MilitaryTechnicalCollege
Kobry El-Kobbah,
Cairo, Egypt

8th International Conference
on Electrical Engineering
ICEENG 2012

Key Partitioning Cryptanalysis of Reduced Rounds AES Algorithm Variant

By

Amr M. Ashry* AlaaEl-Din R. Shehata* Ashraf D. El-Bayoumy*

Abstract:

The majority of the published attacks on reduced-round variants of block ciphers seeks to maximize the number of rounds to be broken, using less data than the entire codebook and less time than exhaustive key search. In this paper, a novel *key partitioning*chosen plaintext attack against reduced-rounds AES variants up to 3 rounds that uses only 33 chosen plaintext-ciphertext pairs, a workload of 2^{19}(for three round variant) and 2^{17}bytes of memory is introduced. The attack depends upon the *internal structure* of the AES round function, the *differential characteristics* of the AES S-BOX and the*key partitioning* in which each key byte will be processed individually independent to the other key bytes. To clarify the idea of the attack we will follow a round by round cryptanalysis till the third round of the AES. The results gives that a bit-level permutation is more efficient than byte-level permutation used in the AES round function.We also introduce a counter measure for this attack by using a bit-level permutation on the AES round function instead a byte level permutation.

Keywords:

AES, Cryptanalysis, bit level permutation, byte level permutation, differential, key partitioning, reduced rounds.

* Egyptian Armed Forces

1. ***Introduction:***

No practical attacks against AES are known to date, but an increasing number of them are now getting close to become practical. Recent attempts using related key boomerang attack techniques have received a lot attention.
At the very end of May 2009, a paper was published by A. Biryukov and D. Khovratovich [1]describing a potential attack on AES based on a related key boomerang attack. Although not currently practical to break AES it was the first attack to be more efficient than pure brute force by lowering the AES-256 complexity from 2^{256} to 2^{119} and AES-192 complexity from 2^{192} to 2^{176}.
Shortly after this paper was published another major breakthrough in the cryptanalysis of AES was made public in August 2009 [2] by an extended team responsible for the first paper; and this time it is almost practical against some variants of AES-256. Respectively using a 9 and 10 rounds variants they lowered the complexity to 2^{39} and 2^{45}.
Recently in mid-2011, Charles Bouillaguetet al [3] considered low data complexity attacks on reduced-round variants of AES. He presented several attacks on up to four rounds of AES given at most 10 known (or chosen) plaintexts, and showed how to leverage such attacks to more complex attacks on variants of AES with more rounds, the results of these attacks will be illustrated shortly in section 4.

2. ***AES S-BOX differential characteristics:***

The differential characteristics [4,5] of the AES S-BOX is a word means that, what is the probability of a specific input difference to the S-BOX for a given S-BOX output difference.
For any output difference ΔY the probability of the occurrence of an input difference ΔX equals to “0” in 129 values out of 256 possible values for ΔX which is called impossible differential [6,7], equals to “$\frac{2}{256}$” in 126 values out 256 and “ $\frac{4}{256}$ ” in only one value of ΔX. These semi-ideal differential characteristics give us an indication to how hard is the differential cryptanalysis of the AES, also it tells us why the AES is immune against differential cryptanalysis since a huge number of plaintext-ciphertext pairs are required to complete the attack because of the very small bias found in the difference distribution table.
But we can notice that, for any given value for ΔY we will need to test only 2^7-1 values of ΔX rather than 2^8, that is true because the other values of ΔX are

impossible differentials, the attack shall consider this fact as will be discussed shortly.

3. Proposed attack

The proposed key partitioning chosen plaintext attack is introduced in this section. We will start with a single round AES variant, then we will extend that attack to two and three rounds AES variants.

3.1 Proposed attack for a single round AES variant:

The main idea of the proposed attack depends upon a novel principle called key partitioning, in key partitioning each key byte is processed independent to the other key bytes, this principle depends upon the initial add round key before the first round, to describe what we want to do we shall choose the two plaintext pairs listed in Table (1), also the target key matrix is listed.

