Available online at www.sciencedirect.com
SCIENCE DIRECT®
Discrete Applied Mathematics 148 (2005) 161–170
DISCRETE APPLIED MATHEMATICS
www.elsevier.com/locate/dam

Affine equivalence in the AES round function

A.M. Youssef[a], S.E. Tavares[b]

[a]*Concordia Institute for Information Systems Engineering, Concordia University, Montreal, Quebec, Canada H3G 1M8*
[b]*Department of Electrical and Computer Engineering, Queen's University, Kingston, Ont., Canada K7M 1B6*

Received 27 November 2002; received in revised form 25 January 2005; accepted 7 February 2005
Available online 19 March 2005

Abstract

In this paper, we show that all the coordinate functions of the advanced encryption standard (AES) round function are equivalent under an affine transformation of the input. We also show that such affine relations will always exist if the AES S-box is replaced by any bijective monomial over $GF(2^8)$.

Keywords: Cryptography; AES; Rijndael, Finite fields; Boolean functions

1. Introduction

Rijndael [2,3] is an iterated block cipher that supports key and block lengths of 128–256 bits in steps of 32 bits. Rijndael versions with a block length of 128 bits, and key lengths of 128,192 and 256 bits have been adopted as the advanced encryption standard (AES) [4]. The main cryptographic criteria in the design of Rijndael have been its resistance against differential [1] and linear cryptanalysis [12]. This motivated the designers to choose an S-box which is optimized against these two attacks. In particular, the designers decided to base their S-box construction on the inversion mapping [15]

$$f(x) = x^{-1}, \quad x \in GF(2^8).$$

Because this inverse mapping has a simple algebraic expression that may enable some attacks such as the interpolation attacks [9,10,16]. This mapping was modified in such a

E-mail addresses: youssef@ciise.concordia.ca (A.M. Youssef), tavares@ee.queensu.ca (S.E. Tavares).

0166-218X/$ - see front matter © 2005 Elsevier B.V. All rights reserved.
doi:10.1016/j.dam.2005.02.001

way that does not modify its resistance towards both linear and differential cryptanalysis, while the overall S-box description becomes complex in $GF(2^8)$. This was achieved by adding a bitwise affine transformation after the inverse mapping. Let $a(x)$ denote the finite field polynomial representation of the S-box input, then the finite field polynomial representation of the output of this affine mapping is given by

$$b(x) = (x^7 + x^6 + x^2 + x) + a(x)(x^7 + x^6 + x^5 + x^4 + 1) \bmod (x^8 + 1). \tag{1}$$

Like many other block ciphers, the Rijndael S-boxes provide the only source of nonlinearity to the Rijndael round function, and hence to the overall algorithm. Weaknesses discovered with these mappings may have some consequences for the security of the overall cipher. Even before the AES proposal, Gong and Golomb [8] introduced a new criterion for S-box design. By showing that many DES-like ciphers can be viewed as a nonlinear feedback shift register with input, Gong and Golomb proposed that S-boxes should not be approximated by a bijective monomial. The reason is that, for $\gcd(c, 2^n - 1) = 1$, the trace functions $Tr(\zeta_j x^c)$ and $Tr(\lambda x), x \in GF(2^n)$, are both m-sequences with the same linear span [7].

Several other concerns were raised about the algebraic structure of the AES [5,14]. Recently, Fuller and Millan [6] showed, using a heuristic search technique, that all the coordinate functions of the Rijndael S-box can be mapped to each other using an affine transformation of the input variables. In this paper we extend their result by using the algebraic properties of the Rijndael S-box. In particular, we show that all the coordinate functions of the Rijndael round function (and not just the S-box) are equivalent under an affine transformation of the input to the round function. We also show that such affine relations will always exist if the Rijndael S-box is replaced by any bijective monomial over $GF(2^8)$.

