Analysis of Venkaiah *et al.*'s AES Design

Jorge Nakahara Jr
Department of Informatics, Universidade Catolica de Santos, UNISANTOS
R. Dr. Carvalho de Mendonça, 144, POBOX 11070-906, São Paulo, Brazil
(Email: jorge_nakahara@yahoo.com.br)

(Received Oct. 25, 2006; revised and accepted June 27, 2007)

Abstract

This paper describes impossible differential (ID) attacks on an AES variant designed by Venkaiah *et al.*. They claim that their cipher has improved resistance to ID attacks due to a new MixColumns matrix with a branch number 4, which is smaller than that of the original AES. We argue against this statement. The contributions of this paper include ID distinguishers for Venkaiah *et al.*'s cipher, and a discussion of the susceptibility of such variants to impossible differential and other modern cryptanalytic techniques.

Keywords: AES, block cipher cryptanalysis, impossible differentials

1 Introduction

Rijndael is a Substitution Permutation Network (SPN) type block cipher designed by Joan Daemen and Vincent Rijmen for the AES Development Process, initiated by the National Institute of Standards and Technology (NIST) in the USA in 1997 [1, 9]. The 128-bit block version of Rijndael, with a key of 128, 192 or 256 bits, is officially known as the AES [10]. Typically, text blocks, keys and subkeys are represented compactly by a $4 \times Nb$ state matrix of bytes, where Nb is the number of 32-bit words in a block. For instance, the state matrix for a $4t$-byte text block, $A = (a_0, a_1, a_2, a_3, a_4, \ldots, a_{4t-1})$, is denoted

$$\text{State} = \begin{pmatrix} a_0 & a_4 & \cdots & a_{4t-4} \\ a_1 & a_5 & \cdots & a_{4t-3} \\ a_2 & a_6 & \cdots & a_{4t-2} \\ a_3 & a_7 & \cdots & a_{4t-1} \end{pmatrix} \qquad (1)$$

namely, with bytes inserted columnwise. Note that byte positions in a state matrix follows the subscripts of the bytes in (1).

There are four layers in a full round of Rijndael, in order: SubBytes (denoted SB), ShiftRows (SR), MixColumns (MC) and AddRoundKey (AK$_i$, where i is the round number) [10].

This paper is organized as follows: Section 2 describes the AES variant by Venkaiah *et al.*. Section 3 gives a brief overview of the impossible-differential technique. Section 5 concludes the paper.

2 Venkaiah *et al.*'s AES Design

In [14], Venkaiah *et al.* suggested a variant of AES with a new S-box, a modified MixColumns matrix, and a new irreducible polynomial for GF(2^8). They used $x^8 + x^6 + x^5 + x + 1$ as primitive irreducible polynomial for GF(2^8), in contrast to the AES irreducible (but not primitive) polynomial $x^8 + x^4 + x^3 + x + 1$. Their new S-box was constructed based on two transformations in this order:

- powers of 3, a primitive element in F^*_{257}. If the power is 256, the result is treated as 0.
- take multiplicative inverse in GF(2^8), with 0 mapped to itself.

