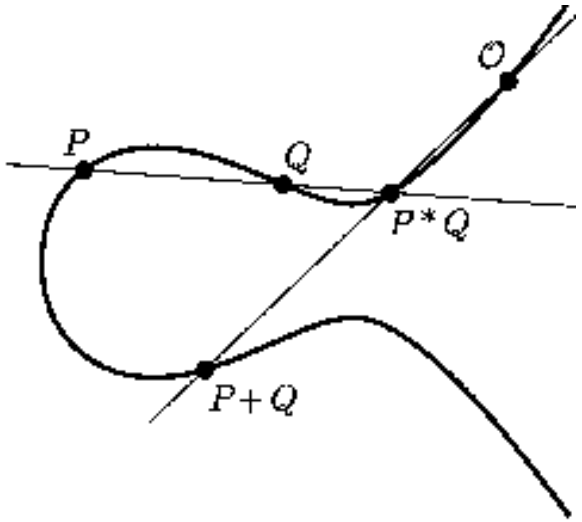
Bahan kuliah II4021 Kriptografi

Elliptic Curve Cryptography (ECC)

(Bagian 1)



Oleh: Rinaldi Munir

Program Studi Sistem dan Teknologi Informasi
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
2025

Referensi:

1. Andreas Steffen, *Elliptic Curve Cryptography,* Zürcher Hochschule Winterthur.
2. Debdeep Mukhopadhyay, *Elliptic Curve Cryptography* , Dept of Computer Sc and Engg IIT Madras.
3. Anoop MS *, Elliptic Curve Cryptography, an Implementation Guide*

Teori Aljabar Abstrak

- Sebelum membahas ECC, perlu dipahami beberapa konsep aljabar abstrak yang mendasarinya.

- Konsep aljabar abstrak:
  1. Grup (*group*)
  2. Cincin (*ring*)
  3. Medan (*field*)
  3. Galois field

Grup

- Grup (*group*) adalah sistem aljabar yang terdiri dari:

  - sebuah himpunan *G*

  - sebuah operasi biner *

  sedemikian sehingga untuk semua elemen *a*, *b*, dan *c* di dalam *G* berlaku aksioma berikut:

  1. *Closure*: $a * b$ harus berada di dalam G
  2. Asosiatif: $a * (b * c) = (a * b) * c$
  3. Elemen netral: terdapat $e \in G$ sedemikian sehingga $a * e = e * a = a$
  4. Elemen invers: terdapat $a' \in G$ sedemikian sehingga $a * a' = a' * a = e$

- Notasi: <G, *>

- <G, +> menyatakan sebuah grup dengan operasi penjumlahan.
- <G, ·> menyatakan sebuah grup dengan operasi perkalian

Contoh-contoh grup:

1. <R, +> : grup dengan himpunan bilangan riil dengan operasi +

   $e = 0$ dan $a' = -a$

2. <R*, ·> : grup dengan himpunan bilangan riil tidak nol (yaitu, R* = R – { 0}) dengan operasi kali (·)

   $e = 1$ dan $a' = 1/a = a^{-1}$

3. <Z, +> dan <Z, ·> masing-masing adalah grup dengan himpunan bilangan bulat (*integer*) dengan operasi + dan ·

4. $<Z_n, \oplus>$: grup dengan himpunan *integer* modulo *n*, yaitu $Z_n = \{0, 1, 2, \ldots, n-1\}$ dan $\oplus$ adalah operasi penjumlahan modulo *n*.

Contoh: n = 5, $Z_n = \{0, 1, 2, 3, 4\}$, $(3 \oplus 4) = (3 + 4) \bmod 5 = 2$

$<Z_p, \oplus>$ **:** grup dengan himpunan *integer* modulo *p*, *p* adalah bilangan prima, yaitu $Z_p = \{0, 1, 2, \ldots, p-1\}$ dan $\oplus$ adalah operasi penjumlahan modulo *p*.

$<Z^*_p, \otimes>$ **:** dengan himpunan integer bukan nol, *p* adalah bilangan prima, yaitu $Z^*_p = \{1, 2, \ldots, p-1\}$ dan $\otimes$ adalah operasi perkalian modulo *p*.

- Sebuah grup <G, *> dikatakan grup komutatif atau grup abelian (atau disingkat abelian saja) jika berlaku aksioma komutatif $a * b = b * a$ untuk semua $a, b \in G$.