Table (1):*Selected input pair for the AES single round attack*

First chosen plaintext					Second chosen plaintext					Target key			
00	00	00	00		FF	00	00	00		W_{00}	W_{10}	W_{20}	W_{30}
00	00	00	00		00	00	00	00		W_{01}	W_{11}	W_{21}	W_{31}
00	00	00	00		00	00	00	00		W_{02}	W_{12}	W_{22}	W_{32}
00	00	00	00		00	00	00	00		W_{03}	W_{13}	W_{23}	W_{33}

The encryption process of the two chosen plaintext pairs with the target key shall give us two encryption paths.The first will force the key by itself to be the input of the first round (after the initial add round key).The other will do the same except for the first key byte which is complemented under the effect of the "FF" byte in the plaintext.We will go through from here for the key point of the attack and look to what will happen. After initial add round key we will get the result listed in Table (2).

Table (2):*The output of the initial add round key*

The first encryption path(plain 1)					The second encryption path(plain 2)			
W_{00}	W_{10}	W_{20}	W_{30}		$\overline{W}_{00}$	W_{10}	W_{20}	W_{30}
W_{01}	W_{11}	W_{21}	W_{31}		W_{01}	W_{11}	W_{21}	W_{31}
W_{02}	W_{12}	W_{22}	W_{32}		W_{02}	W_{12}	W_{22}	W_{32}

W_{03}	W_{13}	W_{23}	W_{33}

W_{03}	W_{13}	W_{23}	W_{33}

Note that the only difference is at the first byte only (W_{00}) which appears by itself in the first encryption path for plain'1' and complemented at second encryption path for plain'2', at the end of the first round (substitute bytes, shift rows, mix-columns and add round key operations) we will get the results shown in Tables (3,4).

Table (3):*The output of the first round for the first chosen plain text*

The first encryption path (plain 1)			
$S(W_{00}).02 \oplus S(W_{11}).03 \oplus S(W_{22}) \oplus S(W_{33}) \oplus W_{40}$	$S(W_{10}).02 \oplus S(W_{21}).03 \oplus S(W_{32}) \oplus S(W_{03}) \oplus W_{50}$	$S(W_{20}).02 \oplus S(W_{31}).03 \oplus S(W_{02}) \oplus S(W_{13}) \oplus W_{60}$	$S(W_{30}).02 \oplus S(W_{01}).03 \oplus S(W_{12}) \oplus S(W_{23}) \oplus W_{70}$
$S(W_{00}) \oplus S(W_{11}).02 \oplus S(W_{22}).03 \oplus S(W_{33}) \oplus W_{41}$	$S(W_{10}) \oplus S(W_{21}).02 \oplus S(W_{32}).03 \oplus S(W_{03}) \oplus W_{51}$	$S(W_{20}) \oplus S(W_{31}).02 \oplus S(W_{02}).03 \oplus S(W_{13}) \oplus W_{61}$	$S(W_{30}) \oplus S(W_{01}).02 \oplus S(W_{12}).03 \oplus S(W_{23}) \oplus W_{71}$
$S(W_{00}) \oplus S(W_{11}) \oplus S(W_{22}).02 \oplus S(W_{33}).03 \oplus W_{42}$	$S(W_{10}) \oplus S(W_{21}) \oplus S(W_{32}).02 \oplus S(W_{03}).03 \oplus W_{52}$	$S(W_{20}) \oplus S(W_{31}) \oplus S(W_{02}).02 \oplus S(W_{13}).03 \oplus W_{62}$	$S(W_{30}) \oplus S(W_{01}) \oplus S(W_{12}).02 \oplus S(W_{23}).03 \oplus W_{72}$
$S(W_{00}).03 \oplus S(W_{11}) \oplus S(W_{22}) \oplus S(W_{33}).02 \oplus W_{43}$	$S(W_{10}).03 \oplus S(W_{21}) \oplus S(W_{32}) \oplus S(W_{03}).02 \oplus W_{53}$	$S(W_{20}).03 \oplus S(W_{31}) \oplus S(W_{02}) \oplus S(W_{13}).02 \oplus W_{63}$	$S(W_{30}).03 \oplus S(W_{01}) \oplus S(W_{12}) \oplus S(W_{23}).02 \oplus W_{73}$