One feature of their new S-box is its algebraic expression in GF(2^8) = GF(2)[x] / (x^8+ x^6 + x^5 + x + 1): $S'[x] = \mathtt{01}_{\mathrm{x}} + \mathtt{2f}_{\mathrm{x}}.x + \mathtt{d2}_{\mathrm{x}}.x^2 + \mathtt{23}_{\mathrm{x}}.x^3 + \mathtt{dd}_{\mathrm{x}}.x^4 + \mathtt{ed}_{\mathrm{x}}.x^5 +$ $\mathtt{a8}_{\mathrm{x}}.x^6 + \mathtt{98}_{\mathrm{x}}.x^7 + \mathtt{49}_{\mathrm{x}}.x^8 + \mathtt{03}_{\mathrm{x}}.x^9 + \mathtt{a4}_{\mathrm{x}}.x^{10} + \mathtt{39}_{\mathrm{x}}.x^{11} +$ $\mathtt{78}_{\mathrm{x}}.x^{12} + \mathtt{8e}_{\mathrm{x}}.x^{13} + \mathtt{94}_{\mathrm{x}}.x^{14} + \mathtt{f2}_{\mathrm{x}}.x^{15} + \mathtt{19}_{\mathrm{x}}.x^{16} + \mathtt{66}_{\mathrm{x}}.x^{17} +$ $\mathtt{bc}_{\mathrm{x}}.x^{18} + \mathtt{46}_{\mathrm{x}}.x^{19} + \mathtt{6f}_{\mathrm{x}}.x^{20} + \mathtt{74}_{\mathrm{x}}.x^{21} + \mathtt{db}_{\mathrm{x}}.x^{22} + \mathtt{70}_{\mathrm{x}}.x^{23} +$ $\mathtt{75}_{\mathrm{x}}.x^{24} + \mathtt{43}_{\mathrm{x}}.x^{25} + \mathtt{e3}_{\mathrm{x}}.x^{26} + \mathtt{eb}_{\mathrm{x}}.x^{27} + \mathtt{eb}_{\mathrm{x}}.x^{28} + \mathtt{ad}_{\mathrm{x}}.x^{29} +$ $\mathtt{79}_{\mathrm{x}}.x^{30} + \mathtt{22}_{\mathrm{x}}.x^{31} + \mathtt{fb}_{\mathrm{x}}.x^{32} + \mathtt{ed}_{\mathrm{x}}.x^{33} + \mathtt{28}_{\mathrm{x}}.x^{34} + \mathtt{62}_{\mathrm{x}}.x^{35} +$ $\mathtt{f4}_{\mathrm{x}}.x^{36} + \mathtt{24}_{\mathrm{x}}.x^{37} + \mathtt{36}_{\mathrm{x}}.x^{38} + \mathtt{4b}_{\mathrm{x}}.x^{39} + \mathtt{31}_{\mathrm{x}}.x^{40} + \mathtt{ae}_{\mathrm{x}}.x^{41} +$ $\mathtt{bf}_{\mathrm{x}}.x^{42} + \mathtt{3f}_{\mathrm{x}}.x^{43} + \mathtt{57}_{\mathrm{x}}.x^{44} + \mathtt{22}_{\mathrm{x}}.x^{45} + \mathtt{9f}_{\mathrm{x}}.x^{46} + \mathtt{a4}_{\mathrm{x}}.x^{47} +$ $\mathtt{b7}_{\mathrm{x}}.x^{48} + \mathtt{96}_{\mathrm{x}}.x^{49} + \mathtt{56}_{\mathrm{x}}.x^{50} + \mathtt{25}_{\mathrm{x}}.x^{51} + \mathtt{56}_{\mathrm{x}}.x^{52} + \mathtt{8e}_{\mathrm{x}}.x^{53} +$ $\mathtt{c7}_{\mathrm{x}}.x^{54} + \mathtt{9c}_{\mathrm{x}}.x^{55} + \mathtt{26}_{\mathrm{x}}.x^{56} + \mathtt{57}_{\mathrm{x}}.x^{57} + \mathtt{05}_{\mathrm{x}}.x^{58} + \mathtt{82}_{\mathrm{x}}.x^{59} +$ $\mathtt{ea}_{\mathrm{x}}.x^{60} + \mathtt{bb}_{\mathrm{x}}.x^{61} + \mathtt{2b}_{\mathrm{x}}.x^{62} + \mathtt{f6}_{\mathrm{x}}.x^{63} + \mathtt{13}_{\mathrm{x}}.x^{64} + \mathtt{96}_{\mathrm{x}}.x^{65} +$ $\mathtt{c8}_{\mathrm{x}}.x^{66} + \mathtt{5a}_{\mathrm{x}}.x^{67} + \mathtt{ba}_{\mathrm{x}}.x^{68} + \mathtt{da}_{\mathrm{x}}.x^{69} + \mathtt{27}_{\mathrm{x}}.x^{70} + \mathtt{60}_{\mathrm{x}}.x^{71} +$ $\mathtt{c8}_{\mathrm{x}}.x^{72} + \mathtt{74}_{\mathrm{x}}.x^{73} + \mathtt{b8}_{\mathrm{x}}.x^{74} + \mathtt{d5}_{\mathrm{x}}.x^{75} + \mathtt{f2}_{\mathrm{x}}.x^{76} + \mathtt{c2}_{\mathrm{x}}.x^{77} +$ $\mathtt{71}_{\mathrm{x}}.x^{78} + \mathtt{a1}_{\mathrm{x}}.x^{79} + \mathtt{c3}_{\mathrm{x}}.x^{80} + \mathtt{85}_{\mathrm{x}}.x^{81} + \mathtt{b7}_{\mathrm{x}}.x^{82} + \mathtt{6d}_{\mathrm{x}}.x^{83} +$ $\mathtt{18}_{\mathrm{x}}.x^{84} + \mathtt{c7}_{\mathrm{x}}.x^{85} + \mathtt{72}_{\mathrm{x}}.x^{86} + \mathtt{ea}_{\mathrm{x}}.x^{87} + \mathtt{07}_{\mathrm{x}}.x^{88} + \mathtt{ac}_{\mathrm{x}}.x^{89} +$ $\mathtt{18}_{\mathrm{x}}.x^{90} + \mathtt{13}_{\mathrm{x}}.x^{91} + \mathtt{85}_{\mathrm{x}}.x^{92} + \mathtt{b7}_{\mathrm{x}}.x^{93} + \mathtt{a4}_{\mathrm{x}}.x^{94} + \mathtt{c2}_{\mathrm{x}}.x^{95} +$ $\mathtt{23}_{\mathrm{x}}.x^{96} + \mathtt{ee}_{\mathrm{x}}.x^{97} + \mathtt{e2}_{\mathrm{x}}.x^{98} + \mathtt{59}_{\mathrm{x}}.x^{99} + \mathtt{46}_{\mathrm{x}}.x^{100} + \mathtt{34}_{\mathrm{x}}.x^{101} +$ $\mathtt{a1}_{\mathrm{x}}.x^{102} + \mathtt{38}_{\mathrm{x}}.x^{103} + \mathtt{3c}_{\mathrm{x}}.x^{104} + \mathtt{0b}_{\mathrm{x}}.x^{105} + \mathtt{7d}_{\mathrm{x}}.x^{106} +$ $\mathtt{b4}_{\mathrm{x}}.x^{107} + \mathtt{41}_{\mathrm{x}}.x^{108} + \mathtt{05}_{\mathrm{x}}.x^{109} + \mathtt{e7}_{\mathrm{x}}.x^{110} + \mathtt{ee}_{\mathrm{x}}.x^{111} +$ $\mathtt{5d}_{\mathrm{x}}.x^{112} + \mathtt{80}_{\mathrm{x}}.x^{113} + \mathtt{b5}_{\mathrm{x}}.x^{114} + \mathtt{15}_{\mathrm{x}}.x^{115} + \mathtt{d4}_{\mathrm{x}}.x^{116} +$ $\mathtt{65}_{\mathrm{x}}.x^{117} + \mathtt{85}_{\mathrm{x}}.x^{118} + \mathtt{8f}_{\mathrm{x}}.x^{119} + \mathtt{ec}_{\mathrm{x}}.x^{120} + \mathtt{50}_{\mathrm{x}}.x^{121} +$ $\mathtt{cc}_{\mathrm{x}}.x^{122} + \mathtt{2a}_{\mathrm{x}}.x^{123} + \mathtt{8f}_{\mathrm{x}}.x^{124} + \mathtt{0c}_{\mathrm{x}}.x^{125} + \mathtt{85}_{\mathrm{x}}.x^{126} +$ $\mathtt{9e}_{\mathrm{x}}.x^{127} + \mathtt{3f}_{\mathrm{x}}.x^{128} + \mathtt{02}_{\mathrm{x}}.x^{129} + \mathtt{e9}_{\mathrm{x}}.x^{130} + \mathtt{6a}_{\mathrm{x}}.x^{131} +$

