Extended Criterion for Absence of Fixed Points

Oleksandr Kazymyrov and Valentyna Kazymyrova

Department of Informatics
University of Bergen, Norway
Valentyna.Kazymyrova@student.uib.no
Oleksandr.Kazymyrov@ii.uib.no

Abstract. One of criteria for substitutions used in block ciphers is the absence of fixed points. In this paper we show that this criterion must be extended taking into consideration a mixing key function. In practice, we give a description of AES when fixed points are reached. Additionally, it is shown that modulo addition 2^n has advantages comparing with the XOR operation.

Keywords: S-box, Block Cipher, Fixed Point, AES

1 Introduction

Substitution boxes (S-boxes) map an n-bit input message to an m-bit output message. They provide confusion in symmetric algorithms. For different tasks S-boxes are used in various forms. In stream ciphers a substitution is represented usually as a vectorial Boolean function [1]. Permutations are a subclass of substitutions and are commonly used in block ciphers as lookup tables. Regardless of ciphers an S-box can be converted from one form to another one.

Substitutions must satisfy various criteria to be resistant against different types of attacks [2]. A substitution satisfying all criteria is perfect. However, such substitutions do not exist nowadays. Therefore, in practice, substitutions satisfying several important criteria are used. They are called optimal S-boxes. Optimality criteria vary from cipher to cipher. Generating permutations with optimal criteria is a quite difficult task, especially for large n and m. The problem of generating a set of S-boxes with similar properties can be particularly solved by using EA- or CCZ-equivalence [3, 4].

One of the criteria is absence of fixed points. It is used in many ciphers for increasing resistance against statistical attacks [5]. Designers of modern cryptographic primitives try to get rid of the fixed points. This is achieved by applying affine equivalence, which is a special case of EA-equivalence. The S-box of advanced encryption standard (AES) was constructed using this technique [5, 6]. However, application of this method does not totally prevent the appearance of fixed points. In this paper we show an isomorphic (equivalent) form of AES when fixed points are reached.

Two ciphers E_i and E_j are isomorphic to each other if there exist invertible maps $\phi : x^i \mapsto x^j$, $\psi : y^i \mapsto y^j$ and $\chi : k^i \mapsto k^j$ such that $y^i = E_i(x^i, k^i)$ and $y^j = E_j(x^j, k^j)$ are equal for all x^i, k^i, x^j and k^j [7, 8]. Obviously, the cipher can have a lot of isomorphic basic transformations as well as full encryption procedures. The cipher BES is a well-known example of isomorphic AES [9]. Another example is the description of encryption procedure using system of equation of degree 2 [10]. We give one more description of AES which includes a substitution with a fixed point while almost all transformations are unmodified.

2 Preliminaries

Arbitrary substitution can be represented at least in three different forms: algebraic normal form (ANF), over field $\mathbb{F}_{2^n}$ and as a lookup table. Most of substitutions used in block ciphers have a table representation because of simplicity of description and understanding [11]. Meanwhile arbitrary S-box can be always associated with a vectorial Boolean function F in $\mathbb{F}_{2^n}[x]$. For bijective substitutions (i.e., permutations) F is defined uniquely [1].

A natural way to represent $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ is an algebraic normal form:

$$\sum_{I \subseteq \{1,\ldots,n\}} a_I \left(\prod_{i \in I} x_i \right), \qquad a_I \in \mathbb{F}_2^m,$$

the sum is being calculated in $\mathbb{F}_2^m$ [1]. The algebraic degree of F is the degree of its ANF. F is called affine if it has algebraic degree at most 1, and it is called linear if it is affine and $F(0) = 0$. A vectorial Boolean function represented as a table can be easily transformed to the ANF form and vice versa.

