Understanding Two-Round Differentials in AES*

Joan Daemen[1] and Vincent Rijmen[2,3]

[1] STMicroelectronics Belgium
joan.daemen@st.com
[2] IAIK, Graz University of Technology
vincent.rijmen@iaik.tugraz.at
[3] Cryptomathic A/S

Abstract. In this paper we study the probability of differentials and characteristics over 2 rounds of the AES with the objective to understand how the components of the AES round transformation interact in this respect. We extend and correct the analysis of the differential properties of the multiplicative inverse in GF(2^n) given in [9]. We study the number of characteristics with EDP > 0 whose probability adds up to the probability of a differential and derive formulas that allow to produce a close estimate of this number for any differential. We use the properties discovered in our study to explain the differentials with the maximum EDP values and describe the impact of the linear transformation in the AES S-box in this respect.

1 Introduction

In this paper we study the probability of differentials and characteristics [1,6] over 2 rounds of the AES where the difference is the bitwise XOR. Bounds on the expected differential probability (EDP) of characteristics were proven in the design documentation of Rijndael [2]. Bounds on the EDP of differentials have been investigated in [3,10,11].

We investigated differential propagation in AES, with the objective to understand how the components of the AES interact. We explain observed EDP values, including the maximum over 2 rounds. The EDP value of differentials is important in the resistance against differential cryptanalysis. In general, the EDP of differentials over multiple rounds of AES is difficult to compute. In this paper we have thoroughly investigated the distribution of the EDP of differentials over two rounds of AES, rather than focusing on upper bounds. As far as we know, this is the first paper that studies the distribution of EDP values in AES. We believe the results of this paper can be used to obtain tighter bounds for the EDP over 4 rounds of AES and generally a better understanding of its distribution.

* The work described in this paper has been partly supported by the European Commission under contract IST-2002-507932 (ECRYPT). The information in this paper is provided as is, and no warranty is given or implied that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

R. De Prisco and M. Yung (Eds.): SCN 2006, LNCS 4116, pp. 78–94, 2006.

In Section 3, we extend and correct the analysis of the differential properties of the multiplicative inverse in GF(2^n) given in [9]. In Section 4 we introduce the concept of bundles, which are classes of related characteristics contributing to the same differential. In Section 5 we study the conditions characteristics must satisfy to have a non-zero EDP. In Section 6 and Section 7 we study the EDP of bundles, which leads in Section 8 to results on the EDP of differentials. We discuss the maximum EDP value of [4] in the light of our results in Section 9 and conclude in Section 10. But first we briefly introduce some new terminology and define notations.

2 AES and Differential Cryptanalysis Basics

2.1 Differentials, Characteristics and Trails

We denote a differential over an arbitrary map by (a, b) and assume that it is clear from the context which map we mean. We call a the input difference and b the output difference. The probability of a differential is denoted by $\mathrm{DP}(a, b)$. We define the expected differential probability (EDP) of a differential over a keyed map as the average of the differential probability $\mathrm{DP}(a, b)$ over all keys. Let $B[k]$ denote a keyed function consisting of a sequence of R transformations $\rho^i[k]$:

$$B[k](x) = (\rho^R[k] \circ \cdots \circ \rho^2[k] \circ \rho^1[k])(x), \tag{1}$$

Then we define a differential trail as follows:

Definition 1. *A* differential trail *through B is a sequence of differences a, b, c, $\ldots$, z such that there are pairs $\{x, x \oplus a\}$ and keys such that*

$$\begin{aligned} \rho^1[k](x) + \rho^1[k](x+a) &= b \\ (\rho^2[k] \circ \rho^1[k])(x) + (\rho^2[k] \circ \rho^1[k])(x+a) &= c \\ &\cdots \\ B[k](x) + B[k](x+a) &= z. \end{aligned}$$

Hence, a differential trail Q is a characteristic with non-zero expected differential probability: $\mathrm{EDP}(Q) > 0$. For Markov ciphers, the EDP of a trail Q is the product of the DP of its S-boxes [6]. A trail $Q = (a, b, \ldots, e)$ is *in* a differential (f, g) if $a = f$ and $e = g$. We denote the number of trails in a differential (a, e) by $\mathrm{N_t}(a, e)$. The EDP of a differential is the sum of the the EDP values of all the trails in that differential

$$\mathrm{EDP}(a, e) = \sum_{Q \text{ in } (a,e)} \mathrm{EDP}(Q) \ . \tag{2}$$

2.2 The AES Super Box

The AES S-box operates on GF(2^8) and can be described as

$$S[x] = L^{-1}(x^{-1}) + q, \tag{3}$$

Here x^{-1} denotes the multiplicative inverse of x in GF(2^8), extended with 0 being mapped to 0. L is a linear transformation over GF(2) and q a constant. Note that L is not linear over GF(2^8) and can be expressed as a so-called *linearized polynomial* [7]. The additive group of the finite field GF(2^8) forms a vector space. In the remainder of this paper, we will sometimes tacitly switch from one representation to another.

For reasons of clarity, we introduce the structure of the (*AES*) *super box* (our notation). The differential probabilities over this structure are equivalent to those over 2 AES rounds. The AES super box maps a 4-byte array $a = [a_0, a_1, a_2, a_3]$ to a 4-byte array e and takes a 4-byte key k. It consists of the sequence of four transformations:

SubBytes $b_i = S[a_i]$ with S the AES S-box
MixColumns $c = \mathrm{M_c} b$ with $\mathrm{M_c}$ a 4×4 matrix
AddRoundKey $d = c \oplus k$ with k the round key
SubBytes $e_i = S[d_i]$

If we consider two AES rounds, swap the steps ShiftRows and SubBytes in the first round, and remove the linear transformations before the first SubBytes transformation and after the second SubBytes transformation, then we obtain a map that can also be described as 4 parallel instances of the AES super box.

