Research Paper

Volume : 2 | Issue : 10 | October 2013 • ISSN No 2277 - 8179

A Novel Chosen Plaintext Attack Against Aes Using Key Partitioning Principle

Communication

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

Amr M. Ashry

Alaa El-Din R. Shehata Chair of communications, Military technical college, Kobry el-kobba , Cairo, Egypt, Egyptian Armed Forces

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 4 rounds that uses only 33 chosen plaintext-ciphertext pairs, a workload of 247 (for three round variant) and 217 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 a round by round cryptanalysis till the fourth round of the AES will be followed. The results will show that a bit-level permutation is more efficient than byte-level permutation used in the AES round function. Hence, the use of a bit-level permutation in the AES round function instead of a byte level permutation is an achievement of this work as a counter measure for such type of attack.

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 Bouillaguet et 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.

This paper consists of six main sections. Section 1 is an introduction to this paper. Section 2 is a description of the AES differential characteristics. Section 3 describes the proposed attack in a round by round cryptanalysis till the fourth round. Section 4 is a comparison to the related previous work from other publications. Section 5 concludes this paper and illustrates the future related work. Section 6 lists the referenced publications in this paper.

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.

It should be noticed that, for any given value for ΔY only 2^7-1 values of ΔX rather than 2^8 needs to be tested, that is true because the other values of ΔX are impossible differentials. The attack shall consider this fact as will be discussed shortly.

Proposed Attack
The proposed key partitioning chosen plaintext attack is introduced in this section. An attack against single round AES variant will be introduced. Then, the attack will be extended to two, three and four 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 that idea the two plaintext pairs listed in Table (1) are chosen, 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 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. The attack will go through from here as the key point. After initial add round key the results listed in Table (2) are achieved.

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

The first encryption path(plain 1)				The second encryption path(plain 2)			
00	W_{10}	W_{20}	W_{30}	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) the results shown in Tables (3, 4) are achieved.

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

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

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

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

Given 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 called the key partitioning.

Assuming a single round AES encryption, then the cipher-text values for both paths is given, then by a simple XOR operation between the corresponding bytes of the cipher-text gives:

$$\begin{aligned} C_{01} \oplus \overline{C}_{01} = {} & C_{02} \oplus \overline{C}_{02} \\ & = S(W_{00}) \oplus S(W_{11}).02 \oplus S(W_{22}).03 \oplus S(W_{33}) \oplus W_{41} \oplus S(\overline{W}_{00}) \\ & \oplus S(W_{11}).02 \oplus S(W_{22}).03 \oplus S(W_{33}) \oplus W_{41} \\ & = S(W_{00}) \oplus S(W_{11}) \oplus S(W_{22}).02 \oplus S(W_{33}).03 \oplus W_{42} \oplus S(\overline{W}_{00}) \\ & \oplus S(W_{11}) \oplus S(W_{22}).02 \oplus S(W_{33}).03 \oplus W_{42} = S(W_{00}) \oplus S(\overline{W}_{00}) \\ & = known\ value \qquad (1) \end{aligned}$$

Equation (1) is valid for any key value after the first round. The first key byte "W_{00}" is 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 find it. To simplify it, a new table that holds the substitutions for each of a 128 possibilities out of 256 XORed with the substitution of their complement is constructed. 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 finding a match, one out of two correct first key byte value (W_{00}) is given and the other is its complement. It should be determined which one is correct. Simply, using any of them as the first byte of the plain-text again and apply a single round AES encryption. Hence, two possible situations after the initial add round key are given, (00_x) or (FF_x) then the bytewill have the two possible values listed in equations (2) and (3) .

$$\begin{aligned} C'_{01} & = S(00x) \oplus S(W_{11}).02 \oplus S(W_{22}).03 \oplus S(W_{33}) \oplus W_{41} \\ & = 63_x \oplus S(W_{11}).02 \oplus S(W_{22}).03 \oplus S(W_{33}) \oplus W_{41} \qquad (2) \end{aligned}$$