Table (4):*The output of the first round for the second chosen plain text*

The second encryption path (plain 2)			
$S(\overline{W}_{00}).02 \oplus S(W_{11}).03 \oplus S(W_{22}) \oplus S(W_{33}) \oplus W_{40}$	$S(W_{10}).02 \oplus S(W_{21}).03 \oplus S(W_{32}) \oplus S(W_{03}) \oplus W_{50}$	$S(W_{20}).02 \oplus S(W_{31}).03 \oplus S(W_{02}) \oplus S(W_{13}) \oplus W_{60}$	$S(W_{30}).02 \oplus S(W_{01}).03 \oplus S(W_{12}) \oplus S(W_{23}) \oplus W_{70}$
$S(\overline{W}_{00}) \oplus S(W_{11}).02 \oplus S(W_{22}).03 \oplus S(W_{33}) \oplus W_{41}$	$S(W_{10}) \oplus S(W_{21}).02 \oplus S(W_{32}).03 \oplus S(W_{03}) \oplus W_{51}$	$S(W_{20}) \oplus S(W_{31}).02 \oplus S(W_{02}).03 \oplus S(W_{13}) \oplus W_{61}$	$S(W_{30}) \oplus S(W_{01}).02 \oplus S(W_{12}).03 \oplus S(W_{23}) \oplus W_{71}$
$S(\overline{W}_{00}) \oplus S(W_{11}) \oplus S(W_{22}).02 \oplus S(W_{33}).03 \oplus W_{42}$	$S(W_{10}) \oplus S(W_{21}) \oplus S(W_{32}).02 \oplus S(W_{03}).03 \oplus W_{52}$	$S(W_{20}) \oplus S(W_{31}) \oplus S(W_{02}).02 \oplus S(W_{13}).03 \oplus W_{62}$	$S(W_{30}) \oplus S(W_{01}) \oplus S(W_{12}).02 \oplus S(W_{23}).03 \oplus W_{72}$
$S(\overline{W}_{00}).03 \oplus S(W_{11}) \oplus S(W_{22}) \oplus S(W_{33}).02 \oplus W_{43}$	$S(W_{10}).03 \oplus S(W_{21}) \oplus S(W_{32}) \oplus S(W_{03}).02 \oplus W_{53}$	$S(W_{20}).03 \oplus S(W_{31}) \oplus S(W_{02}) \oplus S(W_{13}).02 \oplus W_{63}$	$S(W_{30}).03 \oplus S(W_{01}) \oplus S(W_{12}) \oplus S(W_{23}).02 \oplus W_{73}$

Now we have the output of the first round for both encryption paths, it is obviously can be noticed that for any key value the output for the two chosen

plaintexts ‘1’&’2’ will be identical after the first round except for the first word (column) of the cipher-text, in addition all terms of the first word of the cipher-text are identical except for the terms***$S(W_{00})$ & $S(\overline{W}_{00})$*** and hence this key byte can processed independently, and that is what we called the key partitioning.
We are assuming a single round AES encryption, then we have the cipher-text values for both paths, then by a simple XOR operation between the corresponding bytes of the cipher-text we must have:

$$C_{01} \oplus \bar{C}_{01} = C_{02} \oplus \bar{C}_{02} = S(W_{00}) \oplus S(W_{11}).02 \oplus S(W_{22}).03 \oplus S(W_{33}) \oplus W_{41} \oplus S(\overline{W}_{00}) \oplus S(W_{11}).02 \oplus S(W$$

Equation (1) is valid for any key value after the first round.Now to get the first key byte “W_{00}” we need to know the byte which has a substitution value when XORed with the substitution value of its complement satisfies the obtained value.It doesn’t seem to be a complicated process.To simplify it we can construct a new table that holds the substitutions for each of a 128 possibilities out of 256 XORed with the substitution of their complement and hence 128 possibilities are enough since all combinations will be covered.The operation of finding the first key byte “W_{00}” will be a simple look-up.

