Annales UMCS Informatica AI XI, 2 (2011) 37–48
DOI: 10.2478/v10065-011-0009-4

Annales UMCS
Informatica
Lublin-Polonia
Sectio AI
http://www.annales.umcs.lublin.pl/

Cryptographic properties of modified AES-like S-boxes

Anna Grocholewska-Czuryło*

Institute of Control and Information Engineering, Poznań University of Technology
pl. Marii Skłodowskiej Curie 5, 60-965 Poznań, Poland

Abstract

Using AES-like S-boxes (generated using finite field inversion) provides an excellent starting point for generating S-boxes with some specific design criteria dictated by the implemented cipher and still maintaining all the most commonly recognized cryptographic criteria to a large extent. This paper presents the results of statistical analysis of fulfilment of those basic cryptographic criteria by the modified AES-like S-boxes that do have neither equivalence nor cycles.

1. Introduction

S-box design is usually the most important task while designing a new cipher. This is because an S-box is the only nonlinear element of the cipher upon which the whole cryptographic strength of the cipher depends. New methods of attacks are constantly being developed by researchers, so S-box design should always be one step ahead of those pursuits to ensure cipher's security.

Recently a set of papers have been published by researchers from the Institute of Control and Information Engineering at Poznań University of Technology, where the three cryptographic ciphers have been proposed - PP-1 [**1, 2, 3, 4**],

*E-mail address: anna.grocholewska-czurylo@put.poznan.pl

PP-2 [to be published] and HAF [to be published]. In the process of designing those ciphers a considerable amount of research went into design of the core nonlinear component of the cipher - the S-box. Different requirements of each of those three ciphers have led to extensive research of S-boxes possessing various properties. This paper presents the results of that research in a combined, comprehensive way.

First, in the **Basics** chapter, some fundamental definitions are given as a refresher, to help better understand the research results given later in the article. In the chapter **Cryptographic Criteria**, the most common cryptographic criteria are briefly described that are usually used when designing and testing S-boxes. Then, in the Research Scope chapter, the types of S-boxes that were extensively studied and tested are described. The next chapter, **Research Results** gives detailed test results for each type of tested S-boxes, in the form of graphs, compared to a set of random S-boxes. Finally, in **Conclusions**, a summary of research findings is given.

2. Basics

2.1. Linear and nonlinear Boolean functions

An n–argument Boolean function f is linear if it can be represented in the following form: $f(x_1, x_2, \ldots, x_n) = a_1x_1 \oplus a_2x_2 \oplus \ldots \oplus a_nx_n$. Let L_n be a set of all n–argument linear Boolean functions. Let $M_n = \{g : \Sigma_n \to \Sigma | g(x_1, x_2, \ldots, x_n) = 1 \oplus f(x_1, x_2, \ldots, x_n)$ and $f \in L_n\}$. A set $A_n = L_n \cup M_n$ is called a set of n–argument affine Boolean functions. A Boolean function $f : \Sigma^n \to \Sigma$ that is not affine is called a nonlinear Boolean function.

2.2. Algebraic normal form

A Boolean function can be represented as a maximum of 2^n coefficients of the Algebraic Normal Form. These coefficients provide a formula for the evaluation of the function for any given input $x = [x_1, x_2, \ldots, x_n]$:

$$f(x) = a_0 \oplus \sum_{i=1}^{n} a_i x_i \oplus \sum_{1 \le i < j \le n} a_{ij} x_i x_j \oplus \ldots \oplus a_{12\ldots n} x_1 x_2 \ldots x_n$$

where $\sum$, $\oplus$ denote the modulo 2 summation.

The order of nonlinearity of a Boolean function $f(x)$ is a maximum number of variables in a product term with the non-zero coefficient a_J, where J is a subset of $\{1, 2, 3, \ldots, n\}$. In the case where J is an empty set the coefficient is denoted as a_0 and is called a zero order coefficient. The coefficients of order 1 are $a_1, a_2, \ldots, a_n$, the coefficients of order 2 are $a_{12}, a_{13}, \ldots, a_{(n-1)n}$, the coefficient of order n is $a_{12\ldots n}$. The number of all ANF coefficients equals 2^n.