We can partition the set of 4-byte vectors by considering *truncated* differences [5]. All vectors in a given equivalence class have zeroes in the same byte positions and non-zero values in the other byte positions. An equivalence class is characterized by an *activity pattern.* The activity pattern has a single bit for each byte position indicating whether its value must be 0 (passive) or not (active). The activity pattern of a differential (a, e) is the couple of the activity patterns of a and e. We say that two differences are *compatible* if they have the same activity pattern. Due to the diffusion properties of $\mathrm{M_c}$, activity patterns of differentials must have a minimum of 5 active positions. In total there are 93 such activity patterns.

A characteristic through the AES super box consists of a sequence of 5 differences: a, b, c, d and e. Since the AES S-box is invertible, EDP(a, b) over SubBytes can be non-zero only if a and b are compatible. Other necessary conditions to have EDP > 0 are $c = d$, $d = \mathrm{M_c} b$, and d has to be compatible with e. In the remaining of this paper we only consider characteristics that satisfy these conditions (and we will omit c from the notation). Such a characteristic is fully determined by the differential (a, e) it is in and the intermediate difference b. We call b_i and d_i corresponding with active S-boxes the *inner differences* of a characteristic. We make the distinction between trails and characteristics because the number of trails in a differential is closely related to its EDP.

3 The Multiplicative Inverse in GF(2^n)

In this section we discuss the differential properties of the single component in AES that is non-linear over GF(2): the multiplicative inverse in GF(2^n), extended with 0 being mapped to 0. In fact this is the operation of raising to the power $2^n - 2$. For readability we use the notation x^{-1} rather than x^{2^n-2}. Hence we adopt the convention that $0^{-1} = 0$. Differential properties of this map were previously already studied in [9]. In the following, a and b denote arbitrary non-zero differences. We need the *trace map* defined over a finite field $\mathrm{GF}(p^n)$ with respect to $\mathrm{GF}(p)$, denoted by $\mathrm{Tr}(x)$:

$$\mathrm{Tr}(x) = \sum_{i=0}^{n-1} x^{p^i} \tag{4}$$

Note that the trace map is linear over $\mathrm{GF}(p)$ and that $\mathrm{Tr}(x^{p^i}) = \mathrm{Tr}(x)$ for any value of i. The differential (a, b) over the multiplicative inverse map has $\mathrm{DP}(a, b) > 0$ if and only if the equation

$$(x + a)^{-1} + x^{-1} = b \tag{5}$$

has solutions. If $x = a$ or $x = 0$ is a solution of (5), we have $b = a^{-1}$ and both are solutions. Otherwise, $x = a$ or $x = 0$ is not a solution, we can transform (5) by multiplying with $b^{-1}x(x + a)$ yielding:

$$x^2 + ax + ab^{-1} = 0,$$

if we substitute x by $a^{-1}y$, this becomes:

$$y^2 + y + (ab)^{-1} = 0, \tag{6}$$

To investigate the condition for this equation to have solutions we have the following lemma:

Lemma 1 ([7, Theorem 2.25]). *$Tr(t) = 0$ iff $t = z^p - z$ for some $z \in GF(p^n)$.*

If we take $p = 2$, from this follows easily that:

Lemma 2. *For $b \neq a^{-1}$, equation (5) has 2 solutions if $Tr((ab)^{-1}) = 0$, and zero solutions otherwise.*

Consider now the case $b = a^{-1}$. Let ν and ν^2 denote the elements of $\mathrm{GF}(2^n)$ of order 3. Then $\nu^2 + \nu = 1$ and $\mathrm{GF}(2^2) = \{0, 1, \nu, \nu^2\}$. We present now the following new result:

Lemma 3. *For even n, the solutions of*

$$(x + a)^{-1} + x^{-1} = a^{-1} \tag{7}$$

form the set $T_a = \{0, a, \nu a, \nu^2 a\}$.

Proof. $x = a$ and $x = 0$ are solutions of (7). Assume there are other solutions. We can write such a solution as a product of a with an element z different from 0 or 1. We have

$$(za + a)^{-1} + (za)^{-1} = a^{-1} \ . \tag{8}$$

Or, equivalently,

$$(z+1)^{-1} + z^{-1} = 1 \; . \tag{9}$$

Multiplication with $z(z+1)$ yields:

$$z^2 + z + 1 = 0 \; . \tag{10}$$

According to Lemma 1, Equation (10) has two solutions iff $\mathrm{Tr}(1) = 0$ and none otherwise. $\mathrm{Tr}(1) = 0$ iff n is even. Since a solution of (10) satisfies $z^3 = 1$, its solutions are the two elements of $\mathrm{GF}(2^n)$ of order three. □

Note that the description of the solutions given in [9]: $T_a = \{0, a, a^{1+d}, a^{1+2d}\}$ with $d = (2^n - 1)/3$ is only correct if $a^d \neq 1$, i.e. if the order of a does not divide $(2^n - 1)/3$. From these lemmas follow several corollaries.

Corollary 1 ([9]). *For odd n,*

$$(x+a)^{-1} + x^{-1} = a^{-1}$$

has two solutions: 0 and a.

Corollary 2. *For even n, the possible output differences b for a given input difference a are those with $Tr((ab)^{-1}) = 0$ except $b = 0$. For odd n, the possible output differences b for a given input difference a are those with $Tr((ab)^{-1}) = 0$ except $b = 0$ and extended with $b = a^{-1}$.*

Together with the fact that (5) has 4 solutions only if $b = a^{-1}$, this leads to the following corollary:

Corollary 3. *For all non-zero $c \in GF(2^n)$ and for all positive integers t:*

$$DP(a,b) = DP(b,a) = DP(ca, bc^{-1}) = DP(a^{2^t}, b^{2^t}),$$

4 Bundles

For the EDP of a differential over the AES super box, we have:

$$\mathrm{EDP}(a,e) = \sum \mathrm{EDP}(a,b,\mathrm{M_c}e) = \sum_b \mathrm{EDP}_S(a,b)\mathrm{EDP}_S(\mathrm{M_c}b,e) \; . \tag{11}$$

with $\mathrm{EDP}_S(x,y)$ the EDP of a differential (x,y) over SubBytes. In order to compute the EDP of a differential, we first determine the number of trails in the differential. The number of trails is determined by means of *bundles*, which we define below. We start with an example.

