СИНТЕЗ И АНАЛИЗ СИМЕТРИЧНЫХ ПРЕОБРАЗОВАНИЙ

UDC 621.3.06

EXTENDED CRITERION FOR ABSENCE OF FIXED POINTS

O. KAZYMYROV

One of the criteria for selecting substitutions used in block ciphers is the absence of fixed points. This paper shows that this criterion must be extended taking into consideration mixing key function. It is shown that modulo addition has more advantages than XOR operation. It is shown in practice that encryption procedure of AES has a natural isomorphic form when fixed points are reached.

Keywords: fixed points, AES, criterion, s-box.

1. INTRODUCTION

Substitution boxes (*S*-boxes) map an n^{th} bit length input message to an m^{th} bit length 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 constitute a subclass of substitutions and are commonly used in block ciphers as a lookup table. Regardless of ciphers an *S*-box can be converted from one form to another one.

Substitutions must satisfy various criteria for providing high level of security against different types of attacks [2]. A substitution satisfying all criteria is perfect. However, such substitutions don't exist up to date. 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 a large n an m. The problem is 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 ciphers try to get rid of the fixed points. This is achieved by using affine equivalence, which is a particular case of *EA*-equivalence. The *S*-box of advanced encryption standard (AES) was constructed using this technique [5, 6]. But the application of this method does not totally prevent the appearance of fixed points. In this paper we show an isomorphic 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 $\varphi: x^i \mapsto x^j$, $\psi: y^i \mapsto y^j$ 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 could 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]. In [10] an example of isomorphic AES in which the differential probability is higher than in the original cipher was shown. We show another example, which is a special case of isomorphic AES. The new cipher 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 $\mathcal{F}_{2^n} = GF(2^n)$ and lookup table. Most of substitutions used in block ciphers have a table representation because of simplicity of description and understanding. Meanwhile arbitrary *S*-box S can be always associated with a vectorial Boolean function F in $\mathcal{F}_{2^n}[x]$. If a substitution is a permutation then F is defined uniquely.

The natural way of representing F as a function from $\mathcal{F}_2^n$ to $\mathcal{F}_2^m$ is by its algebraic normal form:

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

(the sum is being calculated in $\mathcal{F}_2^m$) [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 in table representation can be easily transformed to AFN form and vice versa.

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

$$F(x) = A_1 \circ G \circ A_2(x) + L_3(x). \qquad (1)$$

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 $c_1 \in \mathcal{F}_2^m$, $c_2 \in \mathcal{F}_2^n$. Two functions F and G are linear equivalent if equation (1) is correct when $L_3 = 0$, $c_1 = 0$, $c_2 = 0$. If the equation (1) is preserved only for $L_3 = 0$, then functions F and G are called affine equivalent [11].

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

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

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

For any positive integers *n* and *m*, a function *F* from $\mathcal{F}_2^n$ to $\mathcal{F}_2^m$ is called differentially δ-uniform if for every $a \in \mathcal{F}_2^n \setminus \{0\}$ and every $b \in \mathcal{F}_2^m$, 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 low differential uniformity to allow high resistance to differential cryptanalysis [12].

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

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

where " $\cdot$ " denotes inner products in $\mathcal{F}_2^n$ and $\mathcal{F}_2^m$ respectively [1]. A substitution has an optimum resistance to linear cryptanalysis if the maximum absolute value of Walsh coefficients is small [13]. Substitutions with the limit values 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, 14]. It has been still not proven the importance of the criteria. For example, the substitution used in AES doesn't satisfy most of them. No practical attacks were proposed on block cipher based on the most of 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 input message (plaintext) *M* of length *l* bits to return output message (ciphertext) $E(M,K)$. For each key *K* let $E_K : \{0,1\}^l \times \{0,1\}^l$ be the function defined by $E_K(M) = E(M,K)$. Than *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 based on an iterative procedure. In Figure 1 the iterative function is depicted as the round function.

