The Secure DAES Design for Embedded System Application

Ming-Haw Jing[1], Jian-Hong Chen[1], Zih-Heng Chen[1], and Yaotsu Chang[1,2]

[1] Department of Information Engineering, I-Shou University,
Ta-Hsu, Kaohsiung 84001, Taiwan
mhjing@isu.edu.tw, d9503001@stmail.isu.edu.tw,
d9403001@stmail.isu.edu.tw
[2] Department of Applied Mathematics, I-Shou University,
Ta-Hsu, Kaohsiung 84001, Taiwan
ytchang@isu.edu.tw

Abstract. Recently, Advanced Encryption Standard (AES) has become one of the major symmetric encryption algorithms used in the embedded system applications. Many researches extended use of the algorithm of AES for system security. In this paper, we propose a diversified AES (DAES) to create more variations. In the architecture of the DAES, the diversity results from the modification of the parameters of DAES. In the process of system design, the additional parameters may not only cause operational complexity but also influence the security. In this article, a method to measure the security of DAES is also provided. We propose a strategy to optimize the design of the DAES with higher security from the scope of S-box via repeating property and MixColumn polynomials via branch number. During the analysis procedure, the size of embedded program may also be reduced.

Keywords: Advanced Encryption Standard, branch number, data security, embedded system, repeating property, symmetric encryption algorithms

1 Introduction

In regard to the security of the communication in embedded systems, Advanced Encryption Standard (AES) is the major symmetric encryption algorithm. In 2002, Barkan and Biham proposed a list of a total of 240 dual ciphers of AES which can be used to resist the side channel attacks [1]. Side channel attacks are effective only when a cracker knows the encryption algorithm. Because the dual cipher of AES increases variety in encryption, it raises the level of difficulty in cracking the key. Concerning the measurement of the security of symmetric cryptography, the delay time used to compute the key and S-box in AES is the major factor since the speed of system computation has been continuously improved. In the near future, the safety of AES will face the same tough challenge which can be found in the current circumstances in DES. For this reason, we proposed an extended AES with more variations, which is called Diversified AES (DAES) [2].

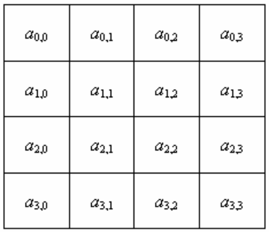
The architecture of DAES is based on the original AES, and the changes of parameters of DAES provide variations. DAES is able to provide higher security against the side channel attacks, and it even has the characteristics of defending unknown attacks in the future. As a result of many combinations of the parameters in DAES, there exist so many ways of implementations of DAES in software. Through the different parameters, DAES are in a huge variety, and these parameters are helpful for the key management in various data security applications. In the embedded system, the software optimization and security must be considered, especially in the applications of relatively large data processing to power-efficient sensors in embedded systems. The first important key factor of security of DAES is the SubBytes with the characteristic of its non-linear transformation. We discovered that the defect of S-box of AES can refer to the repeating property [3]. Another key factor of security is the branch number in the MixColumn operation. The branch number is in direct proportion to the confusion level in the MixColumn operation. According to the above two views of security of DAES, we proposed a method to determine the superior parameters with higher security.

The organization of this article is as follows: The mathematical background of this article and DAES architecture are described in Sect. 2. The properties of S-box and MixColumn polynomials are presented in Sect. 3. The analyses and statistical chart of security of DAES are discussed in Sect. 4. Finally, the brief conclusions are made in Sect. 5.

2 Preliminaries

We know that the cryptanalysis has many ways to attack cryptographic system in key management [4]. The human factors included cause even more problems. For example, the systems have been working for a long period or frequently running in real time with reduced complexity (such as using a simple hashing function to replace the non-linear part). The main reason is that these attacks focus on the keys. Therefore, the most serious problem is key loss due to weak protocol or internal break-in (like betrayer). As a result, the demand for a new cryptographic system rises, in order to prevent from causing an immediate risk of key loss. To meet this demand, extra parameter(s) should be added to the system other than the key without increasing system complexity. The DAES system actually has 4 parameters used in each round: (1) field irreducible polynomial; (2) the substitution through S-box of the SubBytes; (3) the shift in the SifhtRows; and (4) the polynomial $a(x)$ of the MixColumns. The main key and parameters can be negotiated by different channels between the encryption and decryption sides. This will increase the difficulty in gaining access to the information for attackers. Reference [2] also initiated the idea of using dual ciphers to create a Rijndael-like system. Next, the variations of these parameters will be introduced in particular using different irreducible polynomials.

