_{17}, y_{18}, y_{19}, y_{20}, y_{21}, y_{22}, y_{23}, y_{24}, y_{25}, y_{26}, y_{27}, y_{28}, y_{29}, y_{30}, y_{31}, y_{32}],$$

in the manner

$$y = xM,$$

where M is the 32×32 matrix in Fig. 3.

$$y_2 = 8x_1 + 2x_2 + 2x_3 + 4x_4 + 2x_5 + 2x_6 + 4x_7 + 2x_8 + 2x_9 + 4x_{10} + 4x_{11} + x_{12} + x_{13} + 8x_{14} + 16x_{15} + x_{16} + x_{17} + x_{18} + x_{19} + x_{20} + 4x_{21} + 2x_{22} + 4x_{23} + 2x_{24} + x_{25} + x_{26} + x_{27} + x_{28} + 2x_{29} + x_{30} + 2x_{31} + x_{32},$$

(where the arithmetic is modulo 256) as follows from the second column of the matrix M. Multiplication by matrix M provides the *liner layer* of the round that is four times "*shuffling" +"2-PHT"* operations. *Shuffling* is the coordinate permutation [25, 28, 29, 32, 17, 20, 21, 24, 13, 16, 9, 12, 5, 8, 1, 4, 3, 2, 7, 6, 11, 10, 15, 14, 27, 26, 31, 30, 19, 18, 23, 22] and *2-PHT* is Pseudo-Hadamrd matrix $\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$, that has as an input 2 bytes (a_1, a_2) and as an output $(2a_1 + a_2, a_1 + a_2)$ 2-bytes over the ring of integers modulo 256 (all operations are modulo 256).

2.2 SAFER-256 Decryption Round

In the decryption round of SAFER-256 simply invert in reverse order the operations from the encryption round. Thus, the first operation in the decryption round is to postmultiply the 32-byte round input

$$y = [y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8, y_9, y_{10}, y_{11}, y_{12}, y_{13}, y_{14}, y_{15}, y_{16}, y_{17}, y_{18}, y_{19}, y_{20}, y_{21}, y_{22}, y_{23}, y_{24}, y_{25}, y_{26}, y_{27}, y_{28}, y_{29}, y_{30}, y_{31}, y_{32}]$$

by the matrix M^{-1}, which is modulo 256 inverse of M, to give the 32-byte result

$$x = [x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}, x_{12}, x_{13}, x_{14}, x_{15}, x_{16}, x_{17}, x_{18}, x_{19}, x_{20}, x_{21}, x_{22}, x_{23}, x_{24}, x_{25}, x_{26}, x_{27}, x_{28}, x_{29}, x_{30}, x_{31}, x_{32}]$$

in the manner

$$x = yM^{-1},$$

where matrix M^{-1} is the 32×32 matrix in Fig. 4.
For instance, these operations give

$$x_{10} = -2y_1 + 2y_2 - y_3 + y_4 - 4y_5 + 4y_6 - 4y_7 + 8y_8 - 16y_9 + 32y_{10} - y_{11} + y_{12} - y_{13} + y_{14} - 2y_{15} + 2y_{16} - 4y_{17} + 8y_{18} - 2y_{19} + 4y_{20} - y_{21} + 2y_{22} - 8y_{23} + 8y_{24} - 2y_{25} + 4y_{26} - y_{27} + 2y_{28} - 4y_{29} + 8y_{30} - 2y_{31} + 2y_{32}.$$

The round subkey $K_{2r-2i+2}$ is then "subtracted" from x in the manner that the round subkey bytes $1, 2, 3, 4, 9, 10, 11, 12, 17, 18, 19, 20, 25, 26, 27, 28$ are subtracted modulo 256 from the corresponding bytes of x while the round subkey bytes $5, 6, 7, 8, 13, 14, 15, 16, 21, 22, 23, 24, 29, 30, 31, 32$ are added bit-by-bit modulo 2 to the corresponding bytes of x. Then the 16-byte result of this "subtraction" is then processed nonlinearly in the manner that the value x of byte j is converted to $\log_{45} x$ for bytes $j = 1, 2, 3, 4, 9, 10, 11, 12, 17, 18, 19, 20, 25, 26, 27, 28$ (again with the convention that when $x = 0$, then the output $\log_{45} 0$ is represented by 128), while the value x of byte j is converted to $45^x mod\ 257$ for bytes $j = 5, 6, 7, 8, 13, 14, 15, 16, 21, 22, 23, 24, 29, 30, 31, 32$ (again with the convention that when $x = 128$, then $45^{128} mod\ 257 =$

