

Lecture 04

IoT Security

Dept. of AI Cyber Security

Dooho Choi

doohochoi@korea.ac.kr



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)



Securing IoT Device - AES

Multiplicative Inversion in $GF(2^8)$

(4) Reduction to subfield inversion

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

$$\begin{matrix} \omega \\ a \end{matrix} \xrightarrow{} b\chi + c, \quad b, c \in GF(2^4)$$

$$\begin{array}{ccc}
 a & \xrightarrow{\text{"A"}} & b\chi + c \\
 \text{inversion} \downarrow & & \downarrow \text{inversion in } GF((2^4)^2) \\
 a' & \xleftarrow{\text{"A}^{-1}"} & b'\chi + c'
 \end{array}$$

Securing IoT Device - AES

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

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

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

Securing IoT Device - AES



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 $\underline{bx + c} \in \boxed{GF((2^n)^2)}$,

Find $\boxed{(bx + c)(px + q) = 1}$ Goal

Securing IoT Device - AES

Multiplicative Inversion in $GF(2^8)$

defining $X^2 + X + B$.

(4-1) Reduction to subfield inversion

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

$$\Rightarrow bP X^2 + (bg + cp)X + cg = 1$$

Since $X^2 = x+B$ in $GF((2^8)^2)$

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

$$\Rightarrow \underline{bp + bg + cp}x + \underline{bpB + cg} = 1.$$

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

Securing IoT Device - AES



Multiplicative Inversion in $GF(2^8)$

(4-1) Reduction to subfield inversion

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

$$bB P + cg = 1 \quad \leftarrow \times b.$$

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

$$+ \underbrace{b^2Bp + \cancel{bcg}}_{} = b$$

Let $d := \underbrace{(b^2B + bc + c^2)}_{\text{underlined}} p = b$

$$dP = b \Rightarrow P = d^{-1}b \quad //$$

Securing IoT Device - AES

Multiplicative Inversion in $GF(2^8)$

(4-1) Reduction to subfield inversion

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

$$\Rightarrow b^2Bd^{-1} + cg = 1.$$

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

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

$$= (\cancel{b^2B} + \cancel{b^2B} + bd + c^2)d^{-1}$$

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

Securing IoT Device - AES

Multiplicative Inversion in $GF(2^8)$

(4-1) Reduction to subfield inversion

Hence,

