MATH 314 Spring 2018 - Class Notes

3/7/18

Scribe: Ethan Allen

Summary: This lesson began by going over how the SAES S-box values are created. We then go over the main points of SAES. Finally, we go through a detailed example of encrypting a plaintext using SAES.

How S-Box Values Are Created:

To find the S-box value for 1001:

Convert to $\mathbb{F}_{16}$ to get $x^3 + 1$ and find the inverse. (use Euclid's Algorithm)

$$\begin{array}{r|l} & \quad x \qquad \text{R1} \\ \hline x^3+1 & x^4 + x + 1 \\ & -x^4 - x \\ \hline \end{array}$$

so

$x^4 + x + 1 = x(x^3 + 1) + 1$
$(x^4 + x + 1) + (x(x^3 + 1))$
$(x^3 + 1)^{-1} = x(mod x^4 + x + 1)$

$x \to 0010$

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

XOR with 1001 (starting value)

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

0010 is the output

SAES S-box Values

	00	01	10	11
00	1001	0100	1010	1011
01	1101	0001	1000	0101
10	0110	0010	0000	0011
11	1100	1110	1111	0111

First column corresponds to the first two bits. First row corresponds to the last two bits.

Key Expansion for SAES

$K_0 = Masterkey$

Break K_0 into two 8-bit words: W_0, W_1

$W_2 = g(W_1) \oplus W_0$
$W_3 = W_2 \oplus W_1$
$W_4 = g(W_3) \oplus W_2$
$W_5 = W_4 \oplus W_3$

Here is the g-function:

- First, split the word into two "Nibbles", N_0 and N_1
- Next, switch the positions of N_0 and N_1
- Send N_0 and N_1 through the S-box
- XOR the N_1 S-box output with the resulting bits you get from calculating $x^{i+2}(mod x^4 + x + 1)$ where i is 1 for W_2 and 2 for W_4. The result is $N_0^{'}$
- N_0 stays the same and is now called $N_1^{'}$
- Combine $N_0^{'}$ and $N_1^{'}$ for the output

SAES Overview

Recall the SAES overview graphic from last class. We will now go into more detail about the various key operations.

<u>Add Round Key:</u>
XOR with round key

<u>Substitute:</u>
Break into 4 nibbles and convert each using S-box

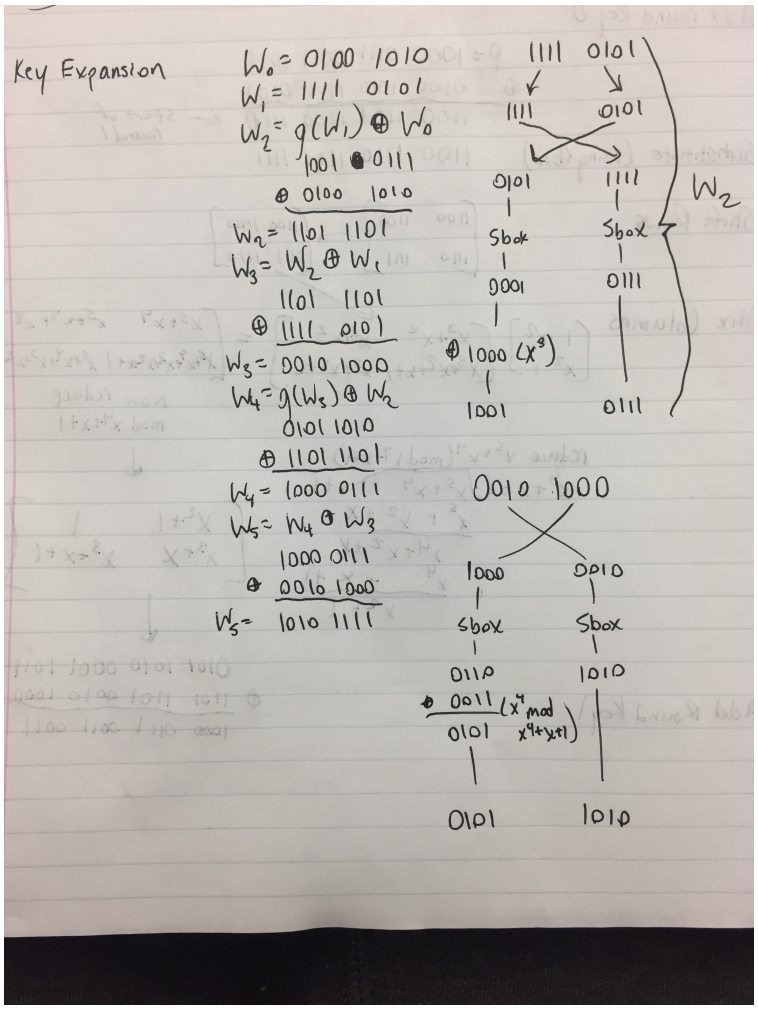
<u>Shift Rows:</u>
Break the 16 bits into nibbles (4 bits each). Write these as a 2x2 matrix, filling in columns first. Swap entries in 2nd row