256 is represented by 0). The round key $K_{2r-2i+1}$ is then "subtracted" from the 16-byte result in the manner that the round subkey bytes $1, 2, 3, 4, 9, 10, 11, 12, 17, 18, 19, 20, 25, 26, 27, 28$ are added bit-by-bit modulo 2 to the corresponding input bytes while the round subkey bytes $5, 6, 7, 8, 13, 14, 15, 16, 21, 22, 23, 24, 29, 30, 31, 32$ are subtracted modulo 256 from the corresponding input bytes to obtain the 32-byte round output.

3. Differential Cryptanalysis

The attack by differential cryptanalysis on an r-round cipher relies on being able to find a $(r-1)$ round differential whose probability is substantially less than the average probability of such a differential, which is $\frac{1}{2^{256}-1} \approx 2^{-256}$ for a 32-byte block length. We have analyzed all the possible "highly probable" 5-round differential chains by [1] and have found that their probabilities are substantially less than 2^{-256}. These results imply that SAFER-256 is secure against differential cryptanalysis only after $r = 6$ rounds in the sense that the attack by differential cryptanalysis is as difficult as the exhaustive key search for the 256 bit key.

The purpose of the linear transform layer is to provide SAFER-256 with diffusion, i.e., to ensure that small changes in round inputs cause large changes in round outputs. If v denotes a vector of 32 bytes, we will write $W(v)$ for the (Hamming) weight of v, i.e., for the number of its nonzero bytes. Because the linear transform layer performs a linear operation over the ring of integers modulo 256 and because "differences" can be taken conveniently as byte differences modulo 256 at the output of the nonlinear layer in Fig. 2, the diffusion in SAFER256 is well measured by how well the linear transform layer converts low weight inputs into high weight outputs vM.

It's easy to see that cryptographic properties of SAFER-256 depends on the chosen permutation of coordinates and its interaction with matrices M in Fig. 3.

$V_1[5,11,19,32](a, -a, 4a, -8a)$ $(4(1) \rightarrow)$will denote the 1-*parametr* set of all weight 4 byte vectors v that are nonzero only in bytes $5, 11, 19, 32$ where their values are $a, -a, 4a, -8a$, respectively, and where the parameter a satisfies $a \in \{0,32, -32,64, -64,128\}$ as is required for v to have weight 4. $V_0[7,8,9](128,64,45)$ $(3(0) \rightarrow)$ will denote the 0-*parameter* set containing a single vector of weight 3 with values $128, 64, 45$ in bytes $7, 8, 9$, respectively.

We define the *effective weight* of a difference chain to be the sum of the weights of the vectors in the chain minus the sum of the number of parameters in the chain.

The reason for introducing the effective weight of a chain is the following. There are not more than 2^8 choices for each parameter and, hence, the probability of difference chain with t parameters is at most 2^{8t} times that of a characteristic with vectors of the same weight. Moreover, 2^{-8} is essentially the average probability of a transition for a specified nonzero byte difference to another specified nonzero byte difference so that when the vectors in the characteristic have total weight w, then the characteristic has probability roughly 2^{-8w}. Hence, the probability of the difference chain can be roughly estimated as $2^{8t} \cdot 2^{-8w} = 2^{-8(w-t)}$, where $w - t$ is the effective weight. In the first round for which the transitions have probability 2^{-5}, all the byte transition probabilities will be less than 2^{-7}. Thus, for any difference chain C with five or more rounds we can be confident that the probability $P(C)$ of C satisfies

$$2^{-7W_{eff}(C)},$$

where $W_{eff}(C)$ is *the effective weight* of C [3].

The following minimal effective weight differential chains were found:

A differential chain with the effective weight 43 having the weight/parameters chain
$5(0) \rightarrow 2(1) \rightarrow 24(1) \rightarrow 6(0) \rightarrow 6(1)$,
$4(0) \rightarrow 3(1) \rightarrow 20(1) \rightarrow 10(0) \rightarrow 6(1)$.

