Mathematical Problems of Computer Science 44, 109--115, 2015.

On Optimality of Regular SAFER+ and Modified SAFER+ 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 regular block cipher SAFER+ and modified SAFER+ provide an optimal diffusion in the sense that ciphers are resistant against differential cryptanalysis attack after minimum possible number of rounds. Moreover, there are 967 680 byte permutations that provide equivalent security.

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

1. Introduction

Shanon's principles of confusion and diffusion remain the most widely accepted principles for the design of block ciphers [1]. Diffusion namely to ensure that changing of single symbol in the vector of symbols input to this transformation causes many output symbols to change allows to reduce the number of rounds, improving the speed of implementation, while ensuring a security against differential cryptanalysis. Diffusion in the block ciphers of SAFER family provides the invertible linear transformation layer of the cipher rounds, which consist of 2-PHT pseudo-Hadamard transformation and permutation of n bytes (Fig. 1), where n is a length of block. 2-PHT is a simple linear transformation by the matrix $\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$, which means that the first output byte is the sum modulo 256 of twice (or one left shift of) the first input byte and the second input byte, while the second output byte is just the sum modulo 256 of the two input bytes. The invertible linear transformation layer performs a linear operation over the ring of integers modulo 256 and is well measured by how well the linear transformation layer converts low weight inputs into high weight outputs. The objective of this paper is to show that the regular cipher SAFER+ [2] and modified SAFER+ [3] provide an optimal diffusion in the sense that the cipher is secure against differential cryptanalysis attack after minimum possible number of rounds. This fact also insures higher processing speed for relevant ciphers. Differential cryptanalysis is the most effective attack

against the block ciphers [1]. The attack on an r-round ciphers of SAFER family through differential cryptanalysis relies on the following circumstance: find a $(r-1)$-round quasi-differentials whose transition probability is greater then $\frac{1}{2^n-1} \approx 2^{-n}$ average probability for an n-byte block length [2], [3], [4].

All research has been done by prior developed software packages created in C++ language.

2. On the Optimality of SAFER+ Diffusion

SAFER+ is one of the block ciphers of SAFER family proposed by Prof. James L. Massey together with Prof. Gurgen H. Khachatrian and Dr. Melsik K. Kuregian and was submitted as a candidate for the Advanced Encryption Standard (AES) [2]. It is a 128-bit block size encryption algorithm.

SAFER+ is an r-round iterated cipher the round function of which consists of

1. A byte-wise mixed $\mathrm{XOR/Byte-Addition\ (XOR/ADD)}$ of 16 input bytes and 16 first round key bytes.
2. A non-linear layer, where each byte is subjected to either the non-linear function EXP: $x \to 45^x \mathrm{mod} 257$ (except that $45^{128} \mathrm{mod} 257$ is taken 0) or its inverse function LOG.
3. A byte-wise mixed $\mathrm{Byte-Addition/XOR\ (ADD/XOR)}$ of 16 input bytes and 16 second round key bytes.
4. Invertible linear transformation (Fig. 1), that is composed of a Pseudo-Hadamard Transformation (2-PHT), that maps the input pair $(X1, X2)$ into $(2X1+X2, X1+X2)$, where addition and multiplication are modulo 256 and fixed byte permutation [9, 12, 13, 16, 3, 2, 7, 6, 11, 10, 15, 14, 1, 8, 5, 4] with the meaning that the first output of the permutation is the ninth input symbol, the second output is the twelfth input symbol, etc.

Byte permutation used in block cipher SAFER+ is one of the best possible diffusion providing permutations, which Massey called Armenian shuffle in honor of its co-inventors (Fig. 1).

There are another byte permutations equivalent to SAFER+ specific Armenian shuffle in the sense that they provide the same security level against differential cryptanalysis and don't reduce cipher processing speed. So changing the byte permutation in cipher SAFER+ we can have another equivalent new cipher. Invertible linear transformation layer corresponds to postmultiplication $\mathrm{modulo}\ 256$ of the n-byte input by the invertible linear transformation matrix [2], [3]. That is to study n-byte permutation is the same to study properties of invertible linear transformation matrix. If matrix doesn't contain nonzero elements, then it provides good key bytes confusion and best diffusion in the cipher and makes the last round attack impossible.

It should be noted that good diffusion provides every byte permutation whose corresponding invertible linear transformation matrix's every row contains at least five 1 entries (all odd-numbered rows contain exactly five 1 entries and all even-numbered rows contain exactly eight 1), which means that changing any single input symbol will change at least five output symbols. Moreover, there are changes of an input symbol that will cause only this minimum number of output symbols to change, namely a change by 128 in any odd-numbered symbol position.