A general iterative cipher can be mathematically presented as follows

$$E_K(M) = PW_{k_r+1} \circ \bigcirc_{i=2}^{r} \left(R_{k_i}\right) \circ IW_{k_1}(M),$$

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

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

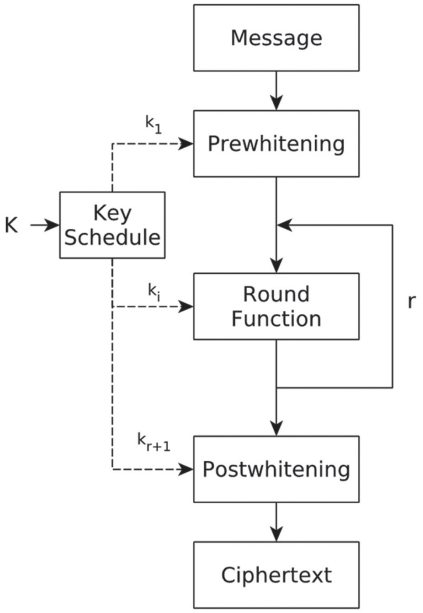

Fig. 1. General structure of an iterative block cipher

3. A BRIEF DESCRIPTION OF AES

AES is a substitution permutation network (SPN) block cipher that 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 whole encryption algorithm is described as follows (Figure 2)

$$E_K(M) = \sigma_{k_r+1} \circ \pi \circ \gamma \circ \bigcirc_{i=2}^{r} \left(\sigma_{k_i} \circ \theta \circ \pi \circ \gamma\right) \circ \sigma_{k_1}(M).$$

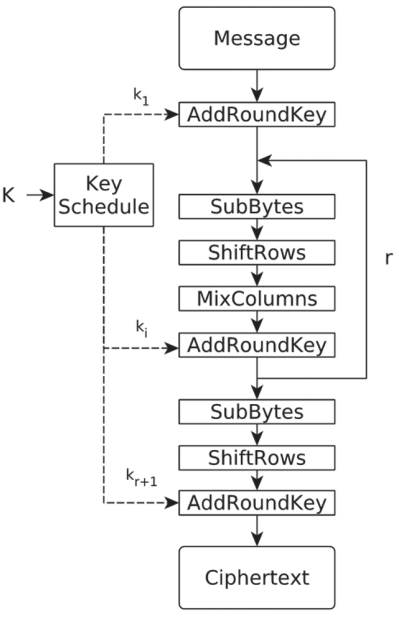

Fig. 2. Encryption algorithm of AES

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 $\mathcal{F}_{2^8}$ followed by applying affine polynomial. In terms of equation (1) the transformation has a form

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

The substitution table generated by vectorial Boolean function $F : \mathcal{F}_{2^8} \mapsto \mathcal{F}_{2^8}$ 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 degree of the component functions is 7 [5, 15].

It should be noticed that the chosen polynomial x^{-1} allows to describe the *S*-box and the whole cipher by overdefined system of equations with degree 2 [16]. But in the same time it is resistant to differential, linear and other statistical methods of cryptanalysis. Additional to general properties the constant of the AES *S*-box has been chosen in such way that it has no fixed points.

The MixColumns transformation takes all of the columns of the state and mixes their data (independently of one another) to produce new columns [6]. This transformation could be represented in different ways. One of them is the matrix multiplication. For 4×4 matrix *m* and input state *x* the output state *y* of the transformation is described as

$$y = M \cdot x.$$

The matrix *M* with maximum distance separable (MDS) property is used in AES. The MDS property associates with a branch number (β)

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

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

From the definition of MDS matrix, it is known that the maximum differential branch number of *m* by *m* MDS matrix is $m+1$ [17]. Hence, MDS matrices have the perfect diffusion property for byte-oriented ciphers.

Multiplication in a filed $\mathcal{F}_{2^n}$ is a linear transformation with respect to XOR, so MixColumns transformation 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 $0 \le i \le 3$. The ShiftRows is also a linear function that preserves $\pi(x + y) = \pi(x) + \pi(y)$ property.

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

AddRoundKey transformation is the mixing key function in which a round key is added to the state using XOR operation. The length of a round key equals the size of the state. XOR operation of two *n*-bit length vectors *a* and *b* can be performed bit by bit *n* times. Therefore, AddRoundKey operation of AES can be done independently of 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 $\mathcal{F}_{2^8}$ [9]. The cipher AES can be also represented as the system of multivariate equations of the 2nd degree over $\mathcal{F}_2$ [16]. These two examples are based on the algebraic features of the substitution. But there is another approach based on linear properties of the basic functions (i.e. MixColumns and ShiftRows).

The cipher AES is based on Rijndael that was proposed by Daemen and Rijmen to AES process [18]. Authors have used design simplicity principle, which led to performance improvement and code compactness properties of the cipher on a wide range of platforms. For increasing decryption performance of software implementation they use precomputed lookup tables and the linear properties of basic functions.