Two functions $F, G : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ are called extended affine equivalent (EA-equivalent) if there exist an affine permutation A_1 of $\mathbb{F}_2^m$, an affine permutation A_2 of $\mathbb{F}_2^n$ and a linear function L_3 from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ such that

$$F(x) = A_1 \circ G \circ A_2(x) + L_3(x). \tag{1}$$

Clearly, A_1 and A_2 can be presented as $A_1(x) = L_1(x) + c_1$ and $A_2(x) = L_2(x) + c_2$ for some linear permutations L_1 and L_2, and some $c_1 \in \mathbb{F}_2^m$, $c_2 \in \mathbb{F}_2^n$. Two functions F and G are linear equivalent if equation (1) is hold for $L_3(x) = 0$, $c_1 = 0$, $c_2 = 0$. If the equation (1) is preserved only for $L_3(x) = 0$, then functions F and G are called affine equivalent [12].

In the binary matrix form EA-equivalence is represented as follows

$$F(x) = M_1 \cdot G(M_2 \cdot x \oplus V_2) \oplus M_3 \cdot x \oplus V_1$$

where elements of $\{M_1, M_2, M_3, V_1, V_2\}$ have dimensions $\{m \times m, n \times n, m \times n, m, n\}$ [3].

An element $a \in \mathbb{F}_2^n$ is a fixed point of $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ if $F(a) = a$. The absence of fixed points criterion is defined as follows.

Definition 1. *A substitution must not have fixed points, i.e.*

$$F(a) \neq a, \quad \forall a \in \mathbb{F}_2^n.$$

For any positive integers n and m, a function F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ is called differentially δ-uniform if for every $a \in \mathbb{F}_2^n \setminus \{0\}$ and every $b \in \mathbb{F}_2^m$, the equation $F(x) + F(x + a) = b$ admits at most δ solutions [1]. Vectorial Boolean functions used as S-boxes in block ciphers must have a low differential uniformity to be resistant against differential cryptanalysis [13].

The nonlinearity criterion is closely connected to the notion of the Walsh transform which can be described as the function

$$\lambda(u, v) = \sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot F(x) + u \cdot x},$$

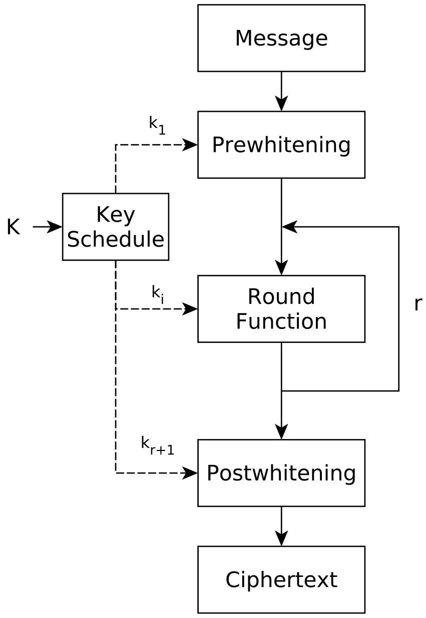


Fig. 1. A General Structure of An Iterative Block Cipher

where "·" denotes inner products in $\mathbb{F}_2^n$ and $\mathbb{F}_2^m$ respectively [1]. A substitution has an optimal resistance to linear cryptanalysis if the maximum absolute value of Walsh coefficients is small [14]. Substitutions with the smallest value of $\lambda(u, v)$ exist for odd n only.

These two criteria are major while selecting substitutions for new ciphers. However, there are many others criteria like propagation criterion, absolute indicator, correlation immunity, strict avalanche criterion, etc [1, 2]. It has been still not proven the importance of many criteria for block ciphers. For example, the substitution used in AES does not satisfy most of them [15]. Moreover, no theoretical or practical attacks were proposed on modern block ciphers based on these criteria.

Let $E : \{0,1\}^l \times \{0,1\}^k \mapsto \{0,1\}^l$ be a function taking a key K of length k bits and an input message (plaintext) M of length l bits and return an output message (ciphertext) $E(M, K)$. For each key K let $E_K : \{0,1\}^l \mapsto \{0,1\}^l$ be a function defined by $E_K(M) = E(M, K)$. Then E is a block cipher if E_K and E_K^{-1} are efficiently computable and E_K is a permutation for every K.

