Crypto Engineering
Finite fields extensions

2021-09-22

Exercise 1: AES field

Most of the elementary operations used in the definition of the AES block cipher are defined over $\mathbb{F}_{2^8}$, represented as $\mathbb{F}_2[X]/\langle X^8 + X^4 + X^3 + X + 1\rangle$.

We define the following C function:

```
uint8_t xtime(uint8_t a)
{
        uint8_t m = a & 0x80 ? 0x1B : 0;

        return ((a << 1) ^ m);
}
```

Q.1: What does this function do?

Q.2: Write your own variant of `xtime` for a different representation of $\mathbb{F}_{2^8}$ (for instance using the polynomial $X^8 + X^6 + X^5 + X^4 + X^3 + X + 1$, which is irreducible over $\mathbb{F}_2[X]$).

Q.3: Write a multiplication function `mul8` that computes the product of two elements of $\mathbb{F}_{2^8}$ in the AES representation.

Exercise 2: Multiplication by a constant in $\mathbb{F}_{2^8}$

Let $P = \sum_{i=0}^{7} p_i X^i$ be an arbitrary polynomial of $\mathbb{F}_2[X]$ of degree < 8.

Q.1: Compute (symbolically) the result of the multiplication of P by X modulo $Q := X^8 + X^4 + X^3 + X + 1$.

Q.2: Considering that P can be embedded into $\mathbb{F}_2^8$ as the row vector $\begin{pmatrix} p_0 & \cdots & p_7 \end{pmatrix}$, write the multiplication of the previous question as a vector-matrix product and give the matrix $\boldsymbol{M}_{\texttt{0x2}}$ of the right multiplication by X modulo Q.

Remark. $\boldsymbol{M}_{\texttt{0x2}}$ is called the *companion matrix* of Q

Q.3: Compute $\boldsymbol{M}_{\texttt{0x4}} := \boldsymbol{M}_{\texttt{0x2}}^2$ and $\boldsymbol{M}_{\texttt{0x8}} := \boldsymbol{M}_{\texttt{0x2}}^3$. What is $\boldsymbol{M}_{\texttt{0xB}}$, the matrix of the right multiplication by $X^3 + X + 1$ modulo Q?

Q.4: Explain how one could compute the inverse of an element in $\mathbb{F}_{2^8}$ using the above representation. Do it for X^2 (either by hand or using `sage`).