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

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

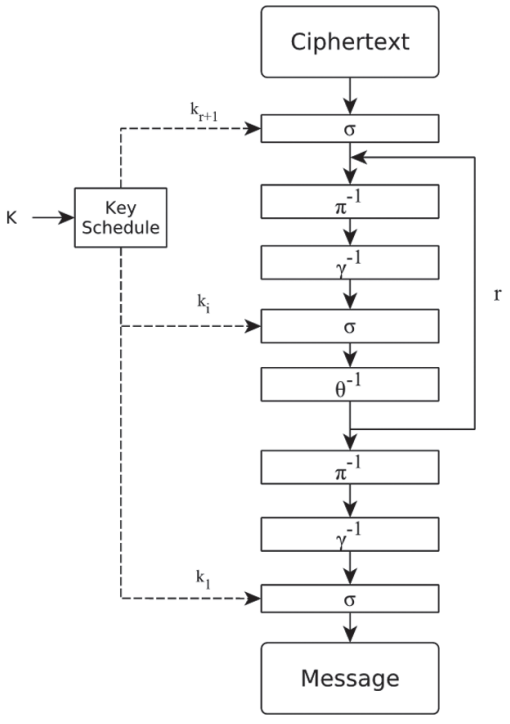

Fig. 3. Decryption algorithm of AES

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

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

Thus, the whole decryption algorithm has the form (Figure 4)

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

The usage of such elementary transformations helps to achieve a significant acceleration of the decryption procedure due to the isomorphic properties of the basic functions [5].

Obviously, the same technique can be applied to the encryption algorithm. However, our task is to find a representation of the cipher in which properties of a new substitution will differ from the original one.

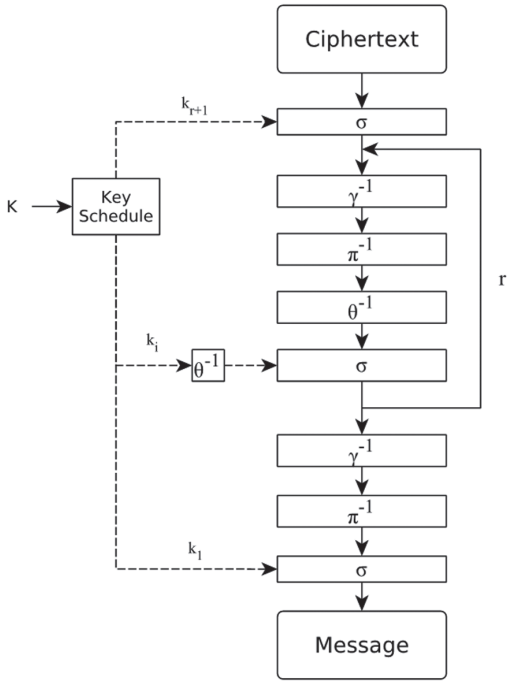

Fig. 4. Algorithm for fast software implementation

For simplicity of description, let us assume that the round keys are independent of each other. Then the encryption procedure takes a form (Figure 5)

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

The equation shows that the last ShiftRows operation is redundant in terms of resistance to attacks. As it was stated above the availability of this function is necessary for fast implementation of the decryption procedure.