Most of the modern block ciphers are iterative (Fig. 1). Usually a round function is run multiple times with different parameters (round keys). An arbitrary iterative block cipher can be mathematically described as follows

$$E_K(M) = PW_{k_{r+1}} \circ \prod_{i=2}^{r} (R_{k_i}) \circ IW_{k_1}(M),$$

where R is a round procedure, IW is a prewhitening procedure and PW is a postwhitening procedure. In Fig. 1 a key schedule is an algorithm that takes a master key K as input and produces the subkeys $k_1, k_2, \ldots, k_{r+1}$ for all stages of an encryption algorithm.

A mixing key procedure of a block cipher is an algorithm which injects a round key into an encryption procedure. In the majority of modern block ciphers, the mixing key function is implemented as the exclusive or (XOR) operation because of the low implementation cost.

3 A Brief Description of AES

AES is a block cipher based on the substitution permutation network (SPN). It supports a fixed block size of 128 bits and a key size of 128, 192 or 256 bits [6]. The number of rounds depends on the key size and is equal to 10, 12 or 14, respectively. The round function consists of four functions: AddRoundKey (σ_k), SubBytes (γ), ShiftRows (π) and MixColumns (θ).

The entire encryption algorithm is described as follows (Fig. 2)

$$E_K(M) = \sigma_{k_{r+1}} \circ \pi \circ \gamma \circ \prod_{i=2}^{r} (\sigma_{k_i} \circ \theta \circ \pi \circ \gamma) \circ \sigma_{k_1}(M).$$

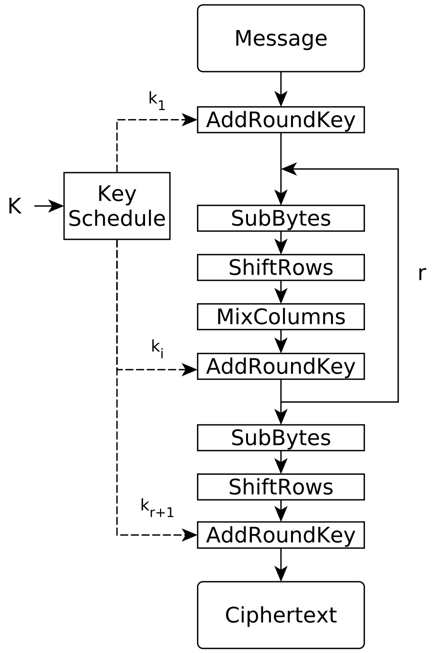


Fig. 2. The Encryption Algorithm of AES

The SubBytes transformation processes the state of the cipher using a nonlinear byte substitution table that operates on each of the state bytes independently [6]. The S-box of AES was generated by finding the inverse element in the field $\mathbb{F}_{2^8}$ followed by applying affine polynomial. In terms of equation (1) the transformation has the form

$$F(x) = A_1(x^{-1}) = L_1(x^{-1}) + c_1.$$

The substitution table generated by the vectorial Boolean function F satisfies the following criteria:

- the maximum value of non-trivial XOR difference transformation probability is 2^{-6},
- the maximum absolute value of linear approximation probability bias is 2^{-4},
- the minimum algebraic degree of the component functions is 7 [5, 16].

It should be noticed that the chosen polynomial x^{-1} allows to describe the S-box and the entire cipher by overdefined system of equations of degree 2 [17]. But in the same time it is resistant to differential, linear and many other cryptanalytical methods. In addition to the general properties, the constant of the AES S-box has been chosen in such a way that it has no fixed points [5].

The MixColumns transformation takes all the columns of the state and mixes their data (independently of one another) to produce new columns [6]. This transformation can be represented in different ways. One of them is the matrix multiplication over $\mathbb{F}_{2^8}$. For an input state x and 4×4 matrix M the output state y of the transformation is described as

$$y = M \cdot x.$$

A matrix with the maximum distance separable (MDS) property is used in AES. In terms of Rijndael the MDS property is associated with a branch number (β)

$$\beta = \min_{x \neq 0}(W(x) + W(y)),$$

where $W(z)$ is the byte weight of a vector z.

From the definition of an MDS matrix it is known that the maximum value of β for m by m matrix is $m + 1$ [11, 18]. Hence, MDS matrices have the perfect diffusion property for byte-oriented ciphers.

