Published in IET Information Security
Received on 26th November 2008
Revised on 12th May 2009
doi: 10.1049/iet-ifs.2008.0116

ISSN 1751-8709

Efficient method for simplifying and approximating the S-boxes based on power functions

A. Farhadian   M.R. Aref

Information Systems & Security Laboratory, Department of Electrical Engineering, Sharif University of Technology, Azadi Avenue, P.O. Box 11155-9363, Tehran, Iran
E-mail: afarhadian@yahoo.com

Abstract: In recently proposed cipher algorithms, power functions over finite fields and specially inversion functions play an important role in the S-box design structure. In this study, a new systematic efficient method is introduced to cryptanalyse (to simplify and approximate) such S-boxes. This method is very simple and does not need any heuristic attempt and can be considered as a quick criterion to find some simple approximations. Using this new method, some approximations can be obtained for advanced encryption standard (AES) like S-boxes, such as AES, Camellia, Shark and so on. Finally as an application of this method, a simple linear approximation for AES S-box is presented.

1 Introduction

Recently, power functions over finite fields are vastly suggested to be used in S-boxes design, because of their good and proper characteristics (as S-box) [1–4]. Inversion mapping [4] is a special form of power functions which is used in S-boxes of advanced encryption standard (AES) [5], Camellia [6], Shark [7] and so on. Often, good properties of such S-boxes prevent penetrating in the cipher structure to perform successful attack. So, finding some simpler expression or approximation may be useful to overcome the design strength of S-boxes and the cipher.

Finding simple expression or approximation in heuristic way seems to be very difficult and inefficient or even not successful. We do not know which simple relations may exist for the function in the field and for which elements of the field are satisfied.

In this paper, a new systematic method is proposed for simplifying and approximating power functions over the finite fields. Using this method, the power function can be defined by a piecewise function with simpler expression for each part of its domain. This form of representation can lead to some different approximations for the function. This method is very simple and does not need any heuristic attempt. This method can be applied to all S-boxes in the form $S(x) = L_1((L_2(x))^d)$, where L_1, L_2 are affine transformations over GF(2). This method can be considered as a quick criterion to find some approximations.

A practical application of the proposed method is given for AES S-box which is based on inversion function, a special form of power functions. This method results in a good simple linear approximation for AES S-box that is better than other obtained approximations for it [8].

The outline of the paper is as follows. In Section 2, some required properties of the finite fields are reviewed. In Section 3, the method is proposed. A practical example of using this method for AES S-box is described in Section 4. Finally, the conclusion is given in Section 5.

2 A glance on some finite field properties

In this section, we focus on some definitions and properties of finite field elements that will be used in the paper.

Let F_q denote a finite field which has a finite number q of elements in it. That is q is a prime power $q = p^f$.

Definition 1: The least positive power k of $\alpha \in F_q - \{0\}$ such that $\alpha^k = 1$ is the 'order of α'.

Theorem 1: If $\alpha \in F_q - \{0\}$, then $\text{ord}(\alpha) | p^f - 1$.

Proof: See [9].

According to Theorem 1, the elements of the finite field have different 'orders' that divide $p^f - 1$. Now, we want to investigate the number of elements which have the same order.

Proposition 1: If k is a divisor of $p^f - 1$, the number of field elements which have this value as their order is

$$N(k) = \phi(k)$$

where $\phi(k)$ is the Euler function.

Proof: It is known that every finite field has a generator. Let g be a generator of F_q, so the order of g is $p^f - 1$ and the power of g run through all of the elements of $F_q - \{0\}$. Therefore every non-zero element of F_q can be represented by g^i ($i \in 1, \ldots, p^f - 1$). The elements with 'order' of k are elements that $(g^i)^k = 1$. So we have $p^f - 1 | i \cdot k$. Since k is a divisor of $p^f - 1$, hence $(p^f - 1)/k | i$. We can write it as $i = r(p^f - 1)/k$, $r \in 1, 2, \ldots, k - 1$.

On the other hand, since k is the least power that $(g^i)^k = 1$, we should have $(k, r) = 1$. Therefore

$$\begin{aligned} N(k) &= \left| \left\{ g^{r(p^f-1)/k} | (r, k) = 1, \quad r \in 1, 2, \ldots, k-1 \right\} \right| \\ &= |\{r \in 1, 2, \ldots, k-1 | (r, k) = 1\}| \\ &= \phi(k) \end{aligned}$$

For the finite field GF(2^{10}), we want to know which 'orders' are possible in this field and how many elements have the same order. The possible 'orders' over GF(2^{10}) are the set of all divisors of 1023($2^{10} - 1$). The divisors set of 1023 is $S = \{1, 3, 11, 31, 33, 93, 341, 1023\}$. The number of elements corresponding to each order is computed according to Proposition 1 and is recorded in Table 1.