$\mathtt{c4}_x.x^{132} + \mathtt{1e}_x.x^{133} + \mathtt{7a}_x.x^{134} + \mathtt{16}_x.x^{135} + \mathtt{c6}_x.x^{136} + \mathtt{cf}_x.x^{137} + \mathtt{3d}_x.x^{138} + \mathtt{1c}_x.x^{139} + \mathtt{9b}_x.x^{140} + \mathtt{ea}_x.x^{141} + \mathtt{fc}_x.x^{142} + \mathtt{96}_x.x^{143} + \mathtt{64}_x.x^{144} + \mathtt{02}_x.x^{145} + \mathtt{85}_x.x^{146} + \mathtt{55}_x.x^{147} + \mathtt{9f}_x.x^{148} + \mathtt{20}_x.x^{149} + \mathtt{96}_x.x^{150} + \mathtt{ac}_x.x^{151} + \mathtt{6d}_x.x^{152} + \mathtt{96}_x.x^{153} + \mathtt{a7}_x.x^{154} + \mathtt{0e}_x.x^{155} + \mathtt{4f}_x.x^{156} + \mathtt{75}_x.x^{157} + \mathtt{29}_x.x^{158} + \mathtt{a8}_x.x^{159} + \mathtt{b5}_x.x^{160} + \mathtt{fd}_x.x^{161} + \mathtt{66}_x.x^{162} + \mathtt{6d}_x.x^{163} + \mathtt{1f}_x.x^{164} + \mathtt{51}_x.x^{165} + \mathtt{fe}_x.x^{166} + \mathtt{6d}_x.x^{167} + \mathtt{98}_x.x^{168} + \mathtt{cb}_x.x^{169} + \mathtt{f2}_x.x^{170} + \mathtt{d6}_x.x^{171} + \mathtt{61}_x.x^{172} + \mathtt{4d}_x.x^{173} + \mathtt{e6}_x.x^{174} + \mathtt{10}_x.x^{175} + \mathtt{4d}_x.x^{176} + \mathtt{80}_x.x^{177} + \mathtt{88}_x.x^{178} + \mathtt{a1}_x.x^{179} + \mathtt{d8}_x.x^{180} + \mathtt{f4}_x.x^{181} + \mathtt{20}_x.x^{182} + \mathtt{f1}_x.x^{183} + \mathtt{17}_x.x^{184} + \mathtt{49}_x.x^{185} + \mathtt{09}_x.x^{186} + \mathtt{f8}_x.x^{187} + \mathtt{90}_x.x^{188} + \mathtt{ce}_x.x^{189} + \mathtt{e6}_x.x^{190} + \mathtt{2f}_x.x^{191} + \mathtt{ac}_x.x^{192} + \mathtt{94}_x.x^{193} + \mathtt{19}_x.x^{194} + \mathtt{b8}_x.x^{195} + \mathtt{32}_x.x^{196} + \mathtt{3e}_x.x^{197} + \mathtt{b7}_x.x^{198} + \mathtt{06}_x.x^{199} + \mathtt{93}_x.x^{200} + \mathtt{60}_x.x^{201} + \mathtt{09}_x.x^{202} + \mathtt{22}_x.x^{203} + \mathtt{ee}_x.x^{204} + \mathtt{85}_x.x^{205} + \mathtt{d1}_x.x^{206} + \mathtt{5e}_x.x^{207} + \mathtt{49}_x.x^{208} + \mathtt{d6}_x.x^{209} + \mathtt{61}_x.x^{210} + \mathtt{47}_x.x^{211} + \mathtt{79}_x.x^{212} + \mathtt{1d}_x.x^{213} + \mathtt{27}_x.x^{214} + \mathtt{7a}_x.x^{215} + \mathtt{19}_x.x^{216} + \mathtt{68}_x.x^{217} + \mathtt{ed}_x.x^{218} + \mathtt{59}_x.x^{219} + \mathtt{c4}_x.x^{220} + \mathtt{e7}_x.x^{221} + \mathtt{4d}_x.x^{222} + \mathtt{7a}_x.x^{223} + \mathtt{75}_x.x^{224} + \mathtt{a3}_x.x^{225} + \mathtt{dd}_x.x^{226} + \mathtt{f0}_x.x^{227} + \mathtt{67}_x.x^{228} + \mathtt{0e}_x.x^{229} + \mathtt{0c}_x.x^{230} + \mathtt{da}_x.x^{231} + \mathtt{53}_x.x^{232} + \mathtt{ce}_x.x^{233} + \mathtt{3c}_x.x^{234} + \mathtt{a6}_x.x^{235} + \mathtt{c0}_x.x^{236} + \mathtt{70}_x.x^{237} + \mathtt{32}_x.x^{238} + \mathtt{77}_x.x^{239} + \mathtt{56}_x.x^{240} + \mathtt{95}_x.x^{241} + \mathtt{20}_x.x^{242} + \mathtt{d1}_x.x^{243} + \mathtt{8b}_x.x^{244} + \mathtt{20}_x.x^{245} + \mathtt{a2}_x.x^{246} + \mathtt{d9}_x.x^{247} + \mathtt{ea}_x.x^{248} + \mathtt{a7}_x.x^{249} + \mathtt{58}_x.x^{250} + \mathtt{49}_x.x^{251} + \mathtt{c9}_x.x^{252} + \mathtt{0d}_x.x^{253} + \mathtt{29}_x.x^{254}$, which is much more involved and certainly not as sparse as AES S-box expression $S[x] = \mathtt{63}_x + \mathtt{8f}_x.x^{127} + \mathtt{b5}_x.x^{191} + \mathtt{01}_x.x^{223} + \mathtt{f4}_x.x^{239} + \mathtt{25}_x.x^{247} + \mathtt{f9}_x.x^{251} + \mathtt{09}_x.x^{253} + \mathtt{05}_x.x^{254}$. The subscript x indicates hexadecimal notation. The motivation for this new S-box, denoted S', may be related to attacks exploiting the sparsity of the algebraic expression of the AES S-box [8].

