On the vulnerability of Simplified AES Algorithm Against Linear Cryptanalysis

S. Davod. Mansoori and H. Khaleghei Bizaki

Malek Ashtar University of Technology, Tehran, Iran

Summary
Linear attack, at the first, introduced for DES encryption system, by Matsui. That cryptanalysis was based on linear approximation of nonlinear S-boxes of algorithm. Then this kind of attack deployed for other kind of block ciphers. The first linear cryptanalysis on SAES introduced by Mohammad A. Musa et all , so they analyzed linear attack on first round of SAES. This paper improve their work on fist round and develop it for full round linear attack. We show that this algorithm is vulnerable against linear attack. Undoubtly, one of the important results of this cryptanalysis is that, it will be possible to propose proper linear attack on Rijndael.

Key words:
Simplified AES, Linear Cryptanalysis, S-box.

1. Introduction

The Advanced Encryption Standard (AES) is the standard algorithm adopted by the National Institute of Standards and Technology (NIST) on 2001 to replace the ageing Data Encryption Standard (DES) for encryption and protection of secure and non-classified information. NIST chose 128-bit block Rijndael to become the AES. Rijndael is a symmetric-key block cipher designed by Joan Daemen and Vincent Rijmen [1].

In this paper, we consider a simplified AES (SAES). SAES is proposed as a purely educational encryption algorithm to aid cryptography and cryptanalysis persons to better understand the concepts behind the real AES [1]. The SAES is simpler than AES for understanding, but it has a good mathematical structure, such as AES. It means that by understanding SAES and expands its concepts; reader can understand AES, simpler.

The first linear cryptanalysis on SAES introduced by Mohammad A.Musa *et all* in[2], so they analyzed linear attack on first round of SAES. This paper improve their work on fist round and develop it for full round linear attack (based on our previous work [3]). We show that this algorithm is vulnerable against linear attack. Undoubtedly, one of important results of this cryptanalysis is that, it will be possible to propose proper linear attack on Rijndael. Note that, there is another simplified version of the AES algorithm as Mini-AES, where linear cryptanalysis is done on second round of it by authors in [4].

The paper is organized as follow. Section 2 reviews briefly structure of SAES. The SAES encryption process is explained, briefly, in section 3. Linear cryptanalysis attack on first and second rounds SAES are presented in sections 4 and 5, respectively. Conclusion is explained in section 6.

2. Structure of SAES

SAES has a 16-bit original key, that denoted as $k_0k_1...k_{15}$. This key need to be expanded to a total of 48 key bits $k_0k_1...k_{47}$,where the first 16 key bits are the same as the original key and others expand according to key expansion. Both the key expansion and encryption algorithms of SAES depend on an S-box, that itself depends on the finite field whit 16 elements. The finite field $GF(2)$ consists of the set $\{0,1\}$ where all operations work modulo 2. $GF(2)[x]$ is used to denote polynomials with coefficients in $GF(2)$. The polynomials with coefficients in $GF(2)$ modulo (x^4+x+1) are defined as field $GF(16)=GF(2)[x]/(x^4+x+1)$.

The S-box is a non linear, invertible map from nibbles to nibbles. Here, at the first, the nibble inverted in $GF(16)$ (the nibble 0000 is not invertible, so at this step it is sent to itself). Then the output of the inversion nibble ($b_0b_1b_2b_3$) associated the element $N(y)=b_0y^3+b_1y^2+b_2y+b_3$ in $GF(2)[y]/(y^4+1)$. $a(y)=y^3+y+1$ and $b(y)=y^3+1$ are elements in $GF(2)[y]/(y^4+1)$. The second step of the S-box is to send the nibble *N(y)* to $a(y)N(y)+b(y)$. Note that $y^4+1=(y+1)^4$ is reducible over $GF(2)$ so $GF(2)[y]/(y^4+1)$ is not a field and not all of its non-zero elements are invertible. The second step can also be described an affine matrix map as Fig.(1).

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} \qquad (1)$$

Fig.(1)- affine map of S-box

Manuscript received July 5, 2007
Manuscript revised July 25, 2007

All affine maps over $GF(2)[y]/(y^4+1)$ are affine matrix maps, but not vise versa. So it is algebraically more informative to know that it is an affine map over $GF(2)[y]/(y^4+1)$. It can be shown that the action of the S-box is as fig. (2).In this figure the intermediary output of the inversion is not shown.

nib	S-box(nib)	nib	S-box(nib)
0000	1001	1000	0110
0001	0100	1001	0010
0010	1010	1010	0000
0011	1011	1011	0011
0100	1101	1100	1100
0101	0001	1101	1110
0110	1000	1110	1111
0111	0101	1111	0111

Fig.(2)-The action of S-box

RC[i] is defined as $RC[i] = x^{i+2} \in GF(16)$ and $RCON[i] = RC[i]0000$ (this is a byte and is an abbreviations for round constant), so $RC[1] = x^3 = 1000$ and $RC[2] = x^4 = x+1 = 0011$. If N_0 and N_1 are nibbles, then their concatenation denoted as N_0N_1. The word nibble refers to a four-bit string (half a byte). In this paper frequently associated an element $b_0x^3 + b_1x^2 + b_2x + b_3$ of $GF(16)$ with the nibble $b_0b_1b_2b_3$. The function *RotNib* is defined to be $RotNib(N_0N_1) = N_1N_0$ and the function *SubNib* to be $SubNib(N_0N_1) = S-box(N_0)S-box(N_1)$ (these are functions for byte to bytes). Their names are abbreviations for rotate nibble and substitute nibble, respectively.

An array W ,whose entries are byte, is considered so that the original key fills $W[0]$ and $W[1]$ in order.

