Class Note 4/6

Logan Smith

May 6, 2020

SAES Box 4 bits $\rightarrow$ 4 bits

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

Key expansion
$K_0 = W_0W_1$
$K_1 = W_1W_2$
$K_2 = W_2W_3$
$W_{2i} = gv(W_{2i-1}) \oplus W_{2i-1}$
$K_{2I+1} = W_0W_1$

SAES: 16 bit blocksize
16 bit masterkey
2 rounds

4 steps:
1) add round key(ARK)
2)substitute(sub)
3) shift rows (SR)
4) mix columns (MC)
Skip mix columns in the last round

-add round key: xor current block with the round key -substitute: break into 4 nibbles, replace each nibble with its sbox
-shift rows: write our block as 4 nibbles, N_0, N_1, N_2, N_3, fill a 2 x 2 matrix
$\begin{pmatrix} N_0 & N_2 \\ N_1 & N_3 \end{pmatrix}$
shift to
$\begin{pmatrix} N_0 & N_2 \\ N_3 & N_1 \end{pmatrix}$

Mix column convert this matrix to entries of F_{16}

$N_0 = A_0A_1A_2A_3 \rightarrow A_0x^3 + A_1x^2 + A_2x + A_3$

Call this Matrix M(2x2 matrix in F_{16})

Compute EM where

E = $\begin{array}{|c|c|}\hline 1 & x^2 \\ \hline x^2 & 1 \\ \hline \end{array}$

convert to a string of 1s and 0s (read column first)

SAES EX. Masterkey: $K_0 = 0100101011110101 Plaintext : P = 1000011100111011$

Key Expansion $K_0 = W_0W_1$

$W_0 = 01001010$

$W_1 = 11110101$

$W_2 = g(W_1) \oplus W_0$

$g(W_1) = 10010111$

$W_2 = 11011101$

$W_3 = W_2W_1 = 00101000$

$W_4 = g(W_3) \oplus W_2$

$g(W_3) = 01011010$

$W_4 = 10000111$

$W_5 = W_4 \oplus W_3 = 10101111$

$K_1 = W_2W_3 = 1101110100101000$

$K_2 = W_4W_5 = 1000011110101111$

$Pk_0 = 1100110111001110$

sbox substitute to: 1100 1110 1100 1111

shift rows: $\begin{array}{|c|c|}\hline 1100 & 1100 \\ \hline 1110 & 1111 \\ \hline \end{array}$

$\rightarrow \begin{array}{|c|c|}\hline 1100 & 1100 \\ \hline 1111 & 1110 \\ \hline \end{array}$

$\begin{array}{|c|c|}\hline x^3 + x^2 & x^3 + x^2 \\ \hline x^3 + x^2 + x + 1 & x^3 + x^2 + x \\ \hline \end{array}$

Compute EM

EM= $\begin{array}{|c|c|}\hline x^2 + 1 & 1 \\ \hline x^3 + x & x^3 + x^2 + 1 \\ \hline \end{array}$

= $\begin{array}{|c|c|}\hline 0101 & 0001 \\ \hline 1010 & 1011 \\ \hline \end{array}$

EM=0101 1010 0001 1011

$\oplus K_1 = 1001011100110011$

Round 2:

subsitution : 0110 0101 1011 1011

Shift rows: 0110 1011 1011 0101

$\oplus K_2 : 1110110000011010 = C$