Galois Field Derivations

René Peralta
Information Technology Laboratory, NIST

Feb 11, 2018: added equations for squaring and scaling

1 Extensions and constants

In the following, bases will be defined for each of the finite fields. Each base (b_1, b_2) will be such that $b_1 + b_2 = 1$. This identity can be verified by repeated squaring of the defining irreducible polynomial and adding the telescoping sequence (verify $GF(2^k)$ before $GF(2^{2k})$).

- $GF(2^2)$ is built from $GF2$ by adjoining a root W of $x^2 + x + 1$.
- basis for $GF(2^2)$ (W, W^2), with $W + W^2 = 1$.
- $$W^3 = 1$$
- $GF(2^4) = GF16$ is built from $GF(2^2)$ by adjoining a root Z of x^2+x+W^2.
- basis for $GF(2^4)$ is (Z^2, Z^8), with $Z^2 + Z^8 = 1$.

  1. $$Z^4 = W^2Z^2 + WZ^8$$
  2. $$Z^{10} = WZ^2 + WZ^8 = W$$
  3. $$Z^{16} = WZ^2 + W^2Z^8$$

- **Multiplication in** $GF(2^4)$ is given by

  $$(aZ^2+bZ^8)(cZ^2+dZ^8) = (acW^2+(ad+bc+bd)W)Z^2+((ac+ad+bc)W+bdW^2)Z^8.$$

- $GF(2^8) = GF256$ is built from $GF(2^4)$ by adjoining a root V of $x^2 + x + WZ^2$.
- basis for $GF(2^8)$ is (V, V^{16}), with $V + V^{16} = 1$. Let $\Omega = WZ^2$.

1.
$$V^2 = (1+\Omega)V + \Omega V^{16}$$

2.
$$V^{17} = \Omega V + \Omega V^{16} = \Omega$$

3.
$$V^{32} = \Omega V + (1+\Omega)V^{16}$$

- **Multiplication in** $GF(2^8)$ is given by

$$(aV+bV^{16})(cV+dV^{16}) = (ac+(a+b)(c+d)\Omega)V+(bd+(a+b)(c+d)\Omega)V^{16}.$$

- $GF(2^{16}) = GF65536$ is built from $GF(2^8)$ by adjoining a root T of $x^2 + x + WZ^2V$.
- basis for $GF(2^{16})$ is (T, T^{256}), with $T + T^{256} = 1$. Let $\Theta = WZ^2V$.

1.
$$T^2 = (1+\Theta)T + \Theta T^{256}$$

2.
$$T^{17} = \Theta T + \Theta T^{256} = \Theta$$

3.
$$T^{32} = \Theta T + (1+\Theta)T^{256}$$

- **Multiplication in** $GF(2^{16})$ is given by

$$(aT+bT^{256})(cT+dT^{256}) = (ac+\Theta(a+b)(c+d))T+(bd+\Theta(a+b)(c+d))T^{256}$$

- **Derivation of inverse in** $GF(2^{16})$ **and** $GF(2^8)$**.**

  I show the derivation for inverse in $GF(2^{16})$. The same derivation holds in $GF(2^8)$ if you set μ to $\Omega(a+b)$ instead of $\Theta(a+b)$.

$$1 = ac + \Theta(a+b)(c+d) \qquad 1 = bd + \Theta(a+b)(c+d)$$

  setting $\mu = \Theta(a+b)$ and summing yields

$$1 = c(a+\mu) + d\mu \qquad 0 = ac + bd$$

  equate the c coefficients

$$a = ca(a+\mu) + da\mu \qquad 0 = ac(a+\mu) + bd(a+\mu)$$

sum them

$$a = d(b(a+\mu) + a\mu) \Rightarrow d = (b(a+\mu)+a\mu)^{-1}a$$

yields

$$c = bda^{-1} = b(b(a+\mu)+a\mu)^{-1} \qquad d = a(b(a+\mu)+a\mu)^{-1}$$

Therefore

$$c = b(ba + (a+b)\mu)^{-1} \qquad d = a(ba+(a+b)\mu)^{-1}.$$

So

$$c = b(ba + (a+b)^2\Theta)^{-1} \qquad d = a(ba+(a+b)^2\Theta)^{-1}.$$

2 Squaring and scaling

2.1 GF4 squaring and scaling

$$(a_0W + a_1W^2)^2 = a_1W + a_0W^2$$

$$\begin{aligned}(a_0W + a_1W^2)^2W &= (a_1W + a_0W^2)W \\ &= a_1W^2 + a_0 \\ &= (a_1W^2 + a_0(W+W^2)) \\ &= a_0W + (a_0+a_1)W^2\end{aligned}$$

$$\begin{aligned}(a_0W + a_1W^2)^2W^2 &= (a_1W + a_0W^2)W^2 \\ &= a_0W^2 + a_1 \\ &= (a_0W^2 + a_1(W+W^2)) \\ &= a_1W + (a_0+a_1)W^2\end{aligned}$$

i.e.

$$\begin{aligned}(a_0,a_1)^2 &= (a_1,a_0) \\ (a_0,a_1)^2W &= (a_0, a_0+a_1) \\ (a_0,a_1)^2W^2 &= (a_1, a_0+a_1)\end{aligned}$$

Squaring in GF4 just swaps coefficients.

