Mathematical Problems of Computer Science 44, 133-137, 2015.

On Optimality of SAFER-256 Diffusion

Knarik M. Kyuregyan

Institute for Informatics and Automation Problems of NAS RA
e-mail: knarikyuregyan@gmail.com

Abstract

In this paper it is shown that the new block cipher SAFER-256 provides an optimal diffusion in the sense that the cipher is resistant against differential cryptanalysis attack after minimum possible number of rounds.

Keywords: Diffusion, Shuffle, Byte Permutation, Differential cryptanalysis.

1. Introduction

A new 256-bit size block cipher of SAFER family named SAFER-256 consists of 6 rounds followed by an output transformation. To develop a new 256-bit size block cipher we have investigated a construction of regular cipher SAFER+ [1] and modified SAFER+ [2]. As a result we have found, that we can provide the cipher resistance against differential cryptanalysis after minimum possible number of rounds ($r = 5$) in the case of using four iterations of byte shuffling (in case of 3 times shuffle it will be secure against differential cryptanalysis after 6 rounds at the time) (Fig. 1). The classical criteria for the resistance against differential cryptanalysis [3] allow to compute the maximum expected probability that the given input difference leads to a given sequence of output differences after successive rounds in the cipher. Diffusion that ensures the small changes in each round input and results in large changes in the round output, allows to reduce the number of rounds, improving speed of implementation, while ensuring a security against differential cryptanalysis. The purpose of this paper is to show an optimality of the diffusion of a new cipher SAFER-256 with 256-bit block length and key size [4]. This fact also insures higher processing speed for relevant ciphers while keeping their security level intact against differential cryptanalysis attack.

All research has been done by the prior developed C++ code.

2. Optimal Diffusion of SAFER-256

A detailed construction and a differential cryptanalysis of the new cipher SAFER-256 is presented in [4]. The round function is built from four layers:

1. XOR/Addition Layer: Bytes 1,2,3,4,9,10,11,12,17,18,19,20,25,26,27,28 of the round input are XOR-ed with bytes 1,2,3,4,9,10,11,12,17,18,19,20,25,26,27,28 of round first subkey. Bytes 5,6,7,8,13,14,15,16,21,22,23,24,29,30,31,32 of the round input are added modulo 256 with bytes 5,6,7,8,13,14,15,16,21,22,23,24,29,30,31,32 of round first subkey.
2. Nonlinear Layer: The $45^{(x)}$ transformation is applied to bytes 1,2,3,4,9,10,11,12,17,18, 19,20,25,26,27,28 of the output XOR/Addition layer (with the convention $45^{(128)} \mathrm{mod} 257 = 0$) and $\log_{45}(x)$ transformation is applied to bytes 5,6,7,8,13,14,15,16, 21,22,23,24,29,30,31,32, where $x \in \mathbb{Z}_{256}$.
3. Addition/ XOR Layer: Bytes 1,2,3,4,9,10,11,12,17,18,19,20,25,26,27,28 of the output of the nonlinear layer added modulo 256 with bytes 1,2,3,4,9,10,11,12,17,18,19,20,25,26, 27,28 of round second subkey. Bytes 5,6,7,8,13,14,15,16,21,22,23,24,29,30,31,32 of the output of the nonlinear layer are XOR-ed with bytes 5,6,7,8,13,14,15,16,21,22,23,24,29, 30,31,32 of round second subkey.
4. Invertible linear Transformation Layer. At first "Armenian shuffle" is applied on the input of this layer, which 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] with the meaning that the first output byte is the 25th input byte, the second output byte is the 28th input byte, etc. Then 2-PHT linear transformation is applied to the output, that maps a byte pair $(X1, X2)$ to the byte pair $(2X1 + X2, X1 + X2)$ where addition is modulo 256. The effect of the four layers of "Armenian Shuffle"+2-PHT transform on the 32 byte output of the Addition/ XOR layer is to postmultiply 32 byte output with M matrix in Fig. 1.