2.3. Hamming Distance

Hamming weight of a binary vector $x \in \Sigma^n$, denoted as $hwt(x)$, is the number of ones in that vector. The Hamming distance between the two Boolean functions $f, g : \Sigma^n \to \Sigma$ is denoted by $d(f, g)$ and is defined as follows:

$$d(f, g) = \sum_{x \in \Sigma^n} f(x) \oplus g(x).$$

The distance of a Boolean function f from a set of n–argument Boolean functions X_n is defined as follows:

$$\sigma(f) = \min_{g \in X_n} d(f, g)$$

where $d(f, g)$ is the Hamming distance between the functions f and g. The distance of a function f from a set of affine functions A_n is the distance of the function f from the nearest function $g \in A_n$. The distance of the function f from a set of all affine functions is called the nonlinearity of function f and is denoted by N_f.

2.4. SAC - Strict Avalanche Criterion

A Boolean function f satisfies SAC if complementing any single input bit changes the output bit with the probability p of 0.5. So, more formally, a Boolean function $f(x_1, \ldots, x_n)$ satisfies SAC (the strict avalanche criterion) if $f(x) \oplus f(x \oplus \alpha)$ is balanced for any $\alpha \in \Sigma^n$ such that $hwt(\alpha) = 1$.

2.5. Affine Transform and Equivalence Classes

An affine transform of a Boolean function is a transformation defined in terms of a linear transform and a dyadic shift. A linear transform involves the multiplication of the input vector of a Boolean function by a non-singular binary matrix. A dyadic shift (translation) involves the complement of a subset of input bits. An affine transformation is defined as combination of a linear transform and dyadic shift. The addition of an affine function to the output of the Boolean function is also an affine transformation. An equivalence class is a group of Boolean functions related by affine transforms.

2.6. S–box

A substitution operation or an $n \times n$ S–box (or S–box of the size $n \times n$) is a mapping $S : F_2^n \to F_2^n$, where n is a fixed positive integer, $n \geq 2$. An n–argument Boolean function is a mapping $f : F_2^n \to F_2$. An S–box $S : F_2^n \to F_2^n$ can be decomposed into the sequence, $S = (f_1, f_2, \ldots, f_n)$ of Boolean functions such that $S(x_1, x_2, \ldots, x_n) = (f_1(x_1, x_2, \ldots, x_n), f_2(x_1, x_2, \ldots, x_n), \ldots, f_n(x_1, x_2, \ldots, x_n))$. We say that the functions $f_1, f_2, \ldots, f_n$ are component functions of S.

3. Cryptographic criteria

Each attack that is better than exhaustive search explores some weakness in S-boxes. After a new attack is published, a new design criteria for S-boxes can be introduced which makes the cryptographic algorithm immune against that particular attack. Researchers can also examine how S-box design matches up against those cryptanalysis techniques. Because of the continuous progress in the development of cryptanalysis techniques careful design of S-boxes becomes more and more important. Large random S-boxes, increased a number of rounds or long keys may become irrelevant if cryptographic attack exploits an inherent flaw in S-boxes.

Cryptographically strong S-box should possess some properties that are universally agreed upon among researchers. Such S-box should be balanced, highly nonlinear, have the lowest maximum value in its XOR profile (difference distribution table), and complex algebraic description (esp. it should be of higher degree). The above criteria are dictated by linear and differential cryptanalysis and algebraic attacks.

It is a well-known fact that S-boxes generated using finite field inversion mapping fulfil these criteria to a very large extent [**5**]. They are, however, susceptible to (theoretical) algebraic attacks. To resist algebraic attacks multiplicative inverse mapping used to construct an S-box is composed of an additional invertible affine transformation. This affine transformation does not affect nonlinearity of the S-box, its XOR profile nor its algebraic degree. The best known example of such an S-box is the S-box of AES [**5**]. It has been commonly known which does not affect its security.