We know that the computation in GF(2^8) is formed by taking polynomials over GF(2) modulo an irreducible polynomial $f(x)$. The multipliers and multiplicative inverse operations in GF(2^8) are affected by the irreducible polynomial. In AES, Rijndael uses



$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$
$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$
$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$
$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$

FIGURE 1: The state

the irreducible polynomial $f(x)=x^8+x^4+x^3+x+1$ to be a modular polynomial in GF(2^8). According to Rijndael's description: The polynomial $f(x)$ ('11B') for the multiplication in GF(2^8) is the first one in the list of irreducible polynomials of degree 8; the reason to choose this irreducible polynomial is that it's the first polynomial of the degree 8 listed in [5]. In fact, there exist 30 irreducible polynomials with degree 8 over GF(2). Each of them can serve as the irreducible polynomial to be used in a DAES system. With the cipher key, various irreducible polynomials may be regarded as an extra input or key of the DAES system and be helpful in the key management. In addition, two major factors which influence the security of DAES refer to the variations of S-box in the SubBytes, and polynomials in the MixColumns.

2.1 The S-box of SubBytes

In the SubBytes, the S-box applied on the input x is mapped to its multiplicative inverse x^{-1}, where $x \in \mathrm{GF}(2^8)$. The multiplicative inverse varies according to the different field polynomials. In DAES, the S-box is given by Eq. (1)

$$x' = Lx^{-1} + c\,,\ x^{-1} = L^{-1}(x' + c)\,, \tag{1}$$

in encryption and decryption, respectively, where L is one of the invertible 8x8 matrices over GF(2), L^{-1} is the inverse matrix of L, and c is a non-zero constant. According to Eq. (1), the various irreducible polynomial $f(x)$ produces different S-box in SubBytes of DAES.

2.2 The MixColumn polynomial

In MixColumn operation of the DAES system, they can be characterized by a pair of four-term polynomials $c(x)$ and $d(x)$ which are the inverses of each other when are modulo x^4+1, called the MixColumn and InvMixColumn polynomials, respectively. The operations of the AES algorithm are performed on a 4×4 array of bytes called the State and denoted by A, as shown in Fig. 1.

In the encryption process, the function of the MixColumn can be realized by the following steps: First, associate the first column of the State A with a four-term polynomial over GF(2^8); the first column of A gives $a_{0,0}x^3 + a_{1,0}x^2 + a_{2,0}x + a_{3,0}$. Secondly,

Table 1: Four Pairs of Invertible Polynomials

$c(x)$	$d(x)$
$\{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\}$	$\{0b\}x^3 + \{0d\}x^2 + \{09\}x + \{0e\}$
$\{01\}x^3 + \{01\}x^2 + \{02\}x + \{03\}$	$\{0e\}x^3 + \{0b\}x^2 + \{0d\}x + \{09\}$
$\{01\}x^3 + \{02\}x^2 + \{03\}x + \{01\}$	$\{09\}x^3 + \{0e\}x^2 + \{0b\}x + \{0d\}$
$\{02\}x^3 + \{03\}x^2 + \{01\}x + \{01\}$	$\{0d\}x^3 + \{09\}x^2 + \{0e\}x + \{0b\}$

multiply the obtained polynomial by the MixColumn polynomial $c(x)$ which is given by