2.2 GF16 squaring and scaling

2.2.1 Squaring

$$\begin{aligned}(a_0Z^2 + a_1Z^8)^2 &= a_0^2Z^4 + a_1Z^{16} \\ &= a_0^2(W^2Z^2 + WZ^8) + a_1^2(WZ^2 + W^2Z^8) \\ &= (a_0^2W^2 + a_1^2W)Z^2 + (a_0^2W + a_1^2W^2)Z^8\end{aligned}$$

In exploded form this yields the linear transformation:

$$(a, b, c, d)^2 = (a + b + c, b + c + d, a + c + d, a + b + d)$$

2.2.2 Scaling

$$(a, b, c, d)Z^2 \to (a + b + d, a + c + d, b + d, a + b + c + d)$$

$$(aZ^2 + bZ^8)WZ^2 = (a + bW^2)Z^2 + (a + b)W^2Z^8.$$

$$(a, b, c, d)WZ^2 \to (a + c + d, b + c, a + b + c + d, a + c)$$

2.2.3 Squaring and square-scaling

$$(a, b, c, d)^2 \to (a + b + c, b + c + d, a + c + d, a + b + d)$$

$$(a, b, c, d)^2WZ^2 \to (a, a + b, a + b + c + d, b + d)$$

2.3 GF256 squaring and scaling

2.3.1 Squaring

Recall $\Omega = WZ^2$. Then

$$\begin{aligned}(a_0V + a_1V^{16})^2 &= a_0^2V^2 + a_1^2V^{32} \\ &= a_0^2(1 + \Omega)V + a_0^2\Omega V^{16} + a_1^2\Omega V + a_1^2(1 + \Omega)V^{16} \\ &= (a_0^2(1 + \Omega) + a_1^2\Omega)V + (a_0^2\Omega + a_1^2(1 + \Omega))V^{16} \\ &= (a_0^2 + (a_0^2 + a_1^2)\Omega)V + (a_1^2 + (a_0^2 + a_1^2)\Omega)V^{16} \\ &= (a_0^2 + (a_0 + a_1)^2\Omega)V + (a_1^2 + (a_0 + a_1)^2\Omega)V^{16}\end{aligned}$$

This leads to the linear transformation

$$(a0, a1, a2, a3, a4, a5, a6, a7)^2 = (h0, h1, h2, h3, h4, h5, h5, h7)$$

where

$$\begin{aligned}
h0 &= a1 + a2 + a4 \\
h1 &= a0 + a2 + a3 + a4 + a5 \\
h2 &= a1 + a4 + a5 + a6 + a7 \\
h3 &= a0 + a5 + a7 \\
h4 &= a0 + a5 + a6 \\
h5 &= a0 + a1 + a4 + a6 + a7 \\
h6 &= a0 + a1 + a2 + a3 + a5 \\
h7 &= a1 + a3 + a4
\end{aligned}$$

We can compute this with 14 XORs at depth 3:

```
14 gates
8 inputs
a0 a1 a2 a3 a4 a5 a6 a7
8 outputs
h0 h7 h1 h6 h2 h4 h5 h3
begin
T1 = a0 + a5
T2 = a1 + a4
T3 = a6 + a7
T4 = T2 + T3
T5 = a2 + a3
T6 = T1 + T5
h0 = a2 + T2
h7 = a3 + T2
h1 = a4 + T6
h6 = a1 + T6
h2 = a5 + T4
h4 = a6 + T1
h5 = a0 + T4
h3 = a7 + T1
end
```

2.3.2 Scaling

For multiplication in $GF(2^{16})$ I need to scale by V in $GF(2^8)$ (because $\Theta = WZ^2V = \Omega V$). We can use

$$V^2 = (1 + \Omega)V + \Omega V^{16}$$

and

$$V^{17} = \Omega V + \Omega V^{16} = \Omega.$$

Then

$$
\begin{aligned}
(a_0 V + a_1 V^{16})V &= (a_0 V^2 + a_1 V^{17}) \\
&= (a_0 + (a_0 + a_1)\Omega)V + (a_0 + a_1)\Omega V^{16}.
\end{aligned}
$$

3 Mapping the solution to other representations

Consider constructing $GF(2^{16})$ from $GF(2)$ by adjoining a root Δ of $p(x) = x^{16} + x^5 + x^3 + x + 1$. I will call this the target representation and the previous one the tower representation.

We can look for Δ using the algebra developed in the previous sections. There are sixteen possible values. I will pick

$$
\begin{aligned}
\Delta &= (1000100001001000) \\
&= WZ^2VT + WZ^2V^{16}T + W^2Z^2VT^{256} + WZ^2V^{16}T^{256}
\end{aligned}
$$

This gives us linear transformations between the two representations. The transformation from target to tower is given by the matrix

$$
A = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\
1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\
1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\
1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\
0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\
1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\
1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\
1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\
1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0
\end{bmatrix}
$$

The rows of the matrix are the powers (0 through 15) of Δ. A vector v in the target representation is mapped to a vector in the tower representation by computing vA.

The inverse of A is

$$A^{-1} = \begin{bmatrix}
0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\
1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\
1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\
0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\
1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\
1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\
0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\
1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\
1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\
1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\
0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0
\end{bmatrix}$$

A vector v in the tower representation is mapped to a vector in the target representation by computing vA^{-1}.