2. Rijndael round transformation

In this section we briefly describe a typical round function of the 128 bit version of Rijndael. The first and last rounds have slightly different form but our analysis procedure remains the same. The AES defines a round in terms of the following three transformations: byte substitution (ByteSub), shift row (ShiftRow) and mix columns (MixColumns). After performing these three operations, the round keys are XORed with the output of the round functions. According to the AES specifications, the intermediate cipher result is called a state which can be represented by a rectangular array of bytes. The round function operations are defined on these states. The ByteSub is obtained by first taking the multiplicative inverse in $GF(2^8)$ using the irreducible polynomial $x^8 + x^4 + x^3 + x + 1$. Then we apply the affine transformation defined by Eq. (1) above. In the ShiftRow transformation, the rows of the state are cyclically shifted over different offsets depending on the cipher block length. For the 128 bit version, row i is cyclically shifted by i bytes, $i = 0, 1, 2, 3$. In the MixColumn transformation, the columns of the state are considered as polynomials over $GF(2^8)$ and multiplied modulo $x^4 + 1$ with the polynomial $c(x) = 3x^3 + x^2 + x + 2$. For full details on the round transformation the reader is referred to [3,4].

3. Algebraic preliminaries

In this section, we present some algebraic preliminaries required to prove our result. The reader is referred to [11,13] for the theory of finite fields.

Let $\{\alpha_0 \cdots \alpha_{n-1}\}$ be any basis of $GF(2^n)$ over $GF(2)$ and let $\{\beta_0 \cdots \beta_{n-1}\}$ be the corresponding dual basis. Let $f(x_0, \ldots, x_{n-1}) = (f_0(x), \ldots, f_{n-1}(x))$ be a permutation over $GF(2)^n$, then $g(x) = \sum_{i=0}^{n-1} \alpha_i f_i(x_0, \ldots, x_{n-1})$ is also a bijective mapping over $GF(2^n)$. Each output coordinate of $f(x)$ can be expressed as

$$f_i(x) = Tr(g(x)\beta_i),$$

where $x = \sum_{i=0}^{n-1} x_i \alpha_i$. We will denote this one-to-one correspondence by $f \longleftrightarrow g$.

Example 1. Let $n = 4$ and let $GF(2^4)$ be defined by the primitive polynomial $p(x) = x^4 + x + 1$. Let α be a root of $p(x)$. Then $\{\alpha_0, \alpha_1, \alpha_2, \alpha_3\} = \{1, \alpha, \alpha^2, \alpha^3\}$ is a (polynomial) basis of $GF(2^4)$ over $GF(2)$. The dual basis $\{\beta_0, \beta_1, \beta_2, \beta_3\}$ is given by McEliece [13]

$$\beta_j = \sum_{k=0}^{3} b_{kj}\alpha_k,$$

where $B = [b_{ij}] = A^{-1}$, $A = [a_{ij}]$ and $a_{ij} = Tr(\alpha_i \alpha_j)$. Thus we have

$$A = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}, \quad B = A^{-1} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}.$$

Hence we have $\{\beta_0, \beta_1, \beta_2, \beta_3\} = \{1 + \alpha^3, \alpha^2, \alpha, 1\} = \{\alpha^{14}, \alpha^2, \alpha, 1\}$. Let $g(x) = Tr(x^{-1})$. For any $x \in GF(2^4)$, we write $x = x_0 + x_1\alpha + x_2\alpha^2$. Then the output coordinates of $f \longleftrightarrow g$ can be expressed as

$$\begin{aligned} f_0(x) &= Tr(\beta_0 x^{-1}) = Tr(\alpha^{14} x^{-1}), \\ f_1(x) &= Tr(\beta_1 x^{-1}) = Tr(\alpha^2 x^{-1}), \\ f_2(x) &= Tr(\beta_2 x^{-1}) = Tr(\alpha x^{-1}), \\ f_3(x) &= Tr(\beta_3 x^{-1}) = Tr(x^{-1}). \end{aligned}$$

Lemma 1. *Let $g(x) = x^d$, $\gcd(d, 2^{n-1} = 1)$, be a bijective monomial over $GF(2^n)$. Let $h(x_0, \ldots, x_{n-1}) = L(f(x_0, \ldots, x_{n-1}))$ be the function obtained by applying an invertible linear transformation L to the output coordinates of $f \longleftrightarrow g$. Then the output coordinates of h can be mapped to each other using an affine transformation of the input coordinates.*

