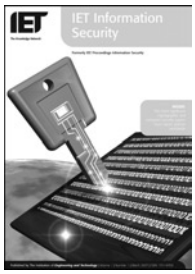
Published in IET Information Security
Received on 14th June 2007
Revised on 5th March 2008
doi: 10.1049/iet-ifs:20070078



ISSN 1751-8709

Impossible differential attack on seven-round AES-128

B. Bahrak M.R. Aref

Information System and Security Laboratory (ISSL), Electrical Engineering Department, Sharif University of Technology, Tehran, Iran
E-mail: bahrak@ee.sharif.edu

Abstract: A specific class of differential cryptanalytic approach, named as impossible differential attack, has been successfully applied to several symmetric cryptographic primitives in particular encryption schemes such as Advanced Encryption Standard (AES). Such attacks exploit differences that are impossible at some intermediate state of the cipher algorithm. The best-known impossible differential attack against AES-128 has applied to six rounds. An attack on AES-128 up to seven rounds is proposed. The proposed attack requires $2^{115.5}$ chosen plaintexts and 2^{109} bytes of memory and performs 2^{119} seven-round AES encryptions. This is also the best-known attack on a reduced version of the AES-128 till now.

1 Introduction

Rijndael is an iterated block cipher with variable key and block lengths of 128–256 bits in steps of 32 bits. Rijndael versions with a block length of 128 bits, and key lengths of 128, 192 and 256 bits have been adopted as the Advanced Encryption Standard (AES) [1]. Because of the worldwide use of AES, it is essential to re-evaluate the security of AES under various cryptanalytic techniques. In this paper, we study the security of 128-bit key version of AES-128 against the impossible differential attack. Differential cryptanalysis [2] analyses the evolvement of the difference between a pair of plaintexts in the following round outputs (differentials) in an iterated block cipher. The basic idea of impossible differential attack is to look for differentials that hold with probability 0 (or impossible differentials) to eliminate the wrong keys and keep the right key [3]. The first impossible differential attack against AES has been applied to five rounds of the AES-128 by Biham and Keller [4]. This attack was improved by Cheon *et al.* [5] to apply to six rounds of the AES-128. In 2004, Phan [6] extended this attack on the AES -192 up to seven rounds. In the case of 128-bit key length, for a seven-round version of AES, only two attacks are known. The first is due to Ferguson *et al.* [7] and requires 2^{120} cipher executions for a number of plaintexts equal to $2^{128}-2^{119}$. The second one, due to Gilbert and Minier [8], is a marginal speed up of the 128-bit key search requiring 2^{32} chosen plaintexts. In this paper, we propose a new impossible differential attack on AES-128 reduced to seven rounds which requires $2^{115.5}$ chosen plaintexts and performs 2^{119} seven-round AES encryptions. This is the best-known attack on a reduced version of AES-128 till now. The paper is organised as follows. In Section 2, we briefly describe the AES algorithm. A new impossible differential property of the AES is introduced in Section 3. In Section 4, we propose the new impossible differential attack on seven rounds of the AES-128, and Section 5 concludes the paper.

2 Brief description of AES

The AES [1] is a symmetric block cipher that supports key sizes of 128, 192 and 256 bits. The 128-bit plaintexts are represented by a 4×4 matrix of bytes, where each byte represents a value in GF(2^8). An AES round is composed of the following four operations:

- SubBytes (SB): a bytewise transformation that applies on each byte of the current block an 8-bit to 8-bit nonlinear S-box.

- ShiftRows (SR): a linear operation that rotates on the left all the rows of the current matrix (0 for the first row, 1 for the second, 2 for the third and 3 for the fourth).

• MixColumns (MC): another linear operation represented by a 4×4 matrix. Each column of the input matrix is multiplied by the MixColumns matrix in GF(2^8).

• AddRoundKey (AK): a simple XOR operation between the input matrix and the subkey of the current round.