One sees from Fig. 1 that every row of the matrix M contains at least eight 1's (all odd-numbered rows contain exactly eight 1's and the remaining rows contain exactly thirteen 1's), which means that every input block with a single non-zero byte will produce an output block with at least eight output non-zero bytes. Moreover, there are changes of an input bytes that will cause only this minimum number of output bytes to change, namely a change by 128 in any odd-numbered symbol position. The diffusion provided by the matrix M is highly resistant to differential cryptanalysis.

If odd-coordinate bytes and even-coordinate bytes in 32-byte block are permuted separately, then in the case of certain permutations out of $(16!)^2$ possible permutations we can obtain matrices with the above mentioned property. The following permutations are some of these, which are obtained from software researches:

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

M=

8	8	1	1	2	2	8	4	4	2	1	1	1	1	4	4	8	4	4	2	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	2	1	1	1	1	1	4	4	2	1	1	1	1	1	2	2	4	2
4	2	8	4	8	4	4	4	1	1	32	16	4	2	2	1	1	1	2	2	8	8	2	1	1	1	2	2	2	2	8	4
4	4	1	1	1	1	8	4	2	1	1	1	1	1	2	2	4	2	4	2	2	1	1	1	16	8	2	1	4	2	2	2
2	2	2	2	1	1	32	16	2	1	4	4	2	2	1	1	2	1	8	4	8	4	1	1	8	4	4	2	4	2	8	8
4	2	4	2	16	8	1	1	2	2	8	4	2	1	2	1	1	1	1	1	2	2	4	2	1	1	1	1	4	4	2	1
8	4	4	2	32	16	1	1	4	4	8	4	2	1	4	2	2	2	1	1	2	2	8	4	2	2	1	1	8	8	2	1
2	2	1	1	1	1	16	8	2	1	2	2	1	1	1	1	2	1	4	2	4	2	1	1	8	4	2	1	4	2	4	4
2	2	1	1	8	8	4	2	8	4	1	1	2	2	2	2	4	2	8	4	2	1	4	4	8	4	2	1	32	16	1	1
8	4	16	8	4	2	1	1	1	1	4	2	4	2	2	1	1	1	2	2	1	1	2	1	2	2	4	4	1	1	2	1
8	4	32	16	4	2	2	2	1	1	8	4	8	4	2	1	1	1	4	4	2	2	2	1	2	2	8	8	1	1	4	2
1	1	1	1	4	4	4	2	4	2	1	1	2	2	1	1	2	1	8	4	2	1	2	2	4	2	2	1	16	8	1	1
1	1	4	4	2	2	8	4	2	1	2	2	8	8	1	1	2	1	32	16	4	2	1	1	4	2	8	4	8	4	2	2
16	8	8	4	4	2	1	1	1	1	4	2	2	1	4	2	2	2	1	1	1	1	2	1	4	4	2	2	1	1	2	1
32	16	8	4	8	4	1	1	2	2	4	2	2	1	8	4	4	4	1	1	1	1	4	2	8	8	2	2	2	2	2	1
1	1	2	2	2	2	4	2	2	1	1	1	4	4	1	1	2	1	16	8	2	1	1	1	4	2	4	2	8	4	1	1
1	1	2	2	1	1	8	4	4	2	8	8	2	2	2	2	8	4	4	2	32	16	1	1	2	1	8	4	2	1	4	4
2	1	4	2	2	1	1	1	1	1	2	1	16	8	8	4	2	2	4	4	1	1	4	2	1	1	2	2	1	1	4	2
2	1	8	4	2	1	2	2	1	1	4	2	32	16	8	4	2	2	8	8	2	2	4	2	1	1	4	4	1	1	8	4
1	1	1	1	1	1	4	2	4	2	4	4	1	1	2	2	8	4	2	1	16	8	1	1	2	1	4	2	2	1	2	2
4	4	1	1	2	2	2	1	8	4	2	2	1	1	8	8	32	16	2	1	8	4	2	2	8	4	4	2	4	2	1	1
4	2	2	1	2	1	1	1	1	1	2	1	8	4	16	8	4	4	2	2	1	1	4	2	2	2	1	1	1	1	4	2
8	4	2	1	4	2	1	1	2	2	2	1	8	4	32	16	8	8	2	2	1	1	8	4	4	4	1	1	2	2	4	2
2	2	1	1	1	1	2	1	4	2	2	2	1	1	4	4	16	8	2	1	8	4	1	1	4	2	4	2	2	1	1	1
1	1	8	8	1	1	4	2	8	4	2	2	4	4	1	1	4	2	8	4	8	4	2	2	2	1	32	16	2	1	2	2
2	1	2	1	2	1	4	4	2	2	4	2	4	2	4	2	1	1	1	1	2	2	8	4	1	1	1	1	1	1	16	8
2	1	4	2	2	1	8	8	2	2	8	4	8	4	4	2	1	1	2	2	4	4	8	4	1	1	2	2	1	1	32	16
1	1	4	4	1	1	2	1	8	4	1	1	2	2	1	1	4	2	4	2	4	2	2	2	2	1	16	8	2	1	1	1
2	2	2	2	4	4	2	1	32	16	1	1	1	1	2	2	8	4	2	1	4	2	8	8	4	2	8	4	8	4	1	1
2	1	2	1	4	2	2	2	4	4	2	1	4	2	4	2	1	1	1	1	1	1	16	8	1	1	1	1	2	2	8	4
4	2	2	1	8	4	2	2	8	8	2	1	4	2	8	4	2	2	1	1	1	1	32	16	2	2	1	1	4	4	8	4
1	1	2	2	2	2	2	1	16	8	1	1	11	1	1	1	4	2	2	1	4	2	4	4	2	1	8	4	4	2	1	1