- <R, +> dan <R, ·> adalah abelian
- <Z, +> dan <Z, ·> adalah abelian

- tetapi, <M, $\times$>, dengan M adalah himpunan matriks 2 x 2 dengan determinan $\neq 0$ bukan abelian (tanya kenapa?)

Ket: Abelian diambil dari kata “abel”, untuk menghormati Niels Abel, seorang Matematikawan Norwegia (1802 – 1829)

Niels Henrik Abel (5 August 1802 – 6 April 1829) was a Norwegian mathematician who made pioneering contributions in a variety of fields. His most famous single result is the first complete proof demonstrating the impossibility of solving the general quintic equation in radicals. This question was one of the outstanding open problems of his day, and had been unresolved for 250 years. He was also an innovator in the field of elliptic functions, discoverer of Abelian functions. Despite his achievements, Abel was largely unrecognized during his lifetime; he made his discoveries while living in poverty and died at the age of 26.

Most of his work was done in six or seven years of his working life.[1] Regarding Abel, the French mathematician Charles Hermite said: "Abel has left mathematicians enough to keep them busy for five hundred years."[1][2] Another French mathematician, Adrien-Marie Legendre, said: "*quelle tête celle du jeune Norvégien!*" ("what a head the young Norwegian has!").[3]

Born	5 August 1802 Nedstrand, Norway
Died	6 April 1829 (aged 26) Froland, Norway
Residence	Norway
Nationality	Norwegian
Fields	Mathematics
Alma mater	Royal Frederick University
Known for	Abel's binomial theorem Abelian category Abelian variety Abelian variety of CM-type Abel equation Abel equation of the first kind Abelian extension Abel function Abelian group Abel's identity Abel's inequality Abel's irreducibility theorem Abel–Jacobi map Abel–Plana formula Abel–Ruffini theorem Abelian means Abel's summation formula Abel's theorem Abel transform Abel transformation Abelian variety Dual abelian variety

Sumber: Wikipedia

Medan (*Field*)

- Medan (*field*) adalah system aljabar yang terdidi dari
  - himpunan elemen (disimbolkan dengan F)
  - operasi biner, yaitu penjumlahan (+) dan perkalian (·).

- Sebuah struktur aljabar <F, +, ·> disebut medan jika dan hanya jika:
  1. <F, +> adalah grup abelian
  2. <F – {0}, ·> adalah grup abelian
  3. Operasi · menyebar terhadap operasi + (sifat distributif)

     Distributif: $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$

     $(x + y) \cdot z = (x \cdot z) + (y \cdot z)$

- Jadi, sebuah medan memenuhi aksioma: *closure*, komutatif, asosiatif, dan distributif

- Contoh medan:

  - medan bilangan bulat, <Z, +, .>

  - medan bilangan riil, <R, +, .>

  - medan bilangan rasional (p/q), <Q, +, .>

- Sebuah medan disebut berhingga (*finite field*) jika himpunannya memiliki jumlah elemen yang berhingga.

  Jika jumlah elemen di dalam himpunan adalah *n*, maka notasinya F_n

  Contoh: F_2 adalah medan dengan elemen 0 dan 1

- Medan berhingga sering dinamakan juga Galois Field, untuk menghormati Evariste Galois, seorang matematikawan Perancis (1811 – 1832)

Evariste Galois

Born	25 October 1811 Bourg-la-Reine, French Empire
Died	31 May 1832 (aged 20) Paris, Kingdom of France
Nationality	French
Fields	Mathematics
Known for	Work on the theory of equations and Abelian integrals

Medan Berhingga F_p

- Kelas medan berhingga yang penting adalah F_p , dengan p adalah bilangan prima.

- F_p adalah adalah medan berhingga dengan himpunan bilangan bulat {0, 1, 2, …, p – 1}, *p* bilangan prima, dan dua operasi yang didefinisikan sbb:

1. Penjumlahan, dilakukan dalam modulus p

Jika a, b $\in$ $F_{p,}$ maka a + b = r, yang dalam hal ini

r = (a + b) mod p, $0 \leq r \leq p - 1$

2. Perkalian, dilakukan dalam modulus p

Jika a, b $\in$ $F_{p,}$ maka a $\cdot$ b = s, yang dalam hal ini

s = (a $\cdot$ b) mod p, $0 \leq s \leq p - 1$

Contoh: F_{23} mempunyai anggota {0, 1, 2, …, 22}.