The MixColumns operation is omitted in the last round and an initial key addition is performed before the first round for whitening. We also assume that the MixColumns operation is omitted in the last round of the reduced-round variants. The number of rounds is variable depending on the key length, 10 rounds for 128-bit key, 12 for 192-bit key and 14 for 256-bit key.

2.1 Notations

In this paper, we use the following notations: x_i^{I} denotes the input of the round i, while x_i^{S}, x_i^{R}, x_i^{M}, and x_i^{O} denote the intermediate values after the application of SubBytes, ShiftRows, MixColumns and AddRoundKey operations of round i, respectively. Obviously, $x_{i-1}^{O} = x_i^{I}$ holds for $i \geq 2$. We denote the subkey of the ith round by k_i, and the initial whitening subkey is k_0. In some cases, we are interested in interchanging the order of the MixColumns operation and the subkey addition. As these operations are linear, they can be interchanged, by first XORing the data with an equivalent key and then applying the MixColumns operation. We denote the equivalent subkey for the changed version by w_i, that is, $w_i = \mathrm{MC}^{-1}(k_i)$, and x_i^W denotes the intermediate value after the application of AddRoundKey with equivalent subkey. Let $x_{i,\mathrm{col}(j)}$ denote the jth column of x_i, where $j \in \{0, 1, 2, 3\}$. We also denote the byte in the mth row and nth column of x_i by byte $x_{i,m,n}$ where $m, n \in \{0, 1, 2, 3\}$. Another notation for bytes of x_i is an enumeration $\{0, 1, 2, \ldots, 15\}$, where the byte $x_{i,m,n}$ corresponds to byte $4n + m$ of x_i, that is x_i is exhibited as an array of 4×4 bytes with byte indexed as shown in Fig. 1.

3 Four-round impossible differential property of AES

In [4], a four-round impossible differential property of AES was presented. This four-round property states that given a pair of x_2^{I} which is equal in all bytes except one in which the pair differs, then the corresponding x_5^{R} cannot be equal in any of the following combinations of byte positions:

0	4	8	12
1	5	9	13
2	6	10	14
3	7	11	15

Figure 1 *Byte coordinate of 128-bit data block*

(0, 7, 10, 13), (1, 4, 11, 14), (2, 5, 8, 15) nor (3, 6, 9, 12). In [4–6], this property was used to attack the reduced round AES. Here we state a new impossible differential property on which our attack is based.

The new impossible differential property states that given a pair of x_2^{I} which is equal in all bytes except one, then the x_5^{R} cannot be equal in all bytes except three bytes in one column in which the pair differs. The reason is that one active byte (a byte which has non-zero difference) in x_2^{I} will result in 16 active bytes in x_3^{O}, but 3 active bytes in one column of x_5^{R} will result in 12 active bytes in x_4^{I}, so the intermediate differences contradict each other. Note that independent of which byte of x_2^{I} is active or which three bytes of a column of x_5^{R} are active, the impossible differential property holds. Fig. 2 illustrates the impossible differential property in one of the possible cases. The boxes with black circle refer to active bytes, whereas the white boxes denote the equal bytes in the pair. Arrows labelled SB, SR, MC and AK denote the SubBytes, ShiftRows, MixColumns and AddRoundKey operations, respectively, and arrows labelled SB^{-1}, SR^{-1}, MC^{-1} and AK^{-1} denote the inverse of the operations.

4 New impossible differential attack on seven rounds of AES

Using the above impossible differential property, we can attack a seven-round variant of AES-128. Fig. 3 illustrates the attack: the white boxes refer to bytes with zero difference, the black boxes represent known bytes that have non-zero difference and the boxes with black circle refer to unknown bytes that have non-zero difference.