Proof. Each output coordinate of *f* can be expressed as

$$f_i(x) = Tr(x^d \gamma_i), \quad \gamma_i \in GF(2^n).$$

Thus, every coordinate of h can be expressed as

$$h_i(x) = \sum_{j=0}^{n-1} b_{i,j} Tr(x^d \gamma_i), \quad b_{i,j} \in GF(2).$$

From the linearity of the trace function and by noting that $Tr(b_{i,j}x) = b_{i,j}Tr(x)$ for $b_{i,j} \in GF(2)$, then

$$h_i(x) = Tr\left(x^d \sum_{j=0}^{n-1} \gamma_i b_{i,j}\right) = Tr(x^d \theta_i),$$

where $\theta = \sum_{j=0}^{n-1} \gamma_i b_{i,j}$. Hence we have

$$h_i(\theta_i^{-1/d} \theta_j^{1/d} x) = Tr(\theta_j x^d) = h_j(x).$$

The lemma follows by noting that for any $\gamma \in GF(2^n)$, the transformation $x \to \gamma x$ over $GF(2^n)$ corresponds to a linear transformation over $GF(2)^n$. □

Example 2. For the function in Example 1, to transform f_1 into f_3 we use the transform $x \to \alpha^2 x$, i.e.,

$$\begin{aligned} x_0 + \alpha x_1 + \alpha^2 x_2 + \alpha^3 x_3 &\to \alpha^2(x_0 + \alpha x_1 + \alpha^2 x_2 + \alpha^3 x_3) \bmod p(x) \\ &= x_2 + (x_2 + x_3)\alpha + (x_0 + x_3)\alpha^2 + x_1\alpha^3, \end{aligned}$$

which corresponds to the linear transformation

$$\begin{bmatrix} x_0' \\ x_1' \\ x_2' \\ x_3' \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{bmatrix}.$$

4. Equivalence between the AES S-box coordinates

In this section, we demonstrate the affine relation between the coordinate functions of the Rijndael S-box. We construct the finite field $GF(2^8)$ using the same irreducible polynomial in the AES specifications, namely $p(x) = x^8 + x^4 + x^3 + x + 1$. Let $\beta = 1 + \alpha$, where α is a root of $p(x)$ (in this case, β is a primitive element). Using the same computation step as in Example 1, the co-ordinate functions of the Rijndael S-box is given by

$$\begin{aligned} f_0(x) &= Tr(\beta^{166} x^{-1}) + 1, \\ f_1(x) &= Tr(\beta^{53} x^{-1}) + 1, \\ f_2(x) &= Tr(\beta^{36} x^{-1}), \\ f_3(x) &= Tr(\beta^{11} x^{-1}), \end{aligned}$$

$$f_4(x) = Tr(\beta^{72}x^{-1}),$$
$$f_5(x) = Tr(\beta^{76}x^{-1}) + 1,$$
$$f_6(x) = Tr(\beta^{51}x^{-1}) + 1,$$
$$f_7(x) = Tr(\beta^{26}x^{-1}).$$

Now suppose that we want to transform f_0 into f_1, then we use the transformation $x \to \beta^{(166-53) \bmod 255}x = \beta^{113}x$ which corresponds to the transformation

$$\begin{aligned}(x_0 + x_1\alpha + \cdots + x_7\alpha^7) &\to (x_0 + x_1\alpha + \cdots x_7\alpha^7)(1+\alpha)^{113} \bmod p(x)\\ &= (x_0 + x_4 + x_5) + (x_1 + x_4 + x_6)\alpha + (x_2 + x_5 + x_7)\alpha^2\\ &\quad + (x_0 + x_3 + x_4 + x_5 + x_6)\alpha^3 + (x_0 + x_1 + x_6 + x_7)\alpha^4\\ &\quad + (x_1 + x_2 + x_7)\alpha^5 + (x_2 + x_3)\alpha^6 + (x_3 + x_4)\alpha^7\end{aligned}$$

which corresponds to the linear transformation

$$\begin{bmatrix} x'_0\\ x'_1\\ x'_2\\ x'_3\\ x'_4\\ x'_5\\ x'_6\\ x'_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0\\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0\\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1\\ 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0\\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1\\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} x_0\\ x_1\\ x_2\\ x_3\\ x_4\\ x_5\\ x_6\\ x_7 \end{bmatrix}.$$

5. Equivalence between the AES round function coordinates

In this section, we demonstrate the affine relation between the coordinate functions of the Rijndael round function. Here we consider the 128 bit version. The same technique can be used for the other versions of the cipher. We do not use the standard AES way of representing the input to the round function as a rectangular array. Let X_i denote the input to the ith S-box of the round function, then we simply view the input to the round function as a column vector. Careful examination of the ShiftRow and MixColumn operations reveals that every output byte of the round function depends only on 4 input bytes of the 16 input bytes. In particular, if we let Y_i denote the ith output byte of the round function, then we have

$Y_0,\ Y_1,\ Y_2,\ Y_3$ depends only on $X_0,\ X_5,\ X_{10},\ X_{15}$,
$Y_4,\ Y_5,\ Y_6,\ Y_7$ depends only on $X_3,\ X_4,\ X_9,\ X_{14}$,
$Y_8,\ Y_9,\ Y_{10},\ Y_{11}$ depends only on $X_2,\ X_7,\ X_8,\ X_{13}$,
$Y_{12},\ Y_{13},\ Y_{14},\ Y_{15}$ depends only on $X_1,\ X_6,\ X_{11},\ X_{12}$.