A differential chain with the effective weight 44 having the weight/parameters chain
$2(0) \rightarrow 5(1) \rightarrow 24(1) \rightarrow 7(0) \rightarrow 6(1)$,
$2(0) \rightarrow 4(1) \rightarrow 24(1) \rightarrow 7(0) \rightarrow 7(1)$,
$3(0) \rightarrow 3(1) \rightarrow 25(1) \rightarrow 6(0) \rightarrow 7(1)$.

A differential chain with the effective weight 45 having the weight/parameters chain
$6(0) \rightarrow 3(1) \rightarrow 22(1) \rightarrow 7(0) \rightarrow 7(1)$.

A differential chain with the effective weight 46 having the weight/parameters chain
$6(0) \rightarrow 2(1) \rightarrow 24(1) \rightarrow 7(0) \rightarrow 7(1)$.

4. Implementation aspects

Differential analysis has shown that new encryption algorithm SAFER-256 based on the structure of SAFER+ is secure after only 7 rounds. Due to structural modifications we have made possible to reduce the required rounds down to 6 and still be secure against differential cryptanalysis attack.

We have implemented 128 bit block cipher and 256 bit cipher in case of 256 bit user selected key and have obtained that 128 bit block cipher implementation time is approximately the same compared with 256 bit block cipher implementation time. However SAFER-256 is much more secure compared with 128-bit cipher against other types of attacks for example against collision attack as was mentioned in the introduction.

5. Conclusion

In this paper a new algorithm called SAFER-256 is introduced. It was shown that the presented cipher is secure against differential cryptanalysis attack after only six rounds and as a result has approximately the same processing speed compared with analogous cipher with 128 bit block length. Thus the new cipher provides the same security level against differential cryptanlysis attack, while having much higher level of security against other possible types of attack due to larger block length .