The highest non-trivial differential probability and maximum non-trivial linear probability of S' are depicted in Table 1, together with the profiles for the AES S-box [9]. These figures are called simply differential and linear profiles of S'.

From a differential cryptanalysis perspective, the AES S-box maximum probability is smaller than Venkaiah *et al.*'s AES S-box. Thus, the former's differential profile is better than the latter's. Also, from a linear cryptanalysis point of view, the original AES S-box linear profile is better than Venkaiah *et al.*'s profile.

Before discussing the minimum number of rounds for a differential and a linear attack, we first discuss the diffusion power of Venkaiah *et al.*'s AES. Another modification suggested in [14] is a new MixColumns matrix, which we denote MC', with branch number four:

$$MC' = \begin{bmatrix} \mathtt{02}_x & \mathtt{01}_x & \mathtt{03}_x & \mathtt{01}_x \\ \mathtt{01}_x & \mathtt{02}_x & \mathtt{01}_x & \mathtt{03}_x \\ \mathtt{03}_x & \mathtt{01}_x & \mathtt{02}_x & \mathtt{01}_x \\ \mathtt{01}_x & \mathtt{03}_x & \mathtt{01}_x & \mathtt{02}_x \end{bmatrix} \qquad (2)$$

An example of an input/output difference tuple with branch number four is $(\delta, 0, \delta, 0) \overset{MC'}{\to} (\delta, 0, \delta, 0)$, where $\delta \neq 0$. Similarly, $(0, \delta, 0, \delta) \overset{MC'}{\to} (0, \delta, 0, \delta)$. These differences tuples show that MC' is not an MDS matrix, since there are 2×2 singular submatrices of MC', such as

$$\begin{bmatrix} \mathtt{01}_x & \mathtt{01}_x \\ \mathtt{01}_x & \mathtt{01}_x \end{bmatrix} \qquad (3)$$