$$c(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\} . \qquad (2)$$

Next, divide the product by the modulus polynomial $x^4 + 1$ to get a four-term polynomial. Finally, associate the resulting four-term polynomial with a vector and then replace the original first column of state *a* by this vector. Running the same procedures for every other column of the State matrix A gives a complete run of the MixColumn transformation. On the other hand, the procedures in the InvMixColumn transformation are almost the same as those in the MixColumn transformation. The only difference is that the resulting polynomial obtained from the first step is multiplied by $d(x)$ instead of by $c(x)$ in the second step, where $d(x)$ is used in the inverse polynomial of $c(x)$ and is given by

$$d(x) = \{0b\}x^3 + \{0d\}x^2 + \{09\}x + \{0e\} . \qquad (3)$$

In the following, a number of pairs of ($c(x)$, $d(x)$) are proposed as examples to replace the default pair of transformations in MixColumn and InvMixColumn, as shown in Table 1.

3 The Properties of Security

3.1 The Cyclic Groups in S-box

In this section, we focus on the repeating property of non-linear layer, SubBytes transformation of DAES. We know each byte in the information block is byte wise substituted by the SubByte using S-box. The influence of each SubByte can be regarded as a function. Combined functions can be denoted by $f^n(I) = f \circ f \circ \cdots \circ f(I)$, where *I* is the input value in the block. The period (the number of repetition) of *f*(*I*) is defined by $f^{period}(I) = I$.

In AES, every input byte of S-box returns to the initial value after *t* period of the substitution [3]; i.e., for any *i* of the S-box = *f*(*i*), $f^t(i) = i$. The 256 values of the input bytes can be classified into five small sets as in Table 2 according to the period *t*. The period of each set is 87, 81, 59, 27 and 2, respectively. Besides, the authors in [3] took the LCM (least common multiple) into consideration to calculate the maximal

Table 2: Classifying the substitution in the S-box of AES

Set 1 (t=87)																			
F2	89	A7	5C	4A	D6	F6	42	2C	71	A3	0A	67	85	97	88	C4	1C	9C	DE
1D	A4	49	3B	E2	98	46	5A	BE	AE	E4	69	F9	99	EE	28	34	18	AD	95
2A	E5	D9	35	96	90	60	D0	70	51	D1	3E	B2	37	9A	B8	6C	50	53	ED
55	FC	B0	E7	94	22	93	DC	86	44	1B	AF	79	B6	4E	2F	15	59	CB	1F
C0	BA	F4	BF	08	30	04													
Set 2 (t=81)																			
7C	10	CA	74	92	4F	84	5F	CF	8A	7E	F3	0D	D7	0E	AB	62	AA	AC	91
81	0C	FE	BB	EA	87	17	F0	8C	64	43	1A	A2	3A	80	CD	BD	7A	DA	57
5B	39	12	C9	DD	C1	78	BC	65	4D	E3	11	82	13	7D	FF	16	47	A0	E0
E1	F8	41	83	EC	CE	8B	3D	27	CC	4B	B3	6D	3C	EB	E9	1E	72	40	09
01																			
Set 3 (t=59)																			
00	63	FB	0F	76	38	07	C5	A6	24	36	05	6B	7F	D2	B5	D5	03	7B	21
FD	54	20	B7	A9	D3	66	33	C3	2E	31	C7	C6	B4	8D	5D	4C	29	A5	06
6F	A8	C2	25	3F	75	9D	5E	58	6A	02	77	F5	E6	8E	19	D4	48	52	
Set 4 (t=27)																			
EF	DF	9E	0B	2B	F1	A1	32	23	26	F7	68	45	6E	9F	DB	B9	56	B1	C8
E8	9B	14	FA	2D	D8	61													
Set 5 (t=2)																			
73	8F																		

period. The maximal period is in direct proportion to the security of S-box. In this case, the LCM is 277182.