Contoh operasi aritmetika di dalam F_{23}:

$12 + 20 = 9$ (karena $12 + 20 = 32 \bmod 23 = 9$)

$8 \cdot 9 = 3$ (karena $8 \times 9 = 72 \bmod 23 = 3$)

Medan Galois (*Galois Field*)

- Medan Galois adalah medan berhingga dengan p^m elemen, p adalah bilangan prima dan $m \geq 1$.
- Notasi: $GF(p^m)$
- Kasus paling sederhana: bila $m = 1 \rightarrow GF(p)$ atau F_p
- GF(p) terdiri dari himpunan {0, 1, 2, …, $p - 1$} dan operasi penjumlahan dan perkalian dilakukan di dalam modulus p.

1. Penjumlahan, dilakukan dalam modulus p

Jika $a, b \in GF(p)$, maka $a + b = r$, yang dalam hal ini $r = (a + b) \bmod p$, $0 \leq r \leq p - 1$

2. Perkalian, dilakukan dalam modulus p

Jika $a, b \in GF(p)$, maka $a \cdot b = s$, yang dalam hal ini $s = (a \cdot b) \bmod p$, $0 \leq s \leq p - 1$

$p = 2 \rightarrow$ *GF*(2):

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

$p = 3 \rightarrow$ *GF*(3):

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

- Contoh: Bentuklah tabel perkalian untuk GF(11), kemudian tentukan solusi untuk $x^2 \equiv 5 \pmod{11}$

·	0	1	2	3	(4)	5	6	(7)	8	9	10
0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10
2	0	2	4	6	8	10	1	3	5	7	9
3	0	3	6	9	1	4	7	10	2	5	8
(4)	0	4	8	1	5	9	2	6	10	4	7
5	0	5	10	4	9	3	8	2	7	1	6
6	0	6	1	7	2	8	3	9	4	10	5
(7)	0	7	3	10	6	2	9	5	1	8	4
8	0	8	5	2	10	7	4	1	9	6	3
9	0	9	7	5	3	1	10	8	6	4	2
10	0	10	9	8	7	6	5	4	3	2	1

$x^2 \equiv 5 \pmod{11}$

Maka:

$x^2 = 16 \rightarrow x_1 = 4$

$x^2 = 49 \rightarrow x_2 = 7$

Cara lain: cari elemen diagonal = 5, lalu ambil elemen mendatar atau elemen Vertikalnya (dilingkari).

Sumber: Andreas Steffen, Elliptic Curve Cryptography

Galois Field GF(2^m)

- Dari GF(p^m), jika p = 2, maka GF(2^m) disebut juga medan berhingga biner.
- GF(2^m) atau $F_2{}^m$ adalah ruang vektor berdimensi *m* pada GF(2). Setiap elemen di dalam GF(2^m) adalah integer dalam representasi biner sepanjang maksimal *m* bit.

  Contoh: GF(2^4), GF(2^8), dst
- String biner $b_{m-1}b_{m-2} \ldots b_1b_0$, $b_i \in \{0,1\}$, dapat dinyatakan sebagai polinom

  $$b_{m-1}x^{m-1} + b_{m-2}x^{m-2} + \ldots + b_1x + b_0$$

- Jadi, setiap a $\in$ GF(2^m) dapat dinyatakan sebagai

  $$b_{m-1}x^{m-1} + b_{m-2}x^{m-2} + \ldots + b_1x + b_0$$

- Contoh: 1101 di dalam GF(2^4) dapat dinyatakan sebagai polinom $x^3 + x^2 + 1$

  01010111 di dalam GF(2^8) dapat dinyatakan sebagai polinom $x^6 + x^4 + x^2 + x + 1$

Operasi aritmetika pada GF(2^m)

Misalkan a = (a_{m-1}..a_1 a_0) dan b = (b_{m-1}...b_1 b_0)$\in$ GF(2^m)

- **Penjumlahan:**

  a + b = c = (c_{m-1}..c_1 c_0), yang dalam hal ini c_i = (a_i + b_i) mod 2, c $\in$ GF(2^m)

- **Perkalian**: a $\cdot$ b = c = (c_{m-1}..c_1 c_0), yang dalam hal ini c adalah sisa pembagian polinom a(x) $\cdot$ b(x) dengan *irreducible polynomial* derajat m, c $\in$ GF(2^m).