Notice that MC' uses the same coefficients as the original MixColumns matrix of the AES, but in a different order. The apparent motivation for the choice of MC' was to speed up the decryption procedure, since MC' is involutory (it is its own inverse). But, this discrepancy between the performance of AES encryption and decryption procedures can be diminished by other means, as pointed out by Barreto in [2], in which the InvMixColumns matrix is split as

$$\begin{bmatrix} \mathtt{0e}_x & \mathtt{0b}_x & \mathtt{0d}_x & \mathtt{09}_x \\ \mathtt{09}_x & \mathtt{0e}_x & \mathtt{0b}_x & \mathtt{0d}_x \\ \mathtt{0d}_x & \mathtt{09}_x & \mathtt{0e}_x & \mathtt{0b}_x \\ \mathtt{0b}_x & \mathtt{0d}_x & \mathtt{09}_x & \mathtt{0e}_x \end{bmatrix} \cdot \begin{bmatrix} \mathtt{05}_x & \mathtt{00}_x & \mathtt{04}_x & \mathtt{00}_x \\ \mathtt{00}_x & \mathtt{05}_x & \mathtt{00}_x & \mathtt{04}_x \\ \mathtt{04}_x & \mathtt{00}_x & \mathtt{05}_x & \mathtt{00}_x \\ \mathtt{00}_x & \mathtt{04}_x & \mathtt{00}_x & \mathtt{05}_x \end{bmatrix} = \begin{bmatrix} \mathtt{02}_x & \mathtt{03}_x & \mathtt{01}_x & \mathtt{01}_x \\ \mathtt{01}_x & \mathtt{02}_x & \mathtt{03}_x & \mathtt{01}_x \\ \mathtt{01}_x & \mathtt{01}_x & \mathtt{02}_x & \mathtt{03}_x \\ \mathtt{03}_x & \mathtt{01}_x & \mathtt{01}_x & \mathtt{02}_x \end{bmatrix} \qquad (4)$$

The matrix in the right-hand-side of (4) is the AES matrix used in encryption mode. The leftmost matrix in (4) is used in decryption mode. According to [2] "InvMixColumn can be efficiently implemented with the same resources as MixColumn, plus six exclusive-ors and four xtime calls".

The main drawback of MC' is that it is not an MDS matrix like AES's MixColumn matrix. Venkaiah *et al.* stated in [14] that MC' "... has branch number 4 and, correspondingly, has low diffusion power. This reduction in branch number may be viewed positively as a way to curtail the effect of impossible differential cryptanalysis". The consequences of the smaller branch number from an ID cryptanalysis perspective are discussed in Section 4.

An immediate consequence of the smaller branch number in Venkaiah *et al.*'s design concerns the resistance to differential [6] and linear [13] cryptanalysis. In (5), we depict an 4-round differential of Venkaiah *et al.*'s AES, constructed to minimize the number of active S-boxes, using MC' and (3). The symbol δ denotes a nonzero exclusive-or byte difference, and 0 a zero byte difference. The round transformations, AddRoundKey (AK$_i$), SubBytes (SB), ShiftRows (SR) and MixColumns (MC) are composed in left-to-right order, for instance, $SR \circ SB \circ AK_0(X) = SR(SB(AK_0(X)))$. Notice that there are 20 active S-boxes in (5). Table 2 compares the number of active S-boxes of the best differential characteristics and linear relations across four rounds of Venkaiah *et al.*'s design and for the AES.

Taking into account Tables 1 and 2, Venkaiah *et al.*'s design not only have a smaller number of active S-boxes (due to weaker diffusion of MC'), but also the differential profile of S' is worse (higher) than that of the AES S-box. Concerning differential cryptanalysis (DC), the estimated number of active S-boxes for four rounds is 20, and the probability of the differential becomes $(2^{-4.41})^{20} = 2^{-88.2}$, while for the AES, the corresponding probability is $(2^{(}-6)^{25}) = 2^{-150}$. Analogously, for LC, Venkaiah *et al.*'s design restricted to four rounds has bias of the linear relation equal to $(2^{-2.83})^{20} = 2^{-56.6}$, while for the AES, it is $(2^{(}-3)^{25}) = 2^{-75}$. Thus, considering conventional DC and LC, the original AES [9] is

Table 1: Differential and linear profiles of S and S'

Cipher	Best nontrivial DC profile of S	Best nontrivial LC profile of S'
AES	2^{-6}	2^{-3}
Venkaiah *et al.*	$12/256 \approx 2^{-4.41}$	$36/256 \approx 2^{-2.83}$

Table 2: Comparison of differential and linear profiles

Cipher	Branch Number	# act. S-boxes DC (4 rounds)	# act. S-boxes LC (4 rounds)
AES	5	25	25
Venkaiah *et al.*'s	4	20	20

# active S-box DC: minimum number of active S-boxes in a differential characteristic across 4 rounds.
# active S-box LC: minimum number of active S-boxes in a linear relation across 4 rounds.

more robust than Venkaiah *et al.*'s design.