Multiplication by a constant in a field $\mathbb{F}_{2^n}$ is a linear transformation with respect to XOR, so it preserves the linear property [9]

$$\theta(x + y) = \theta(x) + \theta(y).$$

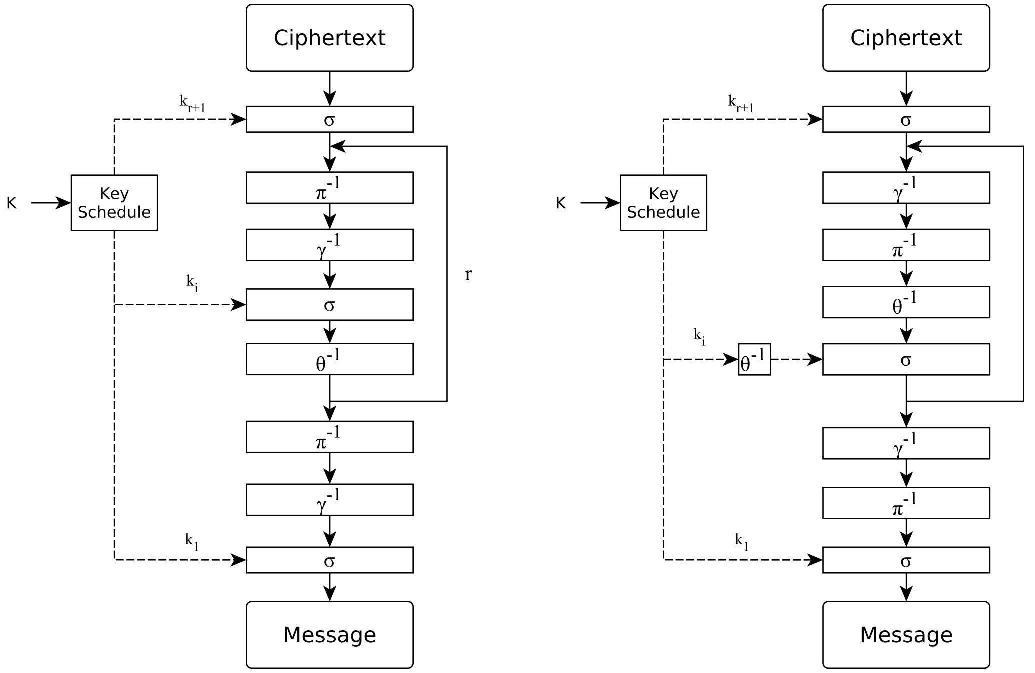
The ShiftRows transformation processes the state by cyclically shifting the last three rows of the state by different offsets [6]. More precisely, row i is moved to the left by i byte positions for $0 \leq i \leq 3$. The ShiftRows is also a linear function that preserves $\pi(x + y) = \pi(x) + \pi(y)$ property.

Both MixColumns and ShiftRows help to ensure that the number of active S-boxes is large even after a few rounds [5]. These functions are the basis of protection offered by the AES against differential and linear cryptanalysis.

The AddRoundKey transformation is the mixing key function in which a round key is added to the state using the XOR operation. The length of a round key is equal to the size of the state. XORing of two n-bit length vectors a and b can be performed bit by bit n times. Therefore, the AddRoundKey operation of AES can be done independently for each byte.

4 A New Cipher Isomorphic to AES

There exist several examples of ciphers isomorphic to AES. For example, the big encryption system (BES) describes AES over $\mathbb{F}_{2^8}$ [9]. On the other hand, the cipher AES



(a) Original

(b) An Algorithm for the Fast Software Implementation

Fig. 3. The Decryption Algorithm of AES

can be also represented as the system of multivariate equations of the 2nd degree over $\mathbb{F}_2$ [17]. These two examples are based on the algebraic features of the substitution. However, there exists another approach, which takes into account the linear properties of the basic functions (MixColumns and ShiftRows).