4.1 Attack procedure

In order to make the attack faster, we first perform a precomputation: For all possible pairs of values of $x_{1,\mathrm{col}(0)}^{\mathrm{M}}$ which differ in only one byte , compute the values of the four bytes 0, 5, 10 and 15 of x_1^{I}, that is compute $x_1^{\mathrm{I}}(0, 5, 10, 15) = \mathrm{SB}^{-1} \circ \mathrm{SR}^{-1} \circ \mathrm{MC}^{-1}(x_{1,\mathrm{col}(0)}^{\mathrm{M}})$ for all possible pairs. Store the pairs of 4-byte values in a hash table H_p indexed by the XOR difference in these bytes. Note that XOR difference of the x_1^{I} is equal to XOR difference of the corresponding plaintexts because $x_1^{\mathrm{I}} = P \oplus k_0$. There are $(2^8)^3 \times 2^{16} \times 4 = 2^{42}$ possible pairs of values of $x_{1,\mathrm{col}(0)}^{\mathrm{M}}$ with the above condition (2^8 possible pairs for each of three bytes with zero difference, about 2^{16} possible pairs for the active byte and 4 possible positions for the active byte). So H_p have 2^{32} rows (possible values for the XOR difference in four bytes) and on average there are $2^{42}/2^{32} = 2^{10}$ pairs in each row.

Also in order to decrease the data complexity, we use 'structures'. A structure is defined as a set of 2^{32} plaintexts which have fixed values in all but four bytes (0, 5, 10, 15). Such a structure proposes $2^{32} \times (2^{32} - 1) \times 1/2 \simeq 2^{63}$ pairs of plaintexts.

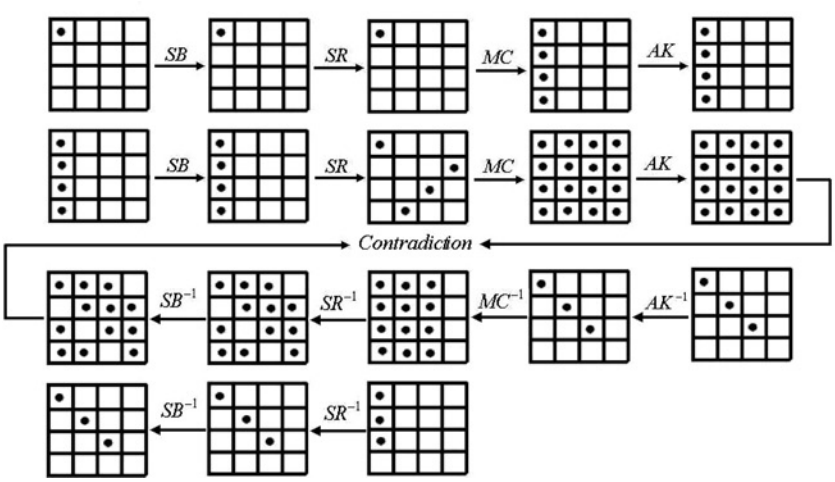


Figure 2 *New impossible differential property of AES*

The procedure of this attack is as follows.

Step 1. Take 2^n structures (i.e. $2^n \times 2^{32} = 2^{n+32}$ plaintexts, so $2^n \times 2^{63} = 2^{n+63}$ plaintext pairs). Perform the following for each structure:

- ask for the encryption of the structure,
- insert all the ciphertexts into a hash table indexed by bytes 1, 2, 4, 5, 8, 11, 14 and 15
- for each row of the hash table with more than one ciphertext, select every pair (C_1, C_2).

At the end of this step, we expect to have $2^{n+63} \times (2^{-8})^8 = 2^{n-1}$ plaintext pairs whose corresponding ciphertext pairs are equal in bytes 1, 2, 4, 5, 8, 11, 14 and 15 (Fig. 3).

Step 2. Guess the 32-bit value at bytes 3, 6, 9 and 12 for the k_7 and partially decrypt these bytes in the last round, that is, compute $x^{\mathrm{O}}_{6,\mathrm{col}(3)} = \mathrm{SB}^{-1} \circ \mathrm{SR}^{-1}[x^{\mathrm{O}}_7(3, 6, 9, 12) \oplus k_7(3,6,9,12)]$. Choose pairs whose difference $\Delta x^{\mathrm{W}}_{6,\mathrm{col}(3)} = \mathrm{MC}^{-1}(\Delta x^{\mathrm{O}}_{6,\mathrm{col}(3)})$ is non-zero at byte $x^{\mathrm{W}}_{6,1,3}$ and zero at other three bytes (Fig. 3). The probability of such a difference is $p'_1 = (2^{-8})^3 = 2^{-24}$ and consequently we expect to have $2^{n-1} \times 2^{-24} = 2^{n-25}$ pairs with this condition.