Example 1. Consider the characteristics in a differential (a,e) with $a = [a_0, 0, 0, 0]$. Then clearly we must have $b = [b_0, 0, 0, 0]$ and thanks to MixColumns we have $d_0 = 2b_0$, $d_1 = b_0$, $d_2 = b_0$ and $d_3 = 3b_0$, or equivalently $d = b_0[2,1,1,3]$, where $b_0[2,1,1,3]$ denotes the scalar multiplication of the vector $[2,1,1,3]$ with the (non-zero) scalar b_0. There are 255 characteristics in the differential, one for each nonzero value of b_0.

This can be generalized to any AES super box differential with 5 active S-boxes. If $Q = (a, b, d, e)$ and $Q' = (a, b', d', e)$ are two trails of the same differential with 5 active S-boxes, then there exists a γ such that $b_i = \gamma b'_i$, and $d_i = \gamma d'_i$, and b, b'.

We define a *bundle* as follows.

Definition 2. *The* bundle $B(u^{\mathrm{b}})$ *associated with the vector* u^{b}*, is the set of 255 vectors defined as follows:*

$$B(u^{\mathrm{b}}) = \{\gamma u^{\mathrm{b}} | \gamma \in GF(2^8) \text{ and } \gamma \neq 0\} \ .$$

Scalar multiplication doesn't change the activity pattern of a vector. Furthermore, the linearity of MixColumns over GF(2^8) implies that $\mathrm{M_c}(\gamma b) = \gamma(\mathrm{M_c} b)$. Hence also the activity pattern of $u^{\mathrm{d}} = \mathrm{M_c} u^{\mathrm{b}}$ is the same for all vectors u^{b} of a bundle. If $(a, u^{\mathrm{b}}, u^{\mathrm{d}}, e)$ is a characteristic through the AES super box, then $(a, b, \mathrm{M_c} b, e)$ is a characteristic through the AES super box $\forall b \in B(u^{\mathrm{b}})$. Hence, the set of characteristics in (a, e) can be partitioned into a number of classes. Each class contains the 255 characteristics $(a, b, \mathrm{M_c} b, e)$ defined by keeping a, e constant and varying b over all the values of a bundle $B(u^{\mathrm{b}})$. In the following, we use 'bundle' also to refer to such a class of characteristics. A characteristic in the bundle $B(u^{\mathrm{b}})$ of the differential (a, e) is uniquely identified by the value of γ.

We can count the number of trails in (a, e) by counting the number of trails in each bundle and adding the results. In the following, we will explain how the number of trails in a bundle can be counted. As explained in Example 1, a differential with 5 active S-boxes only has a single bundle of characteristics. Table 1 lists the activity patterns with 5 active S-boxes and the corresponding

Table 1. Activity patterns with 5 active S-boxes and the corresponding values of $(u^{\mathrm{b}}, u^{\mathrm{d}})$ (in hexadecimal notation)

Activity Pattern	u^{b}	u^{d}
(1000;1111)	[1,0,0,0]	[2,1,1,3]
(1100;1110)	[1,3,0,0]	[7,7,2,0]
(1100;1101)	[1,1,0,0]	[1,3,0,2]
(1100;1011)	[2,1,0,0]	[7,0,3,7]
(1100;0111)	[3,2,0,0]	[0,7,1,7]
(1010;1110)	[1,0,3,0]	[1,4,7,0]
(1010;0111)	[1,0,2,0]	[0,7,5,1]
(1110;1010)	[1,4,7,0]	[9,0,B,0]
(0111;1010)	[0,7,5,1]	[D,0,E,0]
(1110;1100)	[3,7,2,0]	[D,B,0,0]
(1101;1100)	[1,7,0,2]	[9,D,0,0]
(1011;1100)	[1,0,1,1]	[2,3,0,0]
(0111;1100)	[0,7,1,3]	[B,E,0,0]
(1111;1000)	[E,9,D,B]	[1,0,0,0]

values of $(u^{\mathrm{b}}, u^{\mathrm{d}})$. In total there are 56 patterns. They can be derived by rotation of the 14 patterns listed.

For the bundles of a differential with 6 active positions, the u^{b} values can be found by taking (almost) all possible combinations of two u^{b} values of bundles with 5 active positions. For example, for activity pattern (1110; 1110) we combine the bundles for (1010; 1110) and (0110; 1110) as given by Table 1. This gives $u^{\mathrm{b}} = [1, 0, 3, 0] + z[0, 1, 1, 0] = [1, z, 3 + z, 0]$ and $u^{\mathrm{d}} = [1, 4, 7, 0] + z[2, 1, 3, 0] = [1 + 2z, 4 + z, 7 + 3z, 0]$.

This results in 255 different bundles, one for each nonzero value of z. However, for $u^{\mathrm{b}}, u^{\mathrm{d}}$ to have activity pattern (1110; 1110) the value of z must be different from 3, 1/2, 4 and 7/3, where x/y denotes $x.y^{-1}$ in GF(2^8). Hence, a differential with 6 active S-boxes has 251 bundles. We derive the number of bundles for differentials with 7 or 8 active S-boxes in Appendix A.

5 Differentials over SubBytes with EDP > 0

A characteristic $(a, b, \mathrm{M_c}b, e)$ is a trail if both differentials (a, b) and $(\mathrm{M_c}b, e)$ are differentials with EDP > 0. We will now study the conditions this imposes on the trails within a bundle.