4. Research Scope

During S-box design research for PP-1, PP-2 and HAF ciphers such finite field inversion mapping was used to generate 8x8 S-boxes, which were then modified to suit certain needs of each cipher.

One of the requirements was to remove the affine equivalence from the generated S-boxes. It has been shown that all the output functions of the AES S-box can be mapped to each other using affine transformations, and hence they are all in the same equivalence class [**6, 7**]. As the S-box is the only nonlinear element in the cipher, any weakness can lead to possible future attacks (particularly algebraic attacks). The algorithm used by the author to remove this affine equivalence has a penalty of reduced S-box nonlinearity, from 112 for AES-like S-boxes, to 110 for the best S-boxes without affine equivalence.

Another requirement specified for the HAF stream cipher was that S-boxes should not have any cycles. A cycle is such a sequence of S-box values $S_0, S_1, \ldots,$

S_{k-1} where $S_{(i+1) \mod k} = S(S_i)$. HAF S-box should ideally have only one such cycle containing all the values of the S-box, so cycle where $k = 2^n$.

For both PP-1 and PP-2 cycles, input is combined with the round key using both XOR and SUM mod 256 operations. This can be viewed as an S-box modification depending on a key. While using XOR operation does not change any nonlinear properties of such a modified S-box, SUM mod 2 affects its nonlinearity. This influence was also tested.

All of the above S-box modifications were applied to generate AES-like S-boxes and the following properties of such S-boxes were tested: nonlinearity, order of nonlinearity, maximum value in the XOR profile, number of cycles and SAC. The results of those tests are presented in the following chapter. A sample of 10000 S-boxes was generated in each group. The graphs show percentage of S-boxes having a particular value of cryptographic property, like nonlinearity, order, etc.

5. Generating AES-like S-boxes

For the purpose of this article, let us call AES-like S-boxes the S-boxes generated using exactly the same inverse mapping procedure that has been used to construct an AES S-box [**5**], however, with randomly chosen irreducible polynomial defining a Galois Field and random value of ci in the affine transform. See below for details.

These S-boxes constitute the base for generating the S-boxes required by the PP 1, PP 2 and HAF ciphers.

To generate an inverse mapping in Galois Field (GF(2^n)) we need an irreducible polynomial that defines a Galois Field, and another polynomial that would be a so called generator (see below). n–bit elements of Galois Field are treated as polynomials with coefficients in the field Z_2. For example, in the case of 8×8 S-boxes we operate mostly on bytes represented as $b_7b_6b_5b_4b_3b_2b_1b_0$ which correspond to the following polynomial: $b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x^1 + b_0$.

An irreducible polynomial mentioned above is used to calculate multiplication in GF. When two polynomials are multiplied in GF(2^n) the resulting product is a polynomial of degree at most $2n$ – too much to fit in n-bit data that represent polynomials in GF(2^n), so the intermediate product of this multiplication if divided by the irreducible polynomial and the remainder of this division is the result of the multiplication. An irreducible polynomial is a polynomial that cannot be factored into the product of two simpler polynomials. For GF(2^n) an irreducible polynomial should be of degree n. For example, in AES (with

GF(2^8)) an irreducible polynomial selected for construction of the S-box is \$11b (in hexadecimal notation denoted from now on by \$).

A generator in Galois Field is a polynomial whose successive powers take on every element except zero. Which polynomials are generators in a particular Galois Field depends on the irreducible polynomial selected. So say polynomial \$03 is a generator in GF(2^8) with irreducible polynomial \$11b (as in AES), but it is not a generator in GF(2^8) with irreducible polynomial \$1bd, for which the simplest generator is \$07.

In the algorithm presented in this paper, an irreducible polynomial for an S-box being generated is selected in the first step at random. Tables of all existing irreducible polynomials for all values of n ranging from 8 to 16 can be precomputed so that finding an irreducible polynomial and a corresponding generator at random is very time efficient. This inverse mapping is different for every irreducible polynomial selected (randomly) for a particular S-box. It does not depend on a selected generator - all generators would give the same result for a given irreducible polynomial. Generators are then not taken at random. The simplest generator for a given irreducible polynomial is always selected (it can also be precomputed and stored in a table along with irreducible polynomials).

