Composite Field Mapping Example

Jeff Reid (May 26, 2020)

This document will provide an example of mapping from Galois Field $GF(2^8)$ to $GF(((2^2)^2)^2)$, focusing on how the mapping matrix is generated.

Here is a list of the finite fields and the polynomials they are based on used for this example:

$GF(2^8)$: $x^8 + x^4 + x^3 + x^2 + x + 1$, with primitive element $\alpha(x)$ to be determined.

$GF(((2^2)^2)^2)$: $x^2 + x + 1100_2$, with primitive element $\beta(x) = x + 0$

$GF((2^2)^2)$: $x^2 + x + 10_2$, with primitive element $\varphi(x) = x + 0$

$GF(2^2)$: $x^2 + x + 1$, with primitive element $\delta(x) = x + 0$

$GF(2^8)$ is to be mapped to $GF(((2^2)^2)^2)$ with the constraints that the mapping will be isomorphic in addition (xor) and multiplication. Let map() represent the mapping function. While operating in $GF(((2^2)^2)^2)$ the constraints can be stated as (using · to represent multiplication):

```
map(a + b) = map(a) + map(b)
map(a · b) = map(a) · map(b)
```

The mapping converts like powers of the primitive elements and there is an inverse mapping:

$$\beta^k = \mathrm{map}(\alpha^k)$$

$$\alpha^k = \mathrm{map}^{-1}(\beta^k)$$

To meet the constraints, a search is done for any primitive element of $GF(2^8)$ that will satisfy the mapping constraints, and $\alpha(x) = x^4 + x^3 + x^2 + x + 1$ is one of those elements.

The mapping is done with an 8 row by 8 bit matrix and the inverse mapping is done by the inverse of that 8 row by 8 bit matrix, as shown on the next two pages. The mapping is done via a matrix multiply in GF(2), treating the element to be mapped as 8 row by 1 bit matrix, resulting in an 8 row by 1 bit mapped element. It's easier to understand the mapping matrix by noting that the columns of the matrix correspond to the bits, 7 through 0 of elements in $GF(2^8)$, and represent powers of α that result in the values 10000000_2 , 01000000_2 , 00100000_2 , 00010000_2 , 00001000_2 , 00000100_2 , 00000010_2 , 00000001_2.

The indexes to the columns correspond to powers of α shown in hex. This is easier to understand if the identity matrix is used:

α^64	α^c3	α^23	α^82	α^e1	α^41	α^a0	α^00
1	0	0	0	0	0	0	0
0	1	0	0	0	0	0	0
0	0	1	0	0	0	0	0
0	0	0	1	0	0	0	0
0	0	0	0	1	0	0	0
0	0	0	0	0	1	0	0
0	0	0	0	0	0	1	0
0	0	0	0	0	0	0	1

For the mapping matrix, the values in the columns correspond to powers of β, which are the same powers as in the matrix above, since $\beta^k = \text{map}(\alpha^k)$:

β^64	β^c3	β^23	β^82	β^e1	β^41	β^a0	β^00
1	0	1	0	0	0	0	0
1	1	0	1	1	1	1	0
1	0	1	0	1	1	0	0
1	0	1	0	1	1	1	0
1	1	0	0	0	1	1	0
1	0	0	1	1	1	1	0
0	1	0	1	0	0	1	0
0	1	0	0	0	0	1	1
fc	4b	b0	46	74	7c	5f	01

For the inverse mapping matrix, the column indexes correspond to powers of β. Again starting with the identity matrix:

β^67	β^bc	β^ab	β^01	β^66	β^bb	β^aa	β^00
1	0	0	0	0	0	0	0
0	1	0	0	0	0	0	0
0	0	1	0	0	0	0	0
0	0	0	1	0	0	0	0
0	0	0	0	1	0	0	0
0	0	0	0	0	1	0	0
0	0	0	0	0	0	1	0
0	0	0	0	0	0	0	1

The values in the inverse matrix columns correspond to powers of α, which are the same powers as in the matrix above, since $\alpha^k = \text{map}^{-1}(\beta^k)$:

α^67	α^bc	α^ab	α^01	α^66	α^bb	α^aa	α^00
1	1	1	0	0	0	1	0
0	1	0	0	0	1	0	0
0	1	1	0	0	0	1	0
0	1	1	1	0	1	1	0
0	0	1	1	1	1	1	0
1	0	0	1	1	1	1	0
0	0	1	1	0	0	0	0
0	1	1	1	0	1	0	1
84	f1	bb	1f	0c	5d	bc	01