# Multiplicative Inverse Calculation in Composite Fields

(With Characteristic 2)

Christopher Wood

April 8, 2013

Let $\alpha \in GF(2^{2n})$. It is possible to represent $\alpha$ as the polynomial $bx + c$ over $GF(2^n)$ using the irreducible polynomial $p(x) = x^2 + Ax + B$. With this decomposition, it is possible to calculate the multiplicative inverse of $\alpha$ as the inverse of $(bx + c)$ using the following theorem.

**Theorem 1.** $\alpha^{-1} = (bx + c)^{-1} \equiv b(b^2B + bcA + c^2)^{-1}x + (c + bA)(b^2B + bcA + c^2)^{-1}$.

*Proof.* Assume that $(bx + c)^{-1} \equiv dx + e$, for some $d, c \in GF(2^n)$. We then have

$$\begin{aligned} (bx + c)^{-1} &\equiv dx + e \\ 1 \equiv (bx + c)(dx + e) &= k(x^2 + Ax + B) + 1 \\ bdx^2 + cdx + bex + ce &= kx^2 + kAx + kB + 1. \end{aligned}$$

From this, we see that $k = bd$, $(1)(cd + be) = kA$, and $(2)ce = kB + 1$. Substituting $k$ into the (1) and (2) yields two equations with two unknowns. We first solve for $d$ as follows:

$$\begin{aligned} bdA &= cd + be \\ bdA - cd &= be \\ d(bA - c) &= be \\ d &= be(bA - c)^{-1} \end{aligned}$$

By substituting $k$ and $d$ into (2) we can now solve for $e$ as follows:

$$\begin{aligned} b(be(bA - c)^{-1})B &= ce - 1 \\ b^2B &= (ce - 1)(bA - c) \\ b^2eB &= cebA - bA - c^2e + c \\ b^2eB + c^2e - cebA &= c - bA \\ e(b^2B + c^2 - cbA) &= c - bA \\ e &= (c - bA)(b^2B + c^2 - cbA)^{-1} \end{aligned}$$

Now we can solve for $d$ as follows:

$$d = be(bA - c)^{-1}$$
$$d = b(c - bA)(b^2B - bcA + c^2)^{-1}(bA - c)^{-1}$$
$$d = -b(b^2B - bcA + c^2)^{-1}$$

With $d$ and $e$, we now have that $(bx + c)^{-1} = -b(b^2B - bcA + c^2)^{-1}x + (c - bA)(b^2B + c^2 - cbA)^{-1}$, which is congruent to:

$$(bx + c)^{-1} \equiv b(b^2B + bcA + c^2)^{-1}x + (c + bA)(b^2B + c^2 + cbA)^{-1}$$

■