$$\begin{pmatrix} \delta & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & \delta & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \xrightarrow{SR\circ SB\circ AK_0} \begin{pmatrix} \delta & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \delta & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$
$$\xrightarrow{SB\circ AK_1\circ MC'} \begin{pmatrix} \delta & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \delta & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \xrightarrow{SR} \begin{pmatrix} \delta & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & \delta & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$
$$\xrightarrow{SB\circ AK_2\circ MC'} \begin{pmatrix} \delta & 0 & \delta & 0 \\ \delta & 0 & \delta & 0 \\ \delta & 0 & \delta & 0 \\ \delta & 0 & \delta & 0 \end{pmatrix} \xrightarrow{SR} \begin{pmatrix} \delta & 0 & \delta & 0 \\ 0 & \delta & 0 & \delta \\ \delta & 0 & \delta & 0 \\ 0 & \delta & 0 & \delta \end{pmatrix}$$
$$\xrightarrow{SB\circ AK_3\circ MC'} \begin{pmatrix} \delta & 0 & \delta & 0 \\ 0 & \delta & 0 & \delta \\ \delta & 0 & \delta & 0 \\ 0 & \delta & 0 & \delta \end{pmatrix} \xrightarrow{AK_4\circ SR} \begin{pmatrix} \delta & 0 & \delta & 0 \\ \delta & 0 & \delta & 0 \\ \delta & 0 & \delta & 0 \\ \delta & 0 & \delta & 0 \end{pmatrix} \quad (5)$$

3 Impossible Differential Attacks

Unlike differential and linear techniques, which look for events such as text patterns or statistical correlations of high probability, the impossible differential (ID) method looks for events that never happen. The impossible differential (ID) technique operates in a chosen-plaintext setting. This attack was formerly proposed in [11] against the DEAL block cipher, and further applied to Skipjack [3], IDEA and Khufu [4], the AES [5] and several other ciphers.

ID distinguishers currently reported in the literature use the miss-in-the-middle technique described in [3]. This technique requires two differentials (∇ and Δ) both holding with probability one. We denote by ∇ the "top-down" truncated differential, because the difference patterns propagate in the encryption direction. And Δ is the "bottom-up" truncated differential because the difference patterns propagate in the decryption direction. The ID distinguisher consists of the concatenation of both differentials. But, the differentials are constructed such that the output difference pattern of ∇ is incompatible with the output difference pattern of Δ, in the sense that the output difference of ∇ cannot cause the input difference of Δ. This contradiction explains the term "miss-in-the-middle".

In byte-oriented ciphers such as Rijndael (AES), it is typical to use truncated differentials [12] to construct Δ and ∇, because truncated difference patterns hold with certainty, and are independent of the S-box. In truncated differentials, one only distinguishes between zero and nonzero differences, namely, the exact value of the nonzero difference is irrelevant. For bytewise difference patterns (as in Rijndael), a nonzero byte difference will be denoted δ. In contrast, a zero byte difference will be denoted simply 0. Recall that although δ is used throughout the distinguisher, it does not mean that all these bytes contain the same difference value. The difference operator used in Rijndael is exclusive-or.

In the following sections we assume that the user key size is the same as the block size, 128 bits.

4 ID Distinguisher for Venkaiah *et al.*'s AES

In this section we demonstrate that a decrease in the branch number (or diffusion power) in Venkaiah *et al.*'s AES does not curtail the effect of impossible differential attacks.

In (6) we have an example of 4-round ID distinguisher for Venkaiah *et al.*'s AES. This distinguisher is exactly the same one used in [5] by Biham and Keller against AES. The top-down truncated differential covers AK_0 until MC' of the third round. The bottom-up truncated differential covers AK_4 up until MC' of the third round. These two differentials are incompatible. Note the pattern of four nonzero byte differences in the leftmost column of the state matrix before the MC' layer of the third round, and the pattern of four zero byte differences in the same column after the MC' layer. This difference pattern before and after MC' in the leftmost column is contradictory (even with the branch number 4). The symbol → means that the difference pattern on the left-hand side causes the difference pattern on the right-hand side. Contradiction is denoted by $\not\to$.

$$
\begin{pmatrix} \delta & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}
\overset{MC'\circ SR\circ SB\circ AK_0}{\longrightarrow}
\begin{pmatrix} \delta & 0 & 0 & 0 \\ \delta & 0 & 0 & 0 \\ \delta & 0 & 0 & 0 \\ \delta & 0 & 0 & 0 \end{pmatrix}
$$

$$
\overset{SR\circ SB\circ AK_1}{\longrightarrow}
\begin{pmatrix} \delta & 0 & 0 & 0 \\ 0 & 0 & 0 & \delta \\ 0 & 0 & \delta & 0 \\ 0 & \delta & 0 & 0 \end{pmatrix}
\overset{SR\circ SB\circ AK_2\circ MC'}{\longrightarrow}
$$

$$
\begin{pmatrix} \delta & \delta & \delta & \delta \\ \delta & \delta & \delta & \delta \\ \delta & \delta & \delta & \delta \\ \delta & \delta & \delta & \delta \end{pmatrix}
\overset{MC'}{\not\to}
\begin{pmatrix} 0 & \delta & \delta & \delta \\ 0 & \delta & \delta & \delta \\ 0 & \delta & \delta & \delta \\ 0 & \delta & \delta & \delta \end{pmatrix}
$$

$$
\overset{AK_3\circ SB^{-1}\circ SR^{-1}\circ AK_4}{\longleftarrow}
\begin{pmatrix} 0 & \delta & \delta & \delta \\ \delta & \delta & \delta & 0 \\ \delta & \delta & 0 & \delta \\ \delta & 0 & \delta & \delta \end{pmatrix}
\qquad (6)
$$

