Goal

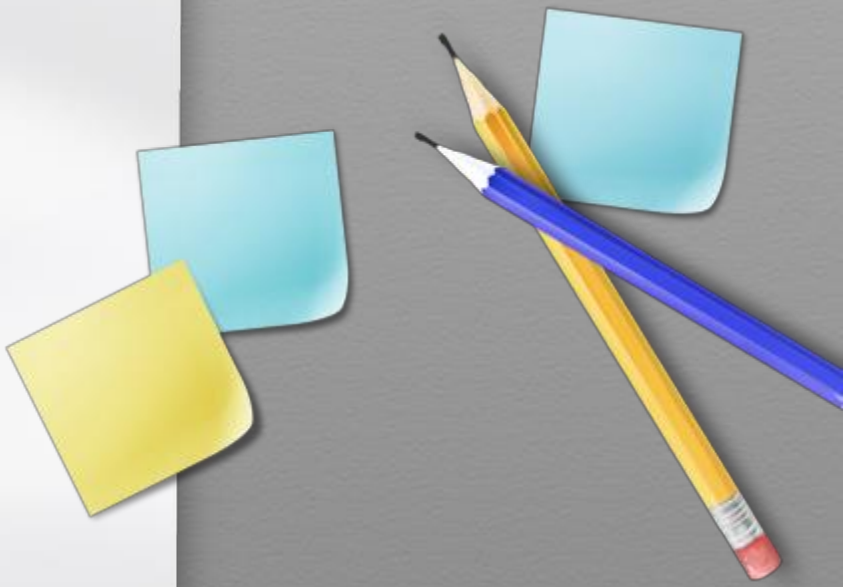
- How to implement the multiplicative inverse of $GF(2^8)$ of AES

  Method using Fermat's Little Theorem

  Itoh-Tsujii method

  Using Extended Euclidian Algorithm

  Reduction to subfield inversion



Multiplicative Inversion in $GF(2^8)$

(3) Using Extended Euclidian Algorithm

- Recall Euclidean Algorithm to find the greatest common divisor(gcd) 최대공약수
- $\gcd(u, v) = c$, $u \geq v$. Then

$u = c \cdot d$, $v = c \cdot d' \Rightarrow u - v = cd - cd' = c(d - d')$

$\therefore \gcd(u, v) = \gcd(u, u - v)$

$u - v \rightarrow u \bmod v$

Therefore, $r_0 = u$, $r_1 = v$ $\quad r_{i+1} = r_{i-1} - q_{i-1} r_i$, $q_{i+1} = \lfloor r_{i-1} / r_i \rfloor$

Then $\gcd(u, v) = \gcd(r_0, r_1) = \gcd(r_1, r_2) = \gcd(r_2, r_3) = \cdots = \gcd(r_k, 0) = r_k$

Multiplicative Inversion in $GF(2^8)$

(3) Using Extended Euclidian Algorithm

"유클리드 호제법".

The Euclidean Algorithm

Input: positive integers u and v, with $u \geq v$

Output: $g = \gcd(u, v)$

While $v > 0$ do

$q \leftarrow \lfloor u/v \rfloor$; $r \leftarrow u - qv$;

$u \leftarrow v$; $v \leftarrow r$;

End While

$g \leftarrow u$;

Return g

(Example)

$1 \mid 5, 3$ → $5 - 3 \cdot 1 = 2$

$1 \mid 2\ 3$ → $3 - 2 \cdot 1 = 1$

$2 \mid 2\ 1$ → $2 - 1 \cdot 2 = 0$

$0\ 1$

return 1

$(\because)$ $\gcd(5, 3) = 1$.

Securing IoT Device - AES

Multiplicative Inversion in $GF(2^8)$

(3) Using Extended Euclidean Algorithm

Recall the following fact:

" $\exists\ s, t$ s.t. $us + vt = \gcd(u, v) = 1$ "

If $\gcd(u, v) = 1$, *i.e.* relatively prime (서로소)

– Then

$us = 1 - vt \Rightarrow us = 1 \bmod v$.

Therefore, this s is the multiplicative inverse of u in modulus v. $G\pi(v)$

Extended Euclidean Algorithm is to find

s, t such that $us + vt = \gcd(u, v)$

return gcd, s, t

Multiplicative Inversion in $GF(2^8)$

(3) Using Extended Euclidian Algorithm

- Consider $r_i = s_i u + t_i v$.
- Let $r_o = u, r_1 = v$.
- That is, $s_0 = 1, t_0 = 0, s_1 = 0, t_1 = 1$.
- Since $r_{i+1} = r_{i-1} - q_{i-1} r_i$, $q_{i-1} = \lfloor r_{i-1} / r_i \rfloor$

$$r_{i+1} = (s_{i-1}u + t_{i-1}v) - q_{i-1}(s_i u + t_i v)$$

$$= (s_{i-1} - q_{i-1}s_i)u + (t_{i-1} - q_{i-1}t_i)v$$

$s_{i+1} = s_{i-1} - q_{i-1} s_i$ and $t_{i+1} = t_{i-1} - q_{i-1} t_i$

Multiplicative Inversion in $GF(2^8)$

(3) Using Extended Euclidian Algorithm

The Extended Euclidean Algorithm

Input: positive integers u and v, with $u \geq v$

Output: $g = \gcd(u, v)$ and integers s, t satisfying $us + vt = g$

$s'' \leftarrow 1 ; s' \leftarrow 0 ; t'' \leftarrow 0 ; t' \leftarrow 1$

While $v > 0$ do

$q \leftarrow \lfloor u/v \rfloor , r \leftarrow u - qv ;$

$s \leftarrow s'' - qs' ; t \leftarrow t'' - qt' ;$

$u \leftarrow v ; v \leftarrow r ;$

$s'' \leftarrow s' ; s' \leftarrow s ; t'' \leftarrow t' ; t' \leftarrow t ;$

End While

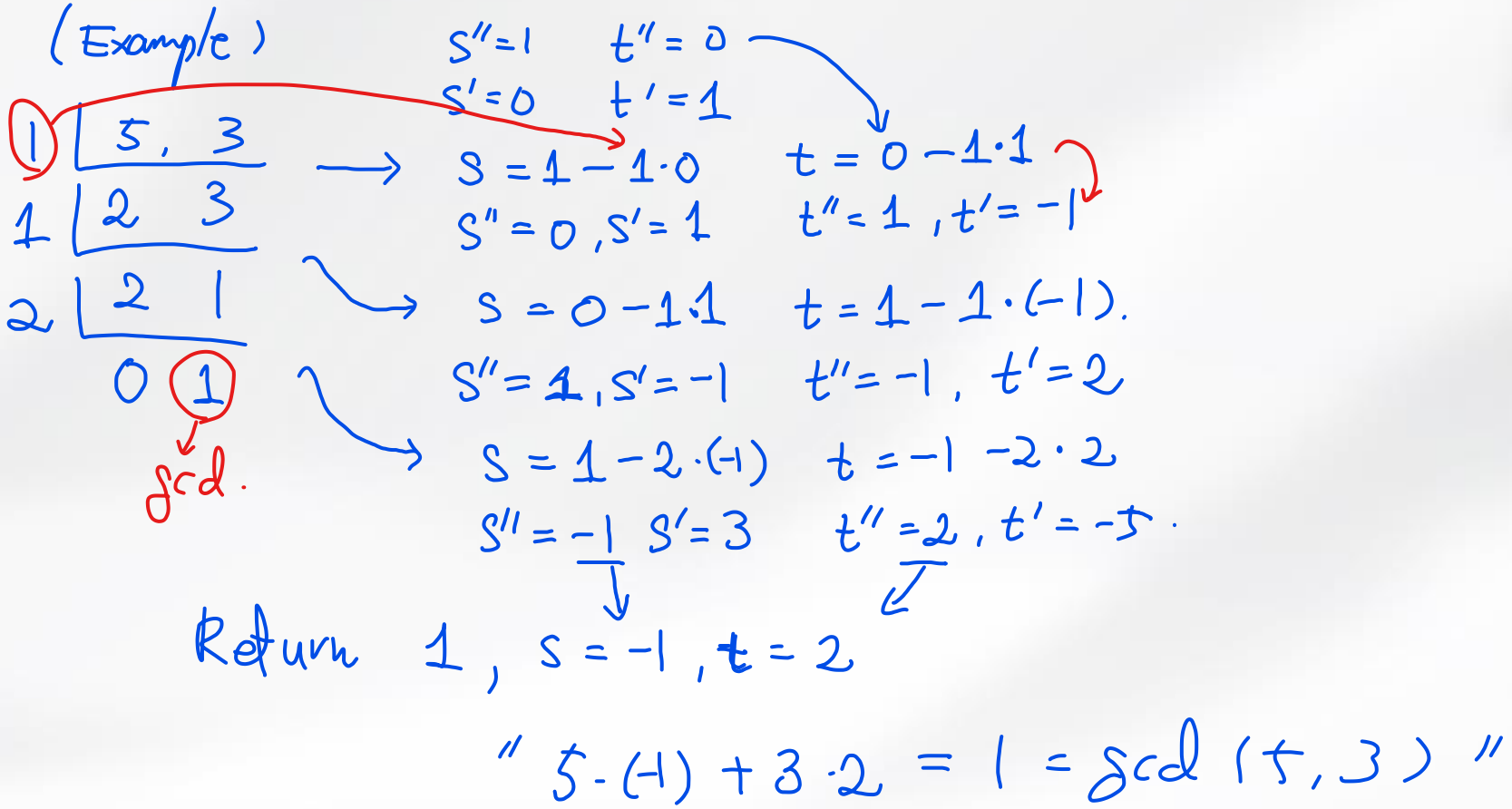
$g \leftarrow u ;$

$s \leftarrow s'' ; t \leftarrow t'' ;$

Return (g, s, t)