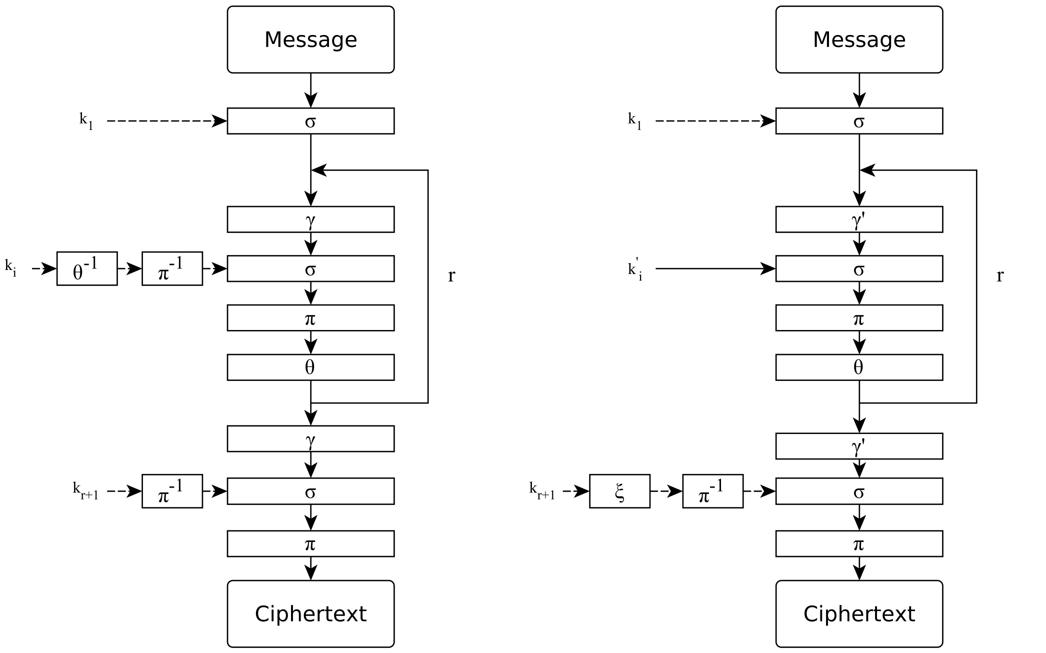
The cipher AES is based on Rijndael that was proposed by Daemen and Rijmen to the AES competition [19]. Authors have used design simplicity principle, which leads to performance improvements and a code compactness of the cipher on a wide range of platforms. To increase decryption performance of software implementation they have used precomputed lookup tables and the linear properties of the basic functions.

The original decryption algorithm for arbitrary ciphertext C mathematically can be represented as follows (Fig. 3(a)) [6]

$$D_K(C) = \sigma_{k_1} \circ \gamma^{-1} \circ \pi^{-1} \circ \prod_{i=2}^{r} (\theta^{-1} \circ \sigma_{k_{r-i+2}} \circ \gamma^{-1} \circ \pi^{-1}) \circ \sigma_{k_{r+1}}(C).$$

To use precomputed tables it is necessary to transform the decryption round function to the similar one of encryption algorithm. Since functions γ^{-1} and π^{-1} can be computed independently they have the commutative property $\gamma^{-1} \circ \pi^{-1} = \pi^{-1} \circ \gamma^{-1}$ [5, 9]. In Section 3 it was stated that functions θ^{-1} and σ are linear with respect to XOR, hence

$$\theta^{-1} \circ \sigma_{k_{r-i+2}} = \sigma_{\theta^{-1}(k_{r-i+2})} \circ \theta^{-1}.$$



(a) A Modified Encryption Algorithm

(b) An Isomorphic Encryption Algorithm with a Fixed Point

Fig. 4. Isomorphic Representations of AES

Thus, the whole decryption algorithm has the form (Fig. 3(b))

$$D_K(C) = \sigma_{k_1} \circ \pi^{-1} \circ \gamma^{-1} \circ \prod_{i=2}^{r} (\sigma_{\theta^{-1}(k_{r-i+2})} \circ \theta^{-1} \circ \pi^{-1} \circ \gamma^{-1}) \circ \sigma_{k_{r+1}}(C).$$

The use of such elementary transformations helps to achieve a significant acceleration of the decryption procedure due to the isomorphic properties of the round function [5].