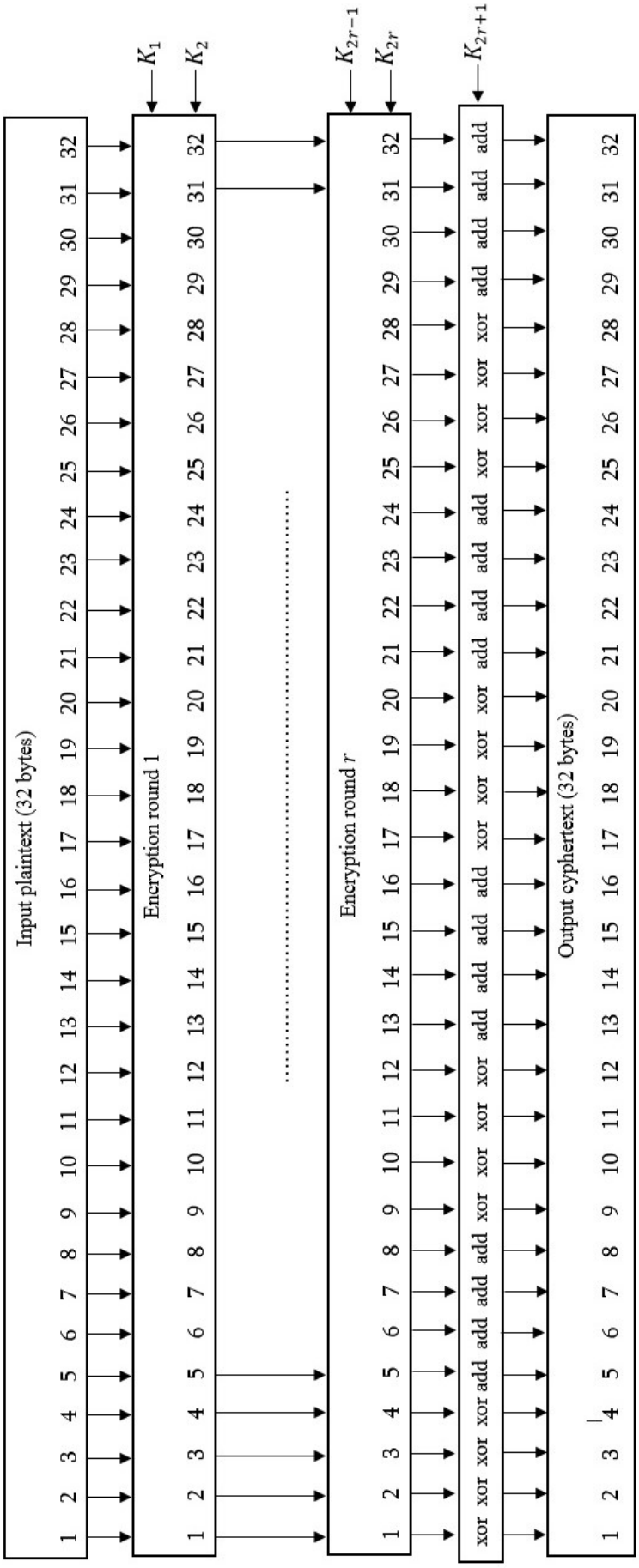

Fig. 1 Encryption structure of SAFER-256

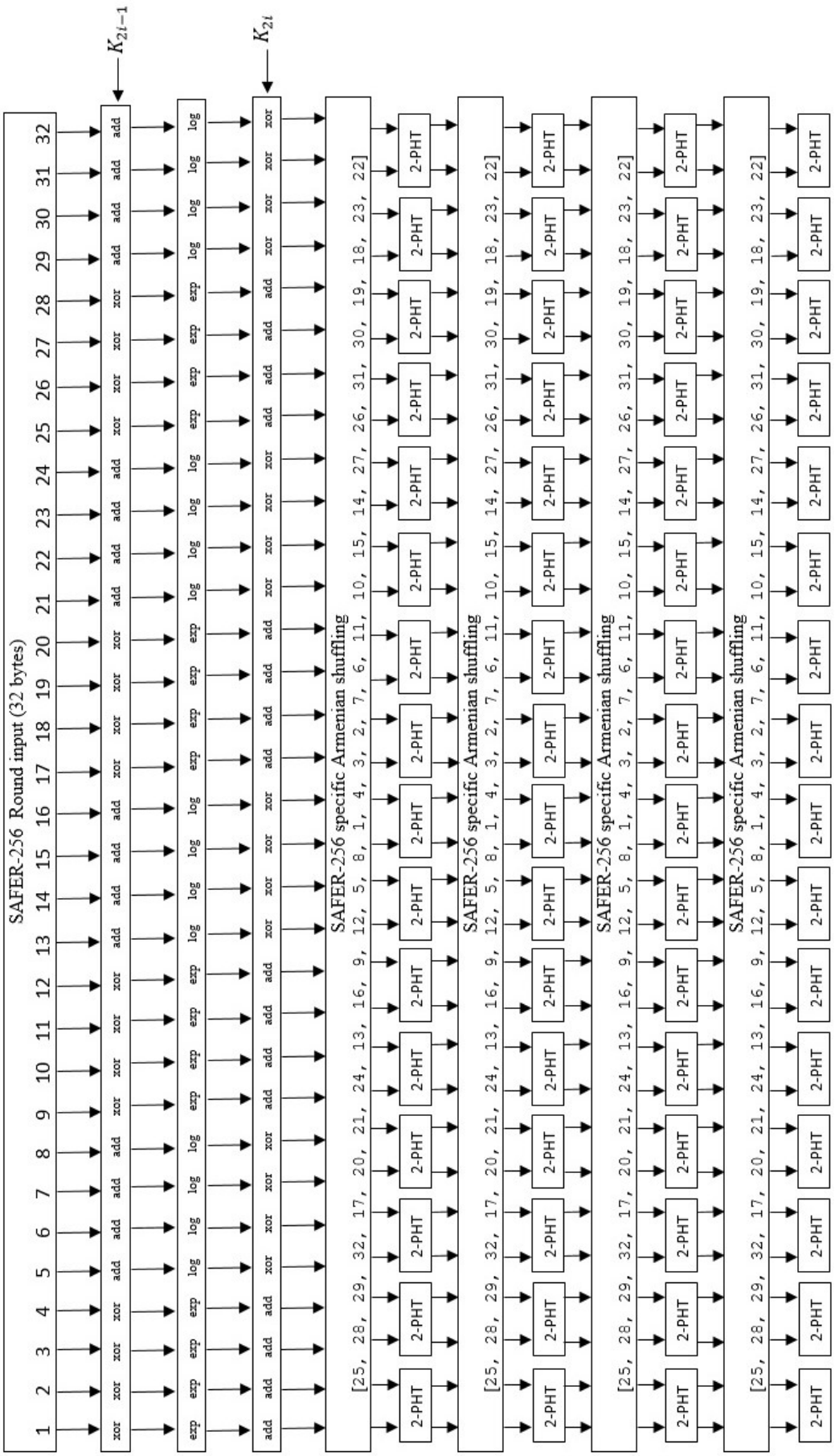

Fig. 2 Encryption round structure of SAFER-256

$$
M=\begin{bmatrix}
8 & 8 & 1 & 1 & 2 & 2 & 8 & 4 & 4 & 2 & 1 & 1 & 4 & 4 & 8 & 4 & 2 & 1 & 2 & 2 & 32 & 16 & 2 & 1 & 8 & 4 & 2 & 2 \\
4 & 2 & 4 & 2 & 8 & 4 & 2 & 2 & 1 & 1 & 16 & 8 & 2 & 1 & 1 & 2 & 1 & 1 & 4 & 2 & 1 & 1 & 1 & 2 & 2 & 2 & 4 & 2 \\
4 & 2 & 8 & 4 & 8 & 4 & 4 & 4 & 1 & 1 & 32 & 16 & 4 & 2 & 2 & 1 & 1 & 1 & 2 & 2 & 1 & 2 & 2 & 2 & 2 & 2 & 8 & 4 \\
4 & 4 & 1 & 1 & 1 & 1 & 8 & 4 & 2 & 1 & 1 & 1 & 2 & 2 & 4 & 2 & 1 & 1 & 16 & 8 & 4 & 2 & 4 & 4 & 2 & 2 & 2 & 2 \\
2 & 2 & 2 & 2 & 1 & 1 & 32 & 16 & 2 & 1 & 4 & 2 & 1 & 1 & 2 & 1 & 1 & 1 & 8 & 4 & 2 & 1 & 8 & 4 & 2 & 2 & 8 & 1 \\
4 & 2 & 4 & 2 & 16 & 8 & 1 & 1 & 2 & 2 & 8 & 4 & 2 & 1 & 1 & 2 & 2 & 1 & 4 & 2 & 1 & 1 & 4 & 4 & 2 & 1 & 2 & 1 \\
8 & 4 & 4 & 2 & 32 & 16 & 1 & 1 & 4 & 4 & 8 & 4 & 2 & 1 & 1 & 2 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 2 & 1 & 1 & 1 & 1 \\
2 & 2 & 1 & 1 & 1 & 1 & 16 & 8 & 2 & 1 & 2 & 1 & 4 & 2 & 2 & 4 & 2 & 1 & 4 & 2 & 1 & 1 & 4 & 2 & 1 & 1 & 4 & 2 \\
2 & 2 & 1 & 1 & 8 & 4 & 2 & 1 & 8 & 4 & 4 & 2 & 8 & 4 & 4 & 2 & 1 & 1 & 2 & 1 & 8 & 4 & 2 & 1 & 8 & 4 & 2 & 1 \\