From the description of the round function, it is clear that the byte structure is respected throughout all three operations of the round function. Combining these observations with

the fact that both the ShiftRow and MixColumns transformations are linear operations, we can easily use the Lagrange interpolation to evaluate the exact form of dependency of the output of the round function on its inputs. Again, let $GF(2^8)$ be defined by the irreducible polynomial $p(x) = x^8 + x^4 + x^3 + x + 1$. Let $\beta = 1 + \alpha$, where α is a root of $p(x)$. The following example gives the algebraic representation of the output coordinates for $i = 0, 1, \ldots, 7$, $i = 24, 25, \ldots, 31$ and $i = 120, 121, \ldots, 127$ (which corresponds to the outputs of the 1st, 4th and 16th S-boxes).

Example 3.

$$
\begin{aligned}
f_0 &= Tr(\beta^{26}X_0^{-1}) + Tr(\beta^{154}X_5^{-1}) + Tr(\beta^{166}X_{10}^{-1}) + Tr(\beta^{166}X_{15}^{-1}) + 1,\\
f_1 &= Tr(\beta^{154}X_0^{-1}) + Tr(\beta^{100}X_5^{-1}) + Tr(\beta^{53}X_{10}^{-1}) + Tr(\beta^{53}X_{15}^{-1}) + 1,\\
f_2 &= Tr(\beta^{53}X_0^{-1}) + Tr(\beta^{104}X_5^{-1}) + Tr(\beta^{36}X_{10}^{-1}) + Tr(\beta^{36}X_{15}^{-1}) + 0,\\
f_3 &= Tr(\beta^{47}X_0^{-1}) + Tr(\beta^{236}X_5^{-1}) + Tr(\beta^{11}X_{10}^{-1}) + Tr(\beta^{11}X_{15}^{-1}) + 0,\\
f_4 &= Tr(\beta^{44}X_0^{-1}) + Tr(\beta^{237}X_5^{-1}) + Tr(\beta^{72}X_{10}^{-1}) + Tr(\beta^{72}X_{15}^{-1}) + 0,\\
f_5 &= Tr(\beta^{72}X_0^{-1}) + Tr(\beta^{172}X_5^{-1}) + Tr(\beta^{76}X_{10}^{-1}) + Tr(\beta^{76}X_{15}^{-1}) + 1,\\
f_6 &= Tr(\beta^{76}X_0^{-1}) + Tr(\beta^{52}X_5^{-1}) + Tr(\beta^{51}X_{10}^{-1}) + Tr(\beta^{51}X_{15}^{-1}) + 1,\\
f_7 &= Tr(\beta^{51}X_0^{-1}) + Tr(\beta^{27}X_5^{-1}) + Tr(\beta^{26}X_{10}^{-1}) + Tr(\beta^{26}X_{15}^{-1}) + 0,
\end{aligned}
$$

