On the Order of Round Components in the AES

Jorge Nakahara Jr
Department or Informatics, UNISANTOS
R. Dr. Carvalho de Mendonça, 144, Santos, Brazil (Email: jorge_nakahara@yahoo.com.br)

(Received June 13, 2006; revised and accepted Oct. 24, 2006)

Abstract

This paper[1] analyses all 24 possible round constructions using different combinations of the four round components of the AES cipher: SubBytes, ShiftRows, AddRoundKey and MixColumns. We investigate how the different round orderings affect the security of AES against differential, linear, multiset, impossible differential and boomerang attacks. The cryptographic strenght of each cipher variant was measured by the size of each distinguisher, their probability or correlation value and the number of active S-boxes. Our analyses indicate that all these permutations of the AES components have similar cryptographic strength (concerning these five attacks), although there are implementation advantages for certain permutations.

Keywords: Active S-box, AES, cryptanalysis

1 Introduction

The Advanced Encryption Standard (AES) is an SPN-type block cipher designed by J. Daemen and V. Rijmen in 1998. The original cipher was called Rijndael, and it was selected out of fifteen candidates during the AES Development Process [1], initiated by the National Institute of Standards and Technology (NIST) in 1997. It is expected that the AES will become the new *de facto* world standard in symmetric cryptography, as the successor of the Data Encryption Standard (DES) algorithm. In Sep. 2000, Rijndael was officially standardized as FIPS PUB 197 [28]. Rijndael (and the AES) have already been implemented in several programming languages and are embedded in several software systems [31]. The AES is the smallest instance of the Rijndael cipher [16], since the AES operates on 128-bit text blocks, under keys of 128, 192 or 256 bits, for which the cipher iterates ten, twelve and fourteen rounds, respectively.

The AES has been intensively analysed since 1998. Most of the known results, though, concern attacks on reduced-round variants: differential and linear analyses [12], square [15, 18], impossible differential [6, 30, 29], collision [20], and boomerang attacks [9]. All of these attacks have time complexity lower than that of an exhaustive key search.

Some papers such as [2, 3] by Biham and Barkan studied AES variants with different component values compared to [28], namely, different matrix constants, primitive and non-primitive irreducible polynomials, and new parameters of affine transformations. This paper, nonetheless, analyses the AES cipher without changing its original components, but only their order, namely, we change the placement of SubBytes, ShiftRows, AddRoundKey and MixColumns layers within a round. But, the order of these four components is the same for all rounds. Furthermore, the key schedule algorithm does not change. The contribution of this paper is a study of the orderings of the round components of AES and its impact on the security of the cipher. Even though the order of round components in the AES may seem intuitive, one may ask if there are other orderings that provide either higher security or significant implementation advantages. This paper studies the security implications of different orderings of the round components with respect to differential (DC) [7], linear (LC) [27], multiset (M) [11, 14], impossible differential (ID) [5, 24] and boomerang (B) attacks [9]. The first two techniques are benchmarks for any modern block cipher. The other ones are considered because they are among the best known attacks on reduced-round AES variants[2].

This paper is organized as follows: Section 2 give essential description of AES. Section 3 describes the multiset attack and its consequences on the 24 round variants of AES. Section 4 presents differential and linear analyses of the AES variants. Section 5 describes the encryption and decryption schemes of the AES variants. Section 6 describes impossible differential distinguishers, and Section 7 describes boomerang distinguishers. Section 8 concludes the paper.

2 Round Variants of the AES

The AES is an iterated cipher. But, it is not a Feistel cipher. It rather has a Substitution-Permutation Network (SPN) structure. One full round of the AES con-

[1] Research funded by FAPESP (Fundação de Amparo à Pesquisa do Estado de São Paulo) under contract 2005/02102-9.

[2] In the sense of requiring much less data than the full codebook, and much less effort than an exhaustive key search.

sists of the following four operations in order: SubBytes, ShiftRows, MixColumns and AddRoundKey. We denote them by SB, SR, MC, and AK_i, respectively, where $0 \leq i \leq Nr$. Only AddRoundKey is subscripted since it is the only key-dependent component (and the subkey value is supposed to change from one round to another). One full (encryption) round of a text block X in the AES can be denoted $\mathrm{AK}_i \circ \mathrm{MC} \circ \mathrm{SR} \circ \mathrm{SB(X)} = \mathrm{AK}_i(\mathrm{MC(SR(SB(X)))})$, namely, composition of operations is evaluated in right-to-left order. The AES round is just one of the 24 possible permutations of the four operations: SB, SR, MC, and AK_i. This paper investigates all 24 possible orderings of round components in the AES, and their security implications. Concerning the computational cost, all of these orderings cost the same, since the same components and the same number of operations are employed in all 24 round variants.

Each round component stands for one quarter of a round. For convenience, the size of distinguishers will be measured in quarters of a round, or 0.25 rounds. This measure is not absolutely precise because some round components, such as SR and MC, are fixed and key independent. It means that they can undone (in the first and last rounds) effectively shortening the distinguisher.

