Mapping GF(256) to GF(16^2)
For Hardware Inversion of GF(256)
rcgldr 3/8/07

There are 2 fields of GF(16) with primitive $\beta = 1\ x + 0$, or 2 hex. This document will only use GF(16) based on the polynomial $x^4 + x + 1$.

There are 16 fields of GF(256) with primitive $\alpha = 1\ x + 0$, or 2 hex. This document will only use 2 of them based on the polynomials $x^8 + x^4 + x^3 + x^2 + 1$ and $x^8 + x^7 + x^2 + x^1 + 1$.

There are 64 fields of GF(16^2) with $\alpha = 1\ x + 0$, or 10 hex, with GF(16) based on $x^4 + x + 1$.

Only a few of the 64 fields can be used to map from any specific GF(256). The requirement for mapping is that math operations of α's in both GF(256) and GF(16^2) fields must be identical. For example, given any *a* and *b*, and defining *c* and *d* as: $\alpha^c = \alpha^a + \alpha^b$ and $\alpha^d = \alpha^a\ \alpha^b$, *c* and *d* will be the same for both GF(256) and GF(16^2) fields. When the two fields meet this requirement, then a field can be mapped to the other by multiplication by an 8 bit by 8 bit matrix and mapped back by with the inverse of the matrix.

For the GF(256) based on the polynomial $x^8 + x^4 + x^3 + x^2 + 1$ (11D hex), there are 4 compatible GF(16^2) fields: $x^2 + 2\ x + 5$, $x^2 + 3\ x + 4$, $x^2 + 4\ x + 2$, and $x^2 + 5\ x + 3$.

For the GF(256) based on the polynomial $x^8 + x^7 + x^2 + x^1 + 1$ (187 hex), there are 4 compatible GF(16^2) fields: $x^2 + 9\ x + 2$, $x^2 + b\ x + 5$, $x^2 + d\ x + 4$, and $x^2 + e\ x + 3$.

After choosing compatible fields, mapping from one to the other is accomplished by matrix multiplication. The byte to be converted is treated as an 8 row by 1 bit wide matrix, with most significant bit at the top. For example naming the byte bits as new and old:

$$
\begin{vmatrix} new_7 \\ new_6 \\ new_5 \\ new_4 \\ new_3 \\ new_2 \\ new_1 \\ new_0 \end{vmatrix}
=
\begin{vmatrix}
1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 1
\end{vmatrix}
\begin{vmatrix} old_7 \\ old_6 \\ old_5 \\ old_4 \\ old_3 \\ old_2 \\ old_1 \\ old_0 \end{vmatrix}
$$

Using GF(256) based on the polynomial $x^8 + x^4 + x^3 + x^2 + 1$ (11D hex), and GF(16^2) based on the polynomial $x^2 + 4x + 2 = x^2 + \beta^2 x + \beta$, the following matrices are used for mapping:

$$
\begin{array}{c}
\mathrm{GF}(256) \rightarrow \mathrm{GF}(16^2) \\
\begin{matrix}
1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 1
\end{matrix}
\end{array}
\qquad
\begin{array}{c}
\mathrm{GF}(16^2) \rightarrow \mathrm{GF}(256) \\
\begin{matrix}
0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\
1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 1
\end{matrix}
\end{array}
$$

Inversion of a GF(256) byte is done by mapping to GF(16^2) with left matrix. Let a_1 represent upper 4 bits of mapped byte, and a_0 represent lower 4 bits, so that mapped GF(16^2) byte can be represented as: $a_1 x + a_0$. Defining the inverse byte as: $b_1 x + b_0$, the equations are:

$$b_1 = \frac{a_1}{2a_1^2 + 4a_1a_0 + a_0^2}$$

$$b_0 = \frac{4a_1 + a_0}{2a_1^2 + 4a_1a_0 + a_0^2}$$

After calculating the *b*'s, map the byte back using the above right matrix.

For GF(256) based on the polynomial $x^8 + x^7 + x^2 + x^1 + 1$ (187 hex), and GF(16^2) field based on $x^2 + 9x + 2 = x^2 + \beta^{14} x + \beta$, the following matrices and equations are used for mapping:

$$
\begin{array}{c}
\mathrm{GF}(256) \rightarrow \mathrm{GF}(16^2) \\
\begin{matrix}
1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\
1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\
1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 0 & 0 & 1
\end{matrix}
\end{array}
\qquad
\begin{array}{c}
\mathrm{GF}(16^2) \rightarrow \mathrm{GF}(256) \\
\begin{matrix}
1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\
1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\
0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\
1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\
1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 1
\end{matrix}
\end{array}
$$

$$b_1 = \frac{a_1}{2a_1^2 + 9a_1a_0 + a_0^2}$$

$$b_0 = \frac{9a_1 + a_0}{2a_1^2 + 9a_1a_0 + a_0^2}$$