$$(b\alpha + c)^{-1} = px + g, \text{ where}$$

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

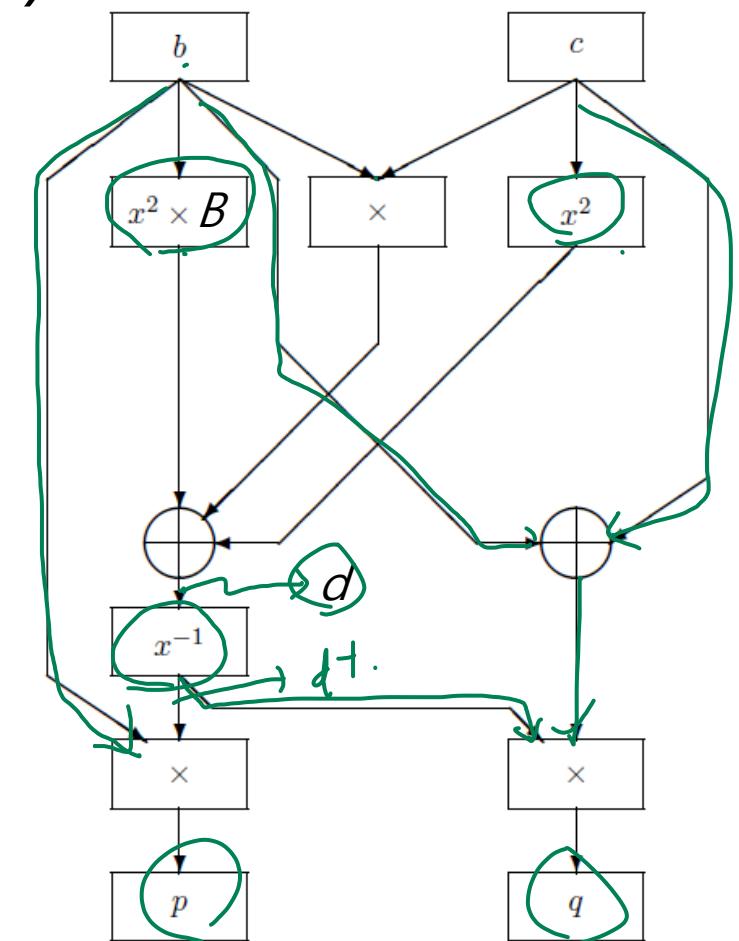


Securing IoT Device - AES

Multiplicative Inversion in $GF(2^8)$

$$b^{-1} + c$$

(4-1) Reduction to subfield inversion



$$\underline{d = b^2B + bc + c^2}$$

$$P = \frac{d + b}{\text{GF}(2^8)}$$

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

$$\text{GF}(2^8) \approx \text{GF}((2^4)^2)$$

$$\boxed{\text{GF}(2^4)}$$

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

Securing IoT Device - AES

Multiplicative Inversion in $GF(2^8)$

(4-2) Reduction to subfield inversion

Itoh-Tsuji 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, $r = \frac{2^{nm} - 1}{2^n - 1}$

$GF(2^8)$
 $GF(2^4)^4$

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

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

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

p-1

Securing IoT Device - AES

Multiplicative Inversion in $GF(2^8)$

(4-2) Reduction to subfield inversion

Consider the following tower field structure.

$$\begin{array}{c}
 \text{GF}(2^8), \underbrace{z^4 + z + 1}_{\sim} \rightsquigarrow z^4 = z + 1 \\
 \downarrow \\
 \text{GF}((2^4)^2), \underbrace{x^2 + x + \phi}_{\sim}, \\
 \phi = z^3 + 1 = (1001)
 \end{array}$$

Securing IoT Device - AES



Multiplicative Inversion in $GF(2^8)$

(4-2) Reduction to subfield inversion

$$\text{Now, let } P = P_H X + P_L \in GF(2^8)$$

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

$$\begin{aligned} P^{16} &= (P_H X + P_L)^{16} = X^{16} \\ &= P_H^{2^4} X^{2^4} + P_L^{2^4} = P_H X^{2^4} + P_L. \end{aligned}$$

$$\text{Since } A^{2^8} = A \quad \text{in } GF(2^8)$$

$$X^{2^4} = ?$$

Securing IoT Device - AES

Multiplicative Inversion in $GF(2^8)$

$$x^2 + x + \phi$$

(4-2) Reduction to subfield inversion

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

$$\begin{aligned}
 x^{2^4} &= (x^2)^{2^3} = (x + \phi)^{2^3} = (x + z^3 + 1)^{2^3} \\
 \\
 &= (x^2 + z^6 + 1)^{2^2} \\
 &= (x + z^3 + 1 + z^6 + 1)^{2^2} \\
 &= (x^2 + z^6 + z^{12})^2 \\
 &= (x + z^3 + z^6 + z^{12} + 1)^2
 \end{aligned}
 \quad \left| \begin{array}{l}
 = x^2 + z^6 + z^{12} + z^{24} + 1. \\
 = x + z^3 + 1 + z^6 + z^{12} + z^{24} + 1 \\
 = x + z^3 + z^6 + z^{12} + z^{24} \\
 \\
 \left(\begin{array}{l}
 z^6 = 2^4 \cdot z^2 \\
 = (z+1)z^2 \\
 = z^3 + z^2
 \end{array} \right)
 \end{array} \right.$$