Every distinguisher contains a number of active S-boxes, namely S-boxes which effectively participate in the construction of the distinguisher. For instance, in the linear cryptanalysis of AES, an active S-box has both nonzero input and output masks. This concept originated with the differential cryptanalysis of DES in [13].

3 Multiset Distinguisher

The multiset technique [11] has similarities with the Square attack [14], the saturation attack [26] and the integral cryptanalysis [22, 25]. All of these techniques operate in a chosen-plaintext (CP) setting, and the first published attack was a dedicated one on the Square block cipher [14]. Nonetheless, this technique has already been applied to several ciphers, with or without wordwise operations [17, 23, 25, 26]. A fundamental concept in a multiset attack is the Λ-set [14], which is a multiset [11] (a set with multiplicities) containing b full n-bit text block elements, where n is the block size and b is typically a power of 2. These n-bit text blocks are analysed by tracing certain patterns in fixed (but not necessarily contiguous) w bits, $w < n$.

The rationale behind the multiset technique is to use balanced sets of bits to attack permutation mappings (ie. cipher rounds and its bijective components). Thus, multiset attacks exploit the bijective nature of internal cipher components. In particular, ciphers that operate on neatly partitioned words are the main targets.

The multiset distinguishers for all AES variants in Table 2 were constructed similar to the one for Rijndael in [15]. The multiset trails depend on the internal components of the cipher and their order. Figure 1(a) shows a multiset trail[3] (dashed line) for a 4th-order multiset distinguisher for an AES variant using round scheme (1) in Table 2. This distinguisher covers 4.25 rounds, holds with certainty, and has 40 active S-boxes along its trail.

4 Differential and Linear Distinguishers

The differential cryptanalysis (DC) technique was developed by Biham and Shamir [7, 8], and initially applied to the DES cipher. The linear cryptanalysis (LC) technique was developed by Matsui in [27]. Both attacks have become benchmarks for any modern block cipher, including the AES [15, 16], as part of the NIST's requirements for the AES Development Process. An important feature of differential and linear distinguishers is the number of active S-boxes, since the S-box is usually the main nonlinear operator in a cipher. Thus, if a cipher has been carefully designed, taking these attacks into account, then the probability associated to a distinguisher becomes (exponentially) smaller with an increasing number of rounds.

Figure 1(b) depicts a differential trail (a linear trail uses bit masks instead of differences of pairs of texts) across four rounds, and involving 25 active S-boxes. The propagation of differences and masks in the 24 round permutations of AES follows similarly to that of the original AES in [15].

Taking into account the maximum differential probability of the AES S-box as 2^{-6}, the probability of any 4-round differential distinguisher [15] is estimated as $(2^{-6})^{25} = 2^{-150}$. As a consequence, an attack using this differential distinguisher would need about 2^{150} chosen plaintext, which is infeasible, since the block size is 128 bits. Similarly, assuming the maximum input-output correlation of the AES S-box as 2^{-3}, the maximum input-output correlation of any 4-round linear distinguisher [15] is estimated as $(2^{-3})^{25} = 2^{-75}$. As a consequence a linear attack using such distinguisher would require about $(2^{-75})^{-2} = 2^{150}$ known plaintexts, which is infeasible.

5 Encryption and Decryption Frameworks

Each of the twenty four round variants induces an encryption and a decryption scheme. We have verified separately that each variant results in similar computational structures for both encryption and decryption, just like in the original AES. For example, for scheme (1) in Table 2, the encryption scheme is $\mathrm{C} = \mathrm{AK}_{Nr} \circ (\mathrm{SR} \circ \mathrm{SB} \circ \mathrm{AK}_{Nr-1}) \circ (\mathrm{MC} \circ \mathrm{SR} \circ \mathrm{SB} \circ \mathrm{AK}_{Nr-2}) \cdots \circ (\mathrm{MC} \circ \mathrm{SR} \circ \mathrm{SB} \circ \mathrm{AK}_0)(P)$.

The corresponding decryption scheme is $P = (\mathrm{AK}_0 \circ \mathrm{SB}^{-1} \circ \mathrm{SR}^{-1} \circ \mathrm{MC}^{-1}) \circ (\mathrm{AK}_1 \circ \mathrm{SB}^{-1} \circ \mathrm{SR}^{-1} \circ$

[3] A trail depicts the cipher components along a path taken by the distinguisher.

