# MATH 314 Fall 2024 - Class Notes

10/1/2024

Scribe: James Knuth

**Summary:** We continue the Simplified AES encryption that we started on September 26, and complete a worksheet with another SAES encryption.

The plaintext and key expansions from the example started on September 26:

$P =$ 1011 1001 1110 0000
$K_0 =$ 1001 1111 0101 1000
$K_1 =$ 0111 1110 0010 0110
$K_2 =$ 1100 0100 1110 0010

Round 0 - Add the key $K_0$ to the plaintext.

$P \oplus K_0 =$ 0010 0110 1011 1000

Run the result through the S-Box to get the below:

$\equiv$ 1010 1000 0011 0110

This converts to the polynomial matrix below:

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

Shift Rows, for SAES the bottom row swaps places:

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

Mix Columns:

$$E * M = \begin{bmatrix} 1 & x^2 \\ x^2 & 1 \end{bmatrix} * \begin{bmatrix} x^3+x & x+1 \\ x^2+x & x^3 \end{bmatrix} \equiv \begin{bmatrix} 1(x^3+x)+(x^4+x^3) & 1(x+1)+(x^5) \\ (x^5+x^3)+(x^2+x) & (x^3+x^2)+1(x^3) \end{bmatrix}$$

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

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

Add Round Key $K_1$:

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

$$\equiv \begin{bmatrix} x^2+x & x^2+x+1 \\ x^2+x & x \end{bmatrix} \pmod{x^4+x+1}$$

This is the end of Round 1. Optionally, temporarily convert to a binary matrix. This may help with the start of the next round.

$$\equiv \begin{bmatrix} 0110 & 0111 \\ 0110 & 0010 \end{bmatrix}$$

Start Round 2

Run the result through the S-Box to get the below, as a polynomial matrix:

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

Shift Rows, for SAES the bottom row swaps places:

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

Add Round Key 2:

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

Convert this back to a binary matrix and then into a single line.

Final Ciphertext: 0100 1110 1011 1010

For additional review, do the Worksheet provided in class.