<u>Shift Rows:</u>
Convert nibbles to $\mathbb{F}_{16}$ (call this M). Multiply this matrix on the left by the encryption matrix (E): $\begin{bmatrix} 1 & x^2 \\ x^2 & 1 \end{bmatrix}$ and we get $E \times M$. Convert back to a 16-bit string, reading columns first.

SAES Example

Encrypt the plaintext P = 1000 0111 0011 1011
Using the key K = 0100 1010 1111 0101

First, we need to determine the three keys: k_0, k_1, and k_2 using the Key Expansion function.



$k_0 = W_0 + W_1 = 0100\ 1010\ 1111\ 0101$
$k_1 = W_2 + W_3 = 1101\ 1101\ 0010\ 1000$
$k_2 = W_4 + W_5 = 1000\ 0111\ 1010\ 1111$

Now that we have our round keys, we can begin by adding k_0 to our plaintext, P

$$\begin{array}{c} 1000\ 0111\ 0011\ 1011 \\ \underline{0100\ 1010\ 1111\ 0101\ \oplus} \\ 1100\ 1101\ 1100\ 1110 \end{array}$$

Substitute (using S-box)

$$1100\ 1110\ 1100\ 1111$$

Shift Rows

$$\begin{bmatrix} 1100 & 1100 \\ 1110 & 1111 \end{bmatrix} \rightarrow \begin{bmatrix} 1100 & 1100 \\ 1111 & 1110 \end{bmatrix}$$

Mix Columns

$$\begin{bmatrix} 1100 & 1100 \\ 1111 & 1110 \end{bmatrix} \rightarrow \begin{bmatrix} x^3+x^2 & x^3+x^2 \\ x^3+x^2+x+1 & x^3+x^2+x \end{bmatrix}$$

left-multiply by encryption matrix

$$\begin{bmatrix} 1 & x^2 \\ x^2 & 1 \end{bmatrix} \times \begin{bmatrix} x^3+x^2 & x^3+x^2 \\ x^3+x^2+x+1 & x^3+x^2+x \end{bmatrix} =$$

$$\begin{bmatrix} x^5+x^4 & x^5+x^4+x^3 \\ x^5+x^4+x^3+x^2+x+1 & x^5+x^4+x^3+x^2+x \end{bmatrix}$$

now reduce $mod x^4+x+1$

$$\begin{array}{r|l} & x+1 \\ \hline x^4+x+1 & x^5+x^4 \\ & -x^5 \quad -x^2 \quad -x \\ \hline & x^4-x^2 \quad -x \\ & -x^4 \quad -x-1 \\ \hline & -x^2-2x-1 \end{array}$$

$$\begin{bmatrix} x^2+1 & 1 \\ x^3+x & x^3+x+1 \end{bmatrix}$$

now write it back as bits

$$0101\ 1010\ 0001\ 1011$$

Add k_1

$$\begin{array}{c} 0101\ 1010\ 0001\ 1011 \\ \underline{1101\ 1101\ 0010\ 1000\ \oplus} \\ 1000\ 0111\ 0011\ 0011 \end{array}$$

Substitute

$$0110\ 0101\ 1011\ 1011$$

Shift Rows

$$\begin{bmatrix} 0110 & 1011 \\ 0101 & 1011 \end{bmatrix} \rightarrow \begin{bmatrix} 0110 & 1011 \\ 1011 & 0101 \end{bmatrix} \rightarrow 0110101110110101$$

Add k_2

$$\begin{array}{c} 0110\ 1011\ 1011\ 0101 \\ \underline{1000\ 0111\ 1010\ 1111\ \oplus} \\ 1110\ 1100\ 0001\ 1010 \\ \uparrow \\ \text{this is our ciphertext!} \end{array}$$