Elliptic Curve Cryptography

Outlines

- Introduction
- Definitions of elliptic curve cryptography
- Elliptic curve families and their operations
- Security over elliptic curve
- Cryptosystems over elliptic curve

Introduction

- ECC was introduced by V. Miller and N. Koblitz in 1985.
- ECC requires smaller key size compared with DSA, RSA under the same level of security.
- Smaller key size helps for faster computations and less storage space.
- ECC is suitable for applications with limited computing power and insufficient storage space such as PDAs, cellular phones and smart cards.

Introduction (Cont.)

Comparable Key Sizes for Equivalent Security

ECC-based scheme	RSA/DSA
112	512
160	1024
224	2048
256	3072
384	7680
512	15360

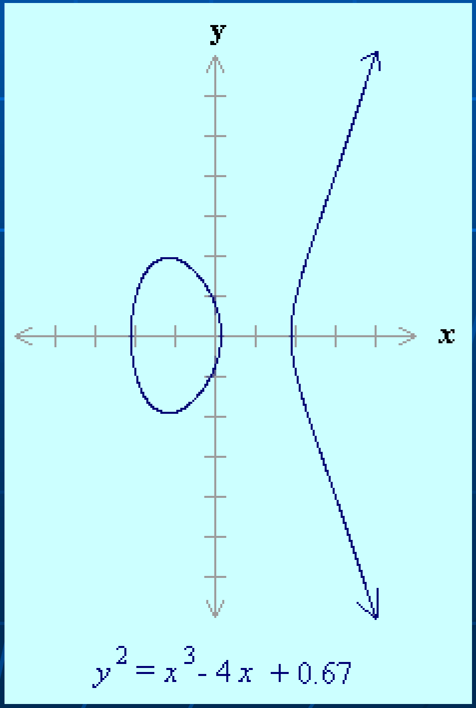
Definition of Elliptic Curves

- An elliptic curve is defined as the set of points (x, y) which satisfy an elliptic curve equation of the form

$$y^2 = x^3 + ax + b$$

where $(x, y, a, b) \in R$.

- If $4a^3 + 27b^2 \neq 0$, then $E: y^2 = x^3 + ax + b$ can be used to form a group.