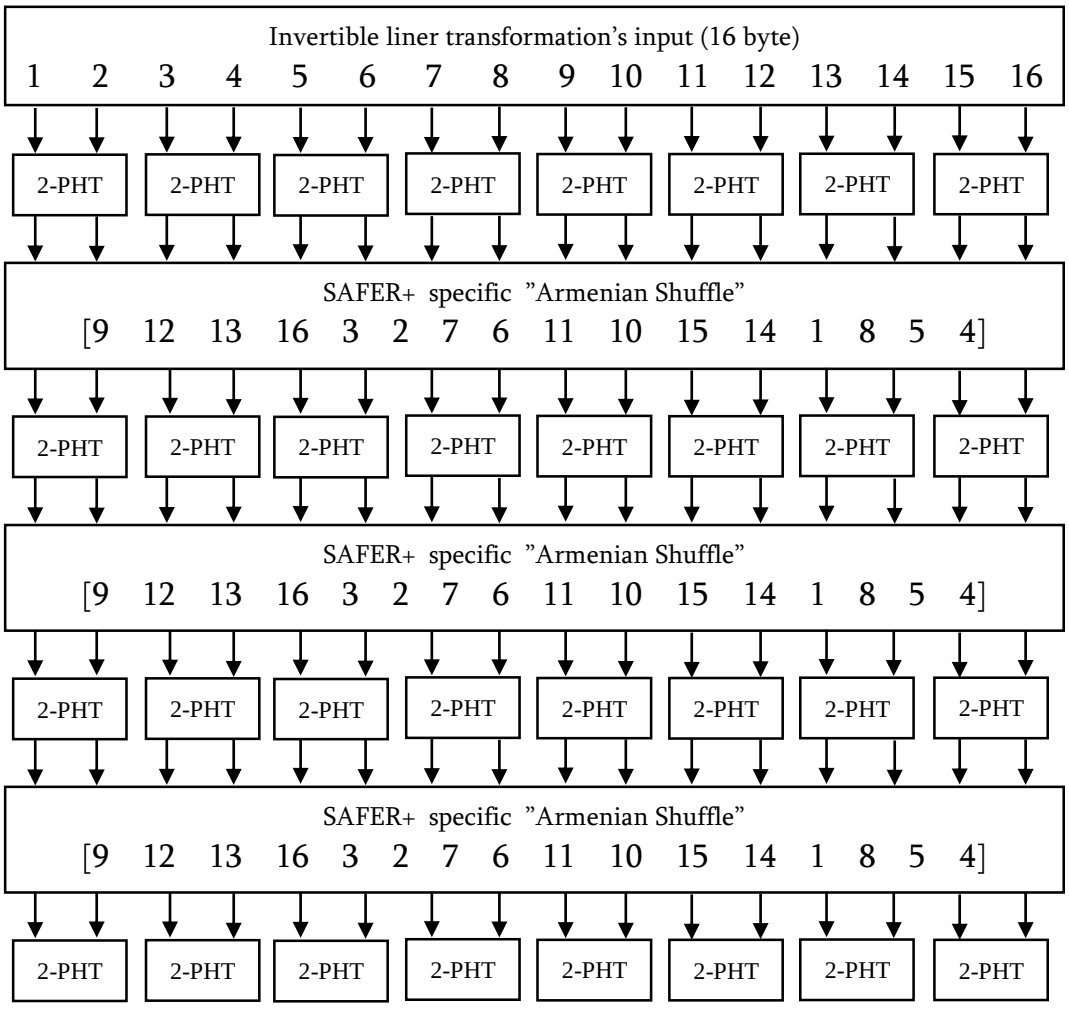

Fig. 1: Invertible linear transformation layer of SAFER+.

One notes further that every column of the corresponding matrix contains at least five 1 entries (and all odd-numbered rows contain exactly five 1 entries), which means that for each output symbol there are at least five input symbols for which a change in any of those input symbols is guaranteed to change that output symbol [5]. For example, in case of permutation 7, 6, 15, 2, 3, 14, 5, 8, 1, 16, 9, 12, 11, 10, 13, 4 the input $X = X1X2X3\ldots X16$ of invertible linear transformation layer is postmultiplied by the following matrix to shape an output $Y = Y1Y2Y3\ldots Y16$ of the linear transformation and of the round:

$$\begin{pmatrix} Y1 \\ Y2 \\ Y3 \\ Y4 \\ Y5 \\ Y6 \\ Y7 \\ Y8 \\ Y9 \\ Y10 \\ Y11 \\ Y12 \\ Y13 \\ Y14 \\ Y15 \\ Y16 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 2 & 1 & 2 & 2 & 4 & 2 & 1 & 1 & 4 & 4 & 16 & 8 & 4 & 2 \\ 1 & 1 & 2 & 1 & 1 & 1 & 4 & 2 & 1 & 1 & 2 & 2 & 8 & 4 & 2 & 1 \\ 16 & 8 & 2 & 2 & 4 & 2 & 4 & 4 & 4 & 2 & 2 & 1 & 1 & 1 & 1 & 1 \\ 8 & 4 & 1 & 1 & 4 & 2 & 2 & 2 & 2 & 1 & 2 & 1 & 1 & 1 & 1 & 1 \\ 4 & 2 & 4 & 4 & 2 & 1 & 2 & 2 & 16 & 8 & 4 & 2 & 1 & 1 & 1 & 1 \\ 2 & 1 & 2 & 2 & 2 & 1 & 1 & 1 & 8 & 4 & 4 & 2 & 1 & 1 & 1 & 1 \\ 2 & 1 & 1 & 1 & 4 & 2 & 1 & 1 & 4 & 2 & 16 & 8 & 4 & 4 & 2 & 2 \\ 2 & 1 & 1 & 1 & 2 & 1 & 1 & 1 & 4 & 2 & 8 & 4 & 2 & 2 & 1 & 1 \\ 1 & 1 & 4 & 2 & 4 & 4 & 2 & 1 & 1 & 1 & 2 & 2 & 4 & 2 & 16 & 8 \\ 1 & 1 & 4 & 2 & 2 & 2 & 2 & 1 & 1 & 1 & 1 & 1 & 2 & 1 & 8 & 4 \\ 2 & 2 & 16 & 8 & 1 & 1 & 4 & 2 & 4 & 4 & 1 & 1 & 2 & 1 & 4 & 2 \\ 1 & 1 & 8 & 4 & 1 & 1 & 2 & 1 & 2 & 2 & 1 & 2 & 2 & 1 & 4 & 2 \\ 4 & 2 & 1 & 1 & 16 & 8 & 1 & 1 & 2 & 1 & 4 & 2 & 2 & 2 & 4 & 4 \\ 4 & 2 & 1 & 1 & 8 & 4 & 1 & 1 & 2 & 1 & 2 & 1 & 1 & 1 & 2 & 2 \\ 4 & 4 & 4 & 2 & 1 & 1 & 16 & 8 & 2 & 2 & 1 & 1 & 4 & 2 & 2 & 1 \\ 2 & 2 & 2 & 1 & 1 & 1 & 8 & 4 & 1 & 1 & 1 & 1 & 4 & 2 & 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} X1 \\ X2 \\ X3 \\ X4 \\ X5 \\ X6 \\ X7 \\ X8 \\ X9 \\ X10 \\ X11 \\ X12 \\ X13 \\ X14 \\ X15 \\ X16 \end{pmatrix} (\mathrm{mod}\, 256)$$

Software researches show that we can build the above mentioned type of matrix if even-coordinate and odd-coordinate bytes aren't permuted with each other. There exist $(8!)^2 = 1625702400$ byte permutations, whose even-coordinate and odd-coordinate bytes are permuted with each other, in case of 967 680 of them we can get a matrix with the above mentioned property. Differential cryptanalysis show that these byte permutations provide security after 5 or 6 rounds, particularly SAFER+ is secure against differential cryptanalysis after 5 rounds (key length is 128 bit). All byte permutations, which are equivalent to the SAFER+ specific Armenian shuffle, i.e., in which case cipher will be secure against differential cryptanalysis after 5 rounds we will call an Armenian shuffle.

Invertible linear transformation part of SAFER+ starts from 2-PHT operations (Fig. 1) [2], after modifications it starts from shuffle of bytes immeedietly [3] and instead of 3 applied 4 times of byte shuffle in linear layer. In case of 4 times of byte shuffle and above mentioned permutation 7, 6, 15, 2, 3, 14, 5, 8, 1, 16, 9, 12, 11, 10, 13, 4 the invertible linear transformation matrix will have the following view:

$$\begin{pmatrix}
1 & 1 & 4 & 2 & 4 & 4 & 2 & 1 & 1 & 1 & 2 & 2 & 4 & 2 & 16 & 8 \\
8 & 4 & 1 & 1 & 4 & 2 & 2 & 2 & 2 & 1 & 2 & 1 & 1 & 1 & 1 & 1 \\
4 & 2 & 4 & 4 & 2 & 1 & 2 & 2 & 16 & 8 & 4 & 2 & 1 & 1 & 1 & 1 \\
2 & 2 & 2 & 1 & 1 & 1 & 8 & 4 & 1 & 1 & 1 & 1 & 4 & 2 & 2 & 1 \\
2 & 1 & 1 & 1 & 4 & 2 & 1 & 1 & 4 & 2 & 16 & 8 & 4 & 4 & 2 & 2 \\
1 & 1 & 2 & 1 & 1 & 1 & 4 & 2 & 1 & 1 & 2 & 2 & 8 & 4 & 2 & 1 \\
1 & 1 & 2 & 1 & 2 & 2 & 4 & 2 & 1 & 1 & 4 & 4 & 16 & 8 & 4 & 2 \\
2 & 1 & 1 & 1 & 2 & 1 & 1 & 1 & 4 & 2 & 8 & 4 & 2 & 2 & 1 & 1 \\
2 & 2 & 16 & 8 & 1 & 1 & 4 & 2 & 4 & 4 & 1 & 1 & 2 & 1 & 4 & 2 \\
4 & 2 & 1 & 1 & 8 & 4 & 1 & 1 & 2 & 1 & 2 & 1 & 1 & 1 & 2 & 2 \\
4 & 2 & 1 & 1 & 16 & 8 & 1 & 1 & 2 & 1 & 4 & 2 & 2 & 2 & 4 & 4 \\
1 & 1 & 8 & 4 & 1 & 1 & 2 & 1 & 2 & 2 & 1 & 1 & 2 & 1 & 4 & 2 \\
4 & 4 & 4 & 2 & 1 & 1 & 16 & 8 & 2 & 2 & 1 & 1 & 4 & 2 & 2 & 1 \\
2 & 1 & 2 & 2 & 2 & 1 & 1 & 1 & 8 & 4 & 4 & 2 & 1 & 1 & 1 & 1 \\
16 & 8 & 2 & 2 & 4 & 2 & 4 & 4 & 4 & 2 & 2 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 4 & 2 & 2 & 2 & 2 & 1 & 1 & 1 & 1 & 1 & 2 & 1 & 8 & 4
\end{pmatrix}$$

Our investigation showed that in case of regular cipher SAFER+ and in case of modified SAFER+ shuffles providing good diffusion are virtually the same. Some of those shuffles are listed below:

1, 10, 3, 14, 7, 12, 5, 16, 11, 8, 13, 4, 15, 6, 9, 2
1, 16, 15, 2, 13, 10, 11, 6, 9, 14, 7, 4, 3, 8, 5, 12
3, 10, 1, 14, 5, 12, 7, 16, 11, 6, 13, 2, 15, 8, 9, 4
3, 16, 15, 4, 13, 10, 11, 6, 9, 14, 7, 2, 1, 8, 5, 12
5, 4, 1, 12, 3, 8, 7, 16, 9, 14, 13, 10, 15, 6, 11, 2
5, 14, 15, 10, 13, 6, 11, 4, 9, 16, 7, 2, 3, 12, 1, 8
7, 10, 1, 14, 3, 12, 5, 16, 9, 8, 11, 4, 15, 6, 13, 2
7, 16, 15, 8, 13, 4, 11, 10, 9, 12, 5, 2, 3, 14, 1, 6
9, 2, 1, 8, 3, 16, 5, 12, 7, 14, 11, 6, 15, 4, 13, 10
9, 16, 15, 10, 13, 4, 11, 8, 7, 12, 5, 2, 3, 14, 1, 6
11, 4, 1, 8, 3, 12, 5, 14, 7, 2, 9, 16, 13, 6, 15, 10
11, 14, 15, 4, 13, 10, 9, 6, 7, 2, 5, 12, 3, 16, 1, 8
13, 2, 1, 10, 3, 14, 5, 16, 7, 12, 9, 4, 11, 8, 15, 6
13, 12, 15, 4, 11, 10, 9, 6, 7, 2, 3, 16, 5, 14, 1, 8
15, 2, 1, 12, 3, 16, 5, 8, 7, 6, 9, 14, 11, 4, 13, 10
15, 12, 13, 2, 11, 6, 9, 16, 7, 4, 3, 8, 1, 14, 5, 10
⋮

Virtually in sense that for example differential analysis showed that SAFER+ specific Armenian shuffle 9, 12, 13, 16, 3, 2, 7, 6, 11, 10, 15, 14, 1, 8, 5, 4 mentioned in the literature [2] isn't one of the best diffusion providing shuffles after modifications, instead there are best diffusion providing shuffles one of which is 7, 12, 9, 14, 5, 8, 13, 10, 11, 4, 3, 6, 15, 2, 1, 16 [3].