Securing IoT Device - AES

Multiplicative Inversion in $GF(2^8)$

(4-2) Reduction to subfield inversion

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

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

$$\begin{aligned}
 &= x + z^3 + z^6 + z^{12} + \cancel{(z^{24})} \cdot (z^6)^4 \\
 &= x + \cancel{z^3} + \cancel{z^3} + z^2 + z^{12} + (z^3 + z^2)^4 \\
 &= x + z^2 + \cancel{z^{12}} + \cancel{z^{12}} + \cancel{(z^8)} = (z^4)^2 . \\
 &= x + z^2 + (z+1)^2 . \\
 &= x + z^2 + z^2 + 1 . \quad \therefore \underline{x^{2^4} = x+1} // \\
 &= x + 1
 \end{aligned}$$

Securing IoT Device - AES

Multiplicative Inversion in $GF(2^8)$

(4-2) Reduction to subfield inversion

Therefore,

Step 1)

$$\begin{aligned}
 p^{16} &= (P_H X + P_L)^{16} = P_H X^{16} + P_L \\
 &= P_H (X+1) + P_L \\
 &= P_H X + (P_H + P_L).
 \end{aligned}$$

Securing IoT Device - AES



Multiplicative Inversion in $GF(2^8)$

(4-2) Reduction to subfield inversion

$$\begin{aligned}
 (\text{Step 2}) \quad P^{19} &= P^8 \cdot P \quad X^2 = X + \phi \\
 &= (P_H X + (P_H + P_L))(P_H X + P_L) \\
 &= P_H^2 X^2 + \cancel{P_H P_L X} + (P_H^2 + \cancel{P_H P_L})X + P_H P_L + \cancel{P_L^2} \\
 &= \cancel{P_H^2}(X + \phi) + \cancel{P_H^2}X + P_H P_L + \cancel{P_L^2} \\
 &= \underline{\cancel{P_H^2} \phi + P_H P_L + P_L^2}.
 \end{aligned}$$

Securing IoT Device - AES

Multiplicative Inversion in $GF(2^8)$

(4-2) Reduction to subfield inversion

$$P \rightarrow P^{16} \rightarrow \underline{P^{16} \cdot P} \xrightarrow{x^{-1}} (P^{17})^{-1} \rightarrow \underline{(P^{17})^{-1} \cdot P^{16}}$$

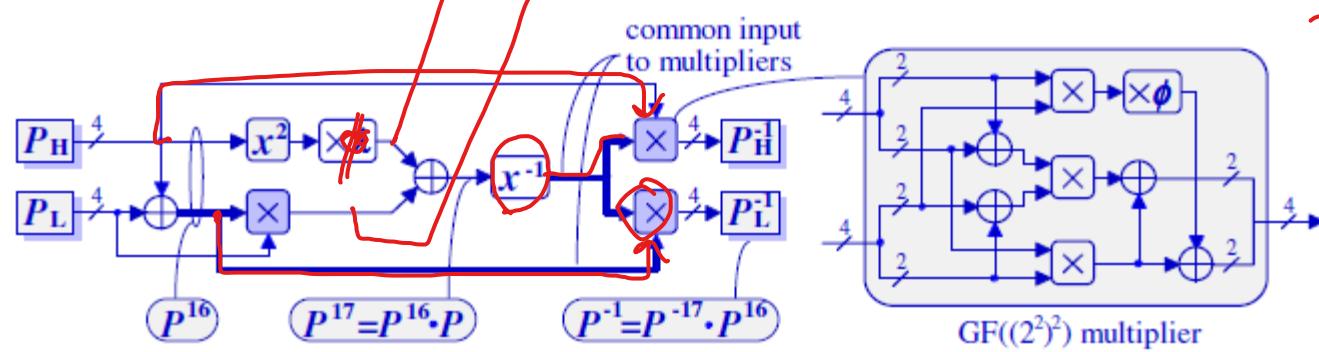
$$P_H \chi + (P_H + P_L)$$

$$\underline{P_H^2 \phi + P_H P_L + P_L}$$

$$\underline{P_H^2 \phi} + \underline{(P_H + P_L) P_L}$$

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

$$(d + P_H) \chi + d + (P_H + P_L)$$



Q&A



KEEP
CALM
AND
STUDY
ON