Obviously, the same technique can be applied to the encryption algorithm. However, the task for an adversary is to find a representation of the cipher that has a new substitution with a fixed point. It is assumed that all round keys are generated by KeySchedule, but it has been excluded from the further figures to simplify the description. Then the encryption procedure takes the form (Fig. 4(a))

$$E_K(M) = \pi \circ \sigma_{\pi^{-1}(k_{r+1})} \circ \gamma \circ \prod_{i=2}^{r} (\theta \circ \pi \circ \sigma_{\pi^{-1} \circ \theta^{-1}(k_i)} \circ \gamma) \circ \sigma_{k_1}(M).$$

The above equation shows that the final ShiftRows operation is redundant and can be ignored in many attacks. As it was stated above the presence of this function is very important for the fast implementation of the decryption procedure.

Arbitrary permutation S can be represented as a vectorial Boolean function $F : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n}$ that has the form [3]

$$F(x) = F'(x) + F(0).$$

Since the characteristic of the field is 2, the constant can be moved to the round keys. Let ξ be a function that XORs the constant $F(0)$ with all bytes of a state. If the round keys $\pi^{-1} \circ \theta^{-1} \circ \xi(k_i)$ are denoted by k'_i then encryption procedure takes the form (Fig. 4(b))

$$E_K(M) = \pi \circ \sigma_{\pi^{-1} \circ \xi(k_{r+1})} \circ \gamma' \circ \prod_{i=2}^{r} (\theta \circ \pi \circ \sigma_{k'_i} \circ \gamma') \circ \sigma_{k_1}(M),$$

where γ' is the SubBytes transformation with the substitution of the form $F(x) = L(x^{-1})$.

Fig. 4(b) shows that the structure of the cipher remains unchanged. It is obvious that if an adversary finds a round key for modified cipher she also automatically obtains corresponding round key of the original cipher because of an bijective mapping of the keys k_i and k'_i. Moreover, the new substitution $F(x) = L(x^{-1})$ has the fixed point at $x = 0$. Consequently, the isomorphic substitution of AES doesn't satisfy the absence of fixed points criterion.

Described features of the cipher appears from the fact that the operation XOR is linear with respect to MixColumns and ShiftRows. If one replaces AddRoundKey with a nonlinear function (i.e., addition modulo 2^n) then it will be impossible to find an isomorphic cipher of such a form. This is because the ShiftRows and MixColumns transformations are become nonlinear with respect to addition modulo 2^n. From the isomorphic point of view a mixed key function based on a modulo addition is cryptographically stronger than a function based on the XOR operation .

Furthermore, fixed points are directly connected with cyclic properties of substitutions. Inserting an invertible linear function (τ) into the encryption procedure gives a new isomorphic cipher (Fig. 5(a)). Herewith, τ becomes a part of a round key and a new substitution, and τ^{-1} is united with π (Fig. 5(b)). The cyclic properties of the new substitution will depend on the selected function τ.