After we find a match, we shall have a one out of two correct first key byte value (W_{00}) and the other is its complement, we need to know which one is correct.Simply we use any of them as the first byte of the plain-text again and apply a single round AES encryption.Hence we have two possible situations after the initial add round key (00_x) or (FF_x) then the byteC'_{01}will have the two possible values listed in equations (2) and (3) .

$$C'_{01} = S(00x) \oplus S(W_{11}).02 \oplus S(W_{22}).03 \oplus S(W_{33}) \oplus W_{41}$$

$$=63_x \oplus S(W_{11}).02 \oplus S(W_{22}).03 \oplus S(W_{33}) \oplus W_{41} \mathbf{(2)}$$

OR;

$$C'_{01} = S(FFx) \oplus S(W_{11}).02 \oplus S(W_{22}).03 \oplus S(W_{33}) \oplus W_{41}$$

$$=16_x \oplus S(W_{11}).02 \oplus S(W_{22}).03 \oplus S(W_{33}) \oplus W_{41} \mathbf{(3)}$$

Then XOR it to the value in equation (1):

$$C_{01} = S(W_{00}) \oplus S(W_{11}).02 \oplus S(W_{22}).03 \oplus S(W_{33}) \oplus W_{41} \mathbf{(4)}$$

We shall get:

$$C'_{01} \oplus C_{01} = X \oplus S(W_{11}).02 \oplus S(W_{22}).03 \oplus S(W_{33}) \oplus W_{41} \oplus S(W_{00}) \oplus S(W_{11}).02 \oplus S(W_{22}).03 \oplus S(W_{33}) \oplus W_{41} = X \oplus S(W_{00})$$

Where “X” Є {16_x , 63_x}, which can be rearranged to :

$$C'_{01} \oplus C_{01} \oplus S(W_{00}) = X \qquad (\square)$$

Since the left hand side is known, “X” has to be either (16_x) or (63_x), the first leads to the correct first key byte value (W_{00}) and the other is the complement of it, else the other value is the one. This Attack can recover the full key by 16 iterations by moving the byte in difference from the first location to the second till the sixteenth byte, each byte is found independently and that is the complete definition of the key partitioning principle.

3.2 Proposed attack for two rounds AES variant:

We have illustrated the single round AES attack, now we will show how to extend the attack against 2-round AES variant.We will keep the steps of the previous attack to the second round.Let us analyze what will happen in the second round, for simplicity we will name the output of the first round as matrices “1 ” and “$\bar{1}$” for the two encryption paths, hence the input to the second round is as listed in Table (5).

Table (5):*The output of the first round*

The first encryption path(plain 1)					The second encryption path(plain 2)			
1_{00}	1_{10}	1_{20}	1_{30}		$\bar{1}_{00}$	1_{10}	1_{20}	1_{30}
1_{01}	1_{11}	1_{21}	1_{31}		$\bar{1}_{01}$	1_{11}	1_{21}	1_{31}
1_{02}	1_{12}	1_{22}	1_{32}		$\bar{1}_{02}$	1_{12}	1_{22}	1_{32}
1_{03}	1_{13}	1_{23}	1_{33}		$\bar{1}_{03}$	1_{13}	1_{23}	1_{33}

Now we will get the output of the second round as we did for the first round, the results are illustrated in Tables(6,7).

Table (6):*The output of the second round*

The first encryption path (plain 1)			
$S(1_{00}).02 \oplus S(1_{11}).03 \oplus S(1_{22}) \oplus S(1_{33}) \oplus W_{80}$	$S(1_{10}).02 \oplus S(1_{21}).03 \oplus S(1_{32}) \oplus S(1_{03}) \oplus W_{90}$	$S(1_{20}).02 \oplus S(1_{31}).03 \oplus S(1_{02}) \oplus S(1_{13}) \oplus W_{10,0}$	$S(1_{30}).02 \oplus S(1_{01}).03 \oplus S(1_{12}) \oplus S(1_{23}) \oplus W_{11,0}$
$S(1_{00}) \oplus S(1_{11}).02 \oplus S(1_{22}).03 \oplus S(1_{33}) \oplus W_{81}$	$S(1_{10}) \oplus S(1_{21}).02 \oplus S(1_{32}).03 \oplus S(1_{03}) \oplus W_{91}$	$S(1_{20}) \oplus S(1_{31}).02 \oplus S(1_{02}).03 \oplus S(1_{13}) \oplus W_{10,1}$	$S(1_{30}) \oplus S(1_{01}).02 \oplus S(1_{12}).03 \oplus S(1_{23}) \oplus W_{11,1}$