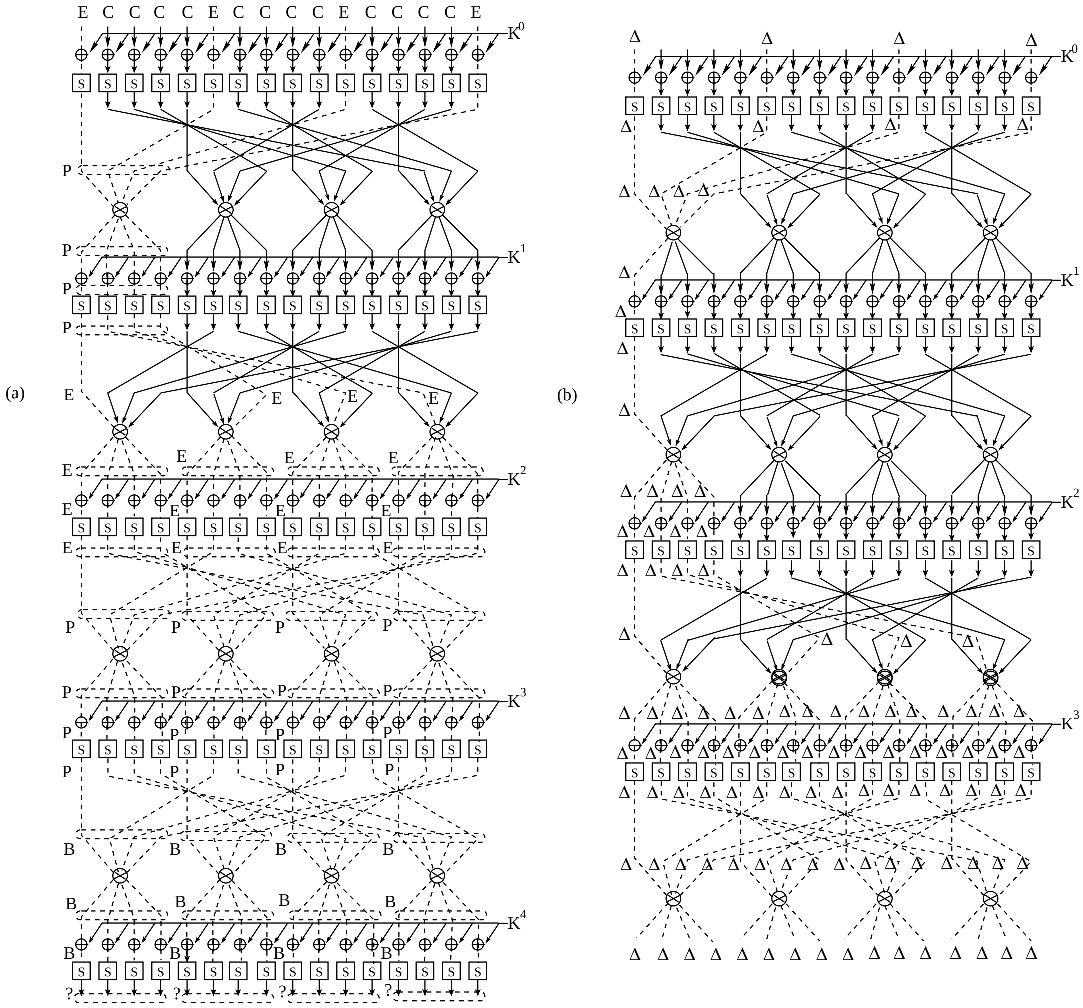

Figure 1: (a) 4th-order multiset (b) differential or linear trail (dashed line) using round scheme (1) of Table 2

Table 1: Differential patterns in ID distinguisher for scheme (1) in Table 2

AK_0	δ	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SB	δ	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SR	δ	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
MC	δ	δ	δ	δ	0	0	0	0	0	0	0	0	0	0	0	0
AK_1	δ	δ	δ	δ	0	0	0	0	0	0	0	0	0	0	0	0
SB	δ	δ	δ	δ	0	0	0	0	0	0	0	0	0	0	0	0
SR	δ	0	0	0	0	0	0	δ	0	0	δ	0	0	δ	0	0
MC	δ	δ	δ	δ	δ	δ	δ	δ	δ	δ	δ	δ	δ	δ	δ	δ
AK_2	δ	0	0	0	0	δ	0	0	0	0	δ	0	0	0	0	δ
SB	δ	0	0	0	0	δ	0	0	0	0	δ	0	0	0	0	δ
SR	δ	0	0	0	0	δ	0	0	0	0	δ	0	0	0	0	δ
MC	δ	δ	δ	δ	0	0	0	0	0	0	0	0	0	0	0	0
AK_3	δ	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SB	δ	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SR	δ	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

$\mathrm{MC}^{-1}) \circ \cdots \circ (\mathrm{AK}_{Nr-1} \circ \mathrm{SB}^{-1} \circ \mathrm{SR}^{-1} \circ \mathrm{AK}_{Nr})(C) = \mathrm{AK}_0 \circ (\mathrm{SR}^{-1} \circ \mathrm{SB}^{-1} \circ \mathrm{AK}_1^*) \circ (\mathrm{MC}^{-1}) \circ \mathrm{SR}^{-1} \circ \mathrm{SB}^{-1} \circ \mathrm{AK}_2^*) \circ \cdots \circ (\mathrm{MC}^{-1}) \circ \mathrm{SR}^{-1} \circ \mathrm{SB}^{-1} \circ \mathrm{AK}_{Nr})(\mathrm{C})$, where AK_i^*=MC(AK_i). Thus, both schemes share a similar computational graph, only requiring new subkeys and inverse round components. A consequence is that both schemes have the same cryptographic strength, namely, there is no advantage in attacking one scheme instead of the other. When a cipher uses significantly different schemes for encryption and decryption, care must be exercised to avoid one of them to become weaker than the other[4], and thus more susceptible to cryptanalytic attacks [4, 21].