8 & 4 & 16 & 8 & 4 & 2 & 1 & 1 & 4 & 2 & 2 & 1 & 2 & 1 & 1 & 4 & 2 & 1 & 1 & 2 & 4 & 2 & 1 & 1 & 4 & 2 & 1 & 1 \\
8 & 4 & 32 & 16 & 4 & 2 & 2 & 2 & 8 & 4 & 4 & 2 & 1 & 1 & 1 & 2 & 1 & 1 & 2 & 1 & 8 & 4 & 2 & 2 & 8 & 4 & 2 & 2 \\
1 & 1 & 1 & 1 & 4 & 4 & 4 & 4 & 2 & 2 & 8 & 4 & 2 & 2 & 2 & 1 & 8 & 4 & 4 & 2 & 2 & 1 & 4 & 4 & 2 & 1 & 1 & 1 \\
1 & 1 & 4 & 4 & 2 & 2 & 8 & 4 & 2 & 1 & 4 & 2 & 1 & 1 & 2 & 1 & 4 & 2 & 2 & 1 & 1 & 1 & 2 & 2 & 1 & 1 & 2 & 2 \\
16 & 8 & 8 & 4 & 2 & 2 & 1 & 1 & 4 & 2 & 2 & 1 & 4 & 2 & 2 & 1 & 2 & 1 & 1 & 2 & 4 & 2 & 1 & 1 & 2 & 1 & 1 & 1 \\
32 & 16 & 8 & 4 & 4 & 2 & 1 & 1 & 2 & 1 & 4 & 2 & 2 & 1 & 4 & 2 & 1 & 1 & 2 & 1 & 2 & 1 & 1 & 1 & 1 & 1 & 2 & 1 \\
1 & 1 & 2 & 2 & 2 & 2 & 4 & 2 & 2 & 1 & 1 & 1 & 4 & 2 & 2 & 1 & 8 & 4 & 2 & 1 & 1 & 1 & 2 & 2 & 1 & 1 & 4 & 2 \\
1 & 1 & 2 & 2 & 1 & 1 & 8 & 4 & 2 & 1 & 1 & 1 & 2 & 1 & 1 & 2 & 4 & 2 & 2 & 1 & 1 & 1 & 2 & 2 & 1 & 1 & 4 & 2 \\
2 & 1 & 4 & 2 & 2 & 1 & 1 & 2 & 1 & 1 & 1 & 1 & 2 & 1 & 1 & 2 & 4 & 2 & 2 & 1 & 1 & 1 & 2 & 2 & 1 & 1 & 4 & 2 \\
2 & 1 & 8 & 4 & 2 & 1 & 1 & 2 & 2 & 1 & 1 & 1 & 2 & 1 & 1 & 2 & 4 & 2 & 2 & 1 & 1 & 1 & 2 & 2 & 1 & 1 & 4 & 2 \\