$S(1_{00}) \oplus S(1_{11}) \oplus S(1_{22}).02 \oplus S(1_{33}).03 \oplus W_{82}$	$S(1_{10}) \oplus S(1_{21}) \oplus S(1_{32}).02 \oplus S(1_{03}).03 \oplus W_{92}$	$S(1_{20}) \oplus S(1_{31}) \oplus S(1_{02}).02 \oplus S(1_{13}).03 \oplus W_{10,2}$	$S(1_{30}) \oplus S(1_{01}) \oplus S(1_{12}).02 \oplus S(1_{23}).03 \oplus W_{11,2}$
$S(1_{00}).03 \oplus S(1_{11}) \oplus S(1_{22}) \oplus S(1_{33}).02 \oplus W_{83}$	$S(1_{10}).03 \oplus S(1_{21}) \oplus S(1_{32}) \oplus S(1_{03}).02 \oplus W_{93}$	$S(1_{20}).03 \oplus S(1_{31}) \oplus S(1_{02}) \oplus S(1_{13}).02 \oplus W_{10,3}$	$S(1_{30}).03 \oplus S(1_{01}) \oplus S(1_{12}) \oplus S(1_{23}).02 \oplus W_{11,3}$

Table (7):*The output of the second round*

The second encryption path (plain 2)			
$S(\bar{1}_{00}).02 \oplus S(1_{11}).03 \oplus S(1_{22}) \oplus S(1_{33}) \oplus W_{80}$	$S(1_{10}).02 \oplus S(1_{21}).03 \oplus S(1_{32}) \oplus S(\bar{1}_{03}) \oplus W_{90}$	$S(1_{20}).02 \oplus S(1_{31}).03 \oplus S(\bar{1}_{02}) \oplus S(1_{13}) \oplus W_{10,0}$	$S(1_{30}).02 \oplus S(\bar{1}_{01}).03 \oplus S(1_{12}) \oplus S(1_{23}) \oplus W_{11,0}$
$S(\bar{1}_{00}) \oplus S(1_{11}).02 \oplus S(1_{22}).03 \oplus S(1_{33}) \oplus W_{81}$	$S(1_{10}) \oplus S(1_{21}).02 \oplus S(1_{32}).03 \oplus S(\bar{1}_{03}) \oplus W_{91}$	$S(1_{20}) \oplus S(1_{31}).02 \oplus S(\bar{1}_{02}).03 \oplus S(1_{13}) \oplus W_{10,1}$	$S(1_{30}) \oplus S(\bar{1}_{01}).02 \oplus S(1_{12}).03 \oplus S(1_{23}) \oplus W_{11,1}$
$S(\bar{1}_{00}) \oplus S(1_{11}) \oplus S(1_{22}).02 \oplus S(1_{33}).03 \oplus W_{82}$	$S(1_{10}) \oplus S(1_{21}) \oplus S(1_{32}).02 \oplus S(\bar{1}_{03}).03 \oplus W_{92}$	$S(1_{20}) \oplus S(1_{31}) \oplus S(\bar{1}_{02}).02 \oplus S(1_{13}).03 \oplus W_{10,2}$	$S(1_{30}) \oplus S(\bar{1}_{01}) \oplus S(1_{12}).02 \oplus S(1_{23}).03 \oplus W_{11,2}$
$S(\bar{1}_{00}).03 \oplus S(1_{11}) \oplus S(1_{22}) \oplus S(1_{33}).02 \oplus W_{83}$	$S(1_{10}).03 \oplus S(1_{21}) \oplus S(1_{32}) \oplus S(\bar{1}_{03}).02 \oplus W_{93}$	$S(1_{20}).03 \oplus S(1_{31}) \oplus S(\bar{1}_{02}) \oplus S(1_{13}).02 \oplus W_{10,3}$	$S(1_{30}).03 \oplus S(\bar{1}_{01}) \oplus S(1_{12}) \oplus S(1_{23}).02 \oplus W_{11,3}$