There are shuffles such that their corresponding linear transformation matrix is the same. In the case of regular SAFER+ the same matrix can be obtained from four different shuffles or from one shuffle. For example, in the case of four shuffles below the same permutation matrix is obtained:

9, 8, 7, 10, 3, 16, 5, 14, 15, 4, 11, 2, 13, 6, 1, 12
13, 6, 5, 14, 11, 2, 7, 10, 1, 12, 3, 16, 9, 8, 15, 4
15, 4, 3, 16, 7, 10, 11, 2, 9, 8, 5, 14, 1, 12, 13, 6
1, 12, 11, 2, 5, 14, 3, 16, 13, 6, 7, 10, 15, 4, 9, 8

and the corresponding matrix of shuffle

13, 4, 15, 14, 11, 16, 9, 8, 1, 6, 3, 12, 5, 2, 7, 10

is obtained only in the case of this one. After modifications the same matrix can be obtained from eight or two different shuffles or from one shuffle. Below examples for each of those shuffles are presented

1. 3, 14, 1, 8, 5, 12, 9, 16, 13, 4, 7, 2, 11, 6, 15, 10
   5, 12, 15, 10, 3, 14, 7, 2, 11, 6, 9, 16, 13, 4, 1, 8
   7, 2, 13, 4, 9, 16, 5, 12, 1, 8, 3, 14, 15, 10, 11, 6
   9, 16, 11, 6, 7, 2, 3, 14, 15, 10, 5, 12, 1, 8, 13, 4
   11, 6, 9, 16, 13, 4, 1, 8, 5, 12, 15, 10, 3, 14, 7, 2
   13, 4, 7, 2, 11, 6, 15, 10, 3, 14, 1, 8, 5, 12, 9, 16
   15, 10, 5, 12, 1, 8, 13, 4, 9, 16, 11, 6, 7, 2, 3, 14
   1, 8, 3, 14, 15, 10, 11, 6, 7, 2, 13, 4, 9, 16, 5, 12
2. 7, 2, 1, 8, 9, 4, 11, 6, 5, 12, 13, 16, 15, 14, 3, 10
   15, 14, 13, 16, 5, 12, 3, 10, 9, 4, 1, 8, 7, 2, 11, 6
3. 7, 12, 9, 14, 5, 8, 13, 10, 11, 4, 3, 6, 15, 2, 1, 16

Thus, it is more convenient and efficient to study cipher through the permutation matrix instead of shuffle.

3. Conclusion

In this paper it is shown that diffusion provided by SAFER+ and modified SAFER+ is optimal from the point of differential analysis view. 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 Kuregian for very useful discussions and comments.

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. Khachatrian and M Kyuregian, “Nomination of SAFER+ as candidate algorithm for the advanced encryption standard”, (AES). *NIST AES Proposal*, 1998.
[3] K. Kyuregyan, “Some Modifications of SAFER+”, *In Reports of NAS RA*, vol. 115, no 1, pp. 33--39, Yerevan, Armenia, 2015.
[4] 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.
[5] J. L. Massey, “On the optimum of SAFER+ diffusion”, *The second AES candidate conference*, March 22-23, Rome, Italy, 1999.

Submitted 20.07.2015, accepted 27.11.2015

SAFER+ և ձևափոխված SAFER + համակարգերի դիֆուզիայի օպտիմալությունը

Ք.Կյուրեղյան

Ամփոփում

Այս հոդվածում ցույց է տրված, որ SAFER+ բլոկային ծածկագրական համակարգը և ձևափոխված SAFER+ համակարգը ապահովում են օպտիմալ դիֆուզիա այն իմաստով, որ համակարգերը կրիպտոկայուն են դիֆերենցիալ վերլուծության նկատմամբ մինիմում թվով ռաունդների դեպքում: Ավելին, գոյություն ունի 16 բայթերի 967 680 տեղադրություն, որոնք ապահովում են համարժեք կրիպտոկայունություն:

Об оптимальности диффузии регулярной SAFER+ и модифицированной SAFER+

К. Кюрегян

Аннотация

В данной статье показано, что регулярный шифр SAFER+ и модифицировнный шифр SAFER+ обеспечивают оптимальную диффузию, в том смысле, что шифры устойчивы по отношению к дифференциальному анализу после минимально возможного количества раундов. Боле того, существуют 967 680 перестановок 16 байтов, которые обеспечивают эквивалентную криптостойкость.