1 & 1 & 1 & 1 & 1 & 1 & 2 & 1 & 1 & 1 & 2 & 1 & 2 & 1 & 1 & 2 & 4 & 2 & 2 & 1 & 1 & 1 & 2 & 2 & 1 & 1 & 4 & 2 \\
4 & 4 & 1 & 1 & 2 & 2 & 4 & 2 & 2 & 1 & 4 & 2 & 2 & 1 & 1 & 2 & 4 & 2 & 2 & 1 & 1 & 1 & 2 & 2 & 1 & 1 & 4 & 2 \\
4 & 2 & 2 & 1 & 4 & 2 & 8 & 4 & 4 & 2 & 8 & 4 & 4 & 2 & 2 & 1 & 8 & 4 & 4 & 2 & 2 & 1 & 4 & 4 & 2 & 1 & 2 & 1 \\
8 & 4 & 2 & 1 & 2 & 1 & 4 & 2 & 2 & 1 & 4 & 2 & 2 & 1 & 1 & 2 & 4 & 2 & 2 & 1 & 1 & 1 & 2 & 2 & 1 & 1 & 4 & 2 \\
2 & 2 & 1 & 1 & 2 & 1 & 2 & 1 & 1 & 1 & 2 & 1 & 1 & 2 & 2 & 1 & 4 & 2 & 2 & 1 & 1 & 1 & 2 & 2 & 1 & 1 & 4 & 2 \\
2 & 1 & 4 & 2 & 2 & 1 & 4 & 2 & 2 & 1 & 4 & 2 & 2 & 1 & 1 & 2 & 4 & 2 & 2 & 1 & 1 & 1 & 2 & 2 & 1 & 1 & 4 & 2 \\
1 & 1 & 4 & 4 & 1 & 1 & 2 & 2 & 4 & 2 & 8 & 4 & 4 & 2 & 2 & 1 & 8 & 4 & 4 & 2 & 2 & 1 & 4 & 4 & 2 & 1 & 2 & 1 \\
2 & 2 & 2 & 2 & 4 & 4 & 2 & 2 & 1 & 1 & 4 & 2 & 2 & 1 & 1 & 2 & 4 & 2 & 2 & 1 & 1 & 1 & 2 & 2 & 1 & 1 & 4 & 2 \\
2 & 1 & 2 & 1 & 4 & 2 & 2 & 2 & 1 & 1 & 4 & 2 & 2 & 1 & 1 & 2 & 4 & 2 & 2 & 1 & 1 & 1 & 2 & 2 & 1 & 1 & 4 & 2 \\
4 & 2 & 1 & 2 & 1 & 1 & 4 & 2 & 2 & 1 & 4 & 2 & 2 & 1 & 1 & 2 & 4 & 2 & 2 & 1 & 1 & 1 & 2 & 2 & 1 & 1 & 4 & 2 \\
1 & 1 & 2 & 2 & 1 & 1 & 2 & 1 & 1 & 1 & 2 & 1 & 2 & 1 & 1 & 2 & 4 & 2 & 2 & 1 & 1 & 1 & 2 & 2 & 1 & 1 & 4 & 2
\end{bmatrix}
$$

