MATH 178 Homework #7

Tamir Enkhjargal

April 2019

AES

2.

Verify, in Simplified AES that SBOX(1100) = 1100. Our system works in $\mathbb{F}_{16} = \mathbb{F}_2[x]/(x^4 + x + 1)$

$$
\begin{align}
(\underline{x^4 + x + 1}) &= (x+1)(\underline{x^3 + x^2}) + (\underline{x^2 + x + 1}) \tag{1}\\
(\underline{x^3 + x^2}) &= (x)(\underline{x^2 + x + 1}) + (\underline{x}) \tag{2}\\
(\underline{x^2 + x + 1}) &= (x+1)(\underline{x}) + (\underline{1}) \tag{3}
\end{align}
$$

$$
\begin{align}
(\underline{1}) &= (\underline{x^2 + x + 1}) + (x+1)(\underline{x}) \tag{4}\\
(\underline{1}) &= (\underline{x^2 + x + 1}) + (x+1)[(\underline{x^3 + x^2}) + (x)(\underline{x^2 + x + 1})] \tag{5}\\
(\underline{1}) &= (\underline{x^2 + x + 1}) + (x+1)(\underline{x^3 + x^2}) + (x+1)(x)(\underline{x^2 + x + 1}) \tag{6}\\
(\underline{1}) &= (x+1)(\underline{x^3 + x^2}) + (x^2 + x + 1)(\underline{x^2 + x + 1}) \tag{7}\\
(\underline{1}) &= (x+1)(\underline{x^3 + x^2}) + (x^2 + x + 1)[(\underline{0}) + (x+1)(\underline{x^3 + x^2})] \tag{8}\\
(\underline{1}) &= (x+1)(\underline{x^3 + x^2}) + (x^2 + x + 1)(x+1)(\underline{x^3 + x^2}) \tag{9}\\
(\underline{1}) &= (x+1)(\underline{x^3 + x^2}) + (x^3 + 1)(\underline{x^3 + x^2}) \tag{10}\\
(\underline{1}) &= (\underline{x^3 + x^2})[(x+1) + (x^3 + 1)] \tag{11}\\
(\underline{1}) &= (\underline{x^3 + x^2})(x^3 + x) \tag{12}
\end{align}
$$

$$
(x^3 + x^2)^{-1} = (x^3 + x) = 1010 \tag{13}
$$

Now working in $\mathbb{F}_2[y]/(y^4 + 1)$

$$
\begin{align}
N(y) \cdot a(y) + b(y) &= (y^3 + y)(y^3 + y^2 + 1) + (y^3 + 1) \tag{1}\\
&= y^6 + y^5 + y^3 + y^4 + y^3 + y + y^3 + 1 \tag{2}\\
&= y^2 + y + 1 + y^3 + y + 1 \tag{3}\\
&= y^3 + y^3 = 1100 \tag{4}
\end{align}
$$

We end up after SBOX(1100) = 1100

3.

Working in mod (z^2+1) and (x^4+x+1).

$= ((a*x^3+b*x^2+c*x+d)*z+(e*x^3+f*x^2+g*x+h))*(x*z+x^3+1)$
$= ax^6z+ax^4z^2+ax^3z+bx^5z+bx^3z^2+bx^2z+cx^4z+cx^2z^2+cxz+dx^3z+dxz^2+$
$dz+ex^6+ex^4z+ex^3+fx^5+fx^3z+fx^2+gx^4+gx^2z+gx+hx^3+hxz+h$
$= a(x^3+x^2)z+a(x+1)+ax^3z+b(x^2+x)z+bx^3+bx^2z+c(x+1)z+cx^2+cxz+dx^3z+dxz^2+$
$dz+e(x^3+x^2)+e(x+1)z+ex^3+f(x^2+x)+fx^3z+fx^2+g(x+1)+gx^2z+gx+hx^3+hxz+h$
$= ax^3z+ax^2z+ax+a+ax^3z+bx^2z+bxz+bx^3+bx^2z+cxz+cz+cx^2+cxz+dx^3z+dxz^2+$
$dz+ex^3+ex^2+exz+ez+ex^3+fx^2+fx+fx^3z+fx^2+gx+g+gx^2z+gx+hx^3+hxz+h$
$= ax^3z+ax^3z+bx^3+dx^3z+ex^3+ex^3+fx^3z+hx^3+ax^2z+bx^2z+bx^2z+cx^2+ex^2+fx^2+$
$fx^2+gx^2z+ax+bxz+cxz+cxz+dx+exz+fx+gx+gx+hxz+a+cz+dz+ez+g+h$
$= dx^3z+fx^3z+bx^3+hx^3+ax^2z+bx^2z+gx^2z+cx^2+ex^2+$
$bxz+exz+hxz+ax+dx+fx+cz+dz+ez+a+g+h$

d⊕f	a⊕b⊕g	b⊕e⊕h	c⊕d⊕e
b⊕h	c⊕e	a⊕d⊕f	a⊕g⊕h

=

$b_3 \oplus b_5$	$b_0 \oplus b_1 \oplus b_6$	$b_1 \oplus b_4 \oplus b_7$	$b_2 \oplus b_3 \oplus b_4$
$b_1 \oplus b_7$	$b_2 \oplus b_4$	$b_0 \oplus b_3 \oplus b_5$	$b_0 \oplus b_6 \oplus b_7$

4.

Recall if i even, then $W[i] = W[i-2] \oplus RCON(i/2) \oplus Sub(Rot(W[i-1]))$ and then if i odd, then $W[i] = W[i-2] \oplus W[i-1]$.
$RCON(1) = 10000000$ and $RCON(2) = 00110000$

i)

$$
\begin{aligned}
W[0] &= 1011\ 1101 && (1)\\
W[1] &= 0010\ 0101 && (2)\\
W[2] &= W[0] \oplus RCON(1) \oplus Sub(Rot(W[1])) && (3)\\
Rot(W[1]) &= 0101\ 0010 && (4)\\
Sub(Rot(W[1])) &= 0001\ 1010 && (5)\\
W[2] &= 1011\ 1101 \oplus 1000\ 0000 \oplus 0001\ 1010 && (6)\\
W[2] &= 0010\ 0111 && (7)\\
W[3] &= W[1] \oplus W[2] && (8)\\
W[3] &= 0010\ 0101 \oplus 0010\ 0111 && (9)\\
W[3] &= 0000\ 0010 && (10)\\
W[4] &= W[2] \oplus RCON(2) \oplus Sub(Rot(W[3])) && (11)\\
Rot(W[3]) &= 0010\ 0000 && (12)\\
Sub(Rot(W[3])) &= 1010\ 1001 && (13)\\
W[4] &= 0010\ 0111 \oplus 0011\ 0000 \oplus 1010\ 1001 && (14)\\
W[4] &= 1011\ 1110 && (15)\\
W[5] &= W[3] \oplus W[4] && (16)\\
W[5] &= 0000\ 0010 \oplus 1011\ 1110 && (17)\\
W[5] &= 1011\ 1100 && (18)
\end{aligned}
$$

K_1=1011 1101 0010 0101
K_2=0010 0111 0000 0010
K_3=1011 1110 1011 1100
K=1011 1101 0010 0101 0010 0111 0000 0010 1011 1110 1011 1100