The distinguisher (6) belongs to a set of related distinguishers, all of which share the same input difference pattern, the same number of rounds, and the same number of zero output byte differences, but the precise output difference pattern changes. For example, (6) contains zero byte differences in the ciphertext positions (0, 7, 10, 13) of the state matrix, but other ciphertext difference patterns also cause contradiction. These patterns contain zero byte differences only in positions (1, 4, 11, 14), (2, 5, 8, 15) and (3, 6, 9, 12). Thus, all of these zero (ciphertext) byte positions are 'forbidden'.

4.1 ID Attack

A key-recovery ID attack on 5-round Venkaiah *et al.*'s AES operates the same way as the one used against 5-round AES in [5]. The distinguisher (6) is positioned in the last four rounds. The attack works as follows:

(i) Create a pool of 2^{32} plaintexts $P_i = (p_0, p_1, \ldots, p_{15})$, such that $(p_0, p_5, p_{10}, p_{15})$ range over all 32-bit values, while the remaining bytes assume arbitrary constant values. Encrypt this pool across 5 rounds and obtain a corresponding ciphertext pool $C_i = (c_0, c_1, \ldots, c_{15})$. Each such pool leads to about $2^{32}(2^{32}-1)/2 \approx 2^{63}$ pairs $C_i \oplus C_j$, with $i \neq j$;

(ii) For each pair of ciphertexts (C_i, C_j) such that only the bytes at position (0,7,10,13) are zero, guess 32 bits of AK_0 in position (0,5,10,15) and decrypt the first round of (P_i, P_j) up to the leftmost column of the first MC' layer. If only one byte difference is nonzero in this column (see (6)), then the guessed 32-bit subkey is wrong;

(iii) Output the (only) 32-bit subkey value that is not eliminated by the filtering in (ii).

The attack procedure and its complexities are the same as the one on the original AES: 2^{31} time, $2^{29.5}$ chosen plaintexts (CP), 2^{32} memory.

Another attack using (6) can recover subkey bits from both AK_0 and AK_6 of 6 rounds of Venkaiah *et al.*'s AES, similar to [7]. This attack works as follows:

(a) Create a pool of 2^{32} plaintexts $P_i = (p_0, p_1, \ldots, p_{15})$ such that $(p_0, p_5, p_{10}, p_{15})$ assume all possible 32-bit values, and the remaining bytes assume arbitrary constant values. Each such pool leads to about $2^{32}(2^{32}-1)/2 \approx 2^{63}$ pairs $C_i \oplus C_j$, with $i \neq j$;

(b) Consider $2^{59.5}$ pools, which mean $2^{91.5}$ chosen plaintexts (CP) and $2^{122.5}$ plaintext pairs. Find ciphertext pairs that contain zero difference in the bottommost two rows of the state matrix (a 2^{-64} filtration condition). The expected number of pairs that satisfy this restriction is $2^{122.5-64} = 2^{58.5}$.

(c) Guess 64 bits of $\text{AK}_6 = (k_{6,0}, k_{6,1}, \ldots, k_{6,15})$ corresponding to the topmost two rows of the state matrix, i.e. ($k_{6,0}$, $k_{6,1}$, $k_{6,4}$, $k_{6,5}$, $k_{6,8}$, $k_{6,9}$, $k_{6,12}$, $k_{6,13}$).

(d) For each ciphertext pair (C_i, C_j) that satisfies step (b), decrypt the last round and compute $\text{MC'}^{-1}(C_i \oplus C_j)$ and check if there are zero byte differences in one of the forbidden positions (0,7,10,13), (1,4,11,14), (2,5,8,15), (3,6,9,12). The joint probability of these difference patterns is $4 \cdot 2^{-32} \approx 2^{-30}$, and the expected number of remaining pairs is $2^{58.5} \cdot 2^{-30} = 2^{28.5}$.

(e) For a plaintext pair (P_i, P_j) corresponding to a ciphertext pair from step (d), guess 32 subkey bits ($k_{0,0}$, $k_{0,5}$, $k_{0,10}$, $k_{0,15}$) of $\text{AK}_0 = (k_{0,0}$, $k_{0,1}$, …, $k_{0,15})$ and encrypt the first round until after the first MC' layer. Keep those pairs for which there is only one nonzero byte difference in the leftmost column after MC'. The probability of this event is $4 \cdot (2^8 - 1)/2^{32} \approx 2^{-22}$ for three zero byte differences in a single column of MC'.