Table of inverses of all elements in Galois Field can be efficiently calculated using two additional tables - the table of powers (exponentials) (of the polynomial being a generator) and the table of inverse powers (logarithms). A multiplicative inverse of polynomial g in GF(2^n) is such a polynomial h that $gh = \$01$.

To avoid algebraic attacks (given multiplicative inversion simple algebraic form) every element of the table of multiplicative inverses is changed using an affine transform, which has to be full permutation (every element gets changed, and all possible elements are represented as the result of a change, so that no two different bytes are changed to the same byte), so that after applying it the table is still a bijective. In the case of AES cipher this affine transformation is given by the following equation:

$$b'_i = b_i \oplus b_{(i+4) \mod 8} \oplus b_{(i+5) \mod 8} \oplus b_{(i+6) \mod 8} \oplus b_{(i+7) \mod 8} \oplus c_i.$$

6. Research results

6.1. Random S-boxes

A sample of random S-boxes was generated to allow depicting cryptographic properties of other S-boxes in comparison to those random ones. One may argue that a secure cipher can also be made using random S-boxes, providing they are large enough (such as 12 input bits). Another way to make a cipher

more secure even while using not optimized S-boxes is to use more rounds. The example of this approach is the FEAL algorithm which becomes immune against linear cryptanalysis when the number of rounds is larger than 32.

The following graphs show distribution of different values of each of the analysed cryptographic properties. In subsequent graphs, where each group of S-boxes is analysed, comparative values for random S-boxes are shown in light grey colour, versus dark grey for the analysed group of S-boxes.

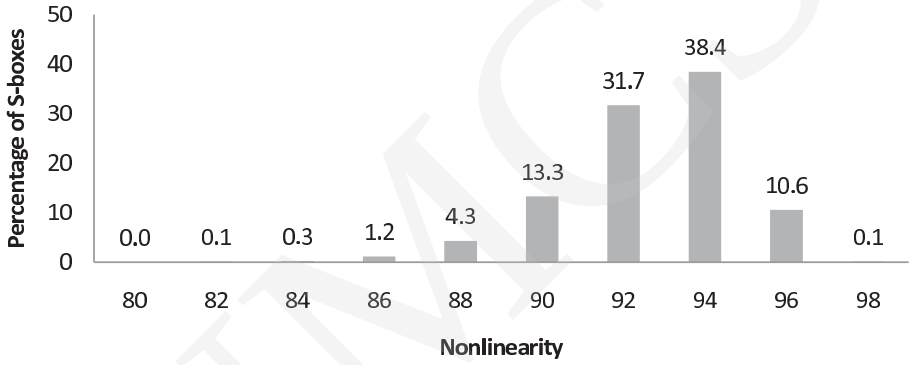

Fig. 1. Nonlinearity of Random 8×8 S–boxes.

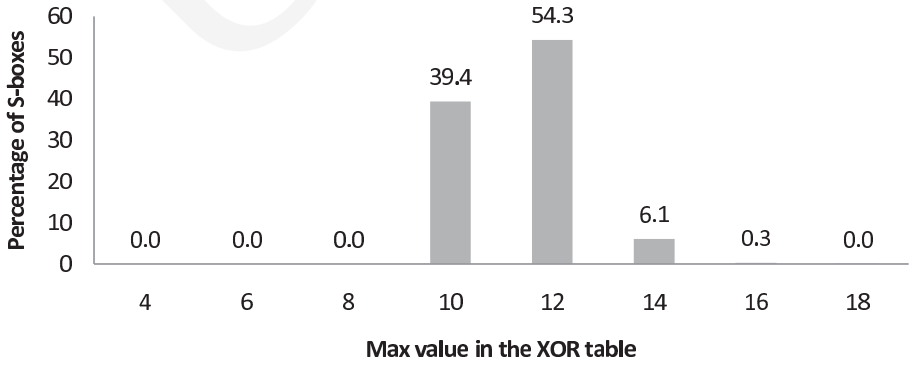

Fig. 2. Max value in the XOR table of Random 8×8 S–boxes.