6 Impossible-Differential Distinguisher

The impossible-differential (ID) technique was due to Knudsen in [24]. Unlike conventional differential attacks that look for differentials or characteristics with high probability, ID techniques look for differentials with probability zero. The ID approach is the opposite of the one used in differential analyses. While in the former, the key suggested most often by the distinguisher is selected as the potential true candidate, in the latter, all keys suggested by the distinguisher are certainly wrong (the key not filtered by the ID distinguisher is the correct one). In this paper, the miss-in-the-middle technique [5] was used to derive ID distinguishers.

An example of an ID distinguisher for an AES variant is given in Table 1. This distinguisher applies to scheme (1) in Table 2 and covers 3.75 rounds. It consists of two differentials whose (truncated) differences contradict each other after the MC layer of the second round (16 active or nonzero byte differences) and before AK_2 (12 passive or zero byte differences). The first (truncated) differential covers AK_0 down to MC in the second round. The second (truncated) differential covers SR in the fourth round up to AK_2 in the decryption direction. Both differentials hold with certainty, but jointly they hold with probability zero, because the input to the first differential cannot cause the output difference of the second differential. The full distinguisher is depicted in Table 1, where δ denotes a nonzero xor-difference byte. Similar distinguishers apply to the other schemes. An good aspect of this distinguisher is the small number of nonzero byte differences after 3.75 rounds, which reduces the number of key bits recovered simultaneously during the attack. On the other hand, the small number of active bytes at the top of the distinguisher restricts the number of pairs formed from a single pool of plaintexts.

7 Boomerang Distinguisher

The boomerang technique is a chosen-plaintext adaptively-chosen-ciphertext (CPACC) attack, developed by Wagner in [32]. The approach used for the AES variants follows that of Biryukov in [9]. The boomerang technique exploits encryption schemes E_K, under a secret key K, that can be decomposed into two pieces $E_K = E_1 \circ E_0$, such that E_0 is weak in the encryption direction, and E_1 is weak in the decryption direction. In our context, the term weak means that a differential (or truncated differential) propagates across the given E_i piece of the cipher with high probability. A boomerang distinguisher is composed of short differentials or truncated differentials covering E_0 and E_1, separately. In this way, the original encryption scheme E_K is covered using both chosen plaintext and chosen ciphertext.

For the AES, the E_0 part covers (the first) three rounds, and E_1 covers the last 2 rounds of 5-round AES (Figure 2). The very last round does not have the MC layer. We have analysed all 24 AES variants separately, and concluded that the same distinguisher and therefore, the same attack as described in [9], can be applied to all 24 round variants of the AES. This is a consequence of the differential patterns that make the E_0 and E_1 halves of the boomerang distinguisher.

Table 2 compares the size and minimum number of active S-boxes (denoted #S) for all 24 round variations of the AES under five attack techniques described previously. The line numbered (13) in Table 2 represents the original AES round structure.

None of the five attacks described in this paper were implemented. We rather focused on determining the distinguishers themselves, their size, the number of active S-boxes and the associated probabilities. These parameters are enough to estimate the attack complexities, and we noticed that they do not provide significant advantages compared to the same attacks on the AES.

From these parameters we also observed a correlation between the minimum number of active S-boxes and the associated probability of the distinguisher. For instance, impossible differential (ID) distinguishers hold with probability zero, and each such distinguisher contains at least 10 active S-boxes. Differential (DC) and linear (LC) distinguishers hold with estimated probability and correlation values 2^{-150} and 2^{-75} (over four rounds [15]), respectively. Both of them contain at least 25 active S-boxes. Boomerang distinguishers hold with probability about $2^{-67.5}$, and involve 33 active S-boxes. Finally, (4th-order) multiset (M) distinguishers hold with probability one and contain at least 40 active S-boxes.

Based on Table 2, we conclude that all permutations of the four round components in the AES have similar cryptographic strength against differential, linear, multiset, impossible differential and boomerang attacks. Some orderings of the round components, though, present slight advantages. For instance, in schemes (19) to (24) in Table 2, the SR and MC layers in the first round can be

[4] For instance, distinct diffusion layers [10].