5.1 Sharp Conditions

Consider differentials over four parallel applications of the multiplicative inverse in GF(2^8). We have from Corollary 2:

$$\mathrm{EDP}(x, y) > 0 \Leftrightarrow \begin{cases} \mathrm{Tr}((x_i y_i)^{-1}) = 0 \\ x_i \neq 0 \text{ iff } y_i \neq 0 \end{cases}, \ 0 \leq i < 4, \tag{12}$$

Since the trace map is linear over GF(2), the solution space of $\mathrm{Tr}(y_0^{-1}v) = 0$ is a vector space of dimension 7 over GF(2). The intersection of $\mathrm{Tr}(y_0^{-1}v) = 0$ and $\mathrm{Tr}(y_1^{-1}v) = 0$ is a vector space of dimension 6 or 7. If the dimension is 7, this implies $y_0 = y_1$. In general, the dimension of the intersection of a system of equations $\mathrm{Tr}(y_j^{-1}v) = 0$ is equal to 8 minus the dimension of the vector space generated by the elements y_j^{-1}. For example, the solution space of $\mathrm{Tr}(y_0^{-1}v) = \mathrm{Tr}(y_1^{-1}v) = \mathrm{Tr}(y_2^{-1}v) = 0$ with $y_0 \neq y_1 \neq y_2 \neq y_0$ has dimension 6 if $y_2 = y_0 + y_1$ and dimension 5 otherwise.

Consider now a bundle $B(u)$ with u compatible with y. The number of vectors x in B with $\mathrm{EDP}(x, y) > 0$ equals the number of non-zero values γ for which

$$\mathrm{Tr}((\gamma u_i y_i)^{-1}) = 0 \ , \ 0 \leq i < 4 \ . \tag{13}$$

This can also be written as:

$$\mathrm{Tr}((u_i y_i)^{-1} \gamma^{-1}) = 0 \ , \ 0 \leq i < 4 \ . \tag{14}$$

The γ^{-1} values satisfying these four conditions form the vector space orthogonal to the vector space generated by the set

$$\mathrm{V}_i = \{(u_0 y_0)^{-1}, (u_1 y_1)^{-1}, (u_2 y_2)^{-1}, (u_3 y_3)^{-1}\} \ . \tag{15}$$

The number of non-zero solutions equals $2^{8-\alpha} - 1$, where α is the dimension of V_i. Hence, in one bundle, there can be 127, 63, 31 or 15 vectors x with $\mathrm{EDP}(x, y) > 0$. Exactly the same analysis can be performed when x is fixed and we want to determine the number of y values in a bundle with $\mathrm{EDP}(x, y) > 0$. We call (14) the *sharp* conditions on trails.

5.2 Blurred Conditions

If we consider differentials over SubBytes then we have to take into account the effect of the linear transformation L in the AES S-box. In order to determine the number of input differences x compatible to a fixed output difference y, it suffices to replace V_i by

$$\mathrm{V}_a = \{(u_0 L(y_0))^{-1}, (u_1 L(y_1))^{-1}, (u_2 L(y_2))^{-1}, (u_3 L(y_3))^{-1}\} \ . \tag{16}$$

However, when determining the number of output differences y compatible with a fixed input difference x, (13) becomes:

$$\mathrm{Tr}((x_i L(\gamma u_i))^{-1}) = 0 \ , \ 0 \le i < 4 \ , \tag{17}$$

which can't be easily reworked and are harder to analyse. Therefore we call these conditions the *blurred* conditions.

6 Number of Trails in a Bundle

The number of trails in a bundle $B(u^{\mathrm{b}})$ for a given differential (a, e) is now the number of γ values that satisfy the sharp conditions due to $(\gamma u^{\mathrm{d}}, e)$ over SubBytes and the blurred conditions due to $(a, \gamma u^{\mathrm{b}})$ over SubBytes. In this section we first derive formulas to estimate the number of trails in $B(u^{\mathrm{b}})$ for the special case of a differential with one active S-box in the first round followed by formulas and a discussion for the general case.

6.1 Bundles with One Active S-Box in the First Round

Consider a differential (a, e) with activity pattern (1000; 1111). There is a single bundle $B(u^{\mathrm{b}})$ with $u^{\mathrm{b}} = [1, 0, 0, 0]$ and $u^{\mathrm{d}} = [2, 1, 1, 3]$. The sharp conditions become:

$$\begin{aligned} \mathrm{Tr}((2L(e_0))^{-1}\gamma^{-1}) &= 0 \\ \mathrm{Tr}((L(e_1))^{-1}\gamma^{-1}) &= 0 \\ \mathrm{Tr}((L(e_2))^{-1}\gamma^{-1}) &= 0 \\ \mathrm{Tr}((3L(e_3))^{-1}\gamma^{-1}) &= 0 \ . \end{aligned}$$

If $e = [L^{-1}(z/2), L^{-1}(z), L^{-1}(z), L^{-1}(z/3)]$ for any nonzero value z, then $\mathrm{V}_a = \{z^{-1}\}$ resulting in $\alpha = 1$ and hence there are 127 trails satisfying the sharp conditions.

The effect of the blurred condition can be modeled as a sampling process. The space sampled are the 255 vectors of $B(u)$. 127 out of the 255 vectors may satisfy the blurred condition. These are called the good ones, the 128 others the bad ones. The joint sharp conditions take a sample with size $2^{8-\alpha} - 1$. This gives rise to a hypergeometric distribution $H(\mathrm{N_t}; n, m, N)$ [8] with the following parameters:

- Number of ways for a good selection $n = 127$.
- Number of ways for a bad selection $m = 255 - 127 = 128$.
- Sample size N: $2^{8-\alpha} - 1$.