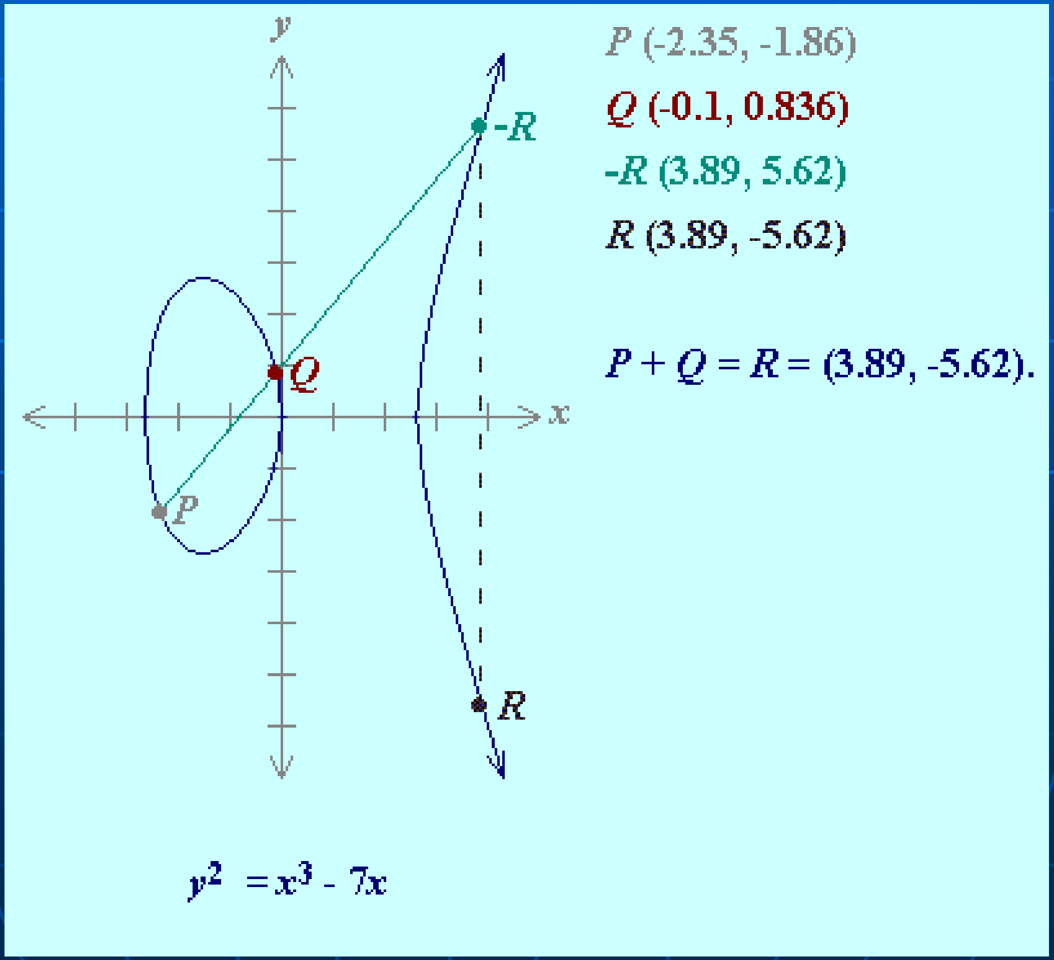


Definition of Elliptic Curves (Cont. 1)

- A point G over E, called the base point.
- A special point, O, called the point at infinity.
- The additive identity of the group operation is the point O; all elliptic curves have an additive identity.
- The negative of a point $P = (x, y)$ is its reflection in the x-axis: the point $-P = (x, -y)$.
- For each point P over E, the point $-P$ is also over E.
- If n is the smallest integer and $nP = O$, then n is the order of P over E.

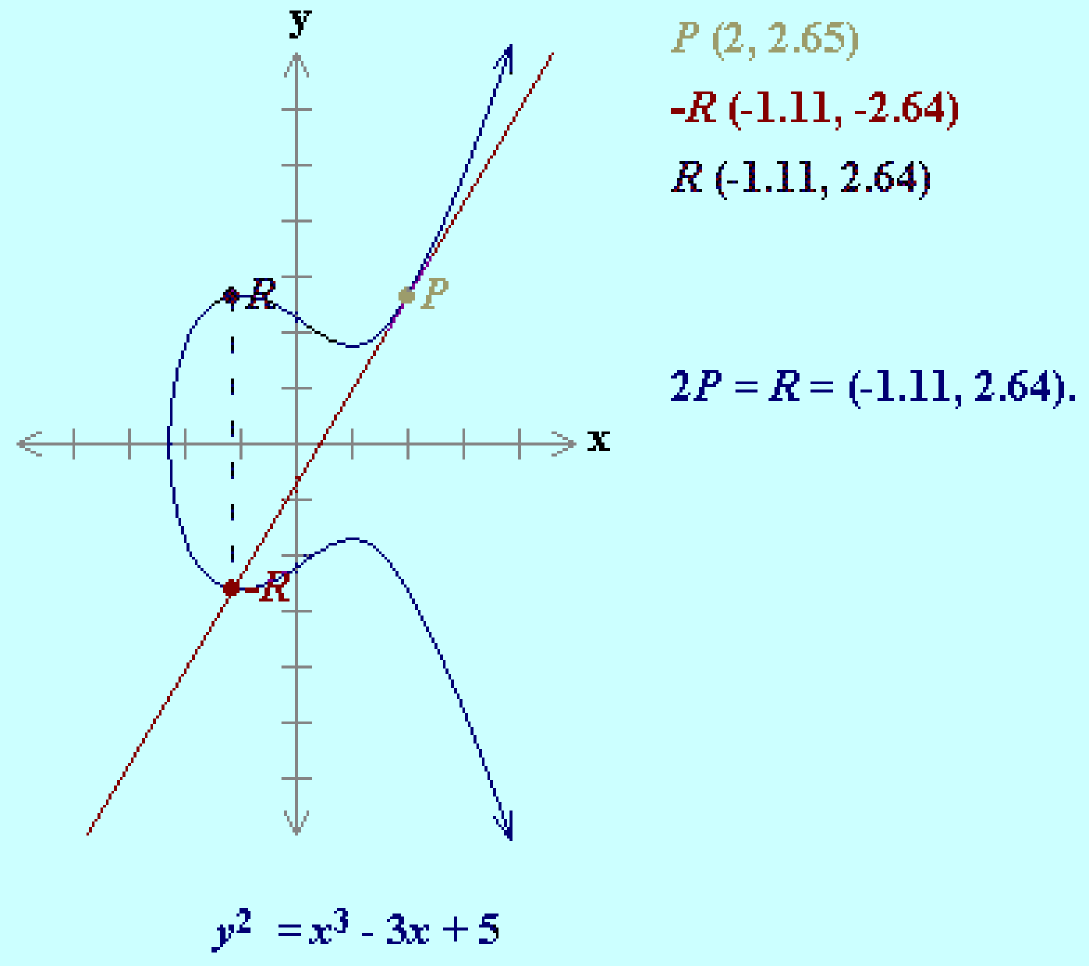
Definition of Elliptic Curves (Cont. 2)