Now we can analyze the output of the second round for the two encryption paths, they will theme to be different if you look at the experimental result. But the analytical results here shows that the difference is only in one term per each corresponding cipher bytes, so as we did for the single round, we can apply for the 2-round AES as follows:

$$2_{1}32 \oplus \bar{2}_{1}32 = 2_{1}33 \oplus \bar{2}_{1}33 = S(1_{1}30) \oplus S(1_{1}01) \oplus S(1_{1}12).02 \oplus S(1_{1}23).03 \oplus W_{1}11,2 \oplus S(1_{1}30)$$

Equation (6) represents an output difference from the S-BOX, hence we can call the differential characteristics as was discussed section 2.We have 127 solutions by looking to the difference distribution table of the AES S-BOX, but we have a condition that should be met only for the correct values, for each input difference { $(1_{01}) \oplus (\bar{1}_{01})$} possible for the output difference { $S(1_{01}) \oplus S(\bar{1}_{01})$} should give a value that lies in the complement pair difference table, but this is not enough to uniquely determine the correct value.

So we will use another pair to act as a distinguisher for the correct value, the first byte of the plain block of that pair is chosen to be "F0" that will give $\bar{\bar{W}}_{0_0}$ which is a first nibble complement of W_{0_0} after the initial add round key, the output of that pair can be represented as given in Table (7).

So we need to do the same analysis to that pair, finally we will have:

Trying all possible values for (1_{01}), the correct solution of these two equations should lie in one row of the complement difference distribution table, and this will give us the correct key byte W_{00}.
This kind of attack requires 33 chosen plaintext-ciphertext pairs to recover all 16 bytes of the key.Hence the two round AES is broken after 16 like iterations moving the byte in difference in the chosen plain-text from the first to the second till the sixteen byte getting a one byte of the key each time, the total complexity of the attack can be calculated as:
2^7-1 …work required to test all possible input difference { $(1_{01})\oplus(\bar{1}_{01})$} corresponds to the output difference { $S(1_{01})\oplus S(\bar{1}_{01})$} for the first two pairs.
2^7-1 …work required to test all possible input difference { $(1_{01})\oplus(\bar{\bar{1}}_{01})$} corresponds to the output difference { $S(1_{01})\oplus S(\bar{1}_{01})$} for the second two pairs.
2^4 …work required to repeat all the above steps for each one of the 16 key bytes.
So we can give the total effort required to break two round AES variant as follows:

The total work required = (2^7-1+2^7-1)*2^4< 2^{12}
The number of chosen pairs = 33 pairs (33*16=528 bytes)

3.3 Proposed attack against three rounds AES variant:

In this section we will get the output of the third round similarlylike we get for second round.We will name the output of the second round given in Tables (6,7)by a matrices “2”& “$\bar{2}$”. Also, we should consider that the input blocks to the third round are totally different from each other’s, but we must recall that there are factors in common.

The first step to step back from the third to the second round given the output difference of the third round is to reverse the mix-columns operation.We have the states difference not the states, but we can proof that the inverse mix-columns operation of the state’s difference equals to the difference of the inverse mix-columns operation for each state individually [8]. For a given State “S_i” and a given round key “W_j”:

Hence we can conclude that, the inverse mix of the difference of states is equivalent to the difference of the inverse mix of the states, so given the difference at the output of the third round which is:

The difference at 3rd. round output			
$3_{00}+\bar{3}_{00}$	$3_{10}+\bar{3}_{10}$	$3_{20}+\bar{3}_{20}$	$3_{30}+\bar{3}_{30}$
$3_{01}+\bar{3}_{01}$	$3_{11}+\bar{3}_{11}$	$3_{21}+\bar{3}_{21}$	$3_{31}+\bar{3}_{31}$
$3_{02}+\bar{3}_{02}$	$3_{12}+\bar{3}_{12}$	$3_{22}+\bar{3}_{22}$	$3_{32}+\bar{3}_{32}$
$3_{03}+\bar{3}_{03}$	$3_{13}+\bar{3}_{13}$	$3_{23}+\bar{3}_{23}$	$3_{33}+\bar{3}_{33}$

