Goal

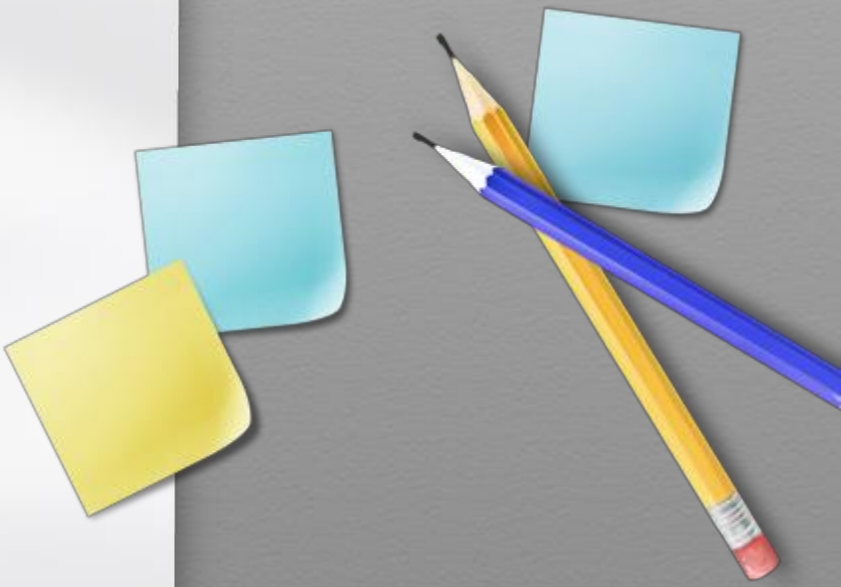
- How to implement the multiplicative inverse of $GF(2^8)$ of AES

  Method using Fermat's Little Theorem

  Itoh-Tsujii method

  Using Extended Euclidian Algorithm

  Reduction to subfield inversion (HW)



Multiplicative Inversion in $GF(2^8)$

(4) Reduction to subfield inversion

$$GF(2^8) \xrightarrow{\text{iso } \tilde{\sim} A} GF\left((2^4)^2\right), x^2 + x + \omega$$

$GF(2^4)[x] / \langle x^2 + x + \omega \rangle$

ω

$a \longmapsto bx + c, \quad b, c \in GF(2^4)$

"A"

$a \longmapsto bx + c$

inversion ↓ ↓ inversion in $GF((2^4)^2)$

"A^{-1}"

$a' \longleftarrow b'x + c'$

Multiplicative Inversion in $GF(2^8)$

(4) Reduction to subfield inversion

– Two Approaches to find the inversion in $GF((2^4)^2)$

(4-1) Direct method: Find $px + q \in GF((2^4)^2)$ such that

$$(bx + c)(px + q) = 1$$

$px+q = (bx+c)^{-1}$

(4-2) Using the following fact: for $p \in GF((2^n)^m)$,

$$p^{-1} = (p^r)^{-1}p^{r-1} \quad p^r \in GF(2^n), r = \frac{2^m - 1}{2^n - 1}$$

Multiplicative Inversion in $GF(2^8)$

(4) Reduction to subfield inversion

Consider $GF((2^n)^2)$ and defining polynomial $x^2 + x + B$

(4-1) For a given $bx + c \in GF((2^n)^2)$,

Find $(bx + c)(px + q) = 1$ Goal

Multiplicative Inversion in $GF(2^8)$

defining $x^2 = x + B$.

(4-1) Reduction to subfield inversion

$$(bx+c)(px+g) = 1$$

$$\Rightarrow bpx^2 + (bg+cp)x + cg = 1$$

Since $x^2 = x + B$ in $GF((2^n)^2)$

$$bp(x+B) + (bg+cp)x + cg = 1.$$

$$\Rightarrow (bp+bg+cp)x + (bpB+cg) = 1.$$

$$\therefore \begin{cases} (b+c)p + bg = 0. \\ bBp + cg = 1. \end{cases}$$

Multiplicative Inversion in $GF(2^8)$

(4-1) Reduction to subfield inversion

$(b+c)p + bq = 0 \quad \leftarrow \times c$

$bBp + cq = 1 \quad \leftarrow \times b$

$(bc+c^2)p + \cancel{bcq} = 0$

$+ \quad b^2Bp + \cancel{bcq} = b$

Let $d := (b^2B + bc + c^2)p = b$

$dp = b \Rightarrow p = d^{-1}b$ //

Multiplicative Inversion in $GF(2^8)$

(4-1) Reduction to subfield inversion

Now, applying $\beta = d + b$ to $b\beta\beta + cg = 1$.