Table 1 The possible orders in GF(2^{10}) and the number of elements by each order

order $= t$	1	3	11	31	33	93	341	1023
number of elements by this order	1	2	10	30	20	60	300	600

3 Simplifying and approximating the power functions

In this section, we want to use 'order' property of finite field elements to simplify and approximate the power functions.

A power function is of the form $F(x) = x^d$. Now we want to know if it is possible to show it in another way. We will show that it can be represented by a piecewise function. It is known that $x^{\text{ord}(x)} = 1$. So, we can rewrite the power function as $F(x) = x^{d \pm k\,\text{ord}(x)}$.

It is noteworthy that by using this form of representation, the power function can be written in different ways for different groups of elements by different 'orders'.

The addition of phrase $\pm k\text{ord}(x)$ to exponent enables us to change the power for the set of elements by the same order. Changing the power can result in simpler function. Adding $\pm k\text{ord}(x)$ can be used to reduce the power amplitude or more important to decrease the Hamming weight of the exponent. It is known that the non-linear degree of the function $f(x) = x^d$ is the Hamming weight of d. It means that if there exists a k such that $d \pm k\text{ord}(x)$ is a power of 2, then the function $f(x) = x^{d \pm k\text{ord}(x)}$ is a completely linear function for all elements whose orders are equal to ord(x).

Suppose function $F(x) = x^{37}$ over F_q. And let there be 18 elements in the field that their order is 11. Therefore we can rewrite function $F(x)$ to $f_{11}(x) = x^{37-3\times11} = x^4$ for those elements. x^4 is a linear function. Therefore we could obtain a simple linear function for 18 elements of the field. It can be used to approximate the function.

Although, some times it is impossible to completely linearise the power function by this method, but it is usually possible to reduce the Hamming weight of the exponent for significant number of field elements.

By this method, a power function is converted to a piecewise function with different formula. The resulted piecewise function can be used to obtain approximations for power functions (or S-boxes). For this purpose, the dominant part can be replaced by the function. Dominant part is a part that has sufficient (significant) number of elements and rather simple relation.

In this method, the order of elements is used to simplify and approximate the function. So we call it 'reducing by order' or 'RBO' method. Let summarise the suggested RBO method to simplify and approximate the function $F(x) = x^d$.

Step 1: Perform the set of all divisors of $p^{\text{f}} - 1 (= S)$.

Step 2: Compute the $N(t)$ for each $t \in S$.

Step 3: Find a proper k for each $t \in S$, such that $d + kt$ has minimum Hamming weight (or amplitude). The function $f_t(s) = x^{d+kt}$ is considered for elements whose orders are t.

Step 4: In the previous step, a piecewise function equal to power function is obtained. If we want to obtain approximation, we should choose one expression of piecewise function to replace the entire function. We should select a group that has significant number of elements and rather simple relation.

Example 1: Assume the power function $F(x) = x^{683}$ over GF(2^{10}). Since the Hamming weight of 683 is 6, the non-linear degree of $F(x)$ is 6. We want to use the RBO method to this function. The possible orders over GF(2^{10}), and the number of elements corresponding to each order are given in Table 1.

For each group of elements, the related function $f_t(s) = x^{683+kt}$ is recorded in Table 2.

The obtained result in Table 2 is very interesting. The result is a piecewise function with identity formula for some part of its domain. We see that for $t = 11, 31, 341$ the function $F(x)$ is an identity function. In other words, for 340 elements of the field, we have $F(x) = x$.

It does not seem to be easy, at all, to predict that $F(x) = x^{683}$ by non-linear degree of 6 can be approximated to an identity function with high probability (more than 340/1024).

Example 2: Assume the function $F(x) = x^{43}$ over GF(2^{10}). The non-linear degree of $F(x)$ is 4. We use again the RBO method to this function. The results are recorded in Table 3.

We see from Table 3 that there is not linear function for large number of elements. f_3 is linear, but it is true for only two elements. Although, we could not obtain a good linear approximation, but $f_{341} = f_{31} = f_{11} = x^{384}$ holds for more than 340 elements of the field and the non-linear degree of it is 2. In other words, while the non-linear degree of $F(x)$ is 4, we could find an approximation for $F(x)$ with non-linear degree of 2, and the probability more than 1/3.