- **Adding distinct points *P* and *Q* ($P \neq -Q$)**
- ***P* + *Q* = *R***



Definition of Elliptic Curves (Cont. 3)

- **Doubling the point *P***
- ***P + P = 2P = R***



Definition of Elliptic Curves (Cont. 4)

- ECC addition is analog of modulo multiplication.
- ECC repeated addition (doubling) is analog of modulo exponentiation.

$$v_i = g^{h(t_i \| ID_i)} \bmod p \Rightarrow V_i = h(t_i \| ID_i)G$$

$$y_i = v_i h(ID_i)^{-1} g^{k_i} \bmod p \Rightarrow Y_i = (h(ID_i)^{-1} \bmod q)(V_i + k_i G)$$

Elliptic Curve Families

- **Commonly used family:**
  - Prime curves $E_p(a, b)$ defined over Z_p

    $y^2 \equiv x^3 + ax + b \pmod{p}$ where $4a^3 + 27b^2 \neq 0$

    - use integers modulo a prime p
    - suitable for software
  - Binary curves $E_{2^m}(a, b)$ defined over $GF(2^m)$

    $y^2 + xy = x^3 + ax^2 + b$ where $a, b \in GF(2^m)$ and $b \neq 0$

    - use polynomials with binary coefficients
    - suitable for hardware

Operations on Elliptic Curve over GF(p)

P and Q be two points $\in E(F_p)$ and O is the point at infinity.

- $P + O = O + P = P$
- If $P = (x, y)$ then $-P = (x, -y)$ and $P + (-P) = O$.
- If $P = (x_1, y_1)$ and $Q = (x_2, y_2)$, and $(P, Q) \neq O$, then $P + Q = (x_3, y_3)$ where

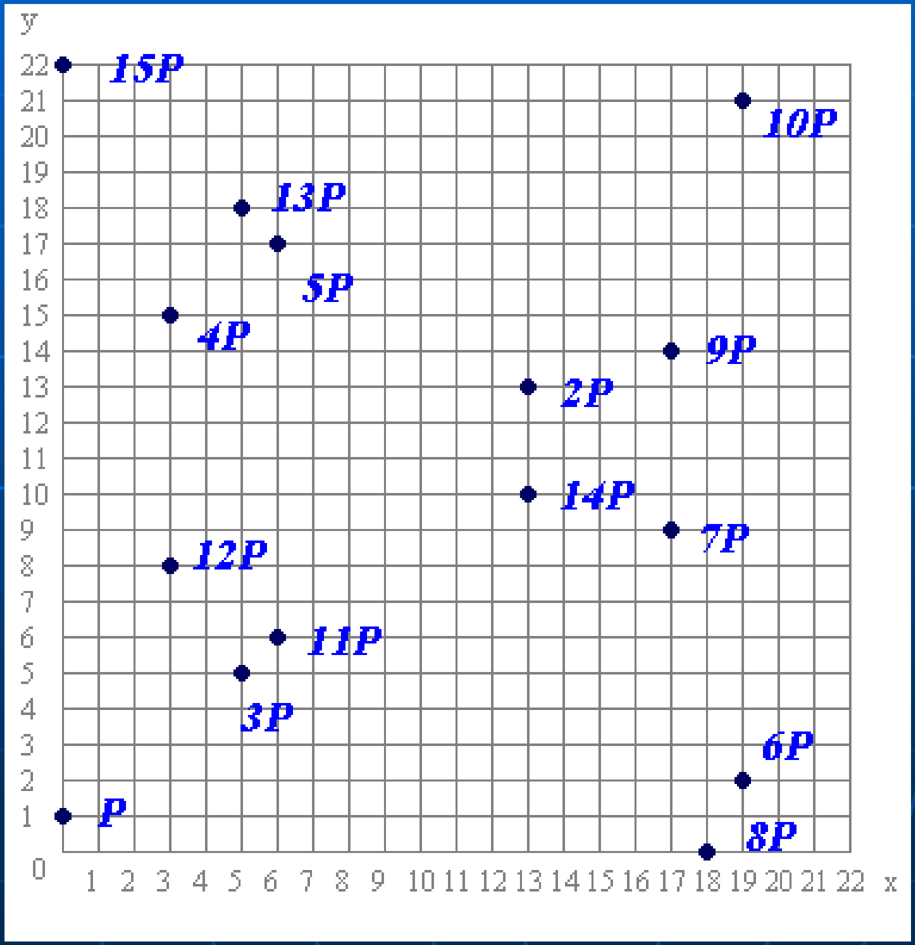
$$x_3 = \lambda^2 - x_1 - x_2 \qquad y_3 = \lambda(x_1 - x_3) - y_1$$