$\Rightarrow b^2\beta d^{-1} + cg = 1.$ $\quad 1 = 1$

$\Rightarrow cg = b^2\beta d^{-1} + 1 = b^2\beta d^{-1} + d^{-1}d$

$= (b^2\beta + d)d^{-1}$

$= (b^2\beta + b^2\beta + bc + c^2)d^{-1}$

$\Rightarrow g = (b + c)d^{-1}$

Multiplicative Inversion in $GF(2^8)$

(4-1) Reduction to subfield inversion

Hence,

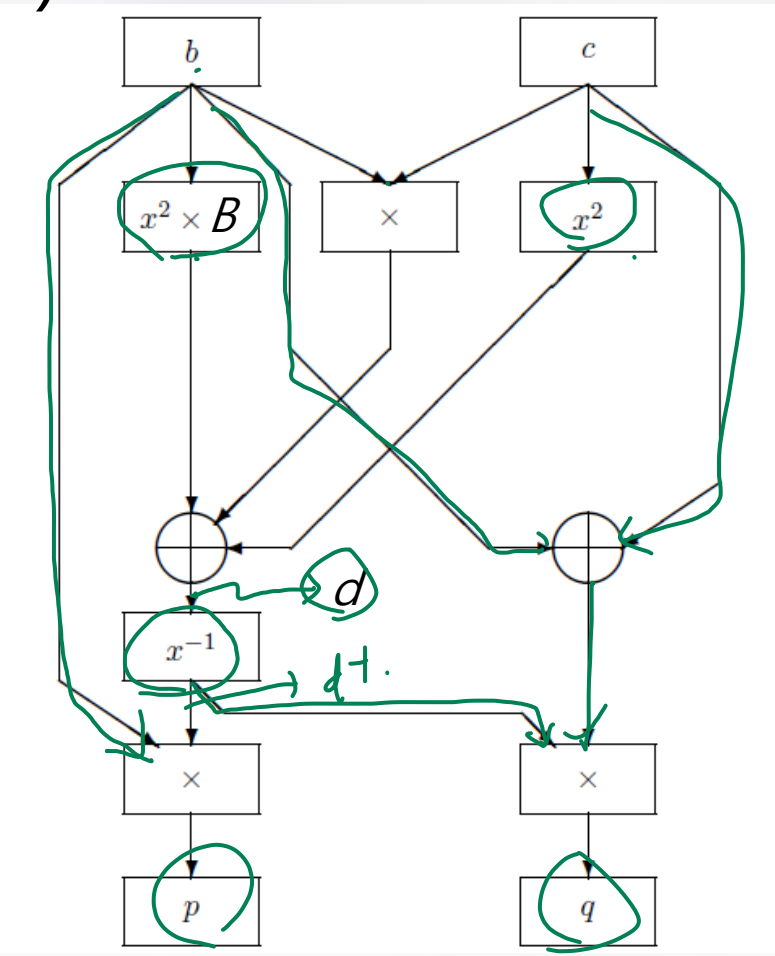
$(bx+c)^{-1} = px+q$, where

$$\begin{cases} p = d+b \\ q = d+(b+c) \end{cases}, \quad \underline{d = b^2B + bc + c^2}$$

Multiplicative Inversion in $GF(2^8)$

$bx + c$.

(4-1) Reduction to subfield inversion



$d = b^2B + bC + C^2$.

$p = d + b$.

$GF(2^4)$ base.

$q = d^{-1}(b + C)$.

$GF(2^8) \approx GF((2^4)^2)$.

$GF(2^4)$

Efficient Implementation of the Rijndael S-box, Vincent Rijmen, 2000

Multiplicative Inversion in $GF(2^8)$

(4-2) Reduction to subfield inversion

Itoh-Tsujii inversion.

- Fact: For $P \in GF((2^n)^m)$ $P^{-1} = (P^r)^{-1} P^{r-1}$

where $P^r \in GF(2^n)$. In fact, $r = \frac{2^{nm}-1}{2^n-1}$

$GF(2^8)$ 의 A

$GF((2^4)^2)$

In our case, $r = \frac{2^{4\cdot 2}-1}{2^4-1} = \frac{255}{15} = 17$

Step 1) compute $P^{r-1} = P^{16}$

Step 2) compute $P^r = (P^{16}) \cdot P$

Step 3) compute $(P^r)^{-1}$ in $GF(2^4)$

Step 4) compute $(P^r)^{-1} \cdot P^{r-1}$ using $GF((2^2)^2)$ arithmetic

p4

Multiplicative Inversion in $GF(2^8)$

(4-2) Reduction to subfield inversion

Consider the following tower field structure.

$GF(2^8)$, z^4+z+1 ⇝ $z^2 = z+1$

↓

$GF((2^4)^2)$, $x^2+x+\phi$,

$\phi = z^3+1 = (1001)$

Multiplicative Inversion in $GF(2^8)$

(4-2) Reduction to subfield inversion

Now, let $P = P_H X + P_L$ in $GF(2^4)^2$.

$P_H, P_L \in GF(2^4)$

Then $P^{16} = (P_H X + P_L)^{16=2^4}$

$= P_H^{2^4} X^{2^4} + P_L^{2^4} = P_H X^{2^4} + P_L$.