The nonlinear order of random S-boxes is 6 for 71% of S-boxes, and 7 for 29% of S-boxes.

6.2. AES-like S-boxes

Most of the analyzed S-box properties are constant among AES-like S-boxes generated using inverse mapping. There are:

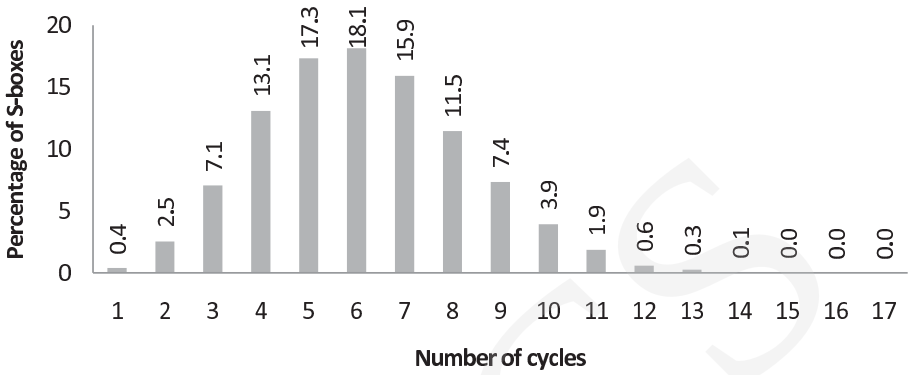

Fig. 3. Number of cycles of Random 8×8 S–boxes.

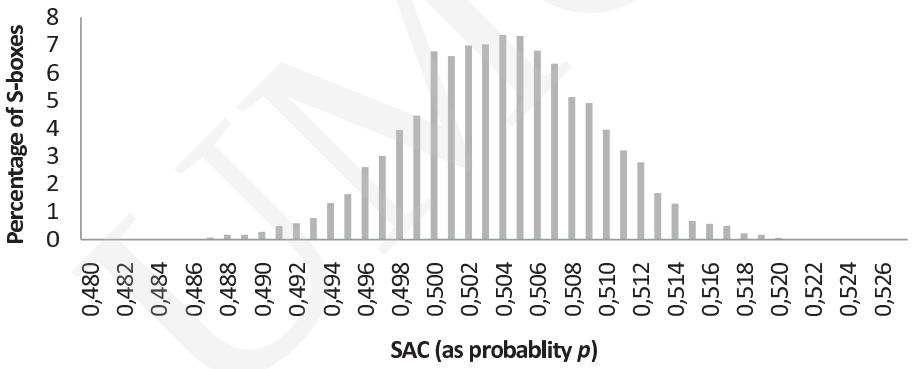

Fig. 4. SAC of Random 8×8 S–boxes.

- Nonlinearity - always equals 112
- Nonlinear order - always equals 7
- Maximum value in the XOR profile - always equals 4

What changes these S-boxes are a number of cycles and SAC. The following graphs show distribution of these values compared to those of random S-boxes.

6.3. S-boxes with removed affine equivalence

Removing affine equivalence from AES-like S-boxes was one of the major requirements for all three ciphers, PP-1, PP-2 and HAF. Removing this potentially unwelcome property can be done without destroying other highly desirable nonlinear properties of AES-like S-boxes, like nonlinearity, high nonlinear order and low value in the XOR profile. Below are the results of analysis of S-boxes with removed affine equivalence.

Nonlinear order of those S-boxes equals 6 for 58% of S-boxes, and 7 for 42%.