Denoting the event that one vector is compatible (the outcome of a single sampling) by x_i, we obtain $E[x_i] = n/(m+n)$. Since $\mathrm{N_t} = \sum_i x_i$,

$$E[\mathrm{N_t}] = \frac{n}{m+n}N = \frac{127}{255}(2^{8-\alpha} - 1).$$

This gives formula (18). For the variance, we obtain:

$$\sigma^2(\mathrm{N_t}) = \frac{mnN(m+n-N)}{(m+n)^2(m+n-1)} = \frac{128 \times 127(2^{8-\alpha}-1)(256-2^{8-\alpha})}{255^2 254} ,$$

which corresponds to (19). The exact distributions of the number of trails per differential for all four values of α are given in Appendix C.

6.2 Any Bundle

Every differential (a, e) imposes on γ a number of sharp conditions, determined by e and u^{d}, and a number of blurred conditions, determined by a and u^{b}. Following (16), the sharp conditions state that γ^{-1} has to be orthogonal to

$$\mathrm{V}_a = \{v_0, v_1, v_2, v_3\},$$

with $v_i^{-1} = {u^{\mathrm{d}}}_i L(e_i)$. The parameter α is defined as the dimension of V_a. Hence γ^{-1} is in a vector space of dimension $8 - \alpha$ ranging from 4 to 7.

The number of blurred conditions is denoted by β, and given by the number of different non-zero elements in the following set of couples:

$$\{(a_0, {u^{\mathrm{b}}}_0), (a_1, {u^{\mathrm{b}}}_1), (a_2, {u^{\mathrm{b}}}_2), (a_3, {u^{\mathrm{b}}}_3)\}.$$

For the vast majority of differentials, β equals the number of active S-boxes in a. β is smaller only when two a_i values are the same and the corresponding u_i in the bundle are also equal. Hence a reduction of β occurs much less often than a reduction of α. Both α and β range from 1 to 4 limited by $\alpha + \beta \leq 5$.

The number of trails in the bundle $B(u^{\mathrm{b}})$ can be described as a stochastic variable with the expected value and variance given by:

$$E[\mathrm{N_t}] = \left(\frac{127}{255}\right)^{\beta} (2^{8-\alpha} - 1) , \tag{18}$$

$$\sigma^2(\mathrm{N_t}) = E\left[\mathrm{N_t}\right] \times \left[1 - \left(\frac{127}{255}\right)^{\beta} + (2^{8-\alpha} - 2)\left(\left(\frac{63}{127}\right)^{\beta} - \left(\frac{127}{255}\right)^{\beta}\right)\right]. \quad (19)$$

We give a derivation for (18) and (19) in Appendix B. The numerical values computed with these formulae are given in Table 2. We have conducted a large number of experiments that confirm the mean and variance predicted by (18) and (19) for any combination of α and β.

Table 2. Mean (left) and variance (right) of the number of trails for a differential given α and β

α,β	1	2	3	4
1	63.25	31.50	15.69	7.81
2	31.38	15.63	7.78	3.88
3	15.44	7.69	3.83	1.91
4	7.47	3.72	1.85	0.92

α,β	1	2	3	4
1	16.00	15.89	10.86	6.38
2	11.91	9.85	6.11	3.40
3	6.83	5.33	3.19	1.73
4	3.54	2.70	1.59	0.85

7 EDP of a Bundle

The distributions for the number of trails in a bundle can be converted to distributions of the EDP of a bundle by taking into account the EDP of the trails. The EDP of a trail is the product of the DP values of its active S-box differentials. If we apply Section 3 to the AES S-box, we see that for an S-box differential with given input (output) difference, there are 126 output (input) differences with DP $= 2^{-7}$ and a single output (input) difference with DP $= 2^{-6} = 2 \times 2^{-7}$. We call the latter double differentials. It follows that the EDP of a trail is $2^i 2^{-7\nu}$ with ν the number of active S-boxes and i the number of double S-box differentials. One could say that the presence of i double S-box differentials multiplies the EDP of the trail by a factor 2^i.

Let (a, b, d, e) be a characteristic in a bundle $B(u^{\mathrm{b}})$ of a differential (a, b), determined by γ. A characteristic has a double S-box differential in the i-th S-box of the first round if and only if

$$b_i = L^{-1}({a_i}^{-1}) \Leftrightarrow \gamma = \left({u^{\mathrm{b}}}_i\right)^{-1} L^{-1}({a_i}^{-1}). \quad (20)$$

The condition for a double S-box differential in the second round is:

$$d_j = L(e_j)^{-1} \Leftrightarrow \gamma = \left({u^{\mathrm{d}}}_j L(e_j)\right)^{-1}. \quad (21)$$

Hence each double S-box differential occurs in exactly one characteristic of the bundle. Two observations can be made here.

Multiple solutions: If a solution of the equations in (20) and (21) is a multiple solution, then the corresponding characteristic (potentially) has a higher EDP. Consider for example a differential with 5 active S-boxes. There are seven different cases, of which the two extremes are:

'Poker': the double differentials are all in the same characteristic,
'No Pair': the double differentials occur in 5 different characteristics,

The other five cases are 'One Pair', 'Two Pairs', 'Three of a Kind', 'Full House' and 'Four of a Kind'. The occurrence of these cases is related to the values of α and β. The number of different solutions for (21) equals the number of different elements in V_a. If α is 1 or 4, this number is equal to α. If α is 2 or 3 and the number of active S-boxes in e is higher than α, the number of solutions can also be $\alpha + 1$. The number of solutions for (21) usually equals β, but it can also be smaller. For a given input difference a there can be at most one output difference e for which all double S-box differentials are in the same trail.