(f) Every subkey that leads to such difference is wrong. After analyzing $2^{28.5}$ pairs, there remains about $2^{32}(1-2^{-22})^{2^{28.5}} \approx 2^{32} \cdot e^{-2^{6.5}} < 1$ wrong key values.

(g) Steps (c) and (d) require $2 \cdot 2^{58.5} \cdot 2^{64} = 2^{123.5}$ 1-round computations, and step (e) requires about 2^{119} 1-round computations [7]. The total time complexity is $(2^{123.5} + 2^{119})/6 \approx 2^{121}$ 6-round computations, $2^{91.5}$ CP and 2^{32} memory. To recover the remaining bits of AK_6, we repeat the same attack, but look for the subkey bits on the lower two rows of the state matrix. Only the time complexity doubles.

Table 3: Complexity of ID attacks on Venkaiah *et al.*'s AES

# Rounds	Time	Data	Memory
5	2^{31}	$2^{29.5}$ CP	2^{32}
6	2^{122}	$2^{91.5}$ CP	2^{32}

5 Conclusion

This paper argued about differential and linear cryptanalysis of Venkaiah *et al.*'s AES design, and concluded that it is not better than the original AES (Table 2).

In [14], it is claimed that "The reduction in branch number leading to low diffusion power may in fact be viewed as a factor that curtails the effect of impossible differential cryptanalysis." We argue against their claim, and described impossible differential (ID) distinguishers and attacks on reduced-round versions of Venkaiah *et al.*'s AES. We used the same approach as [4] and [7] to construct the ID distinguishers and attack 4 and 5 rounds of Venkaiah *et al.*'s design.

Table 3 lists the complexities of ID attacks on reduced-round variants of Venkaiah *et al.*'s design. These complexities are the same as for reduced-round AES. Therefore, we do not agree with their claim that a small branch number effectively curtails the effect of ID attacks.

It is left as an open problem whether there are other ID distinguishers that achieve a better tradeoff (more rounds, smaller attack complexities) on Venkaiah *et al.*'s AES than (6).

Acknowledgments

The research results presented in this paper were funded by FAPESP under contract 2005/02102-9.

References

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

[2] P. S. L. M. Barreto, *On Efficient Implementation of InvMixColumn*, Manuscript. (http://paginas.terra.com.br/informatica/
paulobarreto/)

[3] E. Biham, A. Biryukov, and A. Shamir, *Cryptanalysis of Skipjack Reduced to 31 Rounds using Impossible Differentials*, Techical Report CS0947 revised, Technion, CS Department, 1998.

[4] E. Biham, A. Biryukov, and A. Shamir, "Miss-in-the-middle attacks on IDEA, Khufu and Khafre," *6th Fast Software Encryption Workshop*, LNCS 1636, pp. 124-138, L. R. Knudsen edits, Springer-Verlag, 1999.

[5] E. Biham, and N. Keller, "Cryptanalysis of reduced variants of rijndael," *3rd AES Conference*, New York, USA, 2000.

[6] E. Biham, and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *Journal of Cryptology*, vol. 4, no. 1, pp. 3-72, 1991.

[7] J. H. Cheon, M. Kim, K. Kim, J. Y. Lee, and S. Kang, "Improved impossible differential cryptanalysis of rijndael and crypton," *ICISC 2001*, LNCS 2288, pp. 39-49, K. Kim edits, Springer-Verlag, 2001.

[8] N. T. Courtois, and J. Pieprzyk, "Cryptanalysis of block ciphers with overdefined systems of quadratic equations," *Cryptology, Asiacrypt'02*, LNCS 2501, pp. 267-287, Y. Zheng edits, Springer-Verlag, 2002.

[9] J. Daemen, and V. Rijmen, "AES proposal: Rijndael," *1st AES Conference*, California, USA, 1998.

[10] FIPS197, *Advanced Encryption Standard (AES)*, FIPS PUB 197 Federal Information Processing Standard Publication 197, U. S. Department of Commerce, Nov. 2001.

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

[12] L. R. Knudsen, and T. A. Berson, "Truncated differentials of SAFER," *3rd Fast Software Encryption Workshop*, LNCS 1039, pp. 15-26, D. Gollmann edits, Springer-Verlag, 1996.

[13] M. Matsui, "Linear cryptanalysis method for DES cipher," *Cryptology, Eurocrypt'93*, LNCS 765, pp. 386-397, T. Helleseth edits, Springer-Verlag, 1994.

[14] V. C. Venkaiah, K. Srinathan, and B. Bruhadeshwar, *Variations to S-box and MixColumn Transformations of AES*, Technical Report, Deemed University, Feb. 2006.

Jorge Nakahara Jr is an assistant professor in Computer Science at the Universidade Católica de Santos in Santos, São Paulo, Brazil. He received his MS degree in Electrical Engineering and PhD from the Katholieke Universiteit Leuven, in Leuven, Belgium, 2003. His research interests include: symmetric and asymmetric cryptography, with emphasis on cryptanalysis.