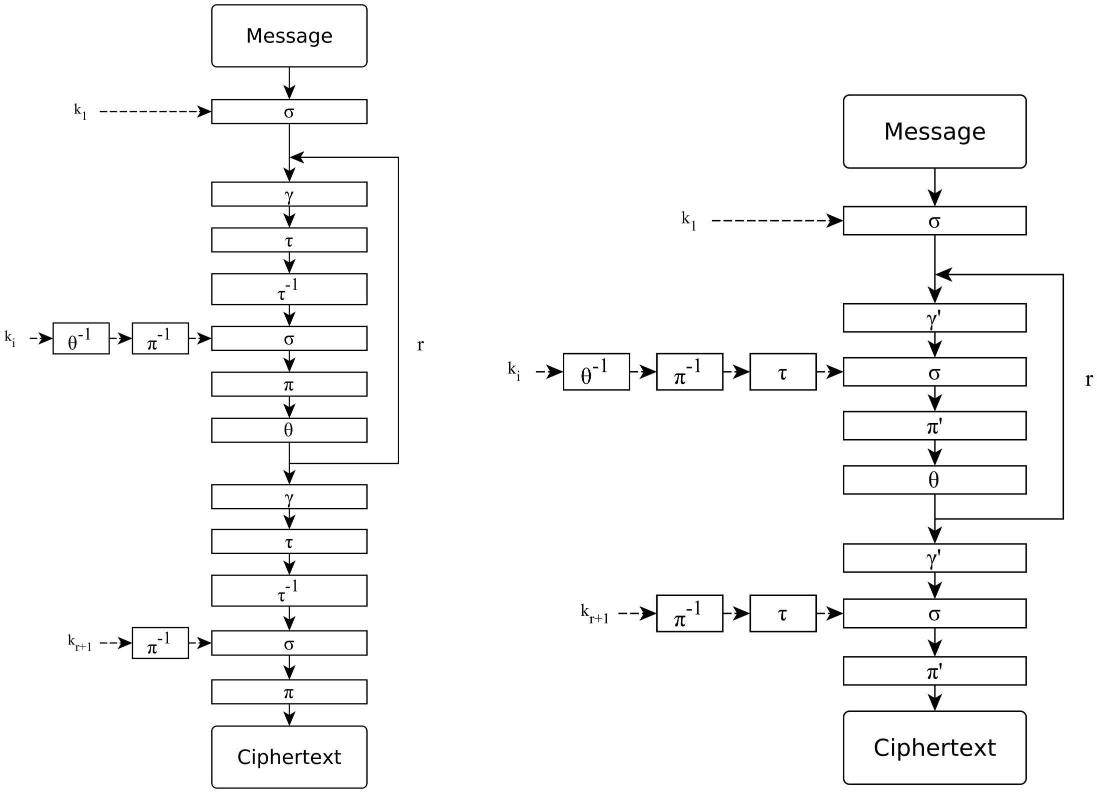
Thereby, the cyclic and the absence of fixed points properties of a substitution can be controlled by an adversary in the case of a linear mixing key function. A new criterion for substitutions follows from the isomorphic properties.

Proposition 1. *Substitutions S_1, S_2, …, S_n used in a nonlinear layer must belong to different classes of equivalence.*

Clearly, if substitutions are in the same class (i.e., EA-equivalent) then an adversary can find an isomorphic cipher which consists of one substitution and a modified linear layer. Consequently, there will be no advantages to use multiple substitutions. The criterion has to be considered both at the design stage of new ciphers and in the analysis of existing ones [20, 21]. Since CCZ-equivalence is the most general case of known equivalences, it makes sense to check whether substitutions belong to different CCZ-equivalent classes.

5 Conclusions

It was shown that the absence of fixed points criterion works only for the case when an S-box is considered as a separate function. However, it is possible to find representations of ciphers which do not meet this criterion. The new method of the AES description allows to reconsider some of the criteria for substitutions from the practical point of view. This may be exploited by in future attacks.



(a) The Initial Cipher

(b) An Isomorphic Cipher

Fig. 5. A Modified AES with an Invertible Linear Function

Since an invertible linear function can be added to an encryption procedure, an adversary can control both the cyclic and absence of fixed points properties of substitutions. It follows from the isomorphic representations that the mixing key function based on a modulo addition has more advantages comparing with the XOR operation.

Isomorphism of ciphers leads to reconsideration of application of multiple substitutions. On the one hand the proposed criterion excludes the possibility to find an isomorphic representation where only one substitution will be used. On the other hand in cryptoprimitives with multiple substitutions the opposite criterion can be applied to increase the performance.

References

1. Carlet, C.: *Vectorial Boolean functions for cryptography.* Boolean Models and Methods in Mathematics, Computer Science, and Engineering. Cambridge University Press, 2010.
2. Daemen, J., Rijmen, V.: *The design of Rijndael: AES - The Advanced Encryption Standard.* Information Security and Cryptography. Springer, 2002.
3. Budaghyan, L., Kazymyrov, O.: Verification of restricted EA-equivalence for vectorial Boolean functions. In Özbudak, F., Rodríguez-Henríquez, F. (eds.), *Arithmetic of Finite Fields*, vol. 7369 of *Lecture Notes in Computer Science*, pp. 108–118. Springer Berlin Heidelberg, 2012.
4. Carlet, C., Charpin, P., Zinoviev, V.: Codes, bent functions and permutations suitable for DES-like cryptosystems. In *Designs, Codes and Cryptography*, vol. 15, pp. 125–156. Kluwer Academic Publishers, 1998.
5. Daemen, J., Rijmen, V.: AES proposal: Rijndael. *Electronic source,* 1998. http://csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf.

