Goal

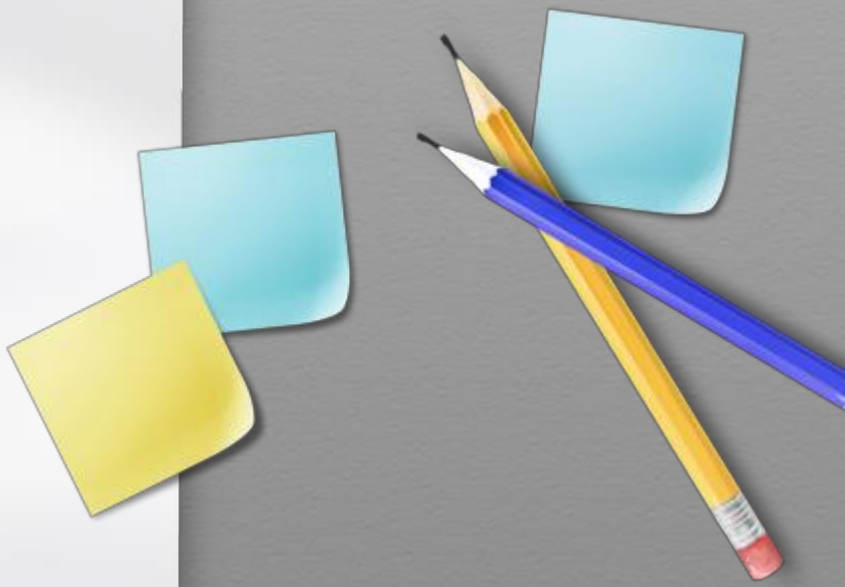
- How to implement the multiplicative inverse of $GF(2^8)$ of AES

  Method using Fermat's Little Theorem

  Itoh-Tsujii method

  Using Extended Euclidian Algorithm

  Reduction to subfield inversion



01. Securing IoT Device – AES

(Multiplicative inversion in $GF(2^8)$)

Multiplicative Inversion in $GF(2^8)$

Recall S-box of AES

$x \in GF(2^8)$, x^{-1} multi. inverse.

$$S(x) = A \cdot x^{-1} + a = b_{i,j}$$

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

Multiplicative Inversion in $GF(2^8)$

(1) Method using Fermat's Little Theorem

[Fermat's Little Theorem] For any $a(\neq 0) \in GF(p^m)$, $a^{p^m-1} = 1$ in $GF(p^m)$

$\Leftrightarrow a^{p^m} = a$

(*Proof*) By Math. induction

(*i*) $1^{p^m} = 1$

(*ii*) Suppose $k^{p^m} = k$. Then $(k+1)^{p^m} = k^{p^m} + 1^{p^m} = k + 1$

Multiplicative Inversion in $GF(2^8)$

(1) Method using Fermat's Little Theorem

[Fermat's Little Theorem] For any $a(\neq 0) \in GF(p^m)$, $a^{p^m-1} = 1$ in $GF(p^m)$

$a \cdot (a^{p^m-2}) = 1$

– Therefore, $a^{-1} = a^{p^m-2}$

a^{p^m-2}

– Now, we will introduce several algorithms to compute $a^{(p^m-2)}$, especially $a^{(2^m-2)}$ $GF(2^m)$

In $GF(2^8)$ $a^{-1} = a^{2^8-2} = a^{254}$

Multiplicative Inversion in $GF(2^8)$

(1) Method using Fermat's Little Theorem

$$2^m - 2 = 2(2^{m-1} - 1)$$
$$= 2(2^{m-1} - 2 + 1)$$
$$= 2(1 + 2(2^{m-2} - 1))$$
$$\vdots$$
$$= 2(1 + 2(1 + 2(1 + \ldots)))$$

$(Example)\ in\ GF(2^4)$

$$2^4 - 2 = 2(2^3 - 1)$$
$$= 2(2^3 - 2 + 1)$$
$$= 2(1 + 2(2^2 - 1))$$
$$= 2(1 + 2(2^2 - 2 + 1))$$
$$= 2(1 + 2(1 + 2(2^1 - 1)))$$
$$= 2(1 + 2(1 + 2))$$

Securing IoT Device - AES

Multiplicative Inversion in $GF(2^8)$

$2^n - 2$. $n = 8$.