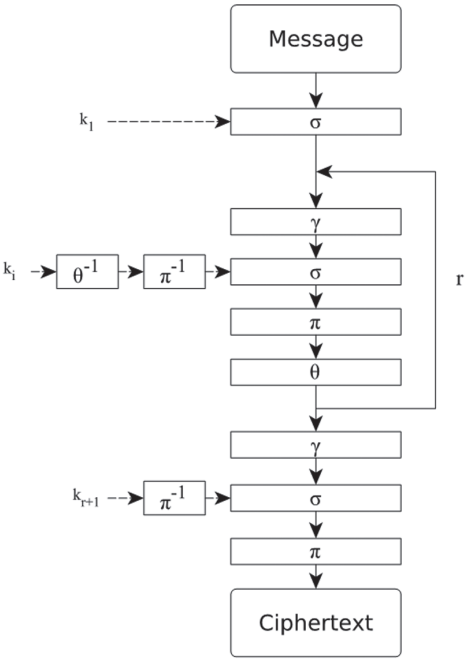

Fig. 5. Modified encryption algorithm

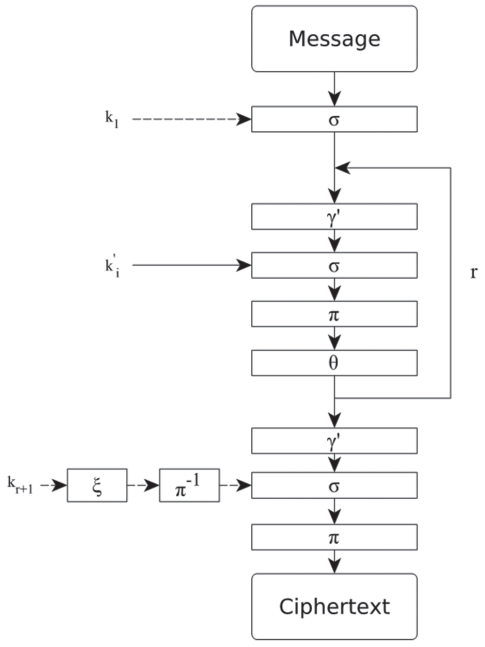

Fig. 6. Isomorphic encryption algorithm with a fixed point

Since arbitrary permutation S can be represented as vectorial Boolean function $F : \mathcal{F}_{2^n} \mapsto \mathcal{F}_{2^n}$ then it can take the form [3]

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

The substitution of AES has more simple form than $F(x) = L(x^{-1}) + c$, where $c = F(0)$. Since the characteristic of the field is 2, the constant can be moved to the round keys. Let ξ be a function in which the constant c is XORed with all bytes of a state. If the round keys $\pi^{-1} \circ \theta^{-1} \circ \xi(k_i)$ are denoted by k_i' than encryption procedure takes the form (Figure 6)

$$E_K(M) = \pi \circ \sigma_{\pi^{-1} \circ \xi(k_r+1)} \circ \gamma' \circ \bigcirc_{i=2}^{r} \left(\theta \circ \pi \circ \sigma_{k_i'} \circ \gamma' \right) \circ \circ \sigma_{k_1}(M),$$

where γ' is the SubBytes function consists of substitutions of the form $F(x) = L(x^{-1})$.

Figure 6 shows that the structure of the cipher remains unchanged. Clearly, if adversary finds a round key for modified cipher she also automatically obtains corresponding round key of the original cipher because of the linear correspondence between the keys k_i and k_i'. However, the new substitution $F(x) = L(x^{-1})$ has the fixed point in $x = 0$. Consequently, the substitution of AES doesn't satisfy the absence of fixed points criterion.

Described feature of the cipher appears from the fact that the operation XOR is linear with respect to MixColumns and ShiftRows. If we replace the mixing key function with some nonlinear function (i.e. addition modulo 2^{32}), then it would be impossible to find an isomorphic cipher of such form. Therefore, a mixed key function based on modulo addition is cryptographically stronger than a function based on 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 (Figure 7). Herewith, the linearized polynomial can be added to the round key and the inverse function can be part of the new substitution (Figure 8). The cyclic properties of the new substitution will depend on the selected function τ.