In DAES, we try to change the parameters in S-box, but it may influence the maximal period in S-box. For example, we replace the nonzero constant 0x63 with the 0xE3. The components in this S-box are classified into 11 sets, of which the period is {103,63,44,27,7,3,3,2,2,1,1}. In this case, there are two elements whose period is one. Although the LCM in this case is 856548, which is more than that in AES (277182), this makes S-box have lower security. For this case, the elements whose period is one are 0x1C and 0x51; i.e., $f(0x1C)=0x1C$ and $f(0x51)=0x51$. Therefore, we can't evaluate the security by LCM. We provide a method to measure the security of DAES comparing with the AES using Eq. (4).

$$R_x = \frac{P_{\max}(DAES)}{P_{\max}(AES)}$$

$$P_{\max}(DAES) = \begin{cases} 0 \quad ,if\ there\ exists\ a\ element\ which\ period\ is\ 1 \\ the\ L.C.M\ of\ the\ set \qquad\qquad\qquad ,others \end{cases} \qquad \textbf{(4)}$$

$P_{\max}(AES) = 277182$.

According to the Eq. (4), the R_x of the DAES whose nonzero constant changes to 0xE3 is 0. There are many varieties of DAES, whose R_x is higher than that of AES. For instance, we replace the nonzero constant with 0x67. The set becomes {76,72,43,36,13,10,6} and P_{max}(DAES)=3823560, R_x=1379.44%. The elements of each set are listed in Table 3.

Table 3: List elements of sets when nenzero constant is changed to 0x67

Set 1 (t=76)																			
78	B8	68	41	87	13	79	B2	33	C7	C2	21	F9	9D	5A	BA	F0	88	C0	BE
AA	A8	C6	B0	E3	15	5D	48	56	B5	D1	3A	84	5B	3D	23	22	97	8C	60
D4	4C	2D	DC	82	17	F4	BB	EE	2C	75	99	EA	83	E8	9F	DF	9A	BC	61
EB	ED	51	D5	07	C1	7C	14	FE	BF	0C	FA	29	A1	36	01				
Set 2 (t=72)																			
73	8B	39	16	43	1E	76	3C	EF	DB	BD	7E	F7	6C	54	24	32	27	C8	EC
CA	70	55	F8	45	6A	06	68	7B	25	3B	E6	8A	7A	DE	19	D0	74	96	94
26	F3	09	05	6F	AC	95	2E	35	92	4B	B7	AD	91	85	93	DB	65	49	3F
71	A7	58	6E	9B	10	CE	8F	77	F1	A5	02								
Set 3 (t=43)																			
F6	46	5E	5C	4E	2B	F5	E2	9C	DA	53	E9	1A	A6	20	B3	69	FD	50	57
5F	CB	1B	AB	66	37	9E	0F	72	44	1F	C4	18	A9	D7	0A	63	FF	12	CD
B9	52	04																	
Set 4 (t=36)																			
2F	11	86	40	0D	D3	62	AE	E0	E5	DD	C5	A2	3E	B6	4A	D2	B1	CC	4F
80	C9	D9	31	C3	2A	E1	FC	B4	89	A3	0E	AF	7D	FB	0B				
Set 5 (t=13)																			
7F	D6	F2	8D	59	CF	8E	1D	A0	E4	6D	38	03							
Set 6 (t=10)																			
67	81	08	34	1C	98	42	28	30	00										
Set 7 (t=6)																			
A4	4D	E7	90	64	47														

3.2 Branch Number in MixColumn

Daemen and Rijmen [6] proposed a definition of branch number to evaluate the security of MixColumn for the suitable choice of the coefficients. In this section, we also use this idea to evaluate the security of all the MixColumn polynomials of DAES. We first give a brief review of the branch number [6]. Let *F* be a linear transformation acting on byte vectors and let the byte weight *W*(*a*) of state *a* be the total number of nonzero bytes in state *a*. The diffusion power of a linear transformation can be quantified and measured by the following definition:

Definition 1. The branch number of a linear transformation *F* is

$$\min_{a\neq 0}(W(a)+W(F(a))) . \qquad \textbf{(5)}$$

Here, a nonzero byte in the state *a* is called an active byte. A state consists of four columns. Each column has four entries. In a byte-weight-one state, there is only one nonzero entry among the 16 entries; i.e., there is only one nonzero column whose byte weight is one. For MixColumn, there are 4 active bytes in the output of state *a*, as MixColumn acts on the columns independently. Hence, the upper bound for the branch number is 5. If the branch number is 5, a difference in 1 input (or output) byte propagates to all 4 output (or input) bytes, a 2-byte input (or output) difference to at least 3 output (or input) bytes. Therefore, the sum of byte weights of the two states, before MixColumn operation and after MixColumn operation, is 5 at least.

