RIJNDAEL CIPHER (CONTINUED): DISCUSSION

MATH 195

First, we discuss the map M. Recall that we define the map

$$M : \mathbb{F}_{256}^4 \to \mathbb{F}_{256}^4$$
$$M(g) \equiv c \cdot g \pmod{Y^4 + 1}.$$

where we identify the word space $\mathbb{F}_{256}^4$ with the set of polynomials

$$\mathbb{F}_{256}^4 = \{g \in \mathbb{F}_{256}[Y] : \deg g < 4\}$$
$$(a_0, a_1, a_2, a_3) = a_0 + a_1 Y + a_2 Y^2 + a_3 Y^3.$$

Here we let $c \in \mathbb{F}_{256}^4$ be

$$c = (X, 1, 1, X+1) = X + Y + Y^2 + (X+1)Y^3,$$

where

$$\mathbb{F}_{256} = \mathbb{F}_2[X]/(X^8 + X^4 + X^3 + X + 1).$$

M has the desirable properties of efficiency and diffusion. Writing this map out, we have

$$c \cdot g \equiv \left(\sum_{i=0}^{3} c_i Y^i \right) \left(\sum_{j=0}^{3} a_j Y^j \right) \pmod{Y^4 + 1}$$

which is

$$\sum_{\ell=0}^{3} \left(\sum_{i+j \equiv \ell \bmod 4} c_i a_j \right) Y^\ell.$$

We want this multiplication to be efficient, so we want to pick the coefficients so that this multiplication is easy: hence we require that they (as polynomials in X) be linear. Then we have

$$X \left(\textstyle\sum_{i=0}^{7} b_i X^i \right) = \textstyle\sum_{i=0}^{7} b_i X^{i+1} = \sum_{j=1}^{7} b_{j-1} X^j + b_7 (X^4 + X^3 + X + 1).$$

Part of the secret of this choice of c, then, is that not only do the coefficients have low degree, but the sum of the coefficients is

$$X + 1 + 1 + (X+1) = 1.$$

It is a homework problem to investigate the consequences of this magical condition.

The diffusion requirement can be put as follows: if w and w' are two words differing in just one byte, then $M(w)$ and $M(w')$ differ in all four bytes. Similarly, if w and w' differ in two, three, or four bytes, respectively, then $M(w)$ and $M(w')$ differ in at least three, at least two, or at least one byte, respectively.

This is some of the material covered April 9, in Math 195: Cryptography, taught by Hendrik Lenstra, prepared by John Voight `jvoight@math.berkeley.edu`.

Definition. If w, w' are two words, then the *Hamming* distance $d(w, w')$ is the number of js such that the jth byte of w is not equal to the jth byte of w'.

The *Hamming weight* $W(w) = d(w, 0)$, i.e. $d(w, w') = W(w+w')$ (we are dealing with bytes). $W(w)$ is the number of nonzero bytes of w.

We see that $d(w, w'') \leq d(w, w') + d(w', w'')$, $d(w, w') = d(w', w)$, and $d(w, w') = 0$ if and only if $w = w'$. We require for Rijndael that for all $w \neq w'$,

$$d(w, w') + d(M(w), M(w')) \geq 5.$$

Equivalently, for all $v = w + w' \neq 0$, we insist that

$$W(w+w')+W(M(w)+M(w')) = W(w+w')+W(M(w+w')) = W(v)+W(M(v)) \geq 5.$$

Theorem. *Let*

$$c = c_0 + c_1 Y + c_2 Y^2 + c_3 Y^3 \in \left(\mathbb{F}_{256}[Y]/(Y^4+1)\right)^*$$

have inverse $d = d_0 + d_1 Y + d_2 Y^2 + d_3 Y^3$. *Define*

$$M : \left(\mathbb{F}_{256}[Y]/(Y^4+1)\right)^* \to \left(\mathbb{F}_{256}[Y]/(Y^4+1)\right)^*$$

by $M(g) = c \cdot g$. *Then* M *satisfies the condition*

$$W(v) + W(M(v)) \geq 5$$

for all $v \neq 0$ *if and only if the following conditions are satisfied:*

(i) *all* $c_i \neq 0$;
(ii) *the elements* $c_1/c_0,\ c_2/c_1,\ c_3/c_2,\ c_0/c_3$ *of* $\mathbb{F}_{256}$ *are pairwise distinct;*
(iii) *the elements* $c_2/c_0,\ c_3/c_1,\ c_0/c_2,\ c_1/c_3$ *of* $\mathbb{F}_{256}$ *are pairwise distinct;*
(iv) *the same conditions are true for* c_j *replaced by* d_j.

This theorem is not deep. It imposes certain limitations on your coefficients which are satisfied by the Rijndael cipher!