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{if } P \neq Q \\[2ex] \dfrac{3{x_1}^2 + a}{2y_1} & \text{if } P = Q \end{cases}$$

Operations on Elliptic Curve over GF(p) (Cont.)

$E(F_{23})$: $y^2 = x^3 + 12x + 1$

$P = (0, 1)$



Operations on Elliptic Curve over GF(2^m)

P and Q be two points $\in E(F_p)$ and O is the point at infinity.

- $P + O = O + P = P$
- If $P = (x, y)$ then $-P = (x, -y)$ and $P + (-P) = O$.
- If $P = (x_1, y_1)$ and $Q = (x_2, y_2)$, and $(P, Q) \neq O$, then $P + Q = (x_3, y_3)$ where

$$x_3 = \begin{cases} \left(\dfrac{y_1 + y_2}{x_1 + x_2}\right)^2 + \dfrac{y_1 + y_2}{x_1 + x_2} + x_1 + x_2 + a \text{ if } P \neq Q \\ {x_1}^2 + \dfrac{b}{{x_1}^2} \quad \text{if } P = Q \end{cases}$$

$$y_3 = \begin{cases} \left(\dfrac{y_1 + y_2}{x_1 + x_2}\right)(x_1 + x_3) + x_3 + y_1 \text{ if } P \neq Q \\ {x_1}^2 + \left(x_1 + \dfrac{y_1}{x_1}\right)x_3 + x_3 \quad \text{if } P = Q \end{cases}$$

Security over Elliptic Curves

- **Elliptic Curve Discrete Logarithm Problem (ECDLP)**

  For every probabilistic polynomial-time algorithm A, every positive polynomial $P(\cdot)$ and all sufficiently large k, s.t. $Q = nB$ and

  $$\Pr[A(i, B, Q) = n : i \leftarrow K(1^k);\ Q, B \leftarrow G_1] \leq 1/P(k).$$

Security over Elliptic Curves (Cont. 1)

- **Bilinear Diffie-Hellman Problem (BDHP)**

  For every probabilistic polynomial-time algorithm A, every positive polynomial $P(\cdot)$ and all sufficiently large k, s.t.

$$\Pr[A(i, B, aB, bB, cB) = e(B, B)^{abc} : i \leftarrow K(1^k);\ a, b, c \leftarrow Z_q^*;\ B, aB, bB, cB \leftarrow G_1] \leq 1/P(k).$$

Security over Elliptic Curves (Cont. 2)

- **Computational Diffie-Hellman Problem (CDHP)**

  For every probabilistic polynomial-time algorithm A, every positive polynomial $P(\cdot)$ and all sufficiently large k, s.t.

$$\mathbf{Pr}[A(i, B, aB, bB) = abB: i \leftarrow K(1^k);\ a, b \leftarrow Z_q^*;\ B, aB, bB \leftarrow G_1] \leq 1/P(k).$$

Security over Elliptic Curves (Cont. 3)

- **Decisional Diffie-Hellman Problem (DDHP)**

  For every probabilistic polynomial-time algorithm A, every positive polynomial $P(\cdot)$ and all sufficiently large k, s.t.

$$\left| \Pr\left(A(i, B, aB, bB, cB : i \leftarrow K(1^k), (a, b, c) \leftarrow Z_q^*, (B, aB, bB, cB) \leftarrow G_1) = 1\right) - \Pr\left(A(i, B, aB, bB, abB : i \leftarrow K(1^k), (a, b) \leftarrow Z_q^*, (B, aB, bB, abB) \leftarrow G_1) = 1\right) \right| \leq 1/P(k)$$

Security over Elliptic Curves (Cont. 4)

- **Gap Diffie-Hellman Problem (GDHP)**

  For every probabilistic polynomial-time algorithm A, