Cryptography

PROF. DR. JOACHIM VON ZUR GATHEN, JÉRÉMIE DETREY

2. Assignment: Finite fields in AES

(Hand in solutions on Thursday, November 22nd during the lecture)

Exercise 2.1 (Dissecting `MixColumns`). (10 points)

The `MixColumns` step in AES is quite complex, as it manipulates polynomials whose coefficients are also polynomials. The purpose of this exercise is to demystify all this messing around with finite fields.

First, we consider the finite field $\mathbb{F}_{2^8}$, defined as $\mathbb{F}_2[x]/(M(x))$. More precisely, it is the field of polynomials over $\mathbb{F}_2 = \{0, 1\}$ (which you also know as $\mathbb{Z}_2$) modulo $M(x)$, where $M(x)$ is the following degree-8 polynomial, irreducible over $\mathbb{F}_2$:

$$M(x) = x^8 + x^4 + x^3 + x + 1.$$

Each element of $\mathbb{F}_{2^8}$ is a polynomial of degree 7, each of its coefficient being either 0 or 1. We use hexadecimal notation to represent the 8 coefficients of such polynomials as a single byte. Given

$$P(x) = \sum_{i=0}^{7} p_i x^i,$$

we will write P as $p_7p_6p_5p_4p_3p_2p_1p_0$ in binary, and then take the hexadecimal representation of this number.

For instance, $P(x) = x^7 + x^5 + x^4 + x^2 + x + 1$ will be represented in hexadecimal as the byte `'B7'`, as its binary expression is 10110111, which corresponds to the coefficients of P, highest-degrees first, reading from left to right.

We now consider a column in the state of an AES round. We note its four bytes as A_0, A_1, A_2 and A_3. All of them can be actually seen as elements of $\mathbb{F}_{2^8}$. We can even write the polynomial $A_3X^3 + A_2X^2 + A_1X + A_0$, which is simply an element of the ring of polynomials over $\mathbb{F}_{2^8}$, namely $\mathbb{F}_{2^8}[X]$ (note that here we have polynomials in the variable X, which is different from the variable x).

This is exactly the same as the ring of polynomials over integers, except that the operations on the coefficients are not integer operations, but operations

over $\mathbb{F}_{2^8}$. Hence, addition of two elements of $\mathbb{F}_{2^8}[X]$ is simply pair-wise addition of the coefficients, and since the coefficents are in $\mathbb{F}_{2^8}$, the additions are computed over this field as the sums of two binary polynomials of degree at most 7.

As far as multiplications are concerned, in order to keep the degree of the product of two polynomials bounded, we consider everything modulo the polynomial $N(X) = \texttt{'01'}X^4 + \texttt{'01'} = X^4 + 1$ (since `'01'` is the constant polynomial 1 in $\mathbb{F}_{2^8}$). The ring over which the `MixColumn` operation is defined is then

$$\mathbb{F}_{2^8}[X]/(N(X)).$$

The `MixColumns` is then defined as follows: given a column $A = A_3X^3 + A_2X^2 + A_1X + A_0 \in \mathbb{F}_{2^8}[X]/(N(X))$, we compute $\texttt{MixColumn}(A)$ as the product

$$\texttt{MixColumn}(A) = \left(\texttt{'03'}X^3 + \texttt{'01'}X^2 + \texttt{'01'}X + \texttt{'02'}\right) \cdot A.$$

Note that the polynomial $C(X) = \texttt{'03'}X^3 + \texttt{'01'}X^2 + \texttt{'01'}X + \texttt{'02'}$ is also an element of $\mathbb{F}_{2^8}[X]/(N(X))$.

[1] (i) Is $\mathbb{F}_{2^8}[X]/(N(X))$ a field? Why?

[2] (ii) Expand the product of A by $\texttt{'03'}X^3 + \texttt{'01'}X^2 + \texttt{'01'}X + \texttt{'02'}$ over $\mathbb{F}_{2^8}[X]$ and reduce it modulo $N(X)$. Do not compute the products of the coefficients over $\mathbb{F}_{2^8}$ (leave them as $\texttt{'03'}A_3$ for instance).

[1] (iii) Look for a way to express this product as a 4 by 4 matrix $\mathcal{M}$ with coefficients in $\mathbb{F}_{2^8}$, so that we can write

$$\begin{bmatrix} B_0 \\ B_1 \\ B_2 \\ B_3 \end{bmatrix} = \mathcal{M} \cdot \begin{bmatrix} A_0 \\ A_1 \\ A_2 \\ A_3 \end{bmatrix},$$

where $B = B_3X^3 + B_2X^2 + B_1X + B_0 = \texttt{MixColumn}(A)$.

[1] (iv) What are the polynomial representations of `'01'`, `'02'` and `'03'`, all three being elements of $\mathbb{F}_{2^8}$?

[2] (v) Give the expression of the product of an element $P = \sum_{i=0}^{7} p_i x^i$ of $\mathbb{F}_{2^8}$ by `'01'`. Same question for `'02'` and `'03'`.

[2] (vi) Switching back to the representation of $P \in \mathbb{F}_{2^8}$ as a byte, give simple formulas or algorithms to easily compute $\texttt{'01'}P$, $\texttt{'02'}P$ and $\texttt{'03'}P$ as if you were to implement them using a typical imperative programming language such as C, C++, Java, ... For instance, such a formula for the sum of two elements P and Q of $\mathbb{F}_{2^8}$ is computed by P XOR Q.

1 (vii) Give a simple algorithm which performs the `MixColumn` operation on a given input column A.

Exercise 2.2 (Inverting `MixColumns`). (12 points)

We now want to look at the inverse transformation, namely `InvMixColumn`. As we want to be able to correctly decrypt any AES encrypted message, we require that, for every possible column A,

$$\texttt{InvMixColumn}(\texttt{MixColumn}(A)) = A.$$

As `MixColumn` is actually a multiplication over $\mathbb{F}_{2^8}[X]/(N(X))$, `InvMixColumn` should be a multiplication by the multiplicative inverse of $\texttt{'03'}X^3 + \texttt{'01'}X^2 + \texttt{'01'}X + \texttt{'02'} = C(X)$ over that same ring.

Computing the greatest common divisor of $N(X)$ and $C(X)$ using the usual Euclidean algorithm gives us:

i	u	v	$u \bmod v$
0	$N(X)$	$C(X)$	$\texttt{'A4'}X^2 + \texttt{'A5'}X + \texttt{'A5'}$
1	$C(X)$	$\texttt{'A4'}X^2 + \texttt{'A5'}X + \texttt{'A5'}$	$\texttt{'4F'}X + \texttt{'C5'}$
2	$\texttt{'A4'}X^2 + \texttt{'A5'}X + \texttt{'A5'}$	$\texttt{'4F'}X + \texttt{'C5'}$	$\texttt{'9A'}$
3	$\texttt{'4F'}X + \texttt{'C5'}$	$\texttt{'9A'}$	0
4	$\texttt{'9A'}$	0	–

Bézout's identity then tells us that there exist two polynomials $P(X)$ and $Q(X)$ in $\mathbb{F}_{2^8}[X]$ such that

$$P(X)N(X) + Q(X)C(X) = \texttt{'9A'}.$$

2 (i) Conclude that $C(X)$ has a multiplicative inverse over $\mathbb{F}_{2^8}[X]/(N(X))$. Explain how to compute this inverse, knowing $P(X)$ and $Q(X)$ from Bézout's identity.

We now have to compute the actual value of $D(X) = C(X)^{-1}$. For that, we will use the extended Euclidean algorithm over $\mathbb{F}_{2^8}[X]$. As this requires quite a lot of multiplications over $\mathbb{F}_{2^8}$, a JavaScript-enabled webpage has been set up to perform those multiplications for you. This page is accessible from the

lecture webpage[1], and you can download it to your own computer to use it even without Internet access.

The extended Euclidean algorithm over $\mathbb{F}_{2^8}[X]$ also requires inversions over $\mathbb{F}_{2^8}$, which will have to be computed using the extended Euclidean algorithm over $\mathbb{F}_2[x]$ this time. The JavaScript multiplication page will hopefully allow you to check your computations (multiplying a element of $\mathbb{F}_{2^8}$ and its inverse should give you `'01'`).

2 (ii) First of all, a simple inversion over $\mathbb{F}_{2^8}$: using the extended Euclidean algorithm over $\mathbb{F}_2[x]$, compute the multiplicative inverse of `'03'` modulo $M(x)$.

6 (iii) Using the extended Euclidean algorithm over $\mathbb{F}_{2^8}[X]$, compute $D(X) = C(X)^{-1}$.

1 (iv) Verify that you have $D(X) \cdot C(X) =$ `'01'`

1 (v) Give the expression of the `InvMixColumn` transformation.

[1] `http://cosec.bit.uni-bonn.de/students/teaching/2007ws/cryptography.html`