Multiplicative Inversion in $GF(2^8)$

(3) Using Extended Euclidian Algorithm



Multiplicative Inversion in $GF(2^8)$

(3) Using Extended Euclidian Algorithm

The Extended Euclidean Algorithm for Polynomials

Input: polynomials $u(x)$ and $v(x)$, with $\deg(u) \geq \deg(v)$

Output: $g(x) = \gcd(u(x), v(x))$ and polynomials $s(x), t(x)$ satisfying $u(x)s(x) + v(x)t(x) = g(x)$

$s''(x) \leftarrow 1 ; s'(x) \leftarrow 0 ; t''(x) \leftarrow 0 ;$
$t'(x) \leftarrow 1$
While $v(x) > 0$ do
  $r(x) \leftarrow u(x) \bmod v(x) ;$
  $q(x) \leftarrow (u(x) - r(x))/v(x) ;$
  $s(x) \leftarrow s''(x) - q(x)s'(x) ;$
  $t(x) \leftarrow t''(x) - q(x)t'(x) ;$
  $u(x) \leftarrow v(x) ; v(x) \leftarrow r(x) ;$
  $s''(x) \leftarrow s'(x) ; s'(x) \leftarrow s(x) ;$
  $t''(x) \leftarrow t'(x) ; t'(x) \leftarrow t(x) ;$
End While
$a \leftarrow$ leading nonzero coefficient of $u(x) ;$
$g(x) \leftarrow a^{-1}u(x) ;$
$s(x) \leftarrow a^{-1}s''(x) ; t(x) \leftarrow a^{-1}t''(x) ;$
Return $(g(x), s(x), t(x))$

Multiplicative Inversion in $GF(2^8)$

(3) Using Extended Euclidian Algorithm

Alg.6: *Algorithm of Computing Inversion Over GF(P)*

Input: $P, a \in GF(P)$

Output: a^{-1}

1. $y_1 = 1$
2. $y_2 = 0$
3. While $(a \neq 1)$
   - 3.1. $q = \left\lfloor \frac{P}{a} \right\rfloor$
   - 3.2. $a = P - qa;\ P = a;\ y_2 = y_1;\ y_1 = y_2 - qy_1$
4. Return (y_1)

$7^{-1} = 5$ over $GF(17)$.

$\left\lfloor \frac{17}{7} \right\rfloor = 2$

$17 - 2 \cdot 7 = 3$

$\begin{cases} y_1 = 0 - 2 \cdot 1 = -2 \\ y_2 = 1 \end{cases}$

$\left\lfloor \frac{7}{3} \right\rfloor = 2$

$7 - 2 \cdot 3 = 1$

$\begin{cases} y_1 = 1 - 2 \cdot (-2) = 5 \\ y_2 = -2 \end{cases}$ ← Return 5

"$7 \cdot 5 = 35 = 1 \mod 17$"

Multiplicative Inversion in $GF(2^8)$

(3) Using Extended Euclidian Algorithm

(Example) Compute inversion of $a = x^3+1$ in $GF(2^8)$ with defining poly. $m = x^8+x^4+x^3+x+1$

$\deg(m) = 8 \geq \deg(a) = 3$.

Multiplicative Inversion in $GF(2^8)$

(3) Using Extended Euclidian Algorithm

In $us + vt = 1$,

$\begin{cases} u = m \\ v = a \end{cases}$ $t_0 = 0$, $t_1 = 1$

Multiplicative Inversion in $GF(2^8)$

$a = x^3+1$

(3) Using Extended Euclidian Algorithm

(00100111)

	Q.	m
		(00100111)
x	x^3+1	x^2
x^2	1	x^2
	1	0

$$x^3+1 \;\big)\; x^8+x^5+x^3+x+1 \;\big(\; x^5+x^2+x+1$$

$$\oplus \;\big|\; x^8+x^5$$

$$x^5+x^3+x+1$$

$$\oplus \;\big|\; x^5+x^2$$

$$x^3+x^2+x+1$$

$$\oplus \;\big|\; x^3+x$$

$$x^2+1$$

$$\oplus \;\big|\; x^2+1$$

$$0$$

Multiplicative Inversion in $GF(2^8)$

(3) Using Extended Euclidian Algorithm

$q_0 = (00100111)$

$q_1 = (00000010) = x$

$q_2 = (00000100) = x^2$.

$t_0 = 0$, $t_1 = 1$

$\Rightarrow t_2 = t_0 + q_0 t_1 = 0 + (00100111) \cdot 1 = 00100111$

$t_3 = t_1 + q_1 t_2 = 1 + x \cdot (00100111)$

$= 1 + 01001110 = (01001111)$

Multiplicative Inversion in $GF(2^8)$

(3) Using Extended Euclidian Algorithm

Now, $t_3 = (01001111) = x^6 + x^3 + x^2 + x + 1$

is an inversion of $a = x^3 + 1$ in $GF(2^8)$

$a \cdot (01001111) = (x^3+1)(01001111) = 01001111 \oplus 01001110 = 00000001 = 1$

$x(01001111) = 10011110$

$x^2(01001111) = 00111100 \oplus (00010011) = 00100111$

$x^3(\quad\quad) = 01001110$