$$
\begin{aligned}
f_{24} &= Tr(\beta^{166}X_0^{-1}) + Tr(\beta^{166}X_5^{-1}) + Tr(\beta^{26}X_{10}^{-1}) + Tr(\beta^{154}X_{15}^{-1}) + 1,\\
f_{25} &= Tr(\beta^{53}X_0^{-1}) + Tr(\beta^{53}X_5^{-1}) + Tr(\beta^{154}X_{10}^{-1}) + Tr(\beta^{100}X_{15}^{-1}) + 1,\\
f_{26} &= Tr(\beta^{36}X_0^{-1}) + Tr(\beta^{36}X_5^{-1}) + Tr(\beta^{53}X_{10}^{-1}) + Tr(\beta^{104}X_{15}^{-1}) + 0,\\
f_{27} &= Tr(\beta^{11}X_0^{-1}) + Tr(\beta^{11}X_5^{-1}) + Tr(\beta^{47}X_{10}^{-1}) + Tr(\beta^{236}X_{15}^{-1}) + 0,\\
f_{28} &= Tr(\beta^{72}X_0^{-1}) + Tr(\beta^{72}X_5^{-1}) + Tr(\beta^{44}X_{10}^{-1}) + Tr(\beta^{237}X_{15}^{-1}) + 0,\\
f_{29} &= Tr(\beta^{76}X_0^{-1}) + Tr(\beta^{76}X_5^{-1}) + Tr(\beta^{72}X_{10}^{-1}) + Tr(\beta^{172}X_{15}^{-1}) + 1,\\
f_{30} &= Tr(\beta^{51}X_0^{-1}) + Tr(\beta^{51}X_5^{-1}) + Tr(\beta^{76}X_{10}^{-1}) + Tr(\beta^{52}X_{15}^{-1}) + 1,\\
f_{31} &= Tr(\beta^{26}X_0^{-1}) + Tr(\beta^{26}X_5^{-1}) + Tr(\beta^{51}X_{10}^{-1}) + Tr(\beta^{27}X_{15}^{-1}) + 0,
\end{aligned}
$$

$$
\begin{aligned}
f_{120} &= Tr(\beta^{166}X_1^{-1}) + Tr(\beta^{166}X_6^{-1}) + Tr(\beta^{26}X_{11}^{-1}) + Tr(\beta^{154}X_{12}^{-1}) + 1,\\
f_{121} &= Tr(\beta^{53}X_1^{-1}) + Tr(\beta^{53}X_6^{-1}) + Tr(\beta^{154}X_{11}^{-1}) + Tr(\beta^{100}X_{12}^{-1}) + 1,\\
f_{122} &= Tr(\beta^{36}X_1^{-1}) + Tr(\beta^{36}X_6^{-1}) + Tr(\beta^{53}X_{11}^{-1}) + Tr(\beta^{104}X_{12}^{-1}) + 0,\\
f_{123} &= Tr(\beta^{11}X_1^{-1}) + Tr(\beta^{11}X_6^{-1}) + Tr(\beta^{47}X_{11}^{-1}) + Tr(\beta^{236}X_{12}^{-1}) + 0,\\
f_{124} &= Tr(\beta^{72}X_1^{-1}) + Tr(\beta^{72}X_6^{-1}) + Tr(\beta^{44}X_{11}^{-1}) + Tr(\beta^{237}X_{12}^{-1}) + 0,\\
f_{125} &= Tr(\beta^{76}X_1^{-1}) + Tr(\beta^{76}X_6^{-1}) + Tr(\beta^{72}X_{11}^{-1}) + Tr(\beta^{172}X_{12}^{-1}) + 1,\\
f_{126} &= Tr(\beta^{51}X_1^{-1}) + Tr(\beta^{51}X_6^{-1}) + Tr(\beta^{76}X_{11}^{-1}) + Tr(\beta^{52}X_{12}^{-1}) + 1,\\
f_{127} &= Tr(\beta^{26}X_1^{-1}) + Tr(\beta^{26}X_6^{-1}) + Tr(\beta^{51}X_{11}^{-1}) + Tr(\beta^{27}X_{12}^{-1}) + 0.
\end{aligned}
$$

A complete listing of the algebraic representation of the 128 output coordinates of the round function is given in [17].

Now we give an example for how to find the transformation matrix used to map one coordinate function to another.

Example 4. To transform the coordinate function

$$f_{31} = Tr(\beta^{26} X_0^{-1}) + Tr(\beta^{26} X_5^{-1}) + Tr(\beta^{51} X_{10}^{-1}) + Tr(\beta^{27} X_{15}^{-1})$$

into

$$f_0 = Tr(\beta^{26} X_0^{-1}) + Tr(\beta^{154} X_5^{-1}) + Tr(\beta^{166} X_{10}^{-1}) + Tr(\beta^{166} X_{15}^{-1}) + 1$$

we use the transformation

$$\begin{aligned}
&X_5 = x_0 + x_1\alpha + \cdots + x_7\alpha^7 \to \beta^{(26-154) \bmod 255} X_5 = \beta^{127} X_5,\\
&X_{10} = x_0' + x_1'\alpha + \cdots + x_7'\alpha^7 \to \beta^{(51-166) \bmod 255} X_{10} = \beta^{140} X_{10},\\
&X_{15} = x_0'' + x_1''\alpha + \cdots + x_7''\alpha^7 \to \beta^{(27-166) \bmod 255} X_{15} = \beta^{116} X_{15},
\end{aligned}$$