For $2 \le i \le 5$; If $i \equiv 0 (\mathrm{mod}\, 2)$ then :

$$W[i] = W[i-2] \oplus RCON(i/2) \oplus SubNib(RotNib(W[i-1]))$$

else :

$$W[i] = W[i-1] \oplus W[[i-2]$$

The bits contained in the entries of W can be denoted $k_0k_1...k_{47}$. For $0 \le i \le 2$ K_i is considered as $K_i = W[2i]W[2i+1]$ So $K_0 = k_0k_1...k_{15}$, $K_1 = k_{16}k_{17}...k_{31}$ and $K_2 = k_{32}k_{33}...k_{47}$. For $1 \le i$, K_i is the round key used at the end of the *i*-th round (K_0 is used before the first round).

As explained before, SAES algorithm operates on 16-bit plaintext and generates 16-bit ciphertext, using the expanded key $k_0k_1...k_{47}$. Suppose $p_0p_1...p_{15}$ be plaintext and the ciphertext be $c_0c_1...c_{15}$. The encryption algorithm consists of the composition of 8 functions applied to plaintext. So :

$$c_0c_1..c_{15} = A_{K_2} o\, SRo\, NSo\, A_{K_1} o\, MCo\, SRo\, NSo\, A_{K_0}(p_0p_1...p_{15}) \quad (2)$$

where $A_{K_i}(p) = K_i \oplus p$ and each function operates on a state. The nibbles configurations are as fig (3).

$p_8p_9p_{10}p_{11}$	$p_0p_1p_2p_3$
$p_{12}p_{13}p_{14}p_{15}$	$p_4p_5p_6p_7$

Fig. (3)-The nibble configuration

The abbreviation *NS* stands for *nibble substitution*. The function of *NS* is defined as :

N_2	N_0	NS	$S-box(N_2)$	$S-box(N_0)$
N_3	N_1	→	$S-box(N_3)$	$S-box(N_1)$

The *SR* stands for *shift row*. Its function is defined as :

N_2	N_0	SR	N_2	N_0
N_3	N_1	→	N_1	N_3

The abbreviation *MC* stands for *mix column*. A column $[N_i, N_j]$ of the state is considered to be the element $N_iz + N_j$ of $GF(16)[z]/(z^2+1)$. The function *MC* multiplies each column by the polynomial $c(z) = x^2z + 1$. This operation can be considered as:

$$\begin{bmatrix} N_0 & N_2 \\ N_1 & N_3 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & x^2 \\ x^2 & 1 \end{bmatrix} \begin{bmatrix} N_0 & N_2 \\ N_1 & N_3 \end{bmatrix} \quad (3)$$

In SAES Encryption, the composition of function $A_{K_i} o\, MC\, o\, SR\, o\, NS$ is considered to be the *i*-th round. This simplified algorithm has two rounds so, A_{K_0} is applied prior of first round and *MC* omitted for second round.

3. Encryption Process of SAES

The encryption process is:

$$c_0c_1...c_{15} = A_{K_2} o\, SRo\, NSo\, A_{K_1} o\, MCo\, SRo\, NSo\, A_{K_0}(p_0p_1...p_{15})$$

At the first step, after $A_{K_0}(p) = K_0 \oplus p$ the output is:

$p_8 \oplus k_8$ $p_9 \oplus k_9$ $p_{10} \oplus k_{10}$ $p_{11} \oplus k_{11}$	$p_0 \oplus k_0$ $p_1 \oplus k_1$ $p_2 \oplus k_2$ $p_3 \oplus k_3$
$p_{12} \oplus k_{12}$ $p_{13} \oplus k_{13}$ $p_{14} \oplus k_{14}$ $p_{15} \oplus k_{15}$	$p_4 \oplus k_4$ $p_5 \oplus k_5$ $p_6 \oplus k_6$ $p_7 \oplus k_7$

Let:

$$S-box(p_i \oplus k_i, p_{i+1} \oplus k_{i+1}, p_{i+2} \oplus k_{i+2}, p_{i+3} \oplus k_{i+3}) = m_i m_{i+1} m_{i+2} m_{i+3} \qquad i = 0,4,8,12$$

and so on. After *NS* and *SR* the state is then :

$m_8 m_9 m_{10} m_{11}$	$m_0 m_1 m_2 m_3$
$m_4 m_5 m_6 m_7$	$m_{12} m_{13} m_{14} m_{15}$

After *MC* the output is:

$m_6 \oplus m_8 \oplus k_{24}, m_4 \oplus m_7 \oplus m_9 \oplus k_{25}$, $m_4 \oplus m_5 \oplus m_{10} \oplus k_{26}, m_5 \oplus m_{11} \oplus k_{27}$	$m_0 \oplus m_{14} \oplus k_{16}, m_1 \oplus m_{12} \oplus m_{15} \oplus k_{17}$, $m_2 \oplus m_{12} \oplus m_{13} \oplus k_{18}, m_3 \oplus m_{13} \oplus k_{19}$
$m_4 \oplus m_{10} \oplus k_{28}, m_5 \oplus m_8 \oplus m_{11} \oplus k_{29}$, $m_6 \oplus m_8 \oplus m_9 \oplus k_{30}, m_7 \oplus m_9 \oplus k_{31}$	$m_2 \oplus m_{12} \oplus k_{20}, m_0 \oplus m_3 \oplus m_{13} \oplus k_{21}$, $m_0 \oplus m_1 \oplus m_{14} \oplus k_{22}, m_1 \oplus m_{15} \oplus k_{23}$