Multiplying by the inverse matrix we shall get:

$$\begin{bmatrix} E & B & D & 9 \\ 9 & E & B & D \\ D & 9 & E & B \\ B & D & 9 & E \end{bmatrix} X$$

The difference at 3rd. round output			
$3_{00}+\bar{3}_{00}$	$3_{10}+\bar{3}_{10}$	$3_{20}+\bar{3}_{20}$	$3_{30}+\bar{3}_{30}$
$3_{01}+\bar{3}_{01}$	$3_{11}+\bar{3}_{11}$	$3_{21}+\bar{3}_{21}$	$3_{31}+\bar{3}_{31}$
$3_{02}+\bar{3}_{02}$	$3_{12}+\bar{3}_{12}$	$3_{22}+\bar{3}_{22}$	$3_{32}+\bar{3}_{32}$
$3_{03}+\bar{3}_{03}$	$3_{13}+\bar{3}_{13}$	$3_{23}+\bar{3}_{23}$	$3_{33}+\bar{3}_{33}$

=

The first encryption path(plain 1)			
$s(2_{00})\oplus s(\bar{2}_{00})$	$s(2_{10})\oplus s(\bar{2}_{10})$	$s(2_{20})\oplus s(\bar{2}_{20})$	$s(2_{30})\oplus s(\bar{2}_{30})$
$s(2_{11})\oplus s(\bar{2}_{11})$	$s(2_{21})\oplus s(\bar{2}_{21})$	$s(2_{31})\oplus s(\bar{2}_{31})$	$s(2_{01})\oplus s(\bar{2}_{01})$
$s(2_{22})\oplus s(\bar{2}_{22})$	$s(2_{32})\oplus s(\bar{2}_{32})$	$s(2_{02})\oplus s(\bar{2}_{02})$	$s(2_{12})\oplus s(\bar{2}_{12})$
$s(2_{33})\oplus s(\bar{2}_{33})$	$s(2_{03})\oplus s(\bar{2}_{03})$	$s(2_{13})\oplus s(\bar{2}_{13})$	$s(2_{23})\oplus s(\bar{2}_{23})$

Now we have a deterministic values for $\{S(2_{32})\oplus S(\bar{2}_{32})\}$ and $\{S(2_{32})\oplus S(\bar{2}_{32})\}$which is an output differences from the S-BOX which have 2^7-1 possible input differences $\{(2_{32})\oplus(\bar{2}_{32})\}$ and $\{(2_{32})\oplus(\bar{\bar{2}}_{32})\}$.All these possible input differences should be examined backwards following the steps in the two rounds and the single round AES attacks discussed in the previous sections; this will increase the complexity of the attack as follows:

2^7-1 …work required to test all possible input difference $\{(2_{32})\oplus(\bar{2}_{32})\}$ corresponds to the output difference $\{S(2_{32})\oplus S(\bar{2}_{32})\}$ for the first two pairs.

2^7-1 …work required to test all possible input difference $\{(2_{32})\oplus(\bar{\bar{2}}_{32})\}$ corresponds to the output difference $\{S(2_{32})\oplus S(\bar{2}_{32})\}$ for the first two pairs.

2^7-1 …work required to test all possible input difference $\{(1_{01})\oplus(\bar{1}_{01})\}$ corresponds to the output difference $\{S(1_{01})\oplus S(\bar{1}_{01})\}$ for the first two pairs.

