MATH 314 Spring 2018 - Class Notes

04/05/2018

Scribe: Long Chen

SAES
plaintext
↓
Add RK_0
↓
Round One steps:
Substitute
Shift Rows
Mix Columns
Add RK_1
↓
Round Two Steps:
Substitute
Shift Rows
Add RK_2
↓
Cipher text

Sbox
take in 4 bits
outputs 4 bits
input (b_0, b_1, b_2, b_3)
$b_0X^3 + b_1x^2 + b_2X + b_3 \in \mathbb{F}_{16}(moduloX^4 + x + 1)$
take inverse
$F^{-1}(x) = C_0x^3 + C_1X^2 + C_2X + C_3$
↓
(C_0, C_1, C_2, C_3)
Now multiply on the left by the matrix
Output:

$$\begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} d_0 \\ d_1 \\ d_2 \\ d_3 \end{pmatrix}$$

Compute Sbox output
for $1001 = 1x^3 + 0x^2 + 0x + 1$
we get $x^3 + 1 \in \mathbb{F}_{16}$
Invert this using Euclid's Algorithm

$(x^4+x+1)/(x^3+1) = x$ **R1**
$(x^4+x+1) = x(x^3+1)+1$
$(x^4+x+1)+x(x^3+1) = 1$
$(x^3+1)^{-1} \equiv x(mod x^4+x+1)$
↓
Now multiply by matrix

$$\begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

output 0010

SAES S-Box

N/A	**00**	**01**	**10**	**11**
00	**1001**	**0100**	**1010**	**1011**
01	**1101**	**0001**	**1000**	**0101**
10	**0110**	**0010**	**0000**	**0011**
11	**1100**	**1110**	**1111**	**1011**

key expansion
(How to get round keys)
$k_0 = k(masterkey)$
Break this into two words w_0, w_1
$\mathbf{w}_2 = g(w_1) \oplus w_0$
$w_3 = w_2 \oplus w_1$
$w_4 = g(w_3) \oplus w_2$
$w_5 = w_4 \oplus w_3$
$k_1 = w_2 w_3$
$\mathbf{k}_2 = w_4 w_5$

SAES g function

- **First, separate a plain text to N_0 and N_1, two different parts.**
- **Then, stwitch N_0 and N_1, and send them to the S-box.**
- **Calculate and get the result from $X^{i+1} = (mod x^4+x+1)$, where $i = 1$ for W_1 and $i = 2$ for W_2, then multiply with N_1 after the oringal one came out of the S-box.**

- **N_0 stay the same after it came out of the S-box, and we combine new N_1 and N_0 to get a piece for a new output.**
- **The iteration will continues depends on the number of repeatation it was asked.**

here are some description of the terms in steps in SAES.
First we will have a plain text, and at least two keys for at least one round. Then we XOR the plain text and the first key K_0, M_1

Substitute
put M_1 to S-box to obtain a new M_1

Shift Row
shift left row with right row(below is just an example)
$$\begin{pmatrix} 1100 & 1100 \\ 1110 & 1111 \end{pmatrix}\begin{pmatrix} 1100 & 1100 \\ 1111 & 1110 \end{pmatrix}$$

Mix Column
Convert M_1 to a two by two matix(below is just an example)
$$\begin{pmatrix} 1100 & 1100 \\ 1111 & 1110 \end{pmatrix} \rightarrow \begin{pmatrix} X^3+X^2 & X^3+X^2 \\ X^3+X^2+X+1 & X^3+X^2+X \end{pmatrix}$$
encryption matrix multiply the M_1 matrix
$$\begin{pmatrix} 1 & X^2 \\ X^2 & 1 \end{pmatrix} \mathbf{x} \begin{pmatrix} X^3+X^2 & X^3+X^2 \\ X^3+X^2+X+1 & X^3+X^2+X \end{pmatrix} =$$
$$\begin{pmatrix} X^5+X^4 & X^5+X^4+X^3 \\ X^5+X^4+X^3+X^2+X+1 & X^5+X^4+X^3+X^2+X \end{pmatrix}$$
then reduce mod to X^4+X+1
$$\begin{pmatrix} X^2+1 & 1 \\ X^3+X & X^3+X+1 \end{pmatrix}$$
convert the two by two matrix back to binary numbers
0101000110101011

Add Round Key
Add the second key K_1 to complete the first round of the SAES

And here you can obtain the cipher text after first round.
To perform n rounds of the SAES, you just need $n-1$ numbers of keys to complete the process above for $n-1$ times, and that's it!