Table 4: The three pairs of invertible polynomials

$c(x)$	$d(x)$
$\{03\}x^3+\{01\}x^2+\{01\}x+\{02\}$	$\{0b\}x^3+\{0d\}x^2+\{09\}x+\{0e\}$
$\{01\}x^3+\{01\}x^2+\{02\}x+\{03\}$	$\{0e\}x^3+\{0b\}x^2+\{0d\}x+\{09\}$
$\{01\}x^3+\{02\}x^2+\{03\}x+\{01\}$	$\{09\}x^3+\{0e\}x^2+\{0b\}x+\{0d\}$
$\{02\}x^3+\{03\}x^2+\{01\}x+\{01\}$	$\{0d\}x^3+\{09\}x^2+\{0e\}x+\{0b\}$

Table 5: The four examples of type 1 polynomials

$b(x)$
$\{01\}x^3+\{02\}x^2+\{01\}x+\{03\}$
$\{05\}x^3+\{0e\}x^2+\{05\}x+\{0f\}$
$\{09\}x^3+\{0a\}x^2+\{09\}x+\{0b\}$
$\{0c\}x^3+\{04\}x^2+\{0c\}x+\{05\}$

In DAES, the branch number of c(x) of MixColumn may be considered necessary. From our analysis, there exist many parameters with branch number being 5. Next, we propose a solution to find the polynomial used in MixColumn with branch number 5.

3.2.1 Property of MixColumn Polynomials

There are three properties of the MixColumn and InvMixColumn polynomials, and these properties will be useful in the security of implementation of the DAES in embedded software. First, each pair of invertible polynomials $c(x)$ and $d(x)$ mentioned above can be used to produce three more pairs of four-term invertible polynomials. Before we state Property 1, we give a new notation: If c, d are vectors, let $c_{(k)}$ be the k-fold left-cyclic-shift of c and $d_{(-k)}$ be the k-fold right-cyclic-shift of d.

Properties 1. $d_{(-1)}(x)=c_{(1)}^{-1}(x)$, $d_{(-2)}(x)=c_{(2)}^{-1}(x)$, and $d_{(-3)}(x)=c_{(3)}^{-1}(x)$.

The three pairs of invertible polynomials promised by the Property 1 are shown in Table 4.

Next, in some special cases, the MixColumn and InvMixColumn polynomials are the same. Property 2 serves as a sufficient condition for this kind of polynomial.

Properties 2. Let $c(x)$ be a four-term polynomial. If $c_1=c_3$, and $c_0+c_2=\{01\}$, then $c^{-1}(x)=c(x)$. Polynomials that satisfy this property are called Type 1 polynomial. Table 5 shows four examples of type 1 polynomials.

Combining the above two properties, one can easily observe the following property.

Table 6: The four examples of type 2 polynomials

$c(x)$
$\{02\}x^3+\{01\}x^2+\{03\}x+\{01\}$
$\{0e\}x^3+\{05\}x^2+\{0f\}x+\{05\}$
$\{0a\}x^3+\{09\}x^2+\{0b\}x+\{09\}$
$\{04\}x^3+\{0c\}x^2+\{05\}x+\{0c\}$