(1) Method using Fermat's Little Theorem

$$a^{2^m-2} = a^{2(2^{m-1}-1)} = (a^{(2^{m-1}-1)})^2$$

$$= (a^{(2^{m-1}-2+1)})^2 = (a \times a^{(2^{m-1}-2)})^2$$

$$(a \times a^{2(2^{m-2}-1)})^2 = (a \times (a^{(2^{m-2}-1)})^2)^2$$

$$\vdots$$

$$= (a(a(\dots a(aa^2)^2 \dots)^2)^2)^2$$

$$a^{2(1+2(1+2))}$$

$$= \left(a^{(1+2(1+2))}\right)^2$$

$$= \left(a \cdot a^{2(1+2)}\right)^2$$

$$= \left(a \cdot (a^{(1+2)})^2\right)^2$$

$$= (a \cdot (a \cdot a^2)^2)^2$$

Multiplicative Inversion in $GF(2^8)$

(1) Method using Fermat's Little Theorem

Want! $(a \cdot (a \cdot a^2)^2)^2$

$b = 2^4 - 2$ $A = a$

Alg.1: *Square and Multiplication Algorithm*

Input $a \in GF(2^m)$

Output $A = a^{2^m-2}$ $= a^{-1}$

1. $b = 2^m - 2$
2. $A = a$
3. while $b \neq 1$
   - 3.1. if (b is even)
     - 3.1.1. $b = b/2$
     - 3.1.2. $A = A \times A$ Sq.
   - 3.2. else
     - 3.2.1. $b = b - 1$
     - 3.2.2. $A = A \times a$ Mul
4. Return A

(1) b even

$b = \frac{2^4 - 2}{2} = 2^3 - 1$

$A = a^2$

(2) b odd

$b = (2^3 - 1) - 1$

$= 2^3 - 2$

$A = A \cdot a = (a \cdot a^2)$

(3) b even

$b = \frac{2^3 - 2}{2} = 2^2 - 1$

$A = A^2 = (a \cdot a^2)^2$

(4) b odd

$b = (2^2 - 1) - 1 = 2^2 - 2$

$A = A \cdot a = a \cdot (a \cdot a^2)^2$

(5) b even

$b = \frac{2^2 - 2}{2} = 2^1 - 1 = 1$

$A = A^2 = (a \cdot (a \cdot a^2)^2)^2$

(6) $b = 1$ return A

$(a \cdot (a \cdot a^2)^2)^2$

Multiplicative Inversion in $GF(2^8)$

(1) Method using Fermat's Little Theorem

$$2^m - 2$$
$$= 2(2^{m-1} - 1)$$
$$= 2(2-1)(2^{m-2} + \cdots + 2 + 1)$$

$x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + x + 1)$

$$= 2(2^{m-2} + \cdots + 2 + 1)$$
$$= 2^{m-1} + \cdots + 2^2 + 2$$

Therefore,

$$a^{2^m - 2} = a^2 \cdot a^{2^2} \cdot a^{2^3} \cdots a^{2^{m-1}}$$

In $GF(2^8)$ (Gh (2^n))

$$a^{-1} = a^2 \cdot a^{2^2} \cdot a^{2^3} \cdot a^{2^4} \cdot a^{2^5} \cdot a^{2^6} \cdot a^{2^7}$$

[Mul : 6, Sq : 7] → In general [Mul : $m-2$, Sq : $m-1$]

(Algorithm 2)

$A \leftarrow a$, $B \leftarrow 1$

For $i = 1$ to $m - 1$

$A \leftarrow A^2$, $B \leftarrow A \cdot B$

Return B

Multiplicative Inversion in $GF(2^8)$

(1) Method using Fermat's Little Theorem

(cf.) Exponentiation Algorithms

Algorithm A (Left - to - Right)

Input : $x, E = (e_k e_{k-1} \cdots e_1)_2$.