or equivalently

$$\begin{aligned}
x_0 + x_1\alpha + \cdots + x_7\alpha^7 \to\ & (x_1 + x_3 + x_5 + x_6 + x_7) + (x_1 + x_2 + x_3 + x_4 + x_5)\alpha\\
&+ (x_2 + x_3 + x_4 + x_5 + x_6)\alpha^2 + (x_1 + x_4)\alpha^3\\
&+ (x_1 + x_2 + x_3 + x_6 + x_7)\alpha^4\\
&+ (x_0 + x_2 + x_3 + x_4 + x_7)\alpha^5\\
&+ (x_1 + x_3 + x_4 + x_5)\alpha^6\\
&+ (x_0 + x_2 + x_4 + x_5 + x_6)\alpha^7,
\end{aligned}$$

$$\begin{aligned}
x_0' + x_1'\alpha + \cdots + x_7'\alpha^7 \to\ & (x_1' + x_2' + x_3' + x_4' + x_7') + (x_0' + x_2' + x_5' + x_7')\alpha\\
&+ (x_1' + x_2' + x_6')\alpha^2 + (x_0' + x_1' + x_4')\alpha^3\\
&+ (x_0' + x_3' + x_4' + x_5' + x_7')\alpha^4\\
&+ (x_0' + x_1' + x_4' + x_5' + x_6')\alpha^5\\
&+ (x_0' + x_1' + x_2' + x_5' + x_6' + x_7')\alpha^6\\
&+ (x_0' + x_1' + x_2' + x_3' + x_6' + x_7')\alpha^7,
\end{aligned}$$

$$\begin{aligned}
x_0'' + x_1''\alpha + \cdots + x_7''\alpha^7 \to\ & (x_0'' + x_1'' + x_5'' + x_7'') + (x_0'' + x_2'' + x_5'' + x_6'' + x_7'')\alpha\\
&+ (x_0'' + x_1'' + x_3'' + x_6'' + x_7'')\alpha^2 + (x_2'' + x_4'' + x_5'')\alpha^3\\
&+ (x_1'' + x_3'' + x_6'' + x_7'')\alpha^4 + (x_2'' + x_4'' + x_7'')\alpha^5\\
&+ (x_3'' + x_5'')\alpha^6 + (x_0'' + x_4'' + x_6'')\alpha^7.
\end{aligned}$$

The corresponding linear transformation matrix, A, is given in Appendix A. In this case, the affine constant is equal to 1.

It is clear that replacing the S-box with any other monomial over $GF(2^8)$ will not change the form of dependency of the output of the round function on its inputs because we still can represent the component functions of the S-box as $Tr(\theta x^d)$. For all these monomials, we will have similar expressions as in Example 3 except that the coefficients inside the trace terms will be different. Thus, a similar equivalence relation will still hold between the coordinates of the round function.

One should also note that, while the analysis above shows that any two of the coordinates of the AES round function can be mapped to one another using an affine transformation, this transformation is not unique for all pairs and hence some care should be exercised when interpreting the cryptanalytic implication of this result.

6. Conclusions

We showed that all the output coordinates of the AES round function are in the same affine equivalence class. Although we were not able to utilize this observation to attack the AES cipher, this observation may raise some concerns regarding the highly structured algebraic properties of the AES round function. The implication of this result on the cryptanalysis on the AES remains an open problem.

Appendix A. The matrix transformation for Example 4

$$A = \begin{bmatrix}
I & - & - & - & - & - & - & - & - & - & - & - & - & - & - & - \\
- & I & - & - & - & - & - & - & - & - & - & - & - & - & - & - \\
- & - & I & - & - & - & - & - & - & - & - & - & - & - & - & - \\
- & - & - & I & - & - & - & - & - & - & - & - & - & - & - & - \\
- & - & - & - & I & - & - & - & - & - & - & - & - & - & - & - \\
- & - & - & - & - & A_5 & - & - & - & - & - & - & - & - & - & - \\
- & - & - & - & - & - & I & - & - & - & - & - & - & - & - & - \\
- & - & - & - & - & - & - & I & - & - & - & - & - & - & - & - \\
- & - & - & - & - & - & - & - & I & - & - & - & - & - & - & - \\
- & - & - & - & - & - & - & - & - & I & - & - & - & - & - & - \\
- & - & - & - & - & - & - & - & - & - & A_{10} & - & - & - & - & - \\
- & - & - & - & - & - & - & - & - & - & - & I & - & - & - & - \\
- & - & - & - & - & - & - & - & - & - & - & - & I & - & - & - \\
- & - & - & - & - & - & - & - & - & - & - & - & - & I & - & - \\
- & - & - & - & - & - & - & - & - & - & - & - & - & - & I & - \\
- & - & - & - & - & - & - & - & - & - & - & - & - & - & - & A_{15}
\end{bmatrix},$$