The following example shows that some finite fields, because of their structure, do not permit the RBO method to have a good efficiency.

Example 3: Suppose the function $F(x) = x^{155}$ over GF(2^9). The non-linear degree of $F(x)$ is 5. According to Table 4, the function can be approximated by $f_t(x) = x^9$ with probability of $p = 74/512 (\approx 0.14)$. The non-linear degree of f_t is 2. The probability is not high, because of the field structure. This example shows that some finite fields may be robust against the RBO method. However, the RBO method results in a piecewise function with simpler relation.

4 Some new approximations for AES like S-boxes

Inversion mapping over GF(2^n) is a special form of power functions. Several block ciphers such as AES, Camellia, Shark use S-boxes that are based on the inversion mapping over GF(2^n).

Here, we want to use the RBO method to such S-boxes. In [8], it is said that using exhaustive search, they verified that the best third degree polynomial approximation for the AES S-box holds with $p = 11/256$. While, we show that using RBO method, without any exhaustive search, it is

Table 2 The piecewise function corresponding to $F(x) = x^{683}$ over GF(2^{10})

order $= t$	1	3	11	31	33	93	341	1023
$x^{683+k \cdot t}$	$x^{683-683\times 1}$	$x^{683-227\times 3}$	$x^{683-62\times 11}$	$x^{683-22\times 31}$	$x^{683-20\times 33}$	$x^{683-7\times 93}$	$x^{683+341}$	x^{683}
$f_t(x)$	x^0	x^2	x^1	x^1	x^{23}	x^{32}	x^1	x^{683}
non-linearity	—	1	1	1	4	1	1	6
number of elements by this order	1	2	10	30	20	60	300	600

Table 3 The piecewise function corresponding to $F(x) = x^{43}$ over GF(2^{10})

order $= t$	1	3	11	31	33	93	341	1023
$x^{43+k \cdot t}$	$x^{43-43\times 1}$	$x^{43+7\times 3}$	$x^{43+31\times 11}$	$x^{43+11\times 31}$	$x^{43+30\times 33}$	x^{43+93}	x^{43+341}	x^{43}
$f_t(x)$	x^0	x^{64}	x^{384}	x^{384}	x^{10}	x^{136}	x^{384}	x^{43}
non-linearity	—	1	2	2	2	2	2	4
number of elements by this order	1	2	10	30	20	60	300	600

Table 4 The piecewise function corresponding to $F(x) = x^{155}$ over GF(2^9)

order = t	1	7	73	511
x^{155}	$x^{155-155\times 1}$	$x^{155-22\times 7}$	$x^{155-2\times 73}$	x^{155}
$f_t(x)$	x^0	x^1	x^9	x^{155}
non-linearity	—	1	2	5
number of elements by this order	1	6	72	432

Table 5 The piecewise function corresponding to Inv(x) $= x^{-1}$ over GF(2^8)

order = t	1	3	5	15	17	51	85	255
$x^{-1+k\cdot t}$	x^{-1+1}	x^{-1+3}	x^{-1+5}	x^{-1+15}	x^{-1+17}	x^{-1+51}	x^{-1+85}	x^{-1+255}
$f_t(x)$	x^0	x^2	x^4	x^{14}	x^{16}	x^{50}	x^{84}	x^{254}
non-linearity	—	1	1	3	1	3	3	7
number of elements by this order	1	2	4	8	16	32	64	128

possible to establish a linear polynomial with $p = 18/256$ for AES S-box. Also, a polynomial with non-linear degree of 3 is possible with $p = 86/256$.

Here we apply the RBO method for the AES S-box. AES S-box is an inversion mapping over GF(2^8) that is followed by a linear function. In other words, $S(x) = L(\mathrm{Inv}(x))$, where Inv($\cdot$) is inversion mapping and $L(\cdot)$ is a linear function. Zero is mapped to zero by Inv($\cdot$). The linear function is considered in design to overcome the attacks that arise from simple algebraic form of S-box, such as interpolation attack, but it does not have any effect on non-linear properties of S-box. The polynomial form of $S(x)$ over GF(2^n) is

$$S(x) = {'63'} + {'05'}x^{254} + {'09'}x^{253} + {'f9'}x^{251} + {'25'}x^{247} + {'f4'}x^{239} + {'01'}x^{223} + {'b5'}x^{191} + {'8f'}x^{127}$$

The hamming weights of all appeared exponents are 7.

Now, we use the RBO method to Inv(x). The possible orders in GF(2^8), the number of elements of each group and corresponding $f_t(\cdot)$ are shown in Table 5.