Fig 1. SAFER-256 invertible linear transformation matrix

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

Some of these permutations provide the best possible diffusion.

3. Conclusion

In this paper it is shown that diffusion provided by SAFER-256 algorithm is optimal from the point of differential analysis. A complete characterization of the corresponding invertible linear transformation matrix that insures an optimum transformation diffusion i.e., provides a resistance against differential cryptanalysis after minimum number of rounds is also given.

Acknowledgement

The author is thankful to Prof. Gurgen Khachatrian and Dr. Melsik Kureghyan for very useful discussions and comments.

References

[1] J. L. Massey, G. Khachatrian and M. Kyuregian, "Nomination of SAFER+ as candidate algorithm for the advanced encryption standard (AES)", *NIST AES Proposl*, 1998.

[2] K. Kyuregyan, "Some modifications of SAFER+", *In Reports of NAS RA,* vol. 115, no 1, pp. 33-39, Yerevan, Armenia, 2015.

[3] 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.

[4] G. H. Khachatrian, M. K. Kyureghyan and K. M. Kyuregyan, "Design and cryptanalysis of a new encryption algorithm SAFER-256", *Transactions of IIAP NAS RA, Mathematical Problems of Computer Science*, vol. 42, pp. 97-106, 2014.

Submitted 20.07.2015, accepted 27.11.2015

SAFER-256 համակարգի դիֆուզիայի օպտիմալությունը

Ք.Կյուրեղյան

Ամփոփում

Այս հոդվածում ցույց է տրված, որ SAFER-256 բլոկային ծածկագրական համակարգը ապահովում է օպտիմալ դիֆուզիա այն իմաստով, որ այն կրիպտոկայուն է դիֆերենցիալ վերլուծության նկատմամբ մինիմալ թվով ռաունդների դեպքում:

Об оптимальности диффузии SAFER-256

К. Кюрегян

Аннотация

В данной статье показано, что блоковый шифр SAFER-256 обеспечивает оптимальную диффузию, в том смысле, что шифр устойчив по отношению к дифференциальному анализу после минимально возможного количества раундов.