where I denotes the 8×8 identity matrix and "$-$" denotes the zero matrix of the same dimension. A_5, A_{10} and A_{15} are given by

$$A_5 = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}, \quad A_{10} = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \end{bmatrix},$$

$$A_{15} = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}.$$

References

[1] E. Biham, A. Shamir, Differential cryptanalysis of DES-like cryptosystems, J. Cryptol. 4 (1) (1991) 3–72.

[2] J. Daemen, V. Rijmen, The block cipher Rijndael, Proceedings of the Third International Conference on Smart Card Research and Applications, CARDIS'98, Lecture Notes in Computer Science, vol. 1820, Springer, Berlin, 2000, pp. 277–284.

[3] J. Daemen, V. Rijmen, The Block Cipher Rijndael, Springer, Berlin, 2002, ISBN 3-540-42580-2.

[4] Federal Information Processing Standards Publication (FIPS 197), Advanced Encryption Standard (AES), 26 November 2001.

[5] N. Ferguson, R. Schroeppel, D. Whiting, A simple algebraic representation of Rijndael, Proceedings of the Eighth International Workshop on Selected Areas in Cryptography (SAC'2001), Lecture Notes in Computer Science, vol. 2259, Springer, Berlin, 2001, pp. 103–111.

[6] J. Fuller, W. Millan, Linear redundancy in S-boxes, Proceedings of the Fast Software Encryption (FSE 2003), Lecture Notes in Computer Science, vol. 2887, Springer, Berlin, 2003, pp. 74–86.

[7] S.W. Golomb, Shift Register Sequences, revised ed., Aegean Park Press, 1982.

[8] G. Gong, S.W. Golomb, Transform domain analysis of DES, IEEE Trans. Inform. Theory IT-45 (6) (1999) 2065–2073.

[9] T. Jakobsen, Cryptanalysis of block ciphers with probabilistic non-linear relations of low degree, Proceedings of Crypto'99, Lecture Notes in Computer Science, vol. 1462, 1999, pp. 213–222.

[10] T. Jakobsen, L. Knudsen, The interpolation attack on block ciphers, fast software encryption, Lecture Notes in Computer Science, vol. 1267, Springer, Berlin, 1997, 28–40.

[11] R. Lidl, H. Niederreiter, Finite Fields, Encyclopedia of Mathematics and its Applications, vol. 20, Addison-Wesley, Reading, MA, 1983.

[12] M. Matsui, Linear cryptanalysis method for DES cipher advances in cryptology, Proceedings of Eurocrypt'93, Lecture Notes in Computer Science, vol. 765, Springer, Berlin, 1994, pp. 386–397.

[13] R.J. McEliece, Finite fields for Computer Scientists and Engineers, Kluwer Academic Publishers, Dordrecht, 1987.

[14] S. Murphy, M.J.B. Robshaw, Essential algebraic structure within the AES, Proceedings of the Crypto 2002, Lecture Notes in Computer Science, vol. 2442, Springer, Berlin, 2002, pp. 1–16.

[15] K. Nyberg, Differentially Uniform Mappings for Cryptography, Proceedings of Eurocrypt'93, Lecture Notes in Computer Science, vol. 765, Springer, Berlin, 1994, pp. 55–64.
[16] A.M. Youssef, G. Gong, On the interpolation attacks on block ciphers, Proceedings of the Fast Software Encryption (FSE 2000), Lecture Notes in Computer Science, vol. 1339 , Springer, Berlin, 2000, pp. 109–120.
[17] A.M. Youssef, S.E. Tavares, On Some Algebraic Structures in the AES Round Function, Technical Report, Department of Electrical and Computer Engineering, Queen's University, Kingston, Ont., Canada, 2002. Also available at http://eprint.iacr.org.