Let :

$$\begin{aligned}
&S-box(m_0 \oplus m_{14} \oplus k_{16}, m_1 \oplus m_{12} \oplus m_{15} \oplus k_{17}, m_2 \oplus m_{12} \\
&\quad \oplus m_{13} \oplus k_{18}, m_3 \oplus m_{13} \oplus k_{19}) = n_0 n_1 n_2 n_3 \\
&S-box(m_2 \oplus m_{12} \oplus k_{20}, m_0 \oplus m_3 \oplus m_{13} \oplus k_{21}, m_0 \oplus m_1 \\
&\quad \oplus m_{14} \oplus k_{22}, m_1 \oplus m_{15} \oplus k_{23}) = n_4 n_5 n_6 n_7 \\
&S-box(m_6 \oplus m_8 \oplus k_{24}, m_4 \oplus m_7 \oplus m_9 \oplus k_{25}, m_4 \oplus m_5 \\
&\quad \oplus m_{10} \oplus k_{26}, m_5 \oplus m_{11} \oplus k_{27}) = n_8 n_9 n_{10} n_{11} \\
&S-box(m_4 \oplus m_{10} \oplus k_{28}, m_5 \oplus m_8 \oplus m_{11} \oplus k_{29}, m_6 \oplus m_8 \\
&\quad \oplus m_9 \oplus k_{30}, m_7 \oplus m_9 \oplus k_{31}) = n_{12} n_{13} n_{14} n_{15}
\end{aligned} \quad (4)$$

At the end of encryption, the final state will be equivalent whit ciphertext:

$n_8 \oplus k_{40}, n_9 \oplus k_{41}, n_{10} \oplus k_{42}, n_{11} \oplus k_{43}$	$n_0 \oplus k_{32}, n_1 \oplus k_{33}, n_2 \oplus k_{34}, n_3 \oplus k_{35}$
$n_4 \oplus k_{44}, n_5 \oplus k_{45}, n_6 \oplus k_{46}, n_7 \oplus k_{47}$	$n_{12} \oplus k_{36}, n_{13} \oplus k_{37}, n_{14} \oplus k_{38}, n_{15} \oplus k_{39}$

so, it is equivalent to :

$c_8 c_9 c_{10} c_{11}$	$c_0 c_1 c_2 c_3$
$c_{12} c_{13} c_{14} c_{15}$	$c_4 c_5 c_6 c_7$

By considering the key expansion:

$$\begin{aligned}
&K_0 = W[0]W[1] = (k_0 k_1 ... k_7)(k_8 k_9 ... k_{15}) \\
&K_1 = W[2]W[3] = (k_{16} k_{17} ... k_{23})(k_{24} k_{25} ... k_{31}) \\
&K_2 = W[4]W[5] = (k_{32} k_{33} ... k_{39})(k_{40} k_{41} ... k_{47}) \\
&W[2] = W[0] \oplus 10000000 \oplus \\
&\qquad S-box(k_{12} k_{13} k_{14} k_{15}) S-box(k_8 k_9 k_{10} k_{11}) \\
&W[3] = W[1] \oplus W[2] \\
&W[4] = W[2] \oplus 00110000 \oplus \\
&\qquad S-box(k_{28} k_{29} k_{30} k_{31}) S-box(k_{24} k_{25} k_{26} k_{27}) \\
&W[5] = W[3] \oplus W[4]
\end{aligned} \quad (5)$$

Let:

$$\begin{aligned}
&S-box(k_{12} k_{13} k_{14} k_{15}) = l_0 l_1 l_2 l_3 \\
&S-box(k_8 k_9 k_{10} k_{11}) = l_4 l_5 l_6 l_7 \\
&S-box(k_{28} k_{29} k_{30} k_{31}) = l_8 l_9 l_{10} l_{11} \\
&S-box(k_{24} k_{25} k_{26} k_{27}) = l_{12} l_{13} l_{14} l_{15}
\end{aligned} \quad (6)$$

Therefore:

$$\begin{aligned}
&k_{16} = k_0 \oplus 1 \oplus l_0 \ , \ k_i = k_{i-16} \oplus l_{i-16} (i = 17,18,...,23) \\
&k_{34} = k_{18} \oplus 1 \oplus l_{10} , \ k_{35} = k_{19} \oplus 1 \oplus l_{11} \\
&k_i = k_{i-16} \oplus l_{i-24} \ (i = 32,33,36,37,38,39)
\end{aligned} \quad (7)$$

By considering $W[3], W[5]$:

$$\begin{aligned}
k_i = k_{i-8} \oplus k_{i-16} : \ & i = 24,25,...31 \\
& i = 40,41,...47
\end{aligned} \quad (8)$$

The above relation will be used in linear analysis in next section.

4. First Round Linear Cryptanalysis

Linear attack, at the first, introduced for DES encryption system, by Matsui [5]. In linear cryptanalysis assumed that a single key has been used to encrypt many plaintexts and that Eve (an eavesdropper) has access to many plaintexts and corresponding cipher texts from this key so, Eve wants determine this key. The idea of linear cryptanalysis is to find equations of the form:

$$b \oplus \sum_{i \in s_1} p_i \oplus \sum_{j \in s_2} c_j = \sum_{l \in s_3} k_l \quad (9)$$

with probability greater than 0.5 (the greater the better). Here b is the bit 0 or 1, p_i denotes the i-th plaintext bit, c_j denotes the j-th cipher text bit, k_l denotes the l-th key bit and each s_m is a subset of $\{0,1,\ldots,15\}$. Since linear cryptanalysis requires that Eve has plaintexts and corresponding ciphertexts, it is called a known plaintext attack [6].