Table 7: The type 3 polynomials generator table I

$\{\{01\}x^3+\{02\}x,\{0e\}x^3+\{0d\}x\}$	$\{\{01\}x^2+\{03\},\{0b\}x^2+\{09\}\}$
$\{\{02\}x^3+\{01\}x,\{0d\}x^3+\{0e\}x\}$	$\{\{03\}x^2+\{01\},\{09\}x^2+\{0b\}\}$
$\{\{04\}x^3+\{07\}x,\{0b\}x^3+\{08\}x\}$	$\{\{04\}x^2+\{06\},\{0e\}x^2+\{0c\}\}$
$\{\{05\}x^3+\{06\}x,\{0a\}x^3+\{09\}x\}$	$\{\{05\}x^2+\{07\},\{0f\}x^2+\{0d\}\}$
$\{\{06\}x^3+\{05\}x,\{09\}x^3+\{0a\}x\}$	$\{\{06\}x^2+\{04\},\{0c\}x^2+\{0e\}\}$
$\{\{07\}x^3+\{04\}x,\{08\}x^3+\{0b\}x\}$	$\{\{07\}x^2+\{05\},\{0d\}x^2+\{0f\}\}$

Table 8: The type 3 polynomials generator table II

$\{\{01\}x^3+\{03\}x,\{09\}x^3+\{0b\}x\}$	$\{\{01\}x^2+\{02\},\{0d\}x^2+\{0e\}\}$
$\{\{03\}x^3+\{01\}x,\{0b\}x^3+\{09\}x\}$	$\{\{02\}x^2+\{01\},\{0e\}x^2+\{0d\}\}$
$\{\{04\}x^3+\{06\}x,\{0c\}x^3+\{0e\}x\}$	$\{\{04\}x^2+\{07\},\{08\}x^2+\{0b\}\}$
$\{\{05\}x^3+\{07\}x,\{0d\}x^3+\{0f\}x\}$	$\{\{05\}x^2+\{06\},\{09\}x^2+\{0a\}\}$
$\{\{06\}x^3+\{04\}x,\{0e\}x^3+\{0c\}x\}$	$\{\{06\}x^2+\{05\},\{0a\}x^2+\{09\}\}$
$\{\{07\}x^3+\{05\}x,\{0f\}x^3+\{0d\}x\}$	$\{\{07\}x^2+\{04\},\{0b\}x^2+\{08\}\}$

Properties 3. Let $c(x)=(c_3,c_2,c_1,c_0)$ be a four-term polynomial. If $c_0=c_2$, and $c_1+c_3=\{01\}$, then $c^{-1}(x)=(c_1,c_2,c_3,c_0)$. Polynomials of this kind are called Type 2 polynomial.

For example, if $c(x)=\{02\}x^3+\{01\}x^2+\{03\}x+\{01\}$, we can get $d(x)=\{03\}x^3+\{01\}x^2+\{02\}x+\{01\}$. Table 6 shows four examples of type 2 polynomials that belong to this class.

Besides the Type 1 and 2 polynomials explained above, the rest of the four-term polynomials are categorized into Type 3. After an exhausting search, we found that all the Type 3 polynomial pairs can be produced by the following steps: Pick up any pair of polynomials from the six pairs of polynomials in the left column of Table 7 (resp. Table 8), and then add these two polynomials to any pair of polynomials from the six pairs of polynomials in the right column of Table 7 (resp. Table 8). The two polynomials obtained will be a Type 3 polynomial pair.

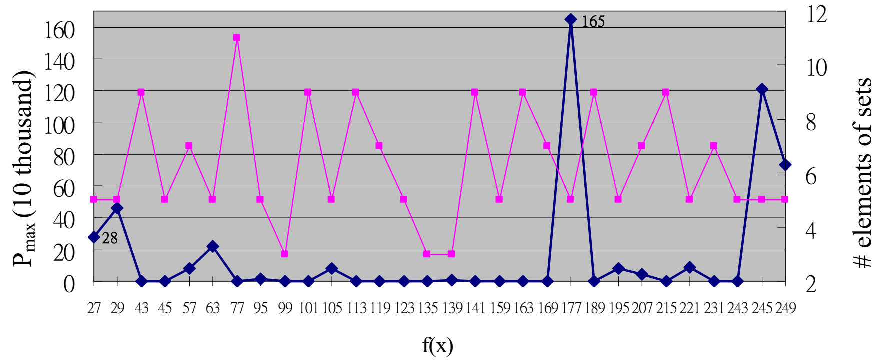


FIGURE 2: The statistic for Pmax v.s. F(x)

For example, taking row 3 from the left column of Table 7 and row 1 in the right column, two polynomial pairs will be obtained, namely, ($\{04\}x^3+\{01\}x^2+\{07\}x+\{03\}$, $\{0b\}x^3+\{0b\}x^2+\{08\}x+\{09\}$) and ($\{04\}x^3+\{01\}x^2+\{07\}x+\{03\}$, $\{0b\}x^3+\{0b\}x^2+\{08\}x+\{09\}$). Obviously, both of them are Type 3 polynomial pairs.