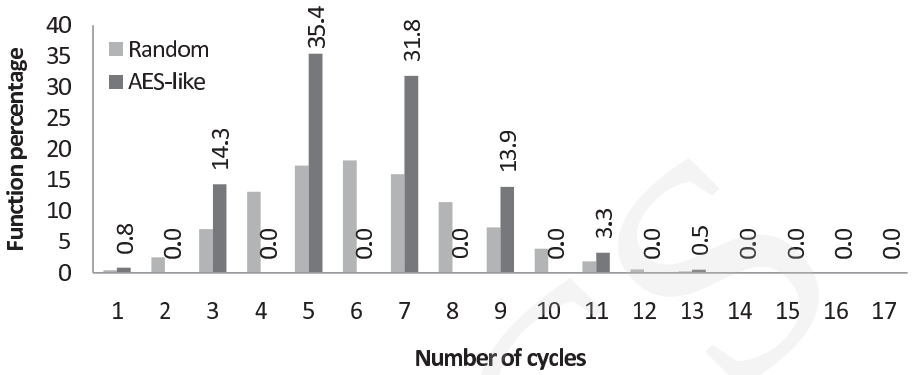

Fig. 5. Number of cycles of AES-like S-boxes.

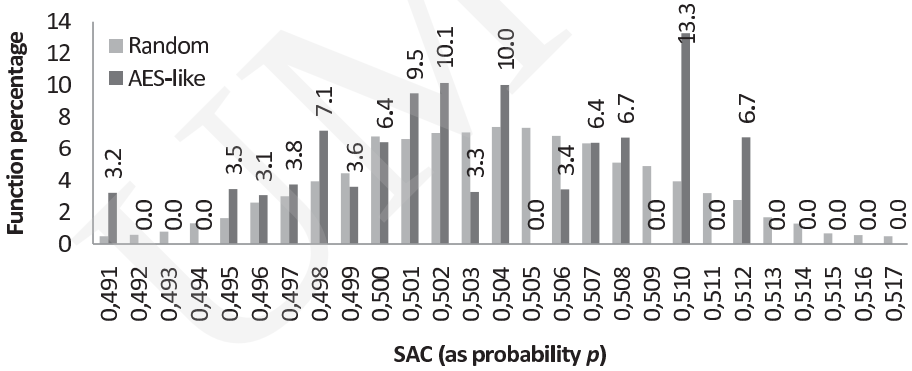

Fig. 6. SAC of AES-like S-boxes.

6.4. S-boxes with removed cycles

Removing cycles from AES-like S-boxes, also from S-boxes with already removed affine equivalence has absolutely no influence on any of the analysed properties. Such S-boxes with exactly one cycle have the same nonlinear characteristics as S-boxes described in the previous paragraph.

6.5. Association with the round key

Associating S-box input with a round key can be seen as altering an S-box itself. While using the XOR operation for such association has no influence on nonlinear properties of an S-box, using the SUM modulo 256 operation has a negative influence on nonlinear characteristics of an S-box, resulting in nonlinear properties resembling those of random S-boxes.

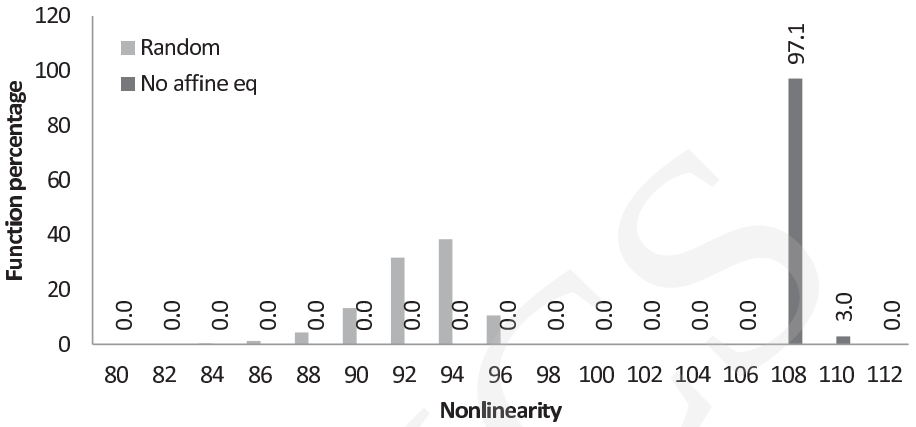

Fig. 7. Nonlinearity of S-boxes with removed affine equivalence.