The only non-linear function in simplified AES is the S-box. It is desired to find the linear equations corresponding input and output bits of the S-box which hold with the highest probabilities (more than0.5). Let $S-box(a_0 a_1 a_2 a_3) = b_0 b_1 b_2 b_3$. It is possible that extract 8 equations with probability 0.75 between input and output of S-boxes. So :

$$\begin{aligned}
&a_3 \oplus b_0 = 1 \quad a_1 \oplus a_2 \oplus b_0 \oplus b_1 = 1 \\
&a_0 \oplus a_1 \oplus b_0 = 1 \quad a_0 \oplus b_0 \oplus b_1 = 1 \\
&a_1 \oplus b_1 = 0 \quad a_0 \oplus b_2 = 0 \\
&a_0 \oplus a_1 \oplus a_2 \oplus a_3 \oplus b_1 = 0 \quad a_0 \oplus a_1 \oplus a_2 \oplus b_2 = 0
\end{aligned} \quad (10)$$

Each of the above equations (according to Fig. (2)), have probability equal to $p = 12/16 = 0.75$. By substitution these equations in equation (8), probability equations system is extracted with probability equal to 0.75. Bu using Fig (2) and relation (10):

$$\begin{aligned}
&c_0 \oplus c_8 \oplus k_8 = m_0 \oplus m_{14} \oplus m_6 \oplus m_8 \\
&c_1 \oplus c_9 \oplus k_9 = m_1 \oplus m_{12} \oplus m_{15} \oplus m_4 \oplus m_7 \oplus m_9 \\
&c_2 \oplus c_{10} \oplus k_{10} = m_2 \oplus m_{12} \oplus m_{13} \oplus m_4 \oplus m_5 \oplus m_{10} \\
&c_3 \oplus c_{11} \oplus k_{11} = m_3 \oplus m_{13} \oplus m_5 \oplus m_{11} \\
&c_4 \oplus c_{12} \oplus k_{12} = m_2 \oplus m_{12} \oplus m_4 \oplus m_{10} \\
&c_5 \oplus c_{13} \oplus k_{13} = m_0 \oplus m_3 \oplus m_{13} \oplus m_5 \oplus m_8 \oplus m_{11} \\
&c_6 \oplus c_{14} \oplus k_{14} = m_0 \oplus m_1 \oplus m_{14} \oplus m_6 \oplus m_8 \oplus m_9 \\
&c_7 \oplus c_{15} \oplus k_{15} = m_1 \oplus m_{15} \oplus m_7 \oplus m_9
\end{aligned} \quad (11)$$

It should be noted that, If x and y be two Boolean By pair wise adding of equations (11) :

$$\begin{aligned} c_0 \oplus c_6 \oplus c_8 \oplus c_{14} \oplus k_8 \oplus k_{14} &= m_1 \oplus m_9 \\ c_3 \oplus c_5 \oplus c_{11} \oplus c_{13} \oplus k_{11} \oplus k_{13} &= m_0 \oplus m_8 \\ c_2 \oplus c_4 \oplus c_{10} \oplus c_{12} \oplus k_{10} \oplus k_{12} &= m_5 \oplus m_{13} \\ c_1 \oplus c_7 \oplus c_9 \oplus c_{15} \oplus k_9 \oplus k_{15} &= m_4 \oplus m_{12} \end{aligned} \quad (12)$$

By using relation (4) and equations related to k_{16} and k_{18} in firs nibble:

$$\begin{aligned} m_0 \oplus m_{14} \oplus k_{16} &= c_0 \\ m_2 \oplus m_{12} \oplus m_{13} \oplus k_{18} &= c_2 \end{aligned} \quad (13)$$

By using probability equations in (10) for relations (12) and (13), linear equations system between plaintext, ciphertext and keys (18 keys) with probability equal 0.625 is extracted. By solution of this probability linear equations system, key can be fined.

For example, for first equation in (13) and using relations $a_0 \oplus b_2 = 0, a_0 \oplus a_1 \oplus a_2 \oplus b_2 = 0$ and $a_3 \oplus b_0 = 1$, probability equations with probability equal 0.75 is extracted, so:

$$\begin{aligned} p_3 \oplus k_3 \oplus m_0 &= 1 \\ p_{12} \oplus k_{12} \oplus m_{14} &= 0 \\ p_{12} \oplus p_{13} \oplus p_{14} \oplus k_{12} \oplus k_{13} \oplus k_{14} \oplus m_{14} &= 0 \end{aligned} \quad (14)$$

By using (10) for (3), two probability equations with probability equal to 0.625 is resulted:

$$\begin{aligned} p_3 \oplus p_{12} \oplus c_0 \oplus 1 &= k_3 \oplus k_{12} \oplus k_{16} \\ p_3 \oplus p_{12} \oplus p_{13} \oplus p_{14} \oplus c_0 \oplus 1 &= k_3 \oplus k_{12} \oplus k_{13} \oplus k_{14} \oplus k_{16} \end{aligned} \quad (15)$$

As described prior, it is possible to extract 18 independent equations with probability equal to 0.625. This final equations system is:

$$\begin{aligned} p_3 \oplus p_{11} \oplus c_3 \oplus c_5 \oplus c_{11} \oplus c_{13} &= k_3 \oplus k_{13} \\ p_7 \oplus p_{15} \oplus c_1 \oplus c_7 \oplus c_9 \oplus c_{15} &= k_7 \oplus k_9 \\ p_1 \oplus p_9 \oplus c_0 \oplus c_6 \oplus c_8 \oplus c_{14} &= k_1 \oplus k_8 \oplus k_9 \oplus k_{14} \\ p_3 \oplus p_{12} \oplus c_0 \oplus 1 &= k_3 \oplus k_{12} \oplus k_{16} \\ p_0 \oplus p_{12} \oplus c_2 \oplus 1 &= k_0 \oplus k_{12} \oplus k_{18} \\ p_5 \oplus p_{13} \oplus c_2 \oplus c_4 \oplus c_{10} \oplus c_{12} &= k_5 \oplus k_{10} \oplus k_{12} \oplus k_{13} \\ p_3 \oplus p_{12} \oplus p_{13} \oplus p_{14} \oplus c_0 \oplus 1 &= k_3 \oplus k_{12} \oplus k_{13} \oplus k_{14} \oplus k_{16} \\ p_0 \oplus p_1 \oplus p_2 \oplus p_{12} \oplus c_2 \oplus 1 &= k_0 \oplus k_1 \oplus k_2 \oplus k_{12} \oplus k_{18} \end{aligned}$$