Table 2: Parameters of attack distinguishers for different round orderings

	Round Type	Inverse Round	Multiset				Diff. Characteristic and Linear Relations		Imposs. Differential		Boomerang	
			1st-order		4th-order							
			#Rounds	#S	#Rounds	#S	#Rounds	#S	#Rounds	#S	#Rounds	#S
(1)	$\mathrm{MC}\circ\mathrm{SR}\circ\mathrm{SB}\circ\mathrm{AK}_i$	$\mathrm{AK}_i\circ\mathrm{SB}^{-1}\circ\mathrm{SR}^{-1}\circ\mathrm{MC}^{-1}$	3.25	21	4.25	40	4	25	3.75	10	5	33
(2)	$\mathrm{MC}\circ\mathrm{SR}\circ\mathrm{AK}_i\circ\mathrm{SB}$	$\mathrm{SB}^{-1}\circ\mathrm{AK}_i\circ\mathrm{SR}^{-1}\circ\mathrm{MC}^{-1}$	3.25	21	4.25	40	4	25	3.75	10	5	33
(3)	$\mathrm{MC}\circ\mathrm{AK}_i\circ\mathrm{SR}\circ\mathrm{SB}$	$\mathrm{SB}^{-1}\circ\mathrm{SR}^{-1}\circ\mathrm{AK}_i\circ\mathrm{MC}^{-1}$	3.25	21	4.25	40	4	25	3.75	10	5	33
(4)	$\mathrm{MC}\circ\mathrm{SB}\circ\mathrm{SR}\circ\mathrm{AK}_i$	$\mathrm{AK}_i\circ\mathrm{SR}^{-1}\circ\mathrm{SB}^{-1}\circ\mathrm{MC}^{-1}$	3.50	21	4.50	40	4	25	3.75	10	5	33
(5)	$\mathrm{MC}\circ\mathrm{SB}\circ\mathrm{AK}_i\circ\mathrm{SR}$	$\mathrm{SR}^{-1}\circ\mathrm{AK}_i\circ\mathrm{SB}^{-1}\circ\mathrm{MC}^{-1}$	3.50	21	4.50	40	4	25	3.75	10	5	33
(6)	$\mathrm{MC}\circ\mathrm{AK}_i\circ\mathrm{SB}\circ\mathrm{SR}$	$\mathrm{SR}^{-1}\circ\mathrm{SB}^{-1}\circ\mathrm{AK}_i\circ\mathrm{MC}^{-1}$	3.25	21	4.25	40	4	25	3.75	10	5	33
(7)	$\mathrm{SR}\circ\mathrm{MC}\circ\mathrm{AK}_i\circ\mathrm{SB}$	$\mathrm{SB}^{-1}\circ\mathrm{AK}_i\circ\mathrm{MC}^{-1}\circ\mathrm{SR}^{-1}$	3.25	21	4.25	40	4	25	4.25	10	5	33
(8)	$\mathrm{SR}\circ\mathrm{MC}\circ\mathrm{SB}\circ\mathrm{AK}_i$	$\mathrm{AK}_i\circ\mathrm{SB}^{-1}\circ\mathrm{MC}^{-1}\circ\mathrm{SR}^{-1}$	3.25	21	4.25	40	4	25	4.25	10	5	33
(9)	$\mathrm{SR}\circ\mathrm{AK}_i\circ\mathrm{MC}\circ\mathrm{SB}$	$\mathrm{SB}^{-1}\circ\mathrm{MC}^{-1}\circ\mathrm{AK}_i\circ\mathrm{SR}^{-1}$	3.25	21	4.25	40	4	25	4.25	10	5	33
(10)	$\mathrm{SR}\circ\mathrm{AK}_i\circ\mathrm{SB}\circ\mathrm{MC}$	$\mathrm{MC}^{-1}\circ\mathrm{SB}^{-1}\circ\mathrm{AK}_i\circ\mathrm{SR}^{-1}$	3.50	21	4.50	40	4	25	4.25	10	5	33
(11)	$\mathrm{SR}\circ\mathrm{SB}\circ\mathrm{AK}_i\circ\mathrm{MC}$	$\mathrm{MC}^{-1}\circ\mathrm{AK}_i\circ\mathrm{SB}^{-1}\circ\mathrm{SR}^{-1}$	3.50	21	4.50	40	4	25	4.25	10	5	33