Occurrence in trails: The solutions of (20) and (21) still have to satisfy the remaining sharp conditions and blurred conditions in order to have an EDP > 0. Clearly, the expected number of characteristics satisfying the remaining conditions decreases when there are more conditions, i.e. when α and β increase. A 'Poker' characteristic, i.e. one in which the S-box differentials of all active S-boxes are double differentials, is always a trail.

7.1 How L Can Make a Difference

If we remove L from the S-box, the set of blurred conditions is replaced by a second set of sharp conditions. The number of trails in a bundle is then given by $2^{8-\alpha} - 1$, with $1 \leq \alpha < 8$. The maximum EDP occurs for differentials with 5 active S-boxes and $\alpha = 1$. There are 56×255 such differentials in the super box. For these, the double S-box differentials are in the same trail and hence the EDP is equal to $2^5 \times 2^{-35} + 126 \times 2^{-35} = 19.75 \times 2^{-32}$, where for AES this is 13.25×2^{-32} [4].

8 N_t and EDP of a Differential

Differentials with 5 active S-boxes contain only a single bundle, hence they are covered by the previous sections. For differentials with more active S-boxes, there are more bundles. Given a differential (a, e), we can compute for each of its bundles the value of (α, β). With α and β we can compute the mean number of trails in the bundle and the variance. The mean number of trails in a differential is the sum of the mean number of trails in these bundles. For the variance of the number of trails, the sum of the variances in the bundles gives a good idea.

The value of the differences a and e determine the distribution of α and β over the different bundles in the differential (a, e). As the number of active S-boxes grows, the analysis becomes more and more involved. Therefore we start with an example.

8.1 Differentials with Activity Pattern (1110; 1110)

There are in total 251 bundles with activity pattern (1110; 1110). The distribution of α over the 251 bundles in (a, e) is completely determined by e, or more

Table 3. Distribution of α for differentials with activity pattern $(1110; 1110)$

α distribution			# couples	mean	standard deviation	
$\alpha = 3$	$\alpha = 2$	$\alpha = 1$	$(L(e_1)/L(e_0), L(e_2)/L(e_0))$		theory	exp.
250	1	0	21	965.2	28.42	25.65
249	2	0	1501	969.1	28.47	25.14
248	3	0	31170	973.1	28.53	25.15
247	4	0	2175	977.0	28.58	25.16
246	5	0	29907	981.0	28.63	25.23
250	0	1	3	973.1	28.42	23.28
249	1	1	248	977.0	28.47	25.01

specifically, by the couple $(L(e_1)/L(e_0), L(e_2)/L(e_0))$. Table 3 lists the seven distributions that are possible and gives for each of them the number of output differences e for which they occur.

The distribution of β depends on the values of a_0, a_1 and a_2. If they are three different values, then β is always equal to 3. For this case, Table 3 gives the theoretical mean and standard deviation of the number of trails (assuming independence between the bundles). If two of the values a_0, a_1 and a_2 are equal, then β will be 2 for at most one bundle and 3 for all other bundles. If they are all three equal, then either β will be 2 for at most three bundles, or β will be 1 for at most one bundle and 3 for all the other bundles.

In principle, the distributions for α and β combine to a two-dimensional distribution. In the worst case, the small values of β occur in bundles with a small value of α. All in all, there are only few bundles where β is smaller than 3, hence we can approximate by working with $\beta = 3$ for all bundles.

We have experimentally verified this theory by computing the number of trails for a large set of differentials with 6, 7 and 8 active S-boxes. The measured mean values coincide with the theoretically predicted values. The measured standard deviations, also listed in Table 3 are systematically smaller than the theoretical ones, implying that the number of trails in the bundles of a differential are not independent.

8.2 A Bound on the Multiplicity

In Section 4 we have shown that the bundles with activity pattern $(1110; 1110)$ can be enumerated by $u^{\mathrm{b}} = [1, z, 3 + z, 0]$ and $u^{\mathrm{d}} = [1 + 2z, 4 + z, 7 + 3z, 0]$ with z different from 0, 3, 1/2, 4 and 7/3.

Lemma 4. *If two double S-box differentials occur in the same characteristic of one bundle with activity pattern* $(1110; 1110)$*, then they occur in different characteristics for the 250 other bundles with the same activity pattern.*

Proof. Assume we have a bundle where the double differential in the first and the second S-box of the second round occur in the same characteristic. Then we have from (21):

$$((1 + 2z)L(e_1))^{-1} = ((4 + 7z)L(e_2))^{-1} .$$

This equation is linear in z and has at most one solution. Hence the double differentials can't be in the same characteristic for any other bundle. The same holds for any other pair of active S-box positions. □

The expected contribution of the double S-box differentials to the EDP of a differential is maximum when there is a bundle in which they are all 6 in the same trail. This trail contributes 64×2^{-42} to the EDP of the differential. Lemma 4 implies that in the remaining 250 bundles, there can be no trails with more than one double S-box differential. Hence each of these bundles will contribute at most $(\mathrm{N_t} + \min(6, \mathrm{N_t}))2^{-42}$ to the EDP of the differential. On the average the presence of the double S-box differentials makes the contribution of these trails only rise from $\mathrm{N_t}2^{-42}$ for the hypothetical case where no double S-box differentials exist to $(132/127)\mathrm{N_t}2^{-42}$.

We conclude that for this type of differential, the distribution of the EDP values is much more centered around its mean value than is the case for differentials with 5 active S-boxes. This is mainly due to the fact that the distribution of the EDP of the differential is the convolution of the distributions of many bundles. Moreover, Lemma 4 implies that the different bundles compensate for one another.

The same phenomena can be observed for the other types of differentials with 6 active S-boxes. For differentials with 7 or 8 active S-boxes the average numbers of trails are even much higher and the EDP values much smaller. Furthermore, the individual trails have all very small EDP values. This all makes that the EDP values of differentials with 6 or more active S-boxes have a very narrow distribution.

