Cryptography

Priv.-Doz. Dr. Adrian Spalka, Konstantin Ziegler

4 Assignment

(Due: Thursday, 25 November 2010, 12^{00})

Exercise 4.1 (The finite ring $\mathbb{F}_{256}[y]/\langle y^4+1\rangle$, `MixColumns`)**.** (10 points) The finite ring $S = \mathbb{F}_{2^8}[y]/\langle y^4+1\rangle$ consists of polynomials of degree less than 4 in the variable y with coefficients in the field $\mathbb{F}_{256}$.

(i) (2 points) The ring S is not a field. In particular, there are nonzero elements in S *without* a multiplicative inverse. Give an example and explain how you could check that property.

(ii) (3 points) The output b_3, b_2, b_1 and b_0 of the `MixColumns`-step for a column with entries a_3, a_2, a_1 and a_0 is determined by the product

$$b_3y^3+b_2y^2+b_1y+b_0 = (\texttt{02}+\texttt{01}y+\texttt{01}y^2+\texttt{03}y^3)\cdot(a_3y^3+a_2y^2+a_1y+a_0).$$

Expand the product over $\mathbb{F}_{256}[y]$, reduce it modulo y^4+1 and collect the terms with equal powers of y to obtain equations for b_3, b_2, b_1 and b_0. Find a 4×4-matrix $\mathcal{M}$ with entries from $\mathbb{F}_{256}$ to express this multiplication as a matrix-vector product

$$\begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{pmatrix} = \mathcal{M}\cdot\begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{pmatrix}.$$

(iii) Find the inverse of $\texttt{02}+\texttt{01}y+\texttt{01}y^2+\texttt{03}y^3$ in S.

(iv) Let us examine the consequence of choosing a different ring

$$S' = \mathbb{F}_{256}[y]/\langle y^4\rangle.$$

The multiplication with the polynomial $\texttt{02}+\texttt{01}y+\texttt{01}y^2+\texttt{03}y^3$ is now represented by the matrix

$$\mathcal{M}' = \begin{pmatrix} \texttt{02} & \texttt{00} & \texttt{00} & \texttt{00} \\ \texttt{01} & \texttt{02} & \texttt{00} & \texttt{00} \\ \texttt{01} & \texttt{01} & \texttt{02} & \texttt{00} \\ \texttt{03} & \texttt{01} & \texttt{01} & \texttt{02} \end{pmatrix}$$

Why would this operation hardly deserve the name *MixColumns*? Elaborate with an example.

Exercise 4.2 (AES)**.** (10 points)

(i) Write down an algorithm to decrypt the 128-bit output state of a single round of AES-128. Be as specific as possible and comment on the cost (space and time) of each step. (For example, employ the result of 4.1 (iii).)

(ii) One of the requirements in the AES-competition was performance. Find benchmarks for *Rijndael* and two other contestants and compare them. (Be careful about the sources you choose.)

(iii) Give examples of software that uses AES.

Exercise 4.3 (mathematical bonus)**.** (+2 points)