4 System Analysis

4.1 Statistic of S-box in DAES

The secure measurement is considerable in the S-box because the S-box is the only non-linear layer transformation in DAES algorithm. We have mentioned in Eq. (4) of the use of the LCM to measure the maximum period that is called P_{max}. It is in direct proportion to the security of S-box. We gather the data of S-box with different *f*(*x*) via simulation software and draw the line chart as Fig. 2. The *x* coordinate axis is *f*(*x*) with decimal representation. The left Y coordinate axis is the P_{max}, whose unit is ten thousand. The right Y coordinate axis is the count of each small group. We have made the following inference:

1. The P_{max} is 1,648,200 while *f*(*x*) is $x^8+x^7+x^5+x^4+1=0$; the representation in decimal without x^8 is 177. It is about 5.95 times more than AES, whose P_{max} is 277,182 with the *f*(*x*) is $x^8+x^4+x^3+x^1+1=0$; the representation in decimal is 27.
2. There exist 16 items whose P_{max} is 0; that is to say, the *f*(*x*) has a great influence on P_{max}.
3. The count of small sets is not in direct proportion to the P_{max}.

4.2 Branch number of MixColumns in DAES

Therefore, after applying the MixColumn, the output of a byte-weight-one state has a byte weight of at most 4 because the MixColumn acts on the columns independently. Hence, the upper bound for the branch number is 5. Therefore, the sum of byte weights of the two States, before MixColumn operation and after MixColumn operation, is at least 5. It is obvious that {00} is invalid. After an exhausting calculation, the branch number of all the Type 3 polynomials mentioned in Section 3 is at least 5. However, in the case of Type 1 and Type 2 polynomials, a byte-weight-two input may produce a byte-weight-two output whose branch number equals 4.

In system design, the complexity of embedded software design using Type 3 polynomials may be reduced, and the security of such software is better than that of the software using Type 1 and Type 2. As a result, type 3 polynomial is considered and analyzed.

5 Conclusions

In this article, we present a way of measurement to design the S-box and MixColumns in DAES, which is related to the embedded data security application. We have proposed approaches to find the specific parameters with better abilities to defend various attacks in the DAES systems. The abilities regarding S-box or MixColumns include the maximum period P_{max} and branch number, respectively. As a result, choosing $f(x) = x^8 + x^7 + x^5 + x^4 + 1$ as the module polynomial and MixColumns polynomials in type 3 has better code efficiency with higher security in DAES.

Acknowledgements. This work is supported in part by the Nation Science Council, Taiwan, under grant NSC 96-2623-7-214-001-D.

References

1. Barkan, E. and Biham, E.: In How Many Ways Can You Write Rijndael?, LNCS 2501 (2002) 160–175
2. Jing, M.H., Chen, Z.H., Chen, J.H., Chen, Y.H.: Reconfigurable System for High-Speed and Diversified AES using FPGA, Microprocessors & Microsystems, Vol. 31 (2007) 94–102
3. Song, B. and Seberry, J.: Further Observations on the Structure of the AES Algorithm. LNCS 2887 (2003) 223–234
4. Dobbertin, H., Knudsen, L., Robshaw, M.: The Cryptanalysis of the AES - a Brief Survey, LNCS 3373 (2005) 1–10
5. Lidl, R. and Niederreiter, H.: Introduction to Finite Fields and Their Applications, Cambridge University Press (1986)
6. Daemen, J. and Rijmen, V.: The Rijndael Block Cipher (1999)