According to Table 5, f_{17} is a linear function and is true for 16 elements of the field. Zero and 1 of the field hold in all f_t too. So $f_{17}(\cdot) = \mathrm{Inv}(\cdot)$ holds for 18 elements of the field. It means that the approximation $S(x) \overset{p}{\simeq} S_{17}(x)$ holds with $p = 18/256$, where $S_{17}(x) = L(f_{17}(x))$ and it is an affine function. The polynomial form of $S_{17}(x)$ is

$$S_{17}(x) = {'63'} + {'f4'}x + {'01'}x^2 + {'b5'}x^4 + {'8f'}x^8 + {'05'}x^{16} + {'09'}x^{32} + {'f9'}x^{64} + {'25'}x^{128}$$

As we see, all the exponents are powers of 2. Since $S_{17}(x)$ is an affine function, it can be written, also, in the form $S_{17}(x) = A_{8\times 8}x + B_{8\times 1}$ over GF$(2)^8$, where $A_{8\times 8}$, $B_{8\times 1}$ are matrices with 0, 1 elements.

The proposed approximation for AES S-box in [8] is in the form $ax^{-1} + b$ with $p = 16/256$. So the new approximation is better. Because, it is linear, simpler and more probable than the last one.

According to Table 5, another good approximation is $S(x) \overset{p}{\simeq} S_{85}(x)$. The non-linear degree of $S_{85}(x)$ transformation is 3, whereas the non-linear degree of $S(x)$ is 7. It means that the output bits of $S_{85}(x)$ transformation can be presented by input bits with degree of 3, while the degree of relations in $S(x)$ is 7. The $S_{85}(x)$ is true for elements whose order is 85 or divides 85, implies 5 and 17. Therefore $S_{85}(x)$ is true for 86 elements of the field ($86 = 64 + 16 + 4 + 2$). Hence, it is an approximation with $p = 86/256$.

5 Conclusion

In this paper a new method, called 'RBO', was introduced. The RBO method gives a systematic and efficient technique to simplify and approximate the S-boxes based on power functions in finite fields, and specially inversion function. We saw some interesting results can be obtained by this method.

The RBO method usually operates efficiently. So it can be considered as a quick criterion to check and investigate the S-boxes based on power functions.

Using this method, we could find a simple linear approximation for AES S-box with $p = 18/256$ over GF(2^8). Another approximation for AES S-box was a polynomial with non-linear degree of 3 and $p > 1/3$. These new approximations are better than the proposed approximations for AES S-box [8], both in probability and simplicity of formula.

6 Acknowledgment

This work was partially supported by Iranian NSF-Cryptography chair.

7 References

[1] DOBBERTIN H.: 'Almost perfect non-linear power functions on GF(2^n): the Welch case', *IEEE Trans. Inf. Theory*, 1999, **45**, (4), pp. 1271–1275

[2] DOBBERTIN H.: 'Almost perfect non-linear power functions on GF(2^n): a new case for *n* divisible by 5'. Proc. Fifth Conf. Finite Field and Applications, Agusburg, 1999, 2001, pp. 113–121

[3] CHEON J.H., LEE D.H.: 'Quadratic equations from APN power functions', *IEICE Trans.*, 2006, **89-A**, (1), pp. 19–27

[4] NYBERG K.: 'Differentially uniform mappings for cryptography'. Proc. Eurocrypt'93, 1994 (*LNCS*, **765**), pp. 55–64

[5] FIPS 197, National Institute of Standards and Technology: 'Advanced Encryption Standard' (26 November 2001)

[6] AOKI K., ICHIKAWA T., KANDA M., *ET AL*.: 'Camellia: a 128-bit block cipher suitable for multiple platforms – design and analysis', *Sel. Areas Cryptogr.*, 2000, **2012**, pp. 39–56

[7] RIJMEN V., DAEMEN J., PRENEEL B., BOSSALAERS A., WIN E.D.: 'The cipher SHARK', *Fast Softw. Encryption*, 1996, **1039**, pp. 99–111

[8] YOUSSEF A.M., TAVARES S.E., GONG G.: 'On some probabilistic approximations for AES-like S-boxes', *Discret. Math.*, 2006, **306**, (16), pp. 2016–2020

[9] LIDL R., NIEDERREITER H.: 'Finite fields, encyclopedia of mathematics and its applications' (Addison Wesley, Reading, MA, 1983, vol. 20)

doi: 10.1049/iet-ifs.2008.0116