Step 3. Guess the 32-bit value at bytes 0, 7, 10 and 13 for the k_7 and partially decrypt these bytes in the last round, that is compute $x^{\mathrm{O}}_{6,\mathrm{col}(0)} = \mathrm{SB}^{-1} \circ \mathrm{SR}^{-1}[x^{\mathrm{O}}_7(0, 7, 10, 13) \oplus k_7(0, 7, 10, 13)]$. Choose pairs whose difference $\Delta x^{\mathrm{W}}_{6,\mathrm{col}(0)} = \mathrm{MC}^{-1}(\Delta x^{\mathrm{O}}_{6,\mathrm{col}(0)})$ is non-zero at byte $x^{\mathrm{W}}_{6,0,0}$ and zero at other three bytes (Fig. 3). The probability of such a difference is $p''_1 = (2^{-8})^3 = 2^{-24}$, so we expect to have $2^{n-25} \times 2^{-24} = 2^{n-49}$ pairs with this condition. The total probability of a desired difference in steps 2 and 3 is equal to $p_1 = p'_1 \times p''_1 = 2^{-48}$. So at the end of this step, we have 2^{n-49} pairs of x^{W}_6 which have zero difference in all bytes except bytes $x^{\mathrm{W}}_{6,0,0}$ and $x^{\mathrm{W}}_{6,1,3}$.

Step 4. Guess the 16-bit value at bytes 0 and 13 for the w_6 and partially decrypt these bytes in the sixth round, that is, compute $x^{\mathrm{O}}_{5,0,0} = \mathrm{SB}^{-1} \circ \mathrm{SR}^{-1}(x^{\mathrm{W}}_{6,0,0} \oplus w_{6,0,0})$ and $x^{\mathrm{O}}_{5,1,0} = \mathrm{SB}^{-1} \circ \mathrm{SR}^{-1}(x^{\mathrm{W}}_{6,1,3} \oplus w_{6,1,3})$. Choose pairs whose difference $\Delta x^{W}_{5,col(0)} = \mathrm{MC}^{-1}(\Delta x^{\mathrm{O}}_{5,col(0)})$ is zero at one byte. The probability of such a difference is $p_2 = 2^{-8} \times 4 = 2^{-6}$ because the probability of a zero difference in one byte is

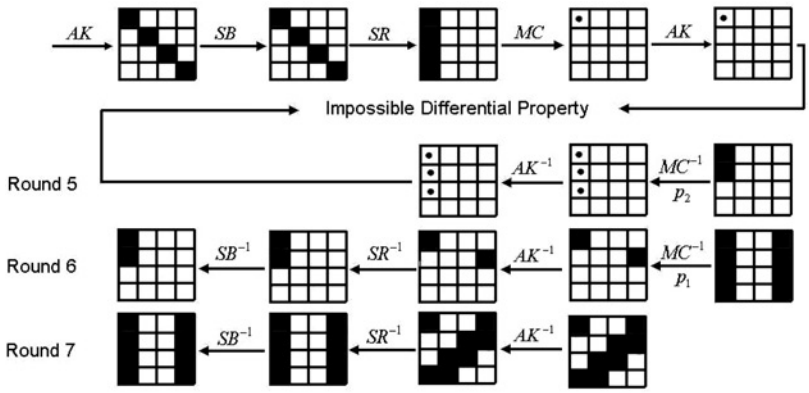


Figure 3 *Seven-round impossible differential attack*

doi: 10.1049/iet-ifs:20070078

2^{-8}, and this byte can be in one of four possible positions in a column. So we expect to have $2^{n-49} \times 2^{-6} = 2^{n-55}$ pairs which have such a difference.