OR;

$$\begin{aligned} C'_{01} & = S(FFx) \oplus S(W_{11}).02 \oplus S(W_{22}).03 \oplus S(W_{33}) \oplus W_{41} \\ & = 16_x \oplus S(W_{11}).02 \oplus S(W_{22}).03 \oplus S(W_{33}) \oplus W_{41} \qquad (3) \end{aligned}$$

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

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

This will give:

$$\begin{aligned} C'_{01} \oplus C_{01} = {} & X \oplus S(W_{11}).02 \oplus S(W_{22}).03 \oplus S(W_{33}) \oplus W_{41} \oplus S(W_{00}) \oplus S(W_{11}).02 \oplus S(W_{22}).03 \\ & \oplus S(W_{33}) \oplus W_{41} = X \oplus S(W_{00}) \qquad (5) \end{aligned}$$

Where "X" ∈ $\{16_x, 63_x\}$, which can be rearranged to :

$$C'_{01} \oplus C_{01} \oplus S(W_{00}) = X \qquad (6)$$

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 calculated independently and that is the complete definition of the key partitioning principle.

3.2 Proposed Attack for Two Rounds AES Variant:

The single round AES attack is illustrated. The extension of the attack against 2-round AES variant is introduced in this section keeping the steps of the previous one. For simplicity the output of the first round will be named 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)			
$_{00}$	1_{10}	1_{20}	1_{30}	$_{00}$	1_{10}	1_{20}	1_{30}
1_{01}	1_{11}	1_{21}	1_{31}	$_{01}$	1_{11}	1_{21}	1_{31}
1_{02}	1_{12}	1_{22}	1_{32}	$_{02}$	1_{12}	1_{22}	1_{32}
1_{03}	1_{13}	1_{23}	1_{33}	$_{03}$	1_{13}	1_{23}	1_{33}

Now the output of the second round is calculated as 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($_{00}$).02 S($_{11}$).03 S($_{22}$) S($_{33}$)	S($_{10}$).02 S($_{21}$).03 S($_{32}$) S($_{03}$)	S($_{20}$).02 S($_{31}$).03 S($_{02}$) S($_{13}$)	S($_{30}$).02 S($_{01}$).03 S($_{12}$) S($_{23}$)
S($_{00}$) S($_{11}$).02 S($_{22}$).03 S($_{33}$)	S($_{10}$) S($_{21}$).02 S($_{32}$).03 S($_{03}$)	S($_{20}$) S($_{31}$).02 S($_{02}$).03 S($_{13}$)	S($_{30}$) S($_{01}$).02 S($_{12}$).03 S($_{23}$)
S($_{00}$) S($_{11}$) S($_{22}$).02 S($_{33}$).03	S($_{10}$) S($_{21}$) S($_{32}$).02 S($_{03}$).03	S($_{20}$) S($_{31}$) S($_{02}$).02 S($_{13}$).03	S($_{30}$) S($_{01}$) S($_{12}$).02 S($_{23}$).03
S($_{00}$).03 S($_{11}$) S($_{22}$) S($_{33}$).02	S($_{10}$).03 S($_{21}$) S($_{32}$) S($_{03}$).02	S($_{20}$).03 S($_{31}$) S($_{02}$) S($_{13}$).02	S($_{30}$).03 S($_{01}$) S($_{12}$) S($_{23}$).02

Table (7): The output of the second round

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

For the output of the second round for the two encryption paths, they will theme to be different looking at the experimental result. But the analytical results here shows that the difference is only in one term per each corresponding cipher bytes. So the 2-round AES attack will be conducted as follows:

$$
\begin{aligned}
\mathbf{2}_{32} \oplus \bar{\mathbf{2}}_{32} = {} & \mathbf{2}_{33} \oplus \bar{\mathbf{2}}_{33} \\
& = \mathbf{S}(\mathbf{1}_{30}) \oplus \mathbf{S}(\mathbf{1}_{01}) \oplus \mathbf{S}(\mathbf{1}_{12}).\mathbf{02} \oplus \mathbf{S}(\mathbf{1}_{23}).\mathbf{03} \oplus \mathbf{W}_{11,2} \oplus \mathbf{S}(\mathbf{1}_{30}) \\
& \oplus \mathbf{S}(\bar{\mathbf{1}}_{01}) \oplus \mathbf{S}(\mathbf{1}_{12}).\mathbf{02} \oplus \mathbf{S}(\mathbf{1}_{23}).\mathbf{03} \oplus \mathbf{W}_{11,2} \\
& = \mathbf{S}(\mathbf{1}_{30}).\mathbf{03} \oplus \mathbf{S}(\mathbf{1}_{01}) \oplus \mathbf{S}(\mathbf{1}_{12}) \oplus \mathbf{S}(\mathbf{1}_{23}).\mathbf{02} \oplus \mathbf{W}_{11,2} \oplus \mathbf{S}(\mathbf{1}_{30}).\mathbf{03} \\
& \oplus \mathbf{S}(\bar{\mathbf{1}}_{01}) \oplus \mathbf{S}(\mathbf{1}_{12}) \oplus \mathbf{S}(\mathbf{1}_{23}).\mathbf{02} \oplus \mathbf{W}_{11,2} = \mathbf{S}(\mathbf{1}_{01}) \oplus \mathbf{S}(\bar{\mathbf{1}}_{01}) \\
& = \boldsymbol{known\ value} \qquad (7)
\end{aligned}
$$

Equation (7) represents an output difference from the S-BOX. Calling the differential characteristics as was discussed section 2, this equation will have 127 solutions by looking to the difference distribution table of the AES S-BOX. But there is a condition that should be met only for the correct values, for each input difference $\{ (\mathbf{1}_{01}) \oplus (\bar{\mathbf{1}}_{01})\}$ possible for the output difference $\{ \mathbf{S}(\mathbf{1}_{01}) \oplus \mathbf{S}(\bar{\mathbf{1}}_{01})\}$ should give a value that lies in the complement pair difference table, but this is not enough to uniquely determine the correct value. So, it should be considered to 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 which is a first nibble complement of . After the initial add round key, the output of that pair can be represented like in Tables (6, 7). Then the same analysis needs to be conducted to that pair. This will give that:

$$
\mathbf{S}^{-1}(S(\mathbf{1}_{01})) \oplus \mathbf{S}^{-1}(S(\bar{\mathbf{1}}_{01})) = S(W_{00}) \oplus S(\overline{W}_{00})
$$
$$
= \boldsymbol{one\ value\ from\ the\ complement\ difference\ \ table}
$$
$$
\mathbf{S}^{-1}(S(\mathbf{1}_{01})) \oplus \mathbf{S}^{-1}(S(\bar{\bar{\mathbf{1}}}_{01})) = S(W_{00}) \oplus S(\overline{\overline{W}}_{00})
$$
$$
= \boldsymbol{one\ value\ from\ the\ 1st.nibble\ complement\ difference\ \ table}
$$

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 the correct key byte .

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 $\{ (\mathbf{1}_{01}) \oplus (\bar{\mathbf{1}}_{01})\}$ corresponds to the output difference $\{ \mathbf{S}(\mathbf{1}_{01}) \oplus \mathbf{S}(\bar{\mathbf{1}}_{01})\}$ for the first two pairs.

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

2^4 ...work required to repeat all the above steps for each one of the 16 key bytes.

So the total effort required to break two round AES variant is calculated as follows:

The total work required = $(2^7\text{-}1+2^7\text{-}1)*2^4< 2^{12}$

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

3.3 Proposed Attack Against Three Rounds AES Variant:

In this section the output of the third round is calculated like for the second round. The output of the second round given in Tables (6, 7) is named as matrices “2”& “”. Also, it should be considered that the input blocks to the third round are totally different from each other’s. But it also should be noticed 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. The states difference is given not the states itself.