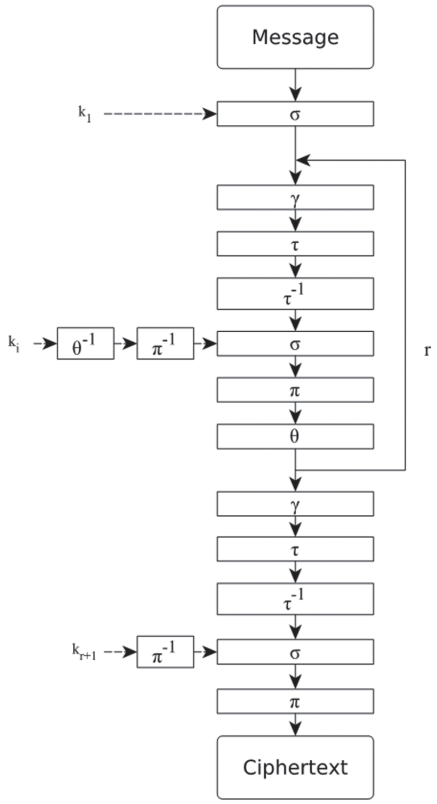

Fig. 7. Modified AES with an invertible linear function

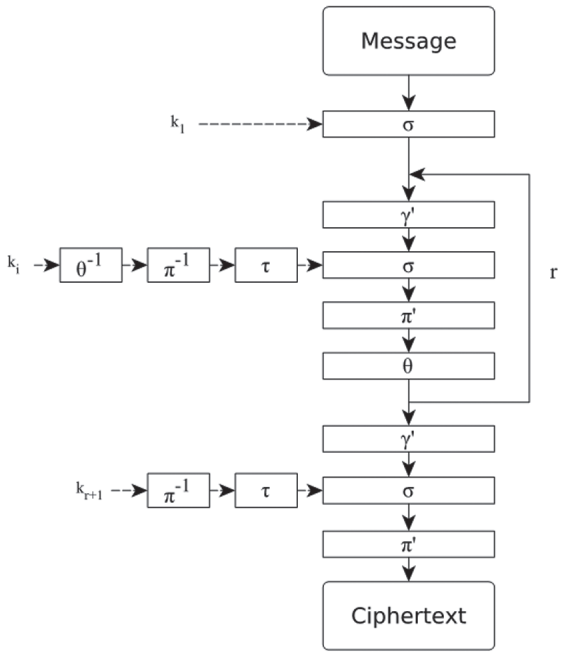

Fig. 8. Isomorphic cipher of modified AES with an invertible linear function

Thereby, adversary in the case of a linear mixing key function can control the cyclic and the absence of fixed points properties of a substitution. Thus, a new criterion for substitutions follows from the description above.

Definition 2. *Substitutions* $S_1, S_2, \ldots, S_n$ *used in diffusion layer must belong to different classes of equivalence.*

Clearly, if substitutions are in the same class (i.e. EA-equivalent) then adversary can find an isomorphic cipher, which consists of one substitution and modified linear layer. So there will be no advantages to use multiple substitutions. The criterion have to be considered both in the design of new ciphers and in the analysis of existing ones [19, 20]. Since CCZ-equivalence is the most general case of known equivalence, it makes sense to check whether substitutions belong to different CCZ-equivalence classes.

5. CONCLUSIONS

It was shown that the absence of fixed points criterion works only in the case if *S*-box is considered as a separate function. There are isomorphic representations of ciphers in which this criterion is not met. This may lead to a weakening of the cipher strength. The method of AES description gives a tool for attacking the cipher, which has been practically secure more than decade.

Since the adversary can add arbitrary invertible linear function to encryption procedure, the cyclic properties also are not important for substitutions. It was shown that mixing key function based on modulo addition is more resistant with respect to the absence of fixed points criterion than function based on XOR operation.

Isomorphism of ciphers adds further restrictions on using multiple substitutions. The proposed

criterion can be used to reduce the number of isomorphic ciphers, thereby reducing the probability of finding the weakest algorithm.

References

[1] Y. Crama and P.L. Hammer. Boolean Models and Methods in Mathematics, Computer Science, and Engineering. Encyclopedia of Mathematics and its Applications v. 2. Cambridge University Press,= 2010. isbn: 9780521847520.

[2] Vincent Rijmen. “Cryptanalysis and design of iterated block ciphers”. Doc- toral thesis. K.U.Leuven, 1997.

[3] Lilya Budaghyan and Oleksandr Kazymyrov. “Verification of Restricted EA-Equivalence for Vectorial Boolean Functions”. In: Arithmetic of Finite Fields. Ed. by Ferruh Ozbudak and Francisco Rodrguez-Henrquez. Vol. 7369. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2012, pp. 108–118. isbn: 978-3-642-31661-6. doi: 10.1007/978-3-642-31662- 3_8.

[4] Claude Carlet, Pascale Charpin, and Victor Zinoviev. “Codes, Bent Func- tions and Permutations Suitable For DES-like Cryptosystems”. In: Des. Codes Cryptography 15.2 (1998), pp. 125–156.

[5. J. Daemen and V. Rijmen. “AES proposal: Rijndael”. In: First Advanced Encryption Standard (AES) Conference. 1998.

[6] National Institute of Standards and Technology. ADVANCED ENCRYP- TION STANDARD (AES). FIPS-197. U.S. DoC/National Institute of Standards and Technology, 2001, pp. 1–47.

[7] Alexander Rostovtsev. Changing probabilities of differentials and linear sums via isomorphisms of ciphers. Cryptology ePrint Archive, Report 2009/117. 2009.

[8] A. Rimoldi. “On algebraic and statistical properties of AES-like ciphers”. PhD thesis. University of Trento, 2009.

[9] Sean Murphy and Matthew J. B. Robshaw. “Essential Algebraic Structure within the AES”. In: Proceedings of the 22nd Annual International Cryp- tology Conference on Advances in Cryptology. CRYPTO ’02. London, UK, UK: Springer-Verlag, 2002, pp. 1–16. isbn: 3-540-44050-X.

[10] Alexander Rostovtsev. Virtual isomorphisms of ciphers: is AES secure against differential/linear attack? Cryptology ePrint Archive, Report 2012/663. 2012.