Step 5. In this step, we eliminate wrong 32-bit values at bytes 0, 5, 10 and 15 for the k_0 by showing that the impossible differential property holds if these keys were used. We use the hash table H_p which has been made in the precomputation stage. The algorithm of this step is as follows.

- Initialise a list A of the 2^{32} possible values of the bytes 0, 5, 10 and 15 of k_0.

- For each of 2^{n-55} remaining pairs (P_1, P_2), compute $P' = P_1 \oplus P_2$ in the four bytes 0, 5, 10 and 15.

- Access the row P' in H_p, and for each pair (x, y) in that row, remove from the list A the value $P_1 \oplus x$, where P_1 is restricted to four bytes (plaintext bytes 0, 5, 10 and 15).

- If A is not empty, output the values in A along with the guess of k_7 at bytes 0, 3, 6, 7, 9, 10, 12 and 13.

Note that there are 2^{10} pairs in each row of H_p on average, so in the third part of this step, we eliminate about 2^{10} wrong keys for each plaintext pair (P_1, P_2). The probability of a wrong 32-bit value at bytes 0, 5, 10 and 15 for k_0 is $(1 - 2^{-32})$, so after analysing all 2^{n-55} pairs, we expect only $N = 2^{32} \times (1 - 2^{-32})^m$ wrong values of the four bytes of k_0 remain, where $m = 2^{n-55} \times 2^{10} = 2^{n-45}$. Suppose $m = 2^k$, the expected number is about $N = 2^{32} \times (1 - 2^{-32})^{2^{32} \times 2^{k-32}} \simeq 2^{32} \times (e^{-1})^{2^{k-32}} \simeq 2^{32} \times 2^{-1.4 \times 2^{k-32}}$. In order to find the right subkey, we should have $N < 1$. On the other hand, we want to eliminate all 32-bit values in the list A, unless the initial guess of the 64-bit value of the last round key k_7 or the 16-bit value of the key w_6 is correct. The wrong values (k_0, w_6, k_7) remains with the probability of $p = (2^8)^{10} \times N$. The probability 'p' should be very small (less than 2^{-10}), so we have $N \times 2^{80} < 2^{-10}$ which leads to $k > 38.45$. Hence with $m = 2^{38.5}$, if there remains a value for k_0, we can assume the guessed 64-bit value for k_7 and the guessed 16-bit value for w_6 are correct.

4.2 Analysis of the attack complexity

In order to derive $m = 2^{38.5}$, we need to have $n = 45 + 38.5 = 83.5$ and consequently the data complexity of the attack is $2^{n+32} = 2^{115.5}$ chosen plaintexts. The time complexity of the attack is composed of four parts: step 2 requires $2 \times 2^{32} \times 2^{n-1} \times 4/16 = 2^{n+30}$ one round encryptions, because for each of 2^{32} guessed keys, we should check four bytes for each of the 2^{n-1} pairs. Step 3 requires $2 \times 2^{32} \times 2^{32} \times 2^{n-25} \times 4/16 = 2^{n+38}$ one-round encryptions, because for each of 2^{32} guessed keys in step 2, we should guess 2^{32} keys in this step and for all of these keys, we should check four bytes for each of the 2^{n-25} remained pairs. Step 4 requires $2 \times 2^{64} \times 2^{16} \times 2^{n-49} \times 2/16 = 2^{n+29}$ one-round encryptions, because for all of 2^{64} guessed keys in steps 2 and 3, we should guess 2^{16} keys in this step and for these keys, we should check two bytes for each of the 2^{n-49} remained pairs. In step 5, 2^{n-55} pairs are analysed, leading to 2^{10} memory access on average to H_p and 2^{10} memory access to A. This step is repeated 2^{80}

Table 1 Comparison of impossible differential cryptanalysis of AES variants

Variant	Rounds	Data	Workload	Memory	Source
AES-128	5	$2^{29.5}$	2^{31}	2^{42}	[4]
AES-128	6	$2^{91.5}$	2^{122}	2^{93}	[5]
AES-128	7	$2^{115.5}$	2^{119}	2^{109}	this paper
AES-192	7	2^{92}	2^{186}	2^{157}	[6]
AES-256	7	$2^{92.5}$	$2^{250.5}$	2^{157}	[6]