Since $A^{2^4} = A$ in $GF(2^4)$

$X^{2^4} = ?$

Multiplicative Inversion in $GF(2^8)$

$x^2+x+\phi$

(4-2) Reduction to subfield inversion

(Fact) $x^{2^4} = x + 1$

$\phi = z^3+1$

$x^{2^4} = (x^2)^{2^3} = (x+\phi)^{2^3} = (x+z^3+1)^{2^3}$

$= (x^2+z^6+1)^{2^2}$

$= (x+z^3+1+z^6+1)^{2^2}$

$= (x^2+z^6+z^{12})^2$

$= (x+z^3+z^6+z^{12}+1)^2$

$= x^2+z^6+z^{12}+z^{24}+1.$

$= x+z^3+1+z^6+z^{12}+z^{24}+1$

$= x+z^3+z^6+z^{12}+z^{24}$

$z^6 = z^4 \cdot z^2$
$= (z+1)z^2$
$= z^3+z^2$

Multiplicative Inversion in $GF(2^8)$

(4-2) Reduction to subfield inversion

(Fact) $x^{2^4} = x + 1$

$z^6 = z^3 + z^2$.

$= x + z^3 + z^6 + z^{12} + z^{24} = (z^6)^4$

$= x + z^3 + z^3 + z^2 + z^{12} + (z^3 + z^2)^4$

$= x + z^2 + z^{12} + z^{12} + z^8 = (z^4)^2$

$= x + z^2 + (z+1)^2$

$= x + z^2 + z^2 + 1$

$= x + 1$

$\therefore x^{2^4} = x + 1$ ///

Multiplicative Inversion in $GF(2^8)$

(4-2) Reduction to subfield inversion

Therefore.

Step1) $p^{16} = (P_H x + P_L)^{16} = P_H x^{16} + P_L$.

$x+1$

$= P_H (x+1) + P_L$.

$= P_H x + (P_H + P_L)$.

Multiplicative Inversion in $GF(2^8)$

(4-2) Reduction to subfield inversion

(Step 2) $p^{17} = p^{16} \cdot p$.

$x^2 = x + \phi$

$= (p_H x + (p_H + p_L))(p_H x + p_L)$.

$= p_H^2 x^2 + p_H p_L x + (p_H^2 + p_H p_L) x + p_H p_L + p_L^2$.

$= p_H^2 (x + \phi) + p_H^2 x + p_H p_L + p_L^2$.

$= p_H^2 \phi + p_H p_L + p_L^2$.

Multiplicative Inversion in $GF(2^8)$

(4-2) Reduction to subfield inversion

$P \to P^{16} \longrightarrow P^{16} \cdot P \xrightarrow{x^{-1}} (P^{17})^{-1} \to (P^{17})^{-1} \cdot P^{16}$

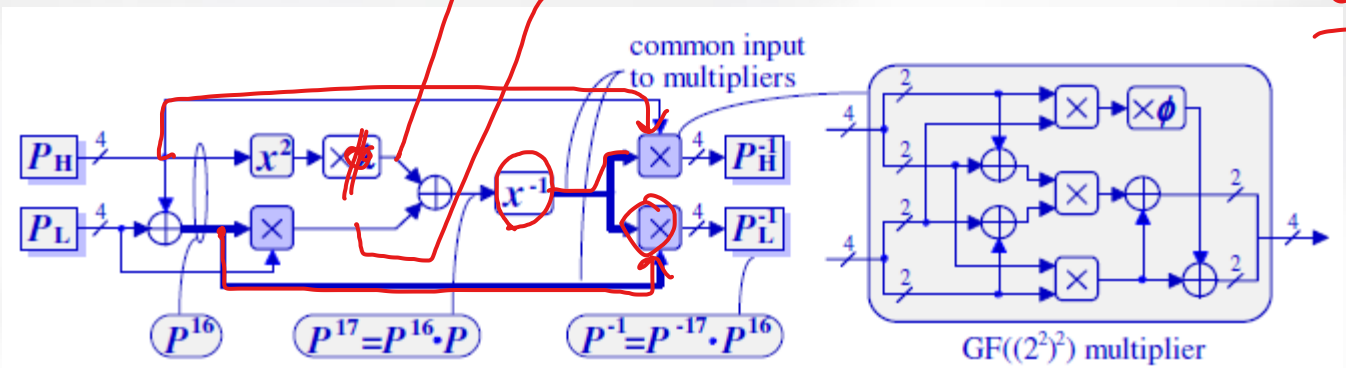
$P_H x + (P_H + P_L)$

$P_H^2 \phi + P_H P_L + P_L^2$

$P_H^2 \phi + (P_H + P_L) P_L$

$d^{-1}(P_H x + (P_H + P_L))$

$(d^{-1} P_H) x + d^{-1}(P_H + P_L)$



Q&A