Output : x^E contained in C.

$C = 1$;

for $i = k$ downto 1

{

$C = C \cdot C$;

if $(e_i = 1)$ then $C = C \cdot x$;

}

Algorithm B (Right - to - Left)

Input : $x, E = (e_k e_{k-1} \cdots e_1)_2$.

Output : x^E contained in C.

$C = 1$; $S = x$;

for $i = 1$ to k

{

if $(e_i = 1)$ then $C = C \cdot S$;

$S = S \cdot S$;

}

Multiplicative Inversion in $GF(2^8)$

(2) Itoh-Tsujii method

When $m = 2^r + 1$

$$2^m - 2 = (2^{m-1} - 1)2$$

$$= (2^{2^r} - 1)2$$

$$= (2^{2^{r-1}} - 1)(2^{2^{r-1}} + 1)2$$

$$= (2^{2^{r-2}} - 1)(2^{2^{r-2}} + 1)(2^{2^{r-1}} + 1)2$$

$$\vdots$$

$$= (2 + 1)(2^2 + 1)(2^{2^2} + 1) \cdots (2^{2^{r-1}} + 1)2$$

Algorithm 1.

$m = 9 = 2^3 + 1$

$$2^{2^3+1} - 2 = (2^{2^3} - 1)2$$

$$= (2 + 1)(2^2 + 1)(2^{2^2} + 1)2$$

$A^{(2+1)(2^2+1)(2^{2^2}+1)2}$

$= ((A^2 \cdot A)^{(2^2+1)(2^{2^2}+1)})^2$ ($A' = A^2 \cdot A$)

$= ((A'^{2^2} \cdot A')^{(2^{2^2}+1)})^2$

$\vdots$

Multiplicative Inversion in $GF(2^8)$

(2) Itoh-Tsujii method Algorithm 1.

ALGORITHM 1. *Multiplicative inverse computation in* $GF(2^n)$ *with* $n = 2^r + 1$ *[5, Theorem 1]*

Input: $A \in GF(2^n)$, $A \neq 0$, $n = 2^r + 1$
Output: $C = A^{-1}$

$C \leftarrow A$
for $i = 0$ to $r - 1$ **do**
  $D \leftarrow C^{2^{2^i}}$ {NOTE: 2^i cyclic shifts}
  $C \leftarrow C \cdot D$
end for
$C \leftarrow C^2$
Return (C)

r iterations
$r = \log_2(n-1)$

Multiplicative Inversion in $GF(2^8)$

(2) Itoh-Tsujii method Algorithm 1.

(Example) $A \in GF(2^{17})$, $17 = 2^4 + 1$

$$A^2 \cdot A = A^3$$

$$\left(A^3\right)^{2^{2^1}} \cdot A^3 = A^{15}$$

$$\left(A^{15}\right)^{2^{2^2}} \cdot A^{15} = A^{255}$$

$$\left(A^{255}\right)^{2^{2^3}} \cdot A^{255} = A^{65535}$$

$$\left(A^{65535}\right)^{2} = A^{131070}$$

# of multiplications : 4
(# of multiplications : 15 by the previous algorithm)

But $8 \neq 2^r + 1$

Therefore, it cannot be applied for $GF(2^8)$

Multiplicative Inversion in $GF(2^8)$

(2) Itoh-Tsujii method

Algorithm 2.

(i) Consider the following "addition chain"

$u_0 = 1, u_t = m-1,\ u_i = u_{k_i} + u_{j_i}$ such that

$k_i, j_i \in \{0, \cdots, i-1\}$

(Example 1) $m = 8$; 1,2,3,6,7 is an addition chain

Example.2: If $m = 193$, then the addition chain could be

1, 2, 3, 6, 12, 24, 48, 96, 192

Multiplicative Inversion in $GF(2^8)$

(2) Itoh-Tsujii method

Algorithm 2.