Fig. 3 SAFER-256 linear transformation matrix

$M^{-1}=$

1	-4	2	-1	1	-1	1	-2	1	-2	1	-1	2	-1	1	-4	2	-2	1	-4	2	-1	1	-2	8	-8	4	-16	4	-2	2	-4
-2	4	-2	2	-2	1	-1	4	-2	2	-1	2	-4	1	-1	8	-4	2	-1	8	-4	1	-1	4	-16	8	-4	32	-8	2	-2	8
8	-1	1	-16	4	-4	2	-4	2	-1	1	-4	2	-2	1	-2	1	-1	1	-1	2	-2	1	-4	1	-2	2	-1	1	-8	4	-2
-16	1	-1	32	-8	4	-2	8	-4	1	-1	8	-4	2	-1	4	-2	1	-1	2	-4	2	-1	8	-2	2	-2	2	-2	8	-4	4
1	-2	1	-1	2	-1	1	-4	1	-4	2	-1	1	-1	1	-2	8	-8	4	-16	4	-2	2	-4	2	-2	1	-4	2	-1	1	-2
-2	2	-1	2	-4	1	-1	8	-2	4	-2	2	-2	1	-1	4	-16	8	-4	32	-8	2	-2	8	-4	2	-1	8	-4	1	-1	4
1	-2	2	-2	1	-4	2	-1	2	-4	4	-4	1	-16	8	-1	1	-1	1	-1	1	-4	2	-2	2	-1	1	-2	4	-2	1	-8
-1	4	-4	2	-1	8	-4	1	-2	8	-8	4	-1	32	-16	1	-1	2	-2	1	-1	8	-4	2	-2	2	-2	2	-4	4	-2	8
2	-4	2	-2	4	-2	2	-8	1	-16	8	-1	1	-4	4	-2	2	-4	2	-4	1	-1	1	-1	1	-2	1	-2	1	-1	1	-1
-2	8	-4	2	-4	4	-4	8	-1	32	-16	1	-1	8	-8	2	-2	8	-4	4	-1	2	-2	1	-1	4	-2	2	-1	2	-2	1
2	-1	1	-4	2	-2	1	-2	8	-1	1	-16	4	-4	2	-4	1	-2	2	-1	1	-8	4	-2	1	-1	1	-1	2	-2	1	-4
-4	1	-1	8	-4	2	-1	4	-16	1	-1	32	-8	4	-2	8	-2	2	-2	2	-2	8	-4	4	-2	1	-1	2	-4	2	-1	8
2	-2	2	-4	1	-8	4	-1	1	-1	1	-2	1	-2	1	-1	4	-1	1	-4	8	-2	1	-16	2	-1	1	-2	2	-4	2	-4
-4	2	-2	8	-2	8	-4	2	-2	1	-1	4	-2	2	-1	2	-8	1	-1	8	-16	2	-1	32	-4	1	-1	4	-4	4	-2	8
2	-8	4	-2	2	-2	2	-4	4	-2	1	-4	8	-1	1	-16	1	-2	1	-2	1	-1	1	-1	2	-4	2	-4	1	-1	1	-1
-4	8	-4	4	-4	2	-2	8	-8	2	-1	8	-16	1	-1	32	-2	2	-1	4	-2	1	-1	2	-4	4	-2	8	-2	1	-1	2
1	-16	8	-1	1	-4	4	-2	2	-4	2	-2	4	-2	2	-8	1	-2	1	-2	1	-1	1	-1	2	-4	2	-4	1	-1	1	-1
-1	32	-16	1	-1	8	-8	2	-2	8	-4	2	-4	4	-4	8	-1	4	-2	2	-1	2	-2	1	-2	8	-4	4	-1	2	-2	1
2	-4	4	-4	1	-16	8	-1	1	-2	2	-2	1	-4	2	-1	2	-1	1	-2	4	-2	1	-8	1	-1	1	-1	1	-4	2	-2
-2	8	-8	4	-1	32	-16	1	-1	4	-4	2	-1	8	-4	1	-2	2	-2	2	-4	4	-2	8	-1	2	-2	1	-1	8	-4	2
1	-1	1	-2	1	-2	1	-1	4	-1	1	-8	2	-4	2	-2	1	-4	4	-1	1	-16	8	-2	1	-2	2	-1	2	-4	2	-4
-1	2	-2	2	-1	4	-2	1	-4	2	-2	8	-2	8	-4	2	-1	8	-8	1	-1	32	-16	2	-1	4	-4	1	-2	8	-4	4
4	-2	1	-4	8	-1	1	-16	2	-8	4	-2	2	-2	2	-4	2	-4	2	-4	1	-1	1	-1	1	-2	1	-2	1	-1	1	-1
-8	2	-1	8	-16	1	-1	32	-4	8	-4	4	-4	2	-2	8	-4	4	-2	8	-2	1	-1	2	-2	2	-1	4	-2	1	-1	2
1	-4	2	-1	1	-1	1	-2	1	-2	1	-1	2	-1	1	-4	1	-4	2	-2	1	-2	2	-1	4	-16	8	-8	2	-4	4	-2
-1	8	-4	1	-1	2	-2	2	-1	4	-2	1	-2	2	-2	4	-1	8	-4	2	-1	4	-4	1	-4	32	-16	8	-2	8	-8	2
4	-1	-	-8	2	-4	2	-2	1	-1	1	-2	1	-2	1	-1	1	-2	2	-1	2	-4	2	-4	1	-4	4	-1	1	-16	8	-2
-4	2	-2	8	-2	8	-4	2	-1	2	-2	2	-1	4	-2	1	-1	4	-4	1	-2	8	-4	4	-1	8	-8	1	-1	32	-16	2
1	-2	1	-1	2	-1	1	-4	1	-4	2	-1	1	-1	1	-2	4	-16	8	-8	2	-4	4	-2	1	-4	2	-2	1	-2	2	-1
-1	4	-2	1	-2	2	-2	4	-1	8	-4	1	-1	2	-2	2	-4	32	-16	8	-2	8	-8	2	-1	8	-4	2	-1	4	-4	1
1	-1	1	-2	1	-2	1	-1	2	-2	2	-4	1	-8	4	-1	2	-1	1	-2	2	-4	2	-4	4	-1	1	-4	8	-2	1	-16
-2	1	-1	4	-2	2	-1	2	-4	2	-2	8	-2	8	-4	2	-4	1	-1	4	-4	4	-2	8	-8	1	-1	8	-16	2	-1	32