9 Differentials with the Maximum EDP Value

The maximum EDP value obtained in [4] occurs for exactly 12 differentials over the AES super box. Due to the rotational symmetry of the AES super box, they come in 3 sets, where the differentials in a set are just rotated versions of each other. It is no surprise that they are differentials with 5 active S-boxes, where the deviations from the average value 2^{-32} are largest. Moreover, they have $\alpha = 1$ and $\beta = 1$ for which the expected number of trails is the highest over all differentials with 5 active S-boxes, as is clear from Figure 1 in Appendix C. The differentials are the following:

$$\begin{gathered}
\left([x,0,0,0],[L^{-1}(y/2),L^{-1}(y),L^{-1}(y),L^{-1}(y/3)]\right), \\
\left([x,x,0,0],[L^{-1}(y),L^{-1}(y/3),0,L^{-1}(y/2)]\right), \\
\left([x,x,x,0],[0,0,L^{-1}(y/2),L^{-1}(y/3)]\right),
\end{gathered}$$

with $x = 75_\mathrm{x}$ and $y = 41_\mathrm{x}$. For these differentials, the number of trails is 75: 74 trails with EDP 2^{-35} and one with EDP 2^{-30}, resulting in EDP value $2^{-30} + 74 \times 2^{-35} = 13.25 \times 2^{-32}$. Clearly all five double S-box differentials are in the same trail. Note that there are differentials with 5 active S-boxes that have 82 trails (see Appendix C) but these have a lower EDP value due to the fact that the double S-box differentials are not in the same trail.

To prove the correctness of the maximum EDP value, [4] uses so-called 5-lists, a concept similar to, but different from, the bundles defined in this paper. Both bundles and 5-lists group sets of 255 b-differences. Bundles with 5 active S-boxes correspond with the 5-lists of type 1. In bundles with more than 5 active S-boxes the ratios between the inner differences are fixed, while in 5-lists of type 2, a number of inner differences are fixed. Their goal is also different: the concept of 5-lists helps in efficiently finding bounds, while bundles help to gain insight in the distribution of trails in differentials.

10 Conclusions and Future Work

The AES super box can be compared with an idealized keyed 32-bit map which is constructed as a family of 2^{32} randomly selected permutations (one permutation for each value of the key). In this idealized model, the distribution of the EDP over all differentials (a, b) with both a and b different from zero has a normal distribution with expected value 2^{-32} and standard deviation $2^{-47.5}$.

The AES super box differentials deviate from the idealized model: differentials with 4 or less active S-boxes have EDP = 0, and differentials with 5 active S-boxes can have EDP values as large as 13.25×2^{-32} [4]. Our results on differentials with 6 active S-boxes indicate that for differentials with 6 or more active S-boxes the distribution of the EDP is very narrowly centered around 2^{-32}. Further analysis can lead to strict bounds.

It is a well known fact that the linear transformation L in the AES S-box doesn't influence the EDP of S-box differentials and the bounds on the EDP of trails as proven in [2]. Our results explain how the presence of L influences the EDP of two-round differentials.

Bounds on the EDP of two-round differentials can be used to derive bounds on the EDP of four-round differentials [3]. The results of our paper allow to describe the full distribution of the EDP of two-round differentials. We expect that this information can be used to derive sharper bounds on the EDP of four-round differentials.

References

1. E. Biham and A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystems," *Journal of Cryptology*, Vol. 4, No. 1, 1991, pp. 3–72.
2. J. Daemen, V. Rijmen, *The design of Rijndael — AES, The Advanced Encryption Standard,* Springer-Verlag, 2002.
3. L. Keliher, "Refined analysis of bounds related to linear and differential cryptanalysis for the AES," *Advanced Encryption Standard – AES, 4th international conference (AES 2004), LNCS 3373,* Springer-Verlag, 2005, pp. 42–57.
4. L. Keliher and J. Sui, "Exact maximum expected differential and linear probability for 2-round advanced encryption standard (AES)," Cryptology ePrint archive, Report 2005/321, 2005, http://eprint.iacr.org.
5. L.R. Knudsen, "Truncated and higher order differentials," *Fast Software Encryption '94, LNCS 1008*, B. Preneel, Ed., Springer-Verlag, 1995, pp. 196–211.

6. X. Lai, J.L. Massey and S. Murphy, “Markov Ciphers and Differential Cryptanalysis,” *Advances in Cryptology, Proc. Eurocrypt’91, LNCS 547*, D.W. Davies, Ed., Springer-Verlag, 1991, pp. 17–38.
7. R. Lidl, H. Niederreiter, *Introduction to finite fields and their applications,* Cambridge University Press, 1986 (Reprinted 1988).
8. Mathworld, `http://mathworld.wolfram.com/`.
9. K. Nyberg, “Differentially uniform mappings for cryptography,” *Advances in Cryptology, Proc. Eurocrypt’93, LNCS 765*, T. Helleseth, Ed., Springer-Verlag, 1994, pp. 55–64.
10. S. Park, S.H. Sung, S. Chee, E-J. Yoon and J. Lim, “On the security of Rijndael-like structures against differential and linear cryptanalysis,” *Advances in Cryptology, Proceedings of Asiacrypt ’02, LNCS 2501,* Y. Zheng, Ed., Springer-Verlag, 2002, pp. 176–191.
11. S. Park, S.H. Sung, S. Lee and J. Lim, “Improving the upper bound on the maximum differential and the maximum linear hull probability for SPN structures and AES,” *Fast Software Encryption ’03, LNCS 2887,* T. Johansson, Ed., Springer-Verlag, 2003, pp. 247–260.