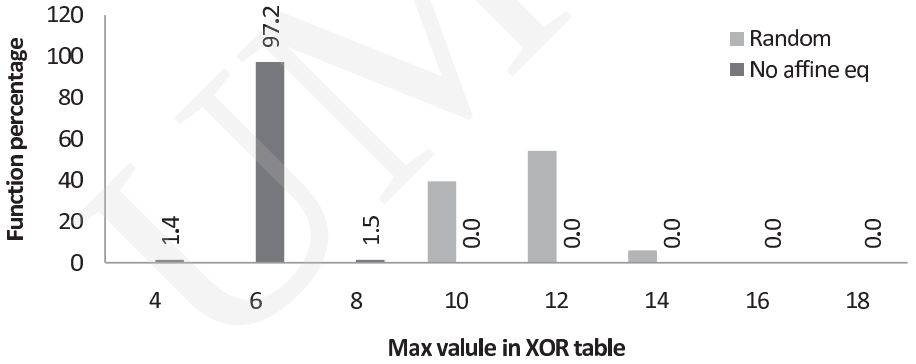

Fig. 8. Max value in the XOR profile of S-boxes with removed affine equivalence.

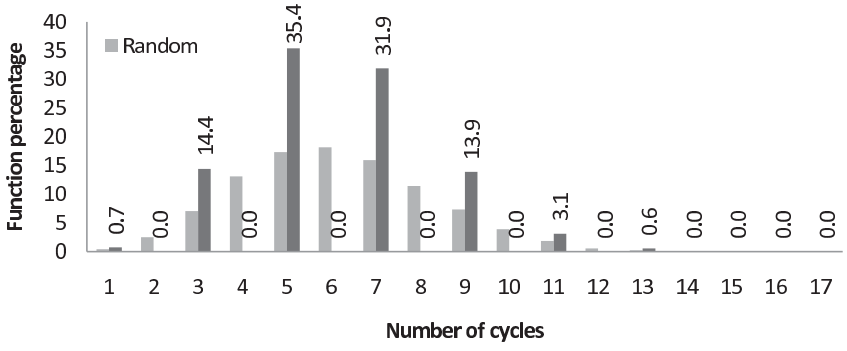

Fig. 9. Number of cycles of S-boxes with removed affine equivalence.

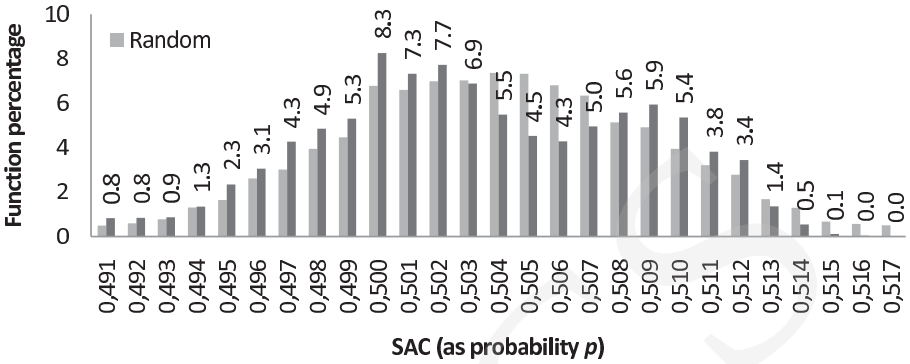

Fig. 10. SAC of S-boxes with removed affine equivalence.