(12)	$\mathrm{SR}\circ\mathrm{SB}\circ\mathrm{MC}\circ\mathrm{AK}_i$	$\mathrm{AK}_i\circ\mathrm{MC}^{-1}\circ\mathrm{SB}^{-1}\circ\mathrm{SR}^{-1}$	3.50	21	4.50	40	4	25	4.25	10	5	33
(13)	$\mathbf{AK}_i\circ\mathbf{MC}\circ\mathbf{SR}\circ\mathbf{SB}$	$\mathbf{SB}^{-1}\circ\mathbf{SR}^{-1}\circ\mathbf{MC}^{-1}\circ\mathbf{AK}_i$	**3.25**	**21**	**4.25**	**40**	**4**	**25**	**4.25**	**10**	**5**	**33**
(14)	$\mathrm{AK}_i\circ\mathrm{MC}\circ\mathrm{SB}\circ\mathrm{SR}$	$\mathrm{SR}^{-1}\circ\mathrm{SB}^{-1}\circ\mathrm{MC}^{-1}\circ\mathrm{AK}_i$	3.50	21	4.50	40	4	25	4.25	10	5	33
(15)	$\mathrm{AK}_i\circ\mathrm{SB}\circ\mathrm{MC}\circ\mathrm{SR}$	$\mathrm{SR}^{-1}\circ\mathrm{MC}^{-1}\circ\mathrm{SB}^{-1}\circ\mathrm{AK}_i$	3.75	21	4.75	40	4	25	4.25	10	5	33
(16)	$\mathrm{AK}_i\circ\mathrm{SB}\circ\mathrm{SR}\circ\mathrm{MC}$	$\mathrm{MC}^{-1}\circ\mathrm{SR}^{-1}\circ\mathrm{SB}^{-1}\circ\mathrm{AK}_i$	3.75	21	4.75	40	4	25	4.25	10	5	33
(17)	$\mathrm{AK}_i\circ\mathrm{SR}\circ\mathrm{MC}\circ\mathrm{SB}$	$\mathrm{SB}^{-1}\circ\mathrm{MC}^{-1}\circ\mathrm{SR}^{-1}\circ\mathrm{AK}_i$	3.25	21	4.25	40	4	25	4.25	10	5	33
(18)	$\mathrm{AK}_i\circ\mathrm{SR}\circ\mathrm{SB}\circ\mathrm{MC}$	$\mathrm{MC}^{-1}\circ\mathrm{SB}^{-1}\circ\mathrm{SR}^{-1}\circ\mathrm{AK}_i$	3.50	21	4.50	40	4	25	4.25	10	5	33
(19)	$\mathrm{SB}\circ\mathrm{MC}\circ\mathrm{SR}\circ\mathrm{AK}_i$	$\mathrm{AK}_i\circ\mathrm{SR}^{-1}\circ\mathrm{MC}^{-1}\circ\mathrm{SB}^{-1}$	3.75	21	4.75	40	4	25	4	10	5	33
(20)	$\mathrm{SB}\circ\mathrm{MC}\circ\mathrm{AK}_i\circ\mathrm{SR}$	$\mathrm{SR}^{-1}\circ\mathrm{AK}_i\circ\mathrm{MC}^{-1}\circ\mathrm{SB}^{-1}$	3.75	21	4.75	40	4	25	4	10	5	33
(21)	$\mathrm{SB}\circ\mathrm{AK}_i\circ\mathrm{MC}\circ\mathrm{SR}$	$\mathrm{SR}^{-1}\circ\mathrm{MC}^{-1}\circ\mathrm{AK}_i\circ\mathrm{SB}^{-1}$	3.75	21	4.75	40	4	25	4	10	5	33
(22)	$\mathrm{SB}\circ\mathrm{AK}_i\circ\mathrm{SR}\circ\mathrm{MC}$	$\mathrm{MC}^{-1}\circ\mathrm{SR}^{-1}\circ\mathrm{AK}_i\circ\mathrm{SB}^{-1}$	3.75	21	4.75	40	4	25	4	10	5	33
(23)	$\mathrm{SB}\circ\mathrm{SR}\circ\mathrm{MC}\circ\mathrm{AK}_i$	$\mathrm{AK}_i\circ\mathrm{MC}^{-1}\circ\mathrm{SR}^{-1}\circ\mathrm{SB}^{-1}$	3.75	21	4.75	40	4	25	4	10	5	33
(24)	$\mathrm{SB}\circ\mathrm{SR}\circ\mathrm{AK}_i\circ\mathrm{MC}$	$\mathrm{MC}^{-1}\circ\mathrm{AK}_i\circ\mathrm{SR}^{-1}\circ\mathrm{SB}^{-1}$	3.75	21	4.75	40	4	25	4	10	5	33