6. FIPS PUB 197: Advanced Encryption Standard (AES). *National Institute of Standards and Technology,* 2001.
7. Rostovtsev, A.: Changing probabilities of differentials and linear sums via isomorphisms of ciphers. *Cryptology ePrint Archive, Report 2009/117*, 2009. `http://eprint.iacr.org/`.
8. Rimoldi, A.: *On algebraic and statistical properties of AES-like ciphers.* Ph.D. thesis, University of Trento, Italy, 2010. `http://eprints-phd.biblio.unitn.it/151/1/Provatemplate.pdf`.
9. Murphy, S., Robshaw, M.: Essential algebraic structure within the AES. In Yung, M. (ed.), *Advances in Cryptology — CRYPTO 2002*, vol. 2442 of *Lecture Notes in Computer Science*, pp. 1–16. Springer Berlin Heidelberg, 2002.
10. Bard, G. V.: *Algebraic cryptanalysis.* Springer, 2009.
11. Knudsen, L. R., Robshaw, M.: *The block cipher companion.* Information Security and Cryptography. Springer Berlin Heidelberg, 2011.
12. Budaghyan, L., Carlet, C., Pott, A.: New classes of almost bent and almost perfect nonlinear polynomials. In *Information Theory, IEEE Transactions*, vol. 52, pp. 1141–1152. Institute of Electrical and Electronics Engineers, 2006.
13. Biham, E., Shamir, A.: Differential cryptanalysis of DES-like cryptosystems. In Menezes, A., Vanstone, S. (eds.), *Advances in Cryptology-CRYPT0'90*, vol. 537 of *Lecture Notes in Computer Science*, pp. 2–21. Springer Berlin Heidelberg, 1991.
14. Matsui, M.: Linear cryptanalysis method for DES cipher. In Helleseth, T. (ed.), *Advances in Cryptology — EUROCRYPT '93*, vol. 765 of *Lecture Notes in Computer Science*, pp. 386–397. Springer Berlin Heidelberg, 1994.
15. Kazymyrov, O., Kazymyrova, V.: Algebraic aspects of the Russian hash standard GOST R 34.11-2012. *In Pre-proceedings of 2nd Workshop on Current Trends in Cryptology (CTCrypt 2013),* pp. 160–176, 2013.
16. Nyberg, K.: Perfect nonlinear S-boxes. In Davies, D. (ed.), *Advances in Cryptology - EUROCRYPT'91*, vol. 547 of *Lecture Notes in Computer Science*, pp. 378–386. Springer Berlin Heidelberg, 1991.
17. Courtois, N., Pieprzyk, J.: Cryptanalysis of block ciphers with overdefined systems of equations. *Cryptology ePrint Archive, Report 2002/044*, 2002. `http://eprint.iacr.org/`.
18. Ailan, W., Yunqiang, L., Xiaoyong, Z.: Analysis of corresponding structure of differential branch of MDS matrixes on finite field. In *Intelligent Networks and Intelligent Systems (ICINIS), 2010 3rd International Conference*, pp. 381–384. Institute of Electrical and Electronics Engineers, 2010.
19. Nechvatal, J., et al.: Report on the development of the Advanced Encryption Standard (AES). *Electronic source,* 2000. `http://csrc.nist.gov/archive/aes/round2/r2report.pdf`.
20. Kwon, D., Kim, J., Park, S., Sung, S., et al.: New block cipher: ARIA. In Lim, J.-I., Lee, D.-H. (eds.), *Information Security and Cryptology - ICISC 2003*, vol. 2971 of *Lecture Notes in Computer Science*, pp. 432–445. Springer Berlin Heidelberg, 2004.
21. Oliynykov, R., Gorbenko, I., Dolgov, V., Ruzhentsev, V.: Results of Ukrainian national public cryptographic competition. In *Tatra Mountains Mathematical Publications*, vol. 47, pp. 99–113. Mathematical Institute of Slovak Academy of Sciences, 2010.