(ii) Set $\beta_k(a) := a^{(2^k-1)}$. Then

(1) $\beta_{j+k} = \beta_k^{2^j} \times \beta_j$

(2) $\beta_{2k} = \beta_k^{2^k+1}$ or $\beta_k^{2^k} \times \beta_k$

(why) $2^{j+k} - 1 =$

$2^{j+k} - 2^j + 2^j - 1$

$= 2^j(2^k - 1) + (2^j - 1)$

β_k β_j

$2^{2k} - 1 = (2^k - 1)(2^k + 1)$

$= 2^k(2^k - 1) + (2^k - 1)$

$= \beta_k \quad \beta_k$

Therefore,

$\beta_{j+k} = a^{2^{j+k}-1} = (a^{2^k-1})^{2^j} \cdot a^{2^j-1} = \beta_k^{2^j} \cdot \beta_j$ $\quad \therefore \beta_k^{2^k} \cdot \beta_k$

Multiplicative Inversion in $GF(2^8)$

(2) Itoh-Tsujii method Algorithm 2.

Example.3: for $m = 193$ and above addition chain, we can write the following calculations

$u_0 = 1$	$\beta_1 = a^{2^1-1}$
$u_1 = 2$	$\beta_2 = (\beta_1)^{2^2-1} = a^{2^2-1}$
$u_2 = 3$	$\beta_3 = (\beta_2)^{2^1-1} \times \beta_1$
$u_3 = 6$	$\beta_6 = (\beta_3)^{2^3} \times \beta_3$
$u_3 = 12$	$\beta_{12} = (\beta_6)^{2^6} \times \beta_6$
$u_3 = 24$	$\beta_{24} = (\beta_{12})^{2^{12}} \times \beta_{12}$
$u_4 = 48$	$\beta_{48} = (\beta_{24})^{2^{24}} \times \beta_{24}$
$u_4 = 96$	$\beta_{96} = (\beta_{48})^{2^{48}} \times \beta_{48}$
$u_4 = 192$	$\beta_{192} = (\beta_{96})^{2^{96}} \times \beta_{96}$

$\beta_{192} = a^{2^{192}-1}$

$a \in GF(2^{193})$

$a^{-1} = a^{(2^{193}-2)}$

$= (a^{2^{192}-1})^2 \cdot$

$= (\beta_{192})^2$

$\hookrightarrow a^{-1}$.

Multiplicative Inversion in $GF(2^8)$

(2) Itoh-Tsujii method Algorithm 2.

Alg.2: *Itoh and Tsujii Algorithm to compute inversion*

Input $a \in GF(2^m)$ $u_0 \cdots$, u_t : addition chain.

Output a^{-1}

1. $\beta_{u0}(a) = a$
2. For $i = 1$ to t do
   2.1. $\beta_{ui}(a) = (\beta_{uki}(a))^{2^{uji}} \times \beta_{uji}(a)$
3. Return $\beta_{ut}(a)$

Multiplicative Inversion in $GF(2^8)$

(2) Itoh-Tsujii method Algorithm 2.

HW

(Quiz) For a given $GF(2^8)$,

(1) Find an addition chain

(2) Give a computation table of the Itoh-Tsujii algorithm by this addition chain

(3) # of multiplications and squaring for this algorithm

Multiplicative Inversion in $GF(2^8)$

(2) Itoh-Tsujii method

Algorithm 2.

Addition Chain	Mult : 4 , Squaring: 6
1	$\beta_1 = a$
2	$\beta_2 = \beta_1^{2} \cdot \beta_1$
4	$\beta_4 = \beta_2^{2^2} \cdot \beta_2$
6 = 4+2	$\beta_6 = \beta_4^{2^2} \cdot \beta_2$
7 = 6+1	$\beta_7 = \beta_6^{2} \cdot \beta_1$
return	$(\beta_7)^2 \Rightarrow a^{-1}$