It can be proved 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”:

Inv.Mix.Col(S_i⊕W_j)=[Inv.Mix.Col (S_i)]⊕[Inv.Mix.Col (W_j)]

Hence it can be concluded 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			
00+00	3_{10+10}	3_{20+20}	3_{30+30}
3_{01+01}	3_{11+11}	3_{21+21}	3_{31+31}
3_{02+02}	3_{12+12}	3_{22+22}	3_{32+32}
3_{03+03}	3_{13+13}	3_{23+23}	3_{33+33}

Multiplying by the inverse matrix will give:

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

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

Now a deterministic values for $\{\mathbf{S}(\mathbf{2}_{32}) \oplus \mathbf{S}(\bar{\mathbf{2}}_{32})\}$ and $\{\mathbf{S}(\mathbf{2}_{32}) \oplus \mathbf{S}(\bar{\bar{\mathbf{2}}}_{32})\}$ is given which is an output differences from the S-BOX which have 2^7-1 possible input differences $\{(\mathbf{2}_{32}) \oplus (\bar{\mathbf{2}}_{32})\}$ and $\{(\mathbf{2}_{32}) \oplus (\bar{\bar{\mathbf{2}}}_{32})\}$.

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 $\{ (\mathbf{2}_{32}) \oplus (\bar{\mathbf{2}}_{32})\}$ corresponds to the output difference $\{ \mathbf{S}(\mathbf{2}_{32}) \oplus \mathbf{S}(\bar{\mathbf{2}}_{32})\}$ for the first two pairs.
2^7-1 …work required to test all possible input difference $\{ (\mathbf{2}_{32}) \oplus (\bar{\bar{\mathbf{2}}}_{32})\}$ corresponds to the output difference $\{\mathbf{S}(\mathbf{2}_{32}) \oplus \mathbf{S}(\bar{\bar{\mathbf{2}}}_{32})\}$ for the first two pairs.
2^7-1 …work required to test all possible input difference $\{ (\mathbf{1}_{01}) \oplus (\bar{\mathbf{1}}_{01})\}$ corresponds to the output difference $\{\mathbf{S}(\mathbf{1}_{01}) \oplus \mathbf{S}(\bar{\mathbf{1}}_{01})\}$ for the first two pairs.
2^7-1 …work required to test all possible input difference $\{ (\mathbf{1}_{01}) \oplus (\bar{\bar{\mathbf{1}}}_{01})\}$ corresponds to the output difference $\{\mathbf{S}(\mathbf{1}_{01}) \oplus \mathbf{S}(\bar{\bar{\mathbf{1}}}_{01})\}$ for the second two pairs.

2^4 ...work required to repeat all the above steps for each one of the 16 key bytes.

So the total effort required to break three rounds AES variant is calculated 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)

3.4 Proposed Attack Against Four Rounds AES Variant:

From the previous analysis to the AES it can be noted that, the mix-columns operation after the shift-rows operation adds a great diffusion to the AES round by round. Also, the Sub-Bytes operation is a great source of nonlinearity that causes confusion to the cipher output. As expected moving forward throughout the AES rounds will raise significantly the time and memory requirements for the attack.

This section will show how the fourth round will affect the proposed attack effort to break such 4-rounds AES variant. The attack will start by the same number of pairs that was required for the two and three rounds AES attack which is 33 chosen plaintext-ciphertext pairs. The plain text of the first pair is all "00x", the other 32 pairs are divided into 16 groups that the attack will act on them together to get one byte of the key each time. Every group$_i$ (i..is the group number) consists of two pairs with the plain text of one of them have only one byte "FF$_x$" in the ith location and the other one have a byte "F0$_x$" in the corresponding location, all other bytes are all "00$_x$". The case of the first group is analyzed to get the first byte of the key, and then all other groups will have the same procedures to get one key of the byte each. As was discussed in the previous sections, the Inverse Mix-Columns operation can be applied to the output difference for each pair with the first pair which is all "00$_x$". Then the inverse shift rows operation will be applied, hence two difference states are achieved which are:

The first group difference (pair 1)			
$S(3_{00}) \oplus S(\bar{3}_{00})$	$S(3_{10}) \oplus S(\bar{3}_{10})$	$S(3_{20}) \oplus S(\bar{3}_{20})$	$S(3_{30}) \oplus S(\bar{3}_{30})$
$S(3_{01}) \oplus S(\bar{3}_{01})$	$S(3_{11}) \oplus S(\bar{3}_{11})$	$S(3_{21}) \oplus S(\bar{3}_{21})$	$S(3_{31}) \oplus S(\bar{3}_{31})$
$S(3_{02}) \oplus S(\bar{3}_{02})$	$S(3_{12}) \oplus S(\bar{3}_{12})$	$S(3_{22}) \oplus S(\bar{3}_{22})$	$S(3_{32}) \oplus S(\bar{3}_{32})$
$S(3_{03}) \oplus S(\bar{3}_{03})$	$S(3_{13}) \oplus S(\bar{3}_{13})$	$S(3_{23}) \oplus S(\bar{3}_{23})$	$S(3_{33}) \oplus S(\bar{3}_{33})$

The second group difference (pair 2)			
$S(3_{00}) \oplus S(\bar{\bar{3}}_{00})$	$S(3_{10}) \oplus S(\bar{\bar{3}}_{10})$	$S(3_{20}) \oplus S(\bar{\bar{3}}_{20})$	$S(3_{30}) \oplus S(\bar{\bar{3}}_{30})$
$S(3_{01}) \oplus S(\bar{\bar{3}}_{01})$	$S(3_{11}) \oplus S(\bar{\bar{3}}_{11})$	$S(3_{21}) \oplus S(\bar{\bar{3}}_{21})$	$S(3_{31}) \oplus S(\bar{\bar{3}}_{31})$
$S(3_{02}) \oplus S(\bar{\bar{3}}_{02})$	$S(3_{12}) \oplus S(\bar{\bar{3}}_{12})$	$S(3_{22}) \oplus S(\bar{\bar{3}}_{22})$	$S(3_{32}) \oplus S(\bar{\bar{3}}_{32})$
$S(3_{03}) \oplus S(\bar{\bar{3}}_{03})$	$S(3_{13}) \oplus S(\bar{\bar{3}}_{13})$	$S(3_{23}) \oplus S(\bar{\bar{3}}_{23})$	$S(3_{33}) \oplus S(\bar{\bar{3}}_{33})$

Now after getting these results, some backward analysis towards the third round will be illustrated. By substituting for the values from the previous round the results will be as follows:

$$\boldsymbol{S(3_{10}) \oplus S(\bar{3}_{10}) = S\big(S(2_{10}).02 \oplus S(2_{21}).03 \oplus S(2_{32}) \oplus S(2_{03}) \oplus W_{13,0}\big) \oplus S\big(S(\bar{2}_{10}).02 \oplus S(\bar{2}_{21}).03 \oplus S(\bar{2}_{32}) \oplus S(\bar{2}_{03}) \oplus W_{13,0}\big)} \tag{8}$$

$$\boldsymbol{S(3_{11}) \oplus S(\bar{3}_{11}) = S\big(S(2_{10}) \oplus S(2_{21}).02 \oplus S(2_{32}).03 \oplus S(2_{03}) \oplus W_{13,1}\big) \oplus S\big(S(\bar{2}_{10}) \oplus S(\bar{2}_{21}).02 \oplus S(\bar{2}_{32}).03 \oplus S(\bar{2}_{03}) \oplus W_{13,1}\big)} \tag{9}$$

$$\boldsymbol{S(3_{12}) \oplus S(\bar{3}_{12}) = S\big(S(2_{10}) \oplus S(2_{21}) \oplus S(2_{32}).02 \oplus S(2_{03}).03 \oplus W_{13,2}\big) \oplus S\big(S(\bar{2}_{10}) \oplus S(\bar{2}_{21}) \oplus S(\bar{2}_{32}).02 \oplus S(\bar{2}_{03}).03 \oplus W_{13,2}\big)} \tag{10}$$

$$\boldsymbol{S(3_{13}) \oplus S(\bar{3}_{13}) = S\big(S(2_{10}).03 \oplus S(2_{21}) \oplus S(2_{32}) \oplus S(2_{03}).02 \oplus W_{13,3}\big) \oplus S\big(S(\bar{2}_{10}).03 \oplus S(\bar{2}_{21}) \oplus S(\bar{2}_{32}) \oplus S(\bar{2}_{03}).02 \oplus W_{13,3}\big)} \tag{11}$$

These equations are conditioned by the following relations that assure the invers mix-columns operation for each encryption path:

$$\boldsymbol{S(2_{10}) \oplus S(\bar{2}_{10}) = \big((3_{10} \oplus \bar{3}_{10}).0E\big) \oplus \big((3_{11} \oplus \bar{3}_{11}).0B\big) \oplus \big((3_{12} \oplus \bar{3}_{12}).0D\big) \oplus \big((3_{13} \oplus \bar{3}_{13}).09\big)\big)} \tag{12}$$

$$\boldsymbol{S(2_{21}) \oplus S(\bar{2}_{21}) = \big((3_{10} \oplus \bar{3}_{10}).09\big) \oplus \big((3_{11} \oplus \bar{3}_{11}).0E\big) \oplus \big((3_{12} \oplus \bar{3}_{12}).0B\big) \oplus \big((3_{13} \oplus \bar{3}_{13}).0D\big)\big)} \tag{13}$$

$$\boldsymbol{S(2_{32}) \oplus S(\bar{2}_{32}) = \big((3_{10} \oplus \bar{3}_{10}).0D\big) \oplus \big((3_{11} \oplus \bar{3}_{11}).09\big) \oplus \big((3_{12} \oplus \bar{3}_{12}).0E\big) \oplus \big((3_{13} \oplus \bar{3}_{13}).0B\big)\big)} \tag{14}$$

$$\boldsymbol{S(2_{03}) \oplus S(\bar{2}_{03}) = \big((3_{10} \oplus \bar{3}_{10}).0B\big) \oplus \big((3_{11} \oplus \bar{3}_{11}).0D\big) \oplus \big((3_{12} \oplus \bar{3}_{12}).09\big) \oplus \big((3_{13} \oplus \bar{3}_{13}).0E\big)\big)} \tag{15}$$

It can be observed that, for equations (12) to (15) the right hand side consists of 4 input differences corresponds to the 4 output differences obtained above, so for finding the correct input differences all possible value which are (< 2^{28}) need to be tested according to the difference distribution table. For each one of these values the attack needs to step back and repeat the three rounds attack to find the correct key value. The total work required for the attack can be summarized as follows:

The total work required = ((2^{28}*2^7-1*2^7-1) + (2^{28}*2^7-1*2^7-1))*2^4 < 2^{47}

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

From these results, it can be noticed that the diffusion and confusion effect of the AES iterations increases significantly starting from the fourth to the rest of the rounds, which makes the cryptanalysis to more further rounds raises to higher order complexity and practically infeasible.

Comparison With Known 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 the case, the number of chosen plaintext-ciphertext pairs for 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, looking to the memory requirements for proposed attack where 2^{17} bytes of memory are needed 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].

For the four rounds attack, both number of chosen plaintext-ciphertext pairs and the time complexity for our proposed attack are higher than those of the introduced Differential – meet in the middle in [3]. However, the memory requirements which may be neglected compared to that for the attack in [3] must be regarded.

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	$< 2^{19}$		
		4	33 CP	$< 2^{47}$		

Conclusion and Future Work:

In this paper, an attack against four rounds AES reduced variant is introduced. The proposed attack requires 33 chosen plaintext-ciphertext pairs, a time complexity of order 2^{47} 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 four 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, the effort required is divided 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, extension of the proposed attack to more round of the AES is planned. Considering the use of practically feasible memory resources rather than the theoretical ones used by other attacks will achieve lower complexity of the extended attacks.

REFERENCE

[1] A. Biryukov and D. Khovratovich, “Related-key Cryptanalysis of the Full AES-192 and AES-256,” University of Luxembourg,Cryptology ePrint 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, Cryptology ePrint 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 Conference, Santa Barbara, California, USA, 1994. | [6] E. Biham, A. Biryukov and A. Shamir, “Impossible Differential Introduction,”Rump session presentation at Crypto Conference, Santa Barbara, California, USA, 1998. | [7] E. Biham, A. Biryukov and A. Shamir, “Impossible Differential Technique –Miss in the Middle Attacks on IDEA,” Crypto Conference, Santa Barbara, California, USA, 1999. | [8] William Stalling, “Cryptography and network security,” 5th. ed., Prentice Hall, 2011. |