[11] L. Budaghyan, C. Carlet, and A. Pott. “New classes of almost bent and al- most perfect nonlinear polynomials”. In: Information Theory, IEEE Trans- actions on 52.3 (2006), pp. 1141–1152.

[12] Eli Biham and Adi Shamir. “Differential Cryptanalysis of DES-like Cryp- tosystems”. In: Proceedings of the 10th Annual International Cryptology Conference on Advances in Cryptology. CRYPTO ’90. London, UK, UK: Springer-Verlag, 1991, pp. 2–21. isbn: 3-540-54508-5.

[13] Mitsuru Matsui. “Linear cryptanalysis method for DES cipher”. In: Work- shop on the theory and application of cryptographic techniques on Advances in cryptology. EUROCRYPT ’93. Lofthus, Norway: Springer-Verlag New York, Inc., 1994, pp. 386–397. isbn: 3-540-57600-2.

[14] Linda Dee Burnett. “Heuristic Optimization of Boolean Functions and Substitution Boxes for Cryptography”. PhD thesis. Queensland University of Technology, 2005.

[15] K. Nyberg. “Perfect nonlinear S-boxes”. In: Advances in CryptologyEU- ROCRYPT91. Springer. 1991, pp. 378–386.

[16] Nicolas Courtois and Josef Pieprzyk. “Cryptanalysis of Block Ciphers with Overdefined Systems of Equations”. In: Proceedings of the 8th Interna- tional Conference on the Theory and Application of Cryptology and Infor- mation Security: Advances in Cryptology. ASIACRYPT ’02. London, UK, UK: Springer-Verlag, 2002, pp. 267–287. isbn: 3-540-00171-9.

[17] Wang Ailan, Li Yunqiang, and Zhang Xiaoyong. “Analysis of Correspond- ing Structure of Differential Branch of MDS Matrixes on Finite Field”. In: Proceedings of the 2010 Third International Conference on Intelligent Net- works and Intelligent Systems. ICINIS ’10. Washington, DC, USA: IEEE Computer Society, 2010, pp. 381–384. isbn: 978-0-7695-4249-2.

[18] J. Nechvatal et al. Report on the development of the Advanced Encryption Standard (AES). Tech. rep. DTIC Document, 2000.

[19] Daesung Kwon et al. “New Block Cipher: ARIA”. In: Information Security and Cryptology - ICISC 2003. Ed. by Jong-In Lim and Dong-Hoon Lee. Vol. 2971. Lecture Notes in Computer Science. Springer Berlin / Heidel- berg, 2004, pp. 432–445. isbn: 978-3-540-21376-5.

[20] Roman Oliynykov et al. Results of Ukrainian National Public Crypto- graphic Competition. http://www.sav.sk/journals/uploads/0317154006ogdr. pdf. 2012.

Manuscript received March, 5, 2013

Kazymyrov Oleksandr Vladimirovich, post-graduate student of information technologies security department at KNURE. Scientific interests: symmetric cryptography and cryptanalysis, vectorial Boolean functions.

УДК 621.3.06

Расширенный критерий для отсутствия фиксированных точек / О.В. Казимиров // Прикладная радиоэлектроника: науч.-техн. журнал. – 2013. – Том 12. – № 2. – С. 209–214.

Одним из критериев для выбора подстановок, используемых в блочных шифрах+, является отсутствие неподвижных точек. В статье показано, что этот критерий необходимо расширить, принимая во внимание функцию смешивания ключа. Показано, что использование модульного сложения более предпочтительно, чем XOR. На практике продемонстрировано, что шифрующее преобразование AES имеет изоморфную форму, в которой присутствуют неподвижные точки.

Ключевые слова: фиксированные точки, AES, критерий, s-бокс.

Ил.: 8. Библиогр.: 20 назв.

УДК 621.3.06

Розширений критерій для відсутності фіксованих точок / О. Казиміров // Прикладна радіоелектроніка: наук.-техн. журнал. – 2013. – Том 12. – № 2. – С. 209–214.

Одним із критеріїв для вибору підстановок, що використовуються у блокових шифрах, є відсутність нерухомих точок. У статті показано, що цей критерій треба розширити, приймаючи до уваги схему розгортання ключа. Показано, що використання модульного додавання краще, ніж XOR. На практиці продемонстровано, що шифруюче перетворення AES має ізоморфну форму, в якій присутні нерухомі точки.

Ключові слова: фіксовані точки, AES, критерій, s-бокс.

Іл.: 8. Бібліогр.: 20 найм.