A Number of Bundles per Differential

The total number of nonzero vectors of 4 bytes is $2^{32}-1$. Each bundle groups 255 such vectors, so the total number of bundles is

$$\frac{2^{32}-1}{2^8-1} = 2^{24} + 2^{16} + 2^8 + 1 \ .$$

The number of bundles with a given activity pattern is determined by the number of active S-boxes in the activity pattern. If we denote the number of bundles for an activity pattern with x active S-boxes by $\mathrm{BN}(x)$, we have:

$$\begin{array}{lcr}
\mathrm{BN}(5) & = & 1 \\
\mathrm{BN}(6) = 255 - 4\mathrm{BN}(5) & = & 251 \\
\mathrm{BN}(7) = 255^2 - 4\mathrm{BN}(6) - 6\mathrm{BN}(5) & = & 64015 \\
\mathrm{BN}(8) = 255^3 - 4\mathrm{BN}(7) - 6\mathrm{BN}(6) - 4\mathrm{BN}(5) & = & 16323805
\end{array}$$

The number of trails with i active S-boxes is

$$\binom{8}{i} 255\mathrm{BN}(i)127^i \ .$$

The total number of trails is 2.8×10^{26}.

B Derivation of (18) and (19)

Assuming that the blurred conditions are independent, we can generalize the sampling model introduced in Section 6.1. The space sampled is now the set of β-component vectors where each of the components can take any nonzero value in $\mathrm{GF}(2^8)$. There are 255^β such vectors. A good selection is one in which the first component satisfies the first condition, the second component satisfies the second condition and so on. There are 127^β such vectors. Denoting by x_{it} the event that characteristic i satisfies condition t, we obtain:

$$E\left[\mathrm{N_t}\right] = \sum_{i=1}^{N} E\left[x_i\right] = \sum_{i=1}^{N} E\left[x_{i1}\right] E\left[x_{i2}\right] \cdots E\left[x_{i\beta}\right] = N\left(\frac{n}{n+m}\right)^{\beta}$$

The variance satisfies

$$\sigma^2(\mathrm{N_t}) = \sum_{i=1}^{N} \sigma^2(x_i) + \sum_{i=1}^{N} \sum_{\substack{j=1 \\ j\neq i}}^{N} \mathrm{Cov}(x_i, x_j).$$

Since x_i takes only the values 0, 1, it is a Bernoulli variable, and

$$\sigma^2(x_i) = E\left[x_i\right]\left(1 - E\left[x_i\right]\right) \qquad (22)$$

$$\mathrm{Cov}(x_i, x_j) = E\left[x_i x_j\right] - E\left[x_i\right] E\left[x_j\right] \qquad (23)$$

$$E\left[x_i\right] = \left(\frac{n}{n+m}\right)^{\beta} . \qquad (24)$$

Since two trails of the same bundle differ in the value of each of their components, we have:

$$E\left[x_i x_j\right] = \left(\frac{n(n-1)}{(n+m)(n+m-1)}\right)^{\beta} . \qquad (25)$$

Putting everything together results in (19).

C Distributions of the Number of Trails per Differential

We have experimentally verified the distributions of the number of trails per differential for all 16 combinations of α and β. For the combination of (α, β) equal to $(1,1)$, $(2,1)$, $(3,1)$, $(4,1)$ and $(1,2)$ we were able to do this exhaustively, covering all possible cases. As a side result we found for these values of (α, β) the minimum and maximum values for the number of trails per differential, listed in Table 4.

Table 4. Minimum and maximum number of trails in differentials with 5 active S-boxes given (α, β)

(α, β)	minimum	maximum
$(1,1)$	48	82
$(2,1)$	14	48
$(3,1)$	3	29
$(4,1)$	0	15
$(1,2)$	10	56

For the other values of (α, β), the number of combinations becomes too large to compute exhaustively. Still, our sampling experiments confirm the shape predicted by formulas (18) and (19). As α and β grow, the mean and variance of the distributions shrink. Clearly, the majority of differentials with 5 active S-boxes and $\alpha = 1$ and $\beta = 1$ have more trails than any differential with 5 active S-boxes where $\alpha + \beta$ has a higher value. Figure 1 depicts the four distributions for $\beta = 1$ on a logarithmic scale. The distributions appear as slightly skewed parabolas, which is the typical shape of hypergeometric distributions.

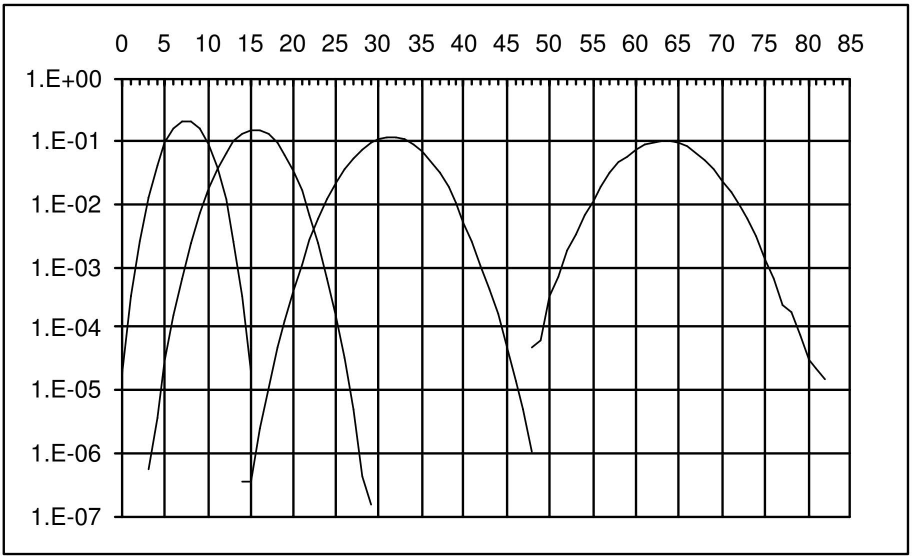

Fig. 1. Distributions of the number of trails per differential for $\beta = 1$ and for α ranging from 4 (leftmost) to 1 (rightmost)