Homework 5 in Advanced Methods of Cryptography - Proposal for Solution -

Prof. Dr. Rudolf Mathar, Michael Reyer, Henning Maier

29.11.2013

Solution to Exercise 14.

$$\begin{pmatrix} r_0 \\ r_1 \\ r_2 \\ r_3 \end{pmatrix} = \begin{pmatrix} x & (x+1) & 1 & 1 \\ 1 & x & (x+1) & 1 \\ 1 & 1 & x & (x+1) \\ (x+1) & 1 & 1 & x \end{pmatrix} \cdot \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{pmatrix} \in \mathbb{F}_{2^8}^4 \tag{1}$$

It is to show that:

$$(c_3u^3 + c_2u^2 + c_1u + c_0)((x+1)u^3 + u^2 + u + x) \equiv \sum_{i=0}^{3} r_i u^i \pmod{(u^4+1)}. \tag{2}$$

Expand the multiplication on the left hand side of (2), reduce it modulo $u^4 + 1 \in \mathbb{F}_{2^8}[u]$, and use the abbreviations $(r_0, r_1, r_2, r_3)'$ according to (1).

$$\begin{aligned}
&(c_3u^3 + c_2u^2 + c_1u + c_0)((x+1)u^3 + u^2 + u + x) \\
=\ & c_3(x+1)u^6 + c_3u^5 + c_3u^4 + c_3xu^3 \\
& c_2(x+1)u^5 + c_2u^4 + c_2u^3 + c_2xu^2 \\
& c_1(x+1)u^4 + c_1u^3 + c_1u^2 + c_1xu \\
& c_0(x+1)u^3 + c_0u^2 + c_0u + c_0x \\
=\ & [c_3(x+1)]u^6 + [c_3 + c_2(x+1)]u^5 + [c_3 + c_2 + c_1(x+1)]u^4 \\
& + [c_3x + c_2 + c_1 + c_0(x+1)]u^3 + [c_2x + c_1 + c_0]u^2 + [c_1x + c_0]u + c_0x.
\end{aligned}$$

Now apply the modulo operation and merge terms:

$$\begin{aligned}
&\equiv [c_3x + c_2 + c_1 + (x+1)c_0]u^3 + [c_3(x+1) + c_2x + c_1 + c_0]u^2 + \\
&\quad [c_3 + c_2(x+1) + c_1x + c_0]u + [c_3 + c_2 + c_1(x+1) + c_0x] \\
&\overset{(1)}{\equiv} r_3u^3 + r_2u^2 + r_1u + r_0 \equiv \sum_{i=0}^{3} r_i u^i \pmod{(u^4+1)}
\end{aligned}$$