Context	CP	CP for DC	KP for LC	CP	CPACC
Probability or Correlation	1	$\approx 2^{-150}$ for DC	$\approx 2^{-75}$ for LC	0	$2^{-67.5}$

CP: Chosen-Plaintext; KP: Known-Plaintext; CPACC: Chosen-Plaintext Adaptively-Chosen Ciphertext.

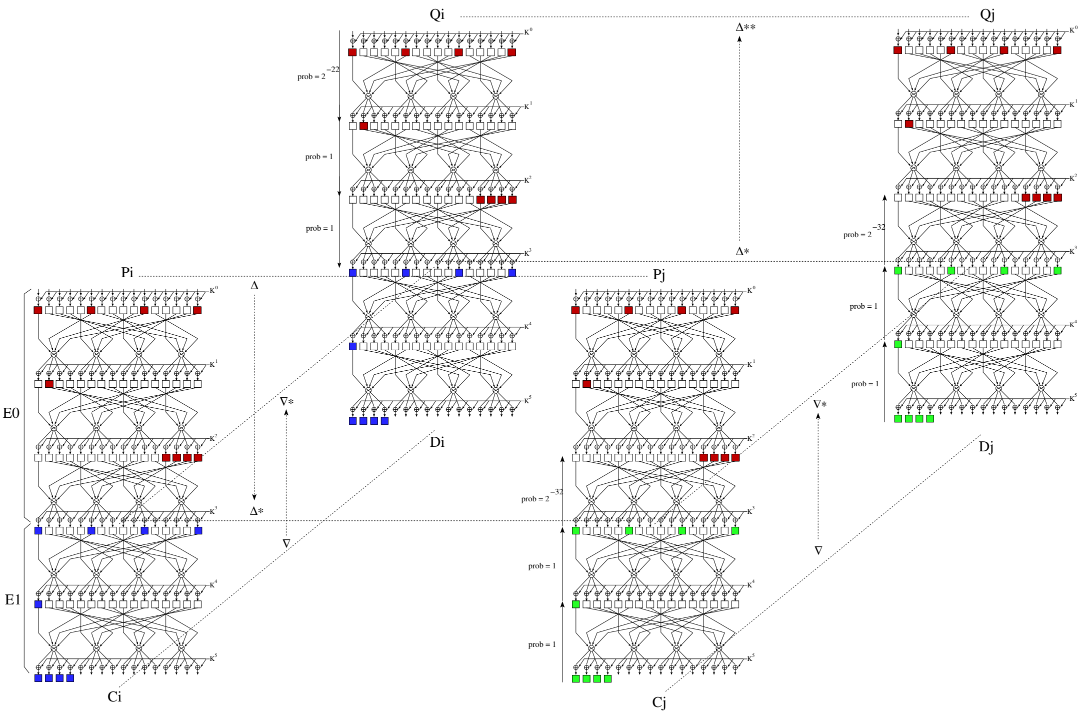

Figure 2: 3D view of a boomerang distinguisher for 5-round AES

easily removed. Moreover, it is irrelevant to add a prewhitening layer to these schemes because an equivalent scheme can be obtained by simply commuting the first subkey after SR and MC, which are all linear operations. Similarly, the SR layer in the last round in schemes (1) to (12) can be removed, even with a post-whitening subkey layer. The AES scheme (13) can also have both the first and the last SR layers removed (just like the IP and IP^{-1} in DES [19]).

8 Conclusions

This paper studied all 24 different orderings of the four round components in the AES cipher against (conventional) differential, (conventional) linear, multiset, impossible differential and boomerang attacks. These five attack techniques were selected since they are among the most relevant attacks on reduced-round instances of the AES.Our security evaluation focused on the size, the probability and the (minimum) number of active S-boxes for the distinguishers. The minimum number of active S-boxes is an important security measure because the S-box is the only nonlinear cipher component in the AES. From the size and probability of the distinguishers one can conclude that the attack complexities do not differ significantly among the 24 permutations of the round components (including the AES). Moreover, we have noticed an apparent correlation between the probability a distinguisher holds, and the (minimum) number of active S-boxes: the higher the probability, the larger the number of active S-boxes (Table 2).

Our analyses provided evidence that the 24 permutations of the round components of the AES have similar cryptographic strength, at least concerning the five attack techniques discussed in this paper. The particular ordering of round components used in the AES, denoted (13), avoids some components to be removed (due to the non-commutativity of round components, and because they are key independent), except for the first and last SR layers. In this case, schemes (8) and (17) (with pre-whitening) in Table 2 are more attractive than (13) since the former forbids the first SR layer to be removed, because the MC and SR operations do not commute.

Whatever the ordering of the round components, though, both the encryption and the decryption operations do share a similar computational framework[5], which implies that both operations have the same cryptographic strength in all 24 round variants. Moreover, this similarity between encryption and decryption also reduces the implementation costs in hardware and software.

References

[1] AES, *The Advanced Encryption Standard Development Process*, 1997. (http://csrc.nist.gov/encryption/aes/)

[2] E. Barkan and E. Biham, *In How Many Ways Can You Write Rijndael*, IACR Cryptology ePrint Archive #157, 2002.

[5] Except for a preprocessing step of the decryption subkeys in the key schedule.

[3] E. Barkan and E. Biham, *The Book of Rijndaels*, IACR Cryptology ePrint Archive #158, 2002.

[4] E. Biham, A. Biryukov, O. Dunkelman, E. Richardson, and A. Shamir, *Initial Observations on Skipjack: Cryptanalysis of Skipjack-3XOR*, Technical Report CS0946, Technion, Computer Science Department, 1998.

[5] E. Biham, A. Biryukov, and A. Shamir, *Cryptanalysis of Skipjack Reduced to 31 Rounds using Impossible Differentials*, Tech Report CS0947, Technion, Computer Science Department, 1998.

[6] E. Biham and N. Keller, "Cryptanalysis of reduced variants of Rijndael," in *3rd AES Conference*, New York, USA, 2000. (http://csrc.nist.gov/aes/index.html)

[7] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems (extended abstract)," in *Advances in Cryptology (Crypto'90)*, LNCS 537, pp. 1-19, Springer-Verlag, 1991.

[8] E. Biham and A. Shamir,"Differential cryptanalysis of the full 16-round DES," in *Advances in Cryptology (Crypto'92)*, LNCS 740, 487-496, Springer-Verlag, 1993.

[9] A. Biryukov, "The boomerang attack on 5 and 6-round reduced AES," in *Proceedings of AES4 Conference*, LNCS 3373, pp. 11-15, Springer-Verlag, 2004.