2^7-1 …work required to test all possible input difference { $(1_{01})\oplus(\bar{\bar{1}}_{01})$} corresponds to the output difference {$S(1_{01})\oplus S(\bar{1}_{01})$} for the second two pairs.
2^4 …work required to repeat all the above steps for each one of the 16 key bytes.
So we can give the total effort required to break two round AES variant as follows:

The total work required = ((2^7-1*2^7-1)+(2^7-1*2^7-1))*2^4< 2^{19}

The total number of chosen pairs = 33 pairs (33*16=528 bytes)

4. *Comparison withknown AES attacks:*

Table (8) gives a comparison between proposed attack and attack published by Charles Bouillaguet et al [3]. The results give that for three rounds AES-128 variant which is our case, the number of chosen plaintext-ciphertext pairs for our proposed attack is a little larger than what was required for the other attack. On the other hand the time complexity for proposed attack is significantly reduced using the introduced key partitioning principle.Also, when we look to the memory requirements for proposed attack where we need 2^{17} bytes of memory to store the difference distribution table for the AES S-BOX and the complement difference distribution table described above, which can be neglected compared to that is required for the attack presented in [3].

Table (8):*Comparison between cryptanalysis attacks against reduced variants of AES*

Year	Attack type	# of rounds	Attack complexity			Authors
			Data	Time	Memory	
2011	Meet in the middle	3	1 KP	2^{120}	1	Charles Bouillaguet, Patrick Derbez, Orr Dunkelman, Nathan Keller and Pierre-Alain Fouque,
		3	1 KP	2^{104}	2^{94}	
	Differential – meet in the middle	3	2 CP	2^{32}	1	
		3	9 KP	2^{40}	2^{35}	
		4	2 CP	2^{104}	1	
		4	5 CP	2^{64}	2^{68}	
		4	10 CP	2^{40}	2^{43}	
2012	A novel adaptive chosen plaintext attack	1	17 CP	2^4	2^{17} bytes	Proposed attack
		2	33 CP	$< 2^{12}$		
		3	33 CP	$< 2^{19}$		

5. *Conclusion and future work:*

In this paper, an attack against three rounds AES reduced variant is introduced. The proposed attack requires 33 chosen plaintext-ciphertext pairs, a time complexity of order $2^{19}$and a memory size of 2^{17} bytes to store the difference distribution table and the complement difference distribution table for the AES S-BOX.

The key partitioning principle is introduced to attack up to three rounds AES variant.It depends on a weak point in the AES architecture.Since the AES round function executes a byte level permutation rather than bit level permutation,we could divide our effort to process each byte individually.This operation could be more complicated if a bit level permutation is performed in the AES round function.

In the future work, we are planning to extend the proposed attack to more round of the AES. We shall consider the use of practically feasible memory resources rather than the theoretical ones used by other attacks to achieve lower complexity of the extended attacks.

6. References:

[1] A. Biryukov and D. Khovratovich, “*Related-key Cryptanalysis of the Full AES-192 and AES-256,*” University of Luxembourg,CryptologyePrint Archive: Report 2009/317, 2009.

[2] A. Biryukov, O. Dunkelman, N. Keller, D. Khovratovich, and A. Shamir, “*Key Recovery Attacks of Practical Complexity on AES Variants With Up To 10 Rounds,*” EUROCRYPT 2010.

[3]Charles Bouillaguet, PatrickDerbez, Orr Dunkelman, Nathan Keller and Pierre-Alain Fouque, *“Low data complexity attacks on AES,*” Weizmann Institute of Science,CryptologyePrint Archive: Report 2010/633, last revised 2011.

[4] E. Biham and A. Shamir; “*Differential Cryptanalysis –Differential Cryptanalysis of DES like cryptosystems,*”Journal of Cryptology, Vol. 4, No. 1, pp. 3-72, 1991.

[5] M. Hellman and S. Langford,*“Differential-linear Cryptanalysis,”* Crypto 1994.

[6] E. Biham, A. Biryukov and A. Shamir, “*Impossible Differential Introduction,*”Rump session presentation at Crypto 1998.

[7] E. Biham, A. Biryukov and A. Shamir, “*Impossible Differential Technique – Miss in the Middle Attacks on IDEA,*”Crypto1999.

[8]William Stalling, *“Cryptography and network security,” 5th.ed.,*Prentice Hall, 2011.

[9] C. Shannon, *“Confusion/Diffusion, Communication theory of secrecy systems,*” Bell System Technical Journal, 1949.