Note: Sebuah polinom dikatakan tidak dapat direduksi (*irreducible polynomial*) jika ia tidak dapat dinyatakan sebagai perkalian dari dua buah polinom lain (kecuali perkalian dengan 1 dan dirinya sendiri).
Polinom $x^2 + 1$ dan $x^4 + x + 1$ adalah *irreducible* di dalam $GF(2^m)$,
tetapi polinom $x^5 + x^2 + x + 1$ *reducible* karena $x^5 + x^2 + x + 1 = (x^5 + x^2 + 1) \cdot (x^2 + 1)$

Contoh 1: Misalkan a = 00001101 = $x^3 + x^2 + 1$ dan b = 00000110 = $x^2 + x$

a dan b $\in$ GF(2^8) (dalam notasi Hex, a = '0D' dan b = '06')

(i) a + b = '0D' + '06' = $(x^3 + x^2 + 1) + (x^2 + x) = x^3 + 2x^2 + x + 1$ (mod 2)

Bagi tiap koefisien dengan 2, lalu ambil sisanya

$= x^3 + 0x^2 + x + 1$

$= x^3 + x + 1$ = 00001011 = '0B'

Dalam representasi biner:

00001101

00000110 +

00001011 → sama dengan hasil operasi XOR

∴ a + b = 00001011 = a XOR b

Contoh 2: Misalkan a = 01010111 = $x^6 + x^4 + x^2 + x + 1$ dan b = 10000011 = $x^7 + x + 1$

a dan b $\in$ GF(2^8) (dalam notasi Hex, a = ’57’ dan b = ’83’)

(i) a + b = ’57’ + ’83’ = $(x^6 + x^4 + x^2 + x + 1) + (x^7 + x + 1)$

$= x^7 + x^6 + x^4 + x^2 + x + 2 \pmod 2$

Bagi tiap koefisien dengan 2, lalu ambil sisanya

$= x^7 + x^6 + x^4 + x^2 + x + 0$

$= x^7 + x^6 + x^4 + x^2 + x$ = 11010100 = ‘D4’

Dalam representasi biner:

01010111

10000011 +

11010100 → sama dengan hasil operasi XOR

∴ a + b = 11010100 = a XOR b

(ii) $a \cdot b = (x^6 + x^4 + x^2 + x + 1) \cdot (x^7 + x + 1)$

$= x^{13} + x^7 + x^6 + x^{11} + x^5 + x^4 + x^9 + x^3 + x^2 + x^8 + x^2 + x + x^7 + x + 1 \pmod 2$

$= x^{13} + x^{11} + x^9 + x^8 + 2x^7 + x^6 + x^5 + x^4 + x^3 + 2x^2 + 2x + 1 \pmod 2$

$= x^{13} + x^{11} + x^9 + x^8 + 0x^7 + x^6 + x^5 + x^4 + x^3 + 0x^2 + 0x + 1$

$= x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1$

Karena m = 8, maka hasil perkalian di atas direduksi menjadi derajat < 8 oleh *irreducible polynomial* .

Contoh, algoritma Rijndael (AES) beroperasi dalam GF(2^8) dan menggunakan *irreducible polynomial* $f(x) = x^8 + x^4 + x^3 + x + 1$

$x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1 \pmod{f(x)} = x^7 + x^6 + 1 = 11000001$

$\therefore a \cdot b = 11000001 =$ ‘C1’

$$
\begin{array}{r|l}
 & x^5 + x^3 + \\
\hline
x^8 + x^4 + x^3 + x + 1 & x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1 \\
 & x^{13} \quad + x^9 + x^8 + x^6 + x^5 \\
\hline
 & x^{11} + \quad + x^4 + x^3 + 1 \\
 & x^{11} + \quad x^7 + x^6 + x^4 + x^3 \\
\hline
 & x^7 + x^6 \quad + 1
\end{array}
$$

Sisa pembagian

Jadi, $x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1 \pmod{f(x)} = x^7 + x^6 + 1 = 11000001$

Contoh 3: $a \cdot b = (x^3 + x^2 + 1) \cdot (x^2 + x) = x^5 + 2x^4 + x^3 + x^2 + x \pmod 2$

$= x^5 + x^3 + x^2 + x = 10110$

Karena m = 4 hasilnya direduksi menjadi derajat < 4 oleh sebuah *irreducible polynomial* $f(x) = x^4 + x + 1$

Proses pembagiannya ditunjukkan sebagai berikut:

$$
\begin{array}{r|l}
 & x \\
\hline
x^4 + x + 1 & x^5 + x^3 + x^2 + x \\
 & \underline{x^5 + \quad x^2 + x \; +} \\
 & x^3 \quad \rightarrow \text{ sisa pembagian}
\end{array}
$$

Jadi, $(x^5 + x^3 + x^2 + x) \bmod f(x) = x^3 = 1000$

$\therefore\ a \cdot b = 1000$

BERSAMBUNG