Table 2 Comparison of our results with previous attacks on seven-round AES-128

Attack	Data	Workload	Memory	Source
partial sum	$2^{128} - 2^{119}$	2^{120}	2^{61}	[7]
collision	2^{32}	2^{128}	2^{80}	[8]
impossible differential	$2^{115.5}$	2^{119}	2^{109}	this paper

times (for the guess of w_6 and k_7). Therefore the time complexity is $2^{n-55} \times (2^{10} + 2^{10}) \times 2^{80} = 2^{n+36}$ memory access, which is equivalent to about 2^{n+30} one-round encryptions. Consequently for $n = 83.5$ the overall complexity of the attack is about $(2^{113.5} + 2^{121.5} + 2^{112.5} + 2^{113.5})/7 \simeq 2^{119}$. We can find eight bytes of k_7 with time complexity of 2^{119}. We can find another eight bytes of k_7 by a simple exhaustive search, so the whole key can be found with time complexity of $2^{119} + 2^{64} \simeq 2^{119}$ encryptions. The precomputation stage requires about $2 \times 2^{42}/7 \simeq 2^{40.5}$ encryptions and the required memory is about 2^{45} bytes. Meanwhile, $2^{112}/2^3 = 2^{109}$ bytes of memory are needed to store the list of deleted key values (k_0, w_6, k_7).

5 Conclusion

We have proposed a new impossible differential attack against AES-128 reduced to seven rounds. The time complexity and required memory of this attack are less expensive than the previous impossible differential attacks. In Table 1, we compare the results of the new attack with the results of previous impossible differential attacks. In Table 2, we compare our attack with other attacks which applied on seven rounds of AES-128.

6 Acknowledgments

The authors would like to thank Taraneh Eghlidos, Frederik Armknecht, Ahmad-Reza Sadeghi and anonymous reviewers for technical discussion and invaluable comments. They also thank the Iranian NSF for establishing the cryptography chair in I.R. Iran. This work was partially supported by Iran Telecommunications Research Center and the cryptography chair of the Iranian NSF.

7 References

[1] DAEMEN J., RIJMEN V.: 'The design of Rijndael: AES – the Advanced Encryption Standard' (Springer Verlag, 2002)

[2] BIHAM E., SHAMIR A.: 'Differential cryptanalysis of DES-like cryptosystems', *J. Cryptol.*, 1991, **4**, (1), pp. 3–72

[3] BIHAM E., BIRYUKOV A., SHAMIR A.: 'Cryptanalysis of Skipjack reduced to 31 rounds'. Advances in Cryptology, Proc. EUROCRYPT 99, *Lect. Notes Comput. Sci.*, 1999, **1592**, pp. 12–23

[4] BIHAM E., KELLER N.: 'Cryptanalysis of reduced variants of Rijndael'. 3rd AES Conf., 2000

[5] CHEON J.H., KIM M., KIM K., LEE J.-Y., KANG S.: 'Improved impossible differential cryptanalysis of Rijndael and Crypton'. Proc. 3rd Int. Conf. Information Security and Cryptology (ICISC), *Lect. Notes Comput. Sci.*, 2001, **2288**, pp. 39–49

[6] PHAN R.C.: 'Impossible differential cryptanalysis of 7-round Advanced Encryption Standard (AES)', *Inf. Process. Lett.*, 2004, **91**, (1), pp. 33–38

[7] FERGUSON N., KELSEY J., LUCKS S., *ET AL.*: 'Improved cryptanalysis of Rijndael'. Proc. Fast Software Encryption (FSE '00), *Lect. Notes Comput. Sci.*, 2001, **1978**, pp. 213–230

[8] GILBERT H., MINIER M.: 'A collision attack on 7 rounds of Rijndael'. Proc. 3rd AES Conf., National Institute of Standards and Technology, April 2000, pp. 230–241

doi: 10.1049/iet-ifs:20070078