Fig. 4 SAFER-256 reverse linear transformation matrix

Acknowledgement

This work was supported by the State Committee Science MES RA, in the frame of the research project SCS 13-1B352.

References

[1] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystem", *Advances in Cryptology-CRYPTO'90, Lecture Notes in Computer Science*, Heidelberg and New York: Springer, no. 537, pp. 212-241, 1990.
[2] J. L. Massey, G.H. Khachatryan and K. M. Kyuregian, "Nomination of SAFER+ as candidate algorithm for the advanced encryption standard (AES)", *NIST AES Proposl*, 1998.
[3] J. L. Massey, "SAFER K-64: One Year Later", *Fast Software Encryption II, Lecture Notes in Computer Science*, New York, Springer, no. 1008, pp. 212-241, 1995.
[4] J. L. Massey, G.H. Khachatryan and K. M. Kyuregian,"Nomination of SAFER++ as candidate algorithm for the new european schemes for signatures, integrity and encryption (NESSIE)", Submission document from Cylink Corporation, 2000.
[5] BLUETOOTH SPECIFICATION Version 1.0B, 29 Nov. 1999, [Online]. Available:

http://www.bluetooth.com/link/pec/bluetooth_b.pdf

Submitted 28.07.2014, accepted 27.11.2014.

SAFER-256 նոր ծածկագրման ալգորիթմի կառուցվածքը և ծածկագրավերլուծությունը

Գ. Խաչատրյան, Մ. Կյուրեղյան և Ք. Կյուրեղյան

Ամփոփում

Այս հոդվածում ներկայացված է SAFER ընտանիքին պատկանող նոր ծածկագրական համակարգ SAFER-256: Այն 256 բիթ երկարությամբ բլոկային համակարգ է 256 բիթ բանալիով և անվտանգ է դիֆերենցիալ անալիզի նկատմամբ 6 ռաունդից հետո:

Дизайн и криптоанализ нового алгоритма шифрования SAFER-256

Г. Хачатрян, М. Кюрегян и К. Кюрегян

Аннотация

В данной статье представлена новая криптографическая система SAFER-256 из семьи SAFER. Это 256 битовая блоковая система с 256 битным ключом, которая устойчива по отношению к дифференциальному анализу после 6 раундов.