[10] A. Biryukov, C. De Cannière, and G. Dellkrantz, "Cryptanalysis of SAFER++," in *Advances in Cryptology (Crypto'03)*, LNCS 2729, pp. 195-211, Springer-Verlag, 2003.

[11] A. Biryukov and A. Shamir, "Structural cryptanalysis of SASAS," in *Advances in Cryptology (Eurocrypt'01)*, LNCS 2045, pp. 394-405, Springer-Verlag, 2001.

[12] J. H. Cheon, M. Kim, K. Kim, J.-Y. Lee, and S. W. Kang, "Improved impossible differential cryptanalysis of Rijndael and Crypton," in *Proceedings of ICISC'01*, LNCS 2288, pp. 39-49, Springer-Verlag, 2001.

[13] D. Coppersmith, "The data encryption algorithm and its strength against attacks," *IBM Journal on Research and Development*, vol. 38, no. 3, pp. 243-250, 1994.

[14] J. Daemen, L. R. Knudsen, and V. Rijmen, "The block cipher SQUARE," in *4th Fast Software Encryption Workshop*, LNCS 1267, pp. 149-165, Springer-Verlag, 1997.

[15] J. Daemen and V. Rijmen, "AES proposal: Rijndael," in *1st AES Conference*, California, USA, 1998. (http://www.nist.gov/aes)

[16] J. Daemen and V. Rijmen, *The Design of Rijndael-AES-The Advanced Encryption Standard*, Springer-Verlag, 2002.

[17] H. Demirci, "Square-like attacks on reduced rounds of IDEA," in *9th Selected Areas in Cryptography Workshop (SAC'02)*, LNCS 2595, pp. 147-159, Springer-Verlag, Aug. 2002.

[18] N. Ferguson, J. Kelsey, S. Lucks, B. Schneier, M. Stay, D. Wagner, and D. Whiting, "Improved cryptanalysis of Rijndael," in *7th Fast Software Encryption Workshop*, LNCS 1978, pp. 213-230, Springer-Verlag, 2000.

[19] FIPS-46-3, *Data Encryption Standard (DES)*, Federal Information Processing Standards Publication 46-3, Oct. 1999.

[20] H. Gilbert and M. Minier, "A collision attack on seven rounds of Rijndael," in *3rd AES Conference*, pp. 230-241, New York, USA, 2000. (http://csrc.nist.gov/archive/aes/index.html)

[21] H. Hwang, W. Lee, S. Lee, S. Lee, and J. Lim, "Saturation attacks on reduced-round skipjack," in *9th Fast Software Encryption Workshop*, LNCS 2365, pp. 100-111, Springer-Verlag, 2002.

[22] Y. Hu, Y. Zhang, and G. Xiao, "Integral cryptanalysis of SAFER+," *Electronic Letters*, vol. 35, no. 17, pp. 1458-1459, Aug. 1999.

[23] I. Kim, Y. Yeom, and H. Kim, "Square attacks on the reduced-round MISTY1," *Symposium on Cryptography and Information Security*, pp. 921-924, 2002.

[24] L. R. Knudsen, *DEAL – a 128-bit Block Cipher*, Technical Report #151, University of Bergen, Department of Informatics, Norway, Feb. 1998.

[25] L. R. Knudsen and D. Wagner, "Integral cryptanalysis," in *9th Fast Software Encryption Workshop*, LNCS 2365, pp. 112-127, Springer-Verlag, 2002.

[26] S. Lucks, "The saturation attack – a bait for twofish," in *8th Fast Software Encryption Workshop*, LNCS 2355, pp. 1-15, Springer-Verlag, 2001.

[27] M. Matsui, "Linear cryptanalysis method for DES cipher," in *Advances in Cryptology (Eurocrypt'93)*, LNCS 765, pp. 386-397, Springer-Verlag, 1994.

[28] NIST, *Advanced Encryption Standard, AES*, FIPS PUB 197 Federal Information Processing Standard Publication 197, U.S. Department of Commerce, Nov. 2001.

[29] R. C. W. Phan and M. U. Siddiqi, "Generalized impossible differentials of advanced encryption standard," *IEE Electronics Letters*, vol. 37, no. 14, pp. 896-898, July 2001.

[30] R. C. W. Phan, "Classes of impossible differentials of advanced encryption standard," *IEE Electronics Letters*, vol. 38, no. 11, pp. 508-510, May 2002.

[31] *The Block Cipher Rijndael.* (http://www.iaik.tugraz.at/research/krypto/AES/#links)

[32] D. Wagner, "The boomerang attack," in *6th Fast Software Encryption Workshop*, LNCS 1636, pp. 156-170, Springer-Verlag, 1999.

Jorge Nakahara Jr obtained his BSc and MSc degrees in Computer Science from the Institute of Mathematics and Statistics of the Univ. of Sao Paulo, in Sao Paulo, Brazil, in 1989 and 1996. He further obtained a MSc and PhD degrees in Electrical Engineering from the Katholieke Universiteit Leuven, in Leuven, Belgium, in 1998 and 2003. He is currently a member of the Distributed Systems group at the Univ. Catolica de Santos, in Santos, Brazil."