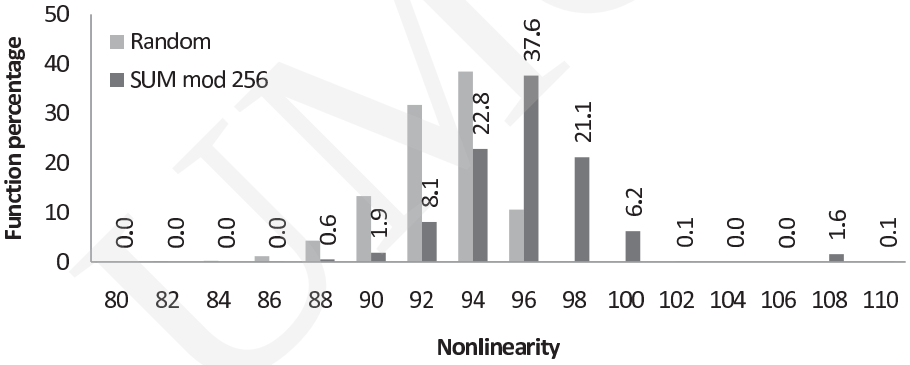

Fig. 11. Nonlinearity of S-boxes combined with a key using SUM mod 256.

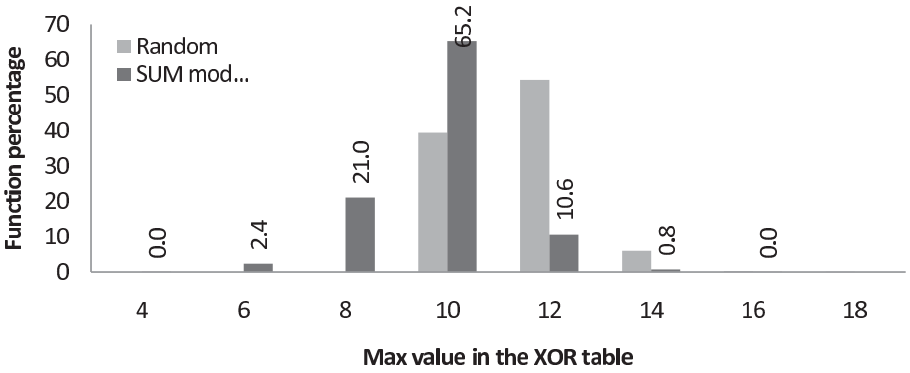

Fig. 12. Nonlinearity of S-boxes combined with a key using SUM mod 256.

7. Conclusions

As one can see from the results presented in the previous chapter, AES-like S-boxes provide an excellent starting point for generating S-boxes with various desired properties and still fulfilling to an extremely high degree the most common cryptographic criteria.

Removing affine equivalence from AES-like S-boxes results in reduced nonlinearity, but only to 110 (from 112 for AES-like S-boxes). Such S-boxes still maintain an excellent XOR profile (maximum value of 4) and high nonlinear order (7). Not all such S-boxes have such excellent properties, but they are relatively easy to find.

Removing cycles from S-boxes does not influence on their cryptographic properties.

Using SUM mod 256 as a round key association operation seems to be inferior to the XOR operation in a sense that if this operation is treated as that modifying the S-box, then the SUM mod 256 operation reduces S-box nonlinearity and gives higher maximum value in its XOR profile.

References

[1] Bucholc K., Chmiel K., Grocholewska-Czuryło A., Stokłosa J., PP-1 Block Cipher, Polish Journal of Environmental Studies 16(5B) (2007): 315.

[2] Bucholc K., Chmiel K., Grocholewska-Czuryło A., Idzikowska E., Janicka-Lipska I., Stokłosa J., Scalable PP-1 Block Cipher, International Journal of Applied Mathematics and Computer Science 20(2) (2010): 401.

[3] Chmiel K., Grocholewska-Czuryło A., Stokłosa J., Involutional Block Cipher for Limited Resources, Proceedings of IEEE GLOBECOM Conference, New Orleans (2008): 1852.

[4] Chmiel K., Grocholewska-Czuryło A., Socha P., Stokłosa J., Scalable Cipher for Limited Resources, Polish Journal of Environmental Studies 17(4C) (2008): 371.

[5] Daemen J., V., AES Proposal: Rijndael, AES'99, http://csrc.nist.gov/CryptoToolkit/aes/rijndael/1999

[6] Fuller J., Millan W., On Linear Redundancy in the AES S-Box, http://eprint.iacr.org/2002/111.

[7] Fuller J., Millan W., On Linear Redundancy in S-Boxes, FSE 2003, LNCS 2887, Springer (2003): 74.