$$\begin{aligned} p_3 \oplus p_8 \oplus p_9 \oplus c_3 \oplus c_5 \oplus c_{11} \oplus c_{13} &= k_3 \oplus k_8 \oplus k_9 \oplus k_{11} \oplus k_{13} \\ p_0 \oplus p_1 \oplus p_8 \oplus p_9 \oplus c_3 \oplus c_5 \oplus c_{11} \oplus c_{13} &= k_0 \oplus k_1 \oplus k_8 \oplus k_9 \oplus k_{11} \oplus k_{13} \\ p_7 \oplus p_{12} \oplus p_{13} \oplus c_1 \oplus c_7 \oplus c_9 \oplus c_{15} &= k_7 \oplus k_9 \oplus k_{12} \oplus k_{13} \oplus k_{15} \\ p_4 \oplus p_5 \oplus p_{12} \oplus p_{13} \oplus c_1 \oplus c_7 \oplus c_9 \oplus c_{15} &= k_4 \oplus k_5 \oplus k_9 \oplus k_{12} \oplus k_{13} \oplus k_{15} \\ p_1 \oplus p_8 \oplus p_9 \oplus p_{10} \oplus p_{11} \oplus c_0 \oplus c_6 \oplus c_8 \oplus c_{14} &= k_1 \oplus k_9 \oplus k_{10} \oplus k_{11} \oplus k_{14} \\ p_0 \oplus p_1 \oplus p_2 \oplus p_3 \oplus p_8 \oplus p_9 \oplus p_{10} \oplus p_{11} \oplus c_0 \oplus c_6 \oplus c_8 \oplus c_{14} &= k_0 \oplus k_1 \oplus k_2 \oplus k_3 \oplus k_9 \oplus k_{10} \oplus k_{11} \oplus k_{14} \\ p_5 \oplus p_{12} \oplus p_{13} \oplus p_{14} \oplus p_{15} \oplus c_2 \oplus c_4 \oplus c_{10} \oplus c_{12} &= k_5 \oplus k_{10} \oplus k_{13} \oplus k_{14} \oplus k_{15} \\ p_4 \oplus p_5 \oplus p_6 \oplus p_7 \oplus p_{12} \oplus p_{13} \oplus p_{14} \oplus p_{15} \oplus c_2 \oplus c_4 \oplus c_{10} \oplus c_{12} &= k_4 \oplus k_5 \oplus k_6 \oplus k_7 \oplus k_{10} \oplus k_{13} \oplus k_{14} \oplus k_{15} \\ p_1 \oplus p_2 \oplus p_9 \oplus p_{10} \oplus c_0 \oplus c_3 \oplus c_5 \oplus c_6 \oplus c_8 \oplus c_{11} \oplus c_{13} \oplus c_{14} &= k_1 \oplus k_2 \oplus k_8 \oplus k_9 \oplus k_{10} \oplus k_{11} \oplus k_{13} \oplus k_{14} \\ p_5 \oplus p_6 \oplus p_{13} \oplus p_{14} \oplus c_1 \oplus c_2 \oplus c_4 \oplus c_7 \oplus c_9 \oplus c_{10} \oplus c_{12} \oplus c_{15} &= k_5 \oplus k_6 \oplus k_9 \oplus k_{10} \oplus k_{12} \oplus k_{13} \oplus k_{14} \oplus k_{15} \end{aligned} \quad (16)$$

As described above, Eve now takes the known plaintetxts and corresponding ciphertexts and evaluates the left-hand side of each of the 18 equations. The main question it that, how many texts is needed for Eve to break the cipher?

Let, Eve wants to be 95% certain that all 18 key bit choices are correct. For *i*=1,…,18, let $\hat{p}_i = 0.625$ denote the random variable whose value is equal to the proportion of the *n* plaintexts and corresponding ciphertexts for which the left-hand side of equation *i* is equal to the correct value (0 or 1) of the right-hand side, for the given key. For each *i* , the expected value of $\hat{p}_i$ is 0.625 and its variance is $\frac{0.625(1-0.625)}{n}$. Therefore the standard deviation of $\hat{p}_i$ is $\sqrt{\frac{0.625(1-0.625)}{n}}$.

It is desired that $prob(\hat{p}_i > 0.5) = \sqrt[18]{0.95} = 0.9972$. For sufficiently large *n*, the random variable $\hat{p}_i$ is essentially normal. So it is possible that, standardize $\hat{p}_i$ by subtracting off its expected value and dividing by its standard deviation, which will give (approximately) the standard normal random variable denoted as Z.

$$prob\left(\frac{\hat{p}_i - 0.625}{\sqrt{\frac{0.625(1-0.625)}{n}}} > \frac{0.5 - 0.625}{\sqrt{\frac{0.625(1-0.625)}{n}}}\right) = 0.9972$$

$$\Rightarrow prob(\frac{\hat{p}_i - 0.625}{\frac{0.4841}{\sqrt{n}}} > \frac{0.5 - 0.625}{\frac{0.4841}{\sqrt{n}}}) = 0.9972$$

Then :

$$p(Z > -0.2582\sqrt{n}) = 0.9972$$
$$p(Z < 0.2582\sqrt{n}) = 1 - 0.9972 = 0.0028 \qquad (17)$$
$$p(Z > 0.2582\sqrt{n}) = Q(0.2582\sqrt{n}) = 0.0028$$

By using standard Z function table:

$$n = 115.1179$$

Then 116 plaintexts are needed for broken the cipher. If none of the keys works, she can get more plaintexts and corresponding ciphertexts.

Thus this linear cryptanalytic attack seems very attractive compared to a pure brute force attack for second round SAES. However when added rounds (for real AES), more addition of equations is needed in order to elimination unknown parameters. In this situation, intermediary bits and the probabilities associated to the equations then tend toward 0.5, is needed (as seen above the probability go from 0.75 to 0.625). The result is that, many more plaintexts and corresponding ciphertexts is needed in order to be fairly certain of picking the correct bit values for the $\sum_{l \in S} k_l$'s.

5. Second Round Linear Cryptanalysis

As told before, the idea of linear cryptanalysis is to find equations of the form (9). In this cryptanalysis, one system with 32 linear equations for 32 keys $k_0, k_1, ..k_{15}, k_{16}, k_{17}, ...k_{23}, k_{32}, k_{33}, ...k_{39}$ with probability equal 0.5625 is extracted. The other expanded keys can be converted to original key in this linear equations system, then it is possible to extract original key by solution this system equations. Note that variable indexes from 0 till 15 correspond to plaintext and cipher text and indexes from 0 till 47 corresponding to keys. In analysis it is preferred the equations be corresponding to original key (if it is possible).

Similar to before section, it is possible to extract 12 equations with probability 0.75 between input and output of S-boxes, i.e.,

$$\begin{array}{ll} a_0 \oplus b_2 = 0 & a_3 \oplus b_0 = 1 \\ a_2 \oplus a_3 \oplus b_3 = 1 & a_0 \oplus a_1 \oplus b_0 = 1 \\ a_2 \oplus b_2 \oplus b_3 = 1 & a_1 \oplus b_1 = 0 \\ a_2 \oplus b_1 \oplus b_3 = 1 & a_0 \oplus a_1 \oplus a_2 \oplus a_3 \oplus b_1 = 0 \\ a_1 \oplus b_0 \oplus b_3 = 0 & a_1 \oplus a_2 \oplus b_0 \oplus b_1 = 1 \\ a_0 \oplus a_1 \oplus b_1 \oplus b_2 \oplus b_3 = 1 & a_0 \oplus b_0 \oplus b_1 = 1 \end{array} \qquad (18)$$

Each of the above equations (according to Fig.(2)), have probability equal to $p = 12/16 = 0.75$. By substitution these equations in four equations of (4), 48 probability equations are extracted with probability equal to 0.75. Some of these equations are:

$$\begin{array}{ll} m_3 \oplus m_{13} \oplus k_{19} \oplus (c_0 \oplus k_{32}) = 1 \\ m_1 \oplus m_{12} \oplus m_{15} \oplus k_{17} \oplus (c_1 \oplus k_{33}) = 1 \\ m_0 \oplus m_{14} \oplus k_{16} \oplus (c_2 \oplus k_{34}) = 0 \\ m_2 \oplus m_3 \oplus m_{12} \oplus k_{18} \oplus k_{19} \oplus (c_3 \oplus k_{35}) = 1 \end{array} \qquad (19)$$

To extract new equations, we should combine above 48 equations so that, the m_i of each equations in (19), correspond to one nibble. The probability of 48 resultant equations (relation (20)) will be equal to $2(0.75)^2 - 2(0.75) + 1 = 0.625$.

As described prior, it is possible to extract 32 independent equations from 48 equations with probability equal to 0.625. These final 32 equations are:

As described above, Eve now takes the known plaintetxts and corresponding ciphertexts and evaluates the left-hand side of each of the 32 equations. The main question it that, how many texts is needed for Eve to break the cipher?

Let, Eve wants to be 95% certain that all 32 key bit choices are correct. For *i*=1,…,32, let $\hat{p}_i = 0.5625$ denote the random variable whose value is equal to the proportion of the *n* plaintexts and corresponding ciphertexts for which the left-hand side of equation *i* is equal to the correct value (0 or 1) of the right-hand side, for the given key. For each *i*, the expected value of $\hat{p}_i$ is 0.5625 and its variance is $\frac{0.5625(1-0.5625)}{n}$. Therefore the standard deviation of $\hat{p}_i$ is $\sqrt{\frac{0.5625(1-0.5625)}{n}}$.

It is desired that $prob(\hat{p}_i > 0.5) = \sqrt[32]{0.95} = 0.998398$. For sufficiently large *n*, the random variable $\hat{p}_i$ is essentially normal. So it is possible that, standardize $\hat{p}_i$ by subtracting off its expected value and dividing by its standard deviation, which will give (approximately) the standard normal random variable denoted as Z.

$$prob(\frac{\hat{p}_i - 0.5625}{\sqrt{\frac{0.5625(1-0.5625)}{n}}} > \frac{0.5 - 0.5625}{\sqrt{\frac{0.5625(1-0.5625)}{n}}}) = 0.9984$$

$$\Rightarrow prob(\frac{\hat{p}_i - 0.5625}{\frac{0.496078}{\sqrt{n}}} > \frac{0.5 - 0.5625}{\frac{0.496078}{\sqrt{n}}}) = 0.998398 \qquad (21)$$

$$
\begin{aligned}
p_3 \oplus c_0 \oplus c_{13} &= k_3 \oplus k_{13} \oplus k_{19} \oplus k_{32} \oplus k_{37} \\
p_0 \oplus p_1 \oplus c_0 \oplus c_{13} &= k_0 \oplus k_1 \oplus k_{13} \oplus k_{19} \oplus k_{32} \oplus k_{37} \\
p_3 \oplus c_0 \oplus c_{12} \oplus c_{15} &= k_3 \oplus k_{12} \oplus k_{15} \oplus k_{19} \oplus k_{20} \oplus k_{21} \oplus k_{23} \oplus k_{32} \oplus k_{36} \oplus k_{39} \\
p_{13} \oplus c_0 \oplus c_{14} \oplus c_{15} &= k_{13} \oplus k_{14} \oplus k_{15} \oplus k_{16} \oplus k_{17} \oplus k_{23} \oplus k_{32} \oplus k_{38} \oplus k_{39} \\
p_{13} \oplus c_0 \oplus c_{13} \oplus c_{15} &= k_{15} \oplus k_{16} \oplus k_{17} \oplus k_{21} \oplus k_{22} \oplus k_{23} \oplus k_{32} \oplus k_{37} \oplus k_{39} \\
p_{15} \oplus c_1 \oplus c_{12} &= k_{12} \oplus k_{15} \oplus k_{17} \oplus k_{20} \oplus k_{23} \oplus k_{33} \oplus k_{36} \\
p_{12} \oplus p_{13} \oplus c_1 \oplus c_{12} &= k_{13} \oplus k_{17} \oplus k_{20} \oplus k_{23} \oplus k_{33} \oplus k_{36} \\
p_2 \oplus c_1 \oplus c_{15} \oplus 1 &= k_2 \oplus k_{15} \oplus k_{16} \oplus k_{17} \oplus k_{18} \oplus k_{19} \oplus k_{22} \oplus k_{33} \oplus k_{39} \\
p_{14} \oplus p_{15} \oplus c_0 \oplus c_1 \oplus c_{15} \oplus 1 &= k_{14} \oplus k_{16} \oplus k_{22} \oplus k_{32} \oplus k_{33} \oplus k_{39} \\
p_1 \oplus c_0 \oplus c_1 \oplus c_{13} \oplus c_{14} \oplus c_{15} &= k_1 \oplus k_{14} \oplus k_{15} \oplus k_{16} \oplus k_{23} \oplus k_{32} \oplus k_{33} \oplus k_{38} \oplus k_{39} \\
p_0 \oplus p_1 \oplus p_2 \oplus p_3 \oplus c_0 \oplus c_1 \oplus c_{14} \oplus c_{15} &= k_0 \oplus k_1 \oplus k_2 \oplus k_3 \oplus k_{14} \oplus k_{15} \oplus k_{16} \oplus k_{23} \oplus k_{32} \oplus k_{33} \oplus k_{38} \oplus k_{39} \\
p_1 \oplus c_0 \oplus c_1 \oplus c_{13} \oplus c_{15} &= k_1 \oplus k_{13} \oplus k_{15} \oplus k_{21} \oplus k_{22} \oplus k_{23} \oplus k_{32} \oplus k_{33} \oplus k_{37} \oplus k_{39} \\
p_1 \oplus c_2 \oplus c_{14} \oplus c_{15} \oplus 1 &= k_1 \oplus k_{14} \oplus k_{15} \oplus k_{16} \oplus k_{23} \oplus k_{34} \oplus k_{38} \oplus k_{39} \\
p_1 \oplus c_2 \oplus c_{13} \oplus c_{15} \oplus 1 &= k_1 \oplus k_{13} \oplus k_{15} \oplus k_{16} \oplus k_{21} \oplus k_{22} \oplus k_{23} \oplus k_{34} \oplus k_{37} \oplus k_{39} \\
p_{12} \oplus p_{13} \oplus c_3 \oplus c_{13} &= k_{12} \oplus k_{18} \oplus k_{19} \oplus k_{20} \oplus k_{22} \oplus k_{23} \oplus k_{35} \oplus k_{37} \\
p_2 \oplus p_3 \oplus c_3 \oplus c_{12} \oplus c_{13} \oplus 1 &= k_2 \oplus k_3 \oplus k_{12} \oplus k_{13} \oplus k_{18} \oplus k_{19} \oplus k_{21} \oplus k_{35} \oplus k_{36} \oplus k_{37} \\
p_2 \oplus p_3 \oplus c_3 \oplus c_{14} &= k_2 \oplus k_3 \oplus k_{14} \oplus k_{18} \oplus k_{19} \oplus k_{20} \oplus k_{22} \oplus k_{35} \oplus k_{38} \\
p_1 \oplus c_2 \oplus c_3 \oplus c_{12} &= k_1 \oplus k_{12} \oplus k_{18} \oplus k_{21} \oplus k_{34} \oplus k_{35} \oplus k_{36} \\
p_{13} \oplus c_2 \oplus c_3 \oplus c_{12} \oplus c_{13} &= k_{12} \oplus k_{18} \oplus k_{21} \oplus k_{34} \oplus k_{35} \oplus k_{36} \oplus k_{37} \\
p_{12} \oplus p_{13} \oplus p_{14} \oplus p_{15} \oplus c_2 \oplus c_3 \oplus c_{12} \oplus c_{13} &= k_{14} \oplus k_{15} \oplus k_{18} \oplus k_{21} \oplus k_{34} \oplus k_{35} \oplus k_{36} \oplus k_{37} \\
p_{13} \oplus c_2 \oplus c_3 \oplus c_{14} \oplus 1 &= k_{13} \oplus k_{14} \oplus k_{18} \oplus k_{20} \oplus k_{22} \oplus k_{34} \oplus k_{35} \oplus k_{38} \\
p_1 \oplus c_2 \oplus c_3 \oplus c_{13} \oplus c_{14} \oplus c_{15} &= k_1 \oplus k_{13} \oplus k_{14} \oplus k_{15} \oplus k_{18} \oplus k_{20} \oplus k_{22} \oplus k_{23} \oplus k_{34} \oplus k_{35} \oplus k_{37} \oplus k_{38} \oplus k_{39} \\
p_1 \oplus c_1 \oplus c_3 \oplus c_{12} &= k_1 \oplus k_{12} \oplus k_{18} \oplus k_{21} \oplus k_{33} \oplus k_{35} \oplus k_{36} \\
p_{13} \oplus c_1 \oplus c_3 \oplus c_{12} \oplus c_{13} &= k_{12} \oplus k_{18} \oplus k_{21} \oplus k_{33} \oplus k_{35} \oplus k_{36} \oplus k_{37} \\
p_{11} \oplus c_5 \oplus c_8 &= k_8 \oplus k_{13} \oplus k_{16} \oplus k_{19} \oplus k_{21} \oplus k_{32} \oplus k_{37} \qquad (20) \\
p_8 \oplus p_9 \oplus c_5 \oplus c_8 &= k_9 \oplus k_{11} \oplus k_{13} \oplus k_{16} \oplus k_{19} \oplus k_{21} \oplus k_{32} \oplus k_{37} \\
p_5 \oplus c_6 \oplus c_7 \oplus c_8 &= k_5 \oplus k_9 \oplus k_{14} \oplus k_{15} \oplus k_{22} \oplus k_{32} \oplus k_{38} \oplus k_{39} \\
p_7 \oplus c_4 \oplus c_9 &= k_7 \oplus k_{15} \oplus k_{23} \oplus k_{33} \oplus k_{36} \\
p_4 \oplus p_5 \oplus c_4 \oplus c_9 &= k_4 \oplus k_5 \oplus k_{15} \oplus k_{23} \oplus k_{33} \oplus k_{36} \\
p_8 \oplus p_9 \oplus c_7 \oplus c_9 &= k_9 \oplus k_{10} \oplus k_{11} \oplus k_{14} \oplus k_{15} \oplus k_{16} \oplus k_{18} \oplus k_{19} \oplus k_{22} \oplus k_{23} \oplus k_{33} \oplus k_{39} \\
p_6 \oplus p_7 \oplus c_7 \oplus c_8 \oplus c_9 \oplus 1 &= k_6 \oplus k_7 \oplus k_9 \oplus k_{14} \oplus k_{15} \oplus k_{17} \oplus k_{22} \oplus k_{23} \oplus k_{32} \oplus k_{33} \oplus k_{39} \\
p_6 \oplus p_7 \oplus c_7 \oplus c_{10} &= k_6 \oplus k_7 \oplus k_8 \oplus k_{10} \oplus k_{14} \oplus k_{15} \oplus k_{16} \oplus k_{18} \oplus k_{22} \oplus k_{23} \oplus k_{34} \oplus k_{39}
\end{aligned}
$$

Then :

$$
\begin{aligned}
&p(Z > -0.125988\sqrt{n}) = 0.998398 \\
&p(Z < -0.125988\sqrt{n}) = 1 - 0.998398 = 0.001602 \qquad (22) \\
&p(Z > 0.125988\sqrt{n}) = Q(0.125988\sqrt{n}) = 0.001602
\end{aligned}
$$

By using standard Z-function table:

$$n = 547.3138$$

Then 548 plaintexts are needed for broken the cipher. If none of the keys works, she can get more plaintexts and corresponding ciphertexts.

Thus this linear cryptanalytic attack seems very attractive compared to a pure brute force attack for second round SAES. However when added rounds (for real AES), more addition of equations is needed in order to elimination unknown parameters. In this situation, intermediary bits and the probabilities associated to the equations then tend toward 0.5, is needed (as seen above the probability go from 0.75 to 0.5625). The result is that, many more plaintexts and corresponding ciphertexts is needed in order to be fairly certain of picking the correct bit values for the $\sum_{l \in S} k_l$'s.

6. Conclusion

The linear attack was developed on full rounds SAES, in this paper. Using this linear cryptanalysis results, was shown that the first and second round SAES is breakable with linear calculations. So, we showed that this algorithm is vulnerable against linear attack. This, as a consequence, can be led to design a better cryptanalytic attack on real AES.

References

[1] Daemen, J. and V. Rijmen, "The design of Rijndael: AES – The Advanced Encryption Standard", Springer-Verlog, Berlin, 2002.

[2] Mohammad A. Musa , Edward F.Schaefer and Stephen Wedig in paper "A Simplified AES Algorithm and its Linear and Differential Cryptanalysis" , cryptologia, vol. 27, No. 2, pp. 148-177, 2003.

[3] S. Davood Mansoori, H. Khaleghi Bizaki, "Linear Cryptanalysis on Second Round Simplified AES", the 8th International Conference on Advanced Communication Technology ICACT, February 2006, pp. 1210- 1214

[4] H Khaleghi, S. D. Mansoori, A. Falahati, "Linear Cryptanalysis on Second Round Mini AES", 2nd IEEE International Conference On Information Communication Technology ICTTA, April 2006

[5] Matsui, M., "Linear cryptanalysis method for DES cipher", in Advances in cryptography – Eurocrypt 1993, Springer-Verlog, Berlin, pp. 386-397.

[6] Keys. M. A, "Tutorial on Linear and Differential Cryptanalysis", cryptologia, vol. 26, pp. 189-221, 2002.

[7] Menezes, A.J. P.C. van Oorschot, P.C. and S.A. Vanstone, "Handbook of Applied Cryptography", 2001, CRC Press.

[8] Schaefer, E.F., "A simplified Data Encryption Standard algorithm", Cryptologia, vol. 10, 1996, pp. 77-84.

[9] Stalling, W., "The Advanced Encryption Standard", Cryptologia, vol. 26, 2002, pp. 165-188.

[10] Eli Biham.,"On Matsui's Linear Cryptanalaysis", Springer-Verlag, 1998, pp. 341-344.

S. Davod Mansoori received the B.S. and M.S. degrees in Applied Mathematics from Gilan University and Tehran University, Tehran, Iran, in 1997 and 2001, respectively. He is now a researcher in Malek Ashtar University. His research areas are Cryptography and Cryptanalysis systems.

H. Khaleghi Bizaki received the B.S. and M.S. degrees in Electrical Engineering from Malek Ashtar University of Technology (MUT), Tehran, Iran, in 1998 and 2001, respectively. He is now PhD candidate in Electrical Engineering (Communication systems) in Iran University of Science & Technology (IUST), Tehran, Iran, from 2003. From 2001 to 2004, he was assigned to work as a research fellow in the Department of Electrical Engineering in MUT. In 2004, he worked as a teaching assistant in the MUT, during his graduate study at IUST. From 2005 he started his PhD thesis on pre-coding over MIMO systems. His research areas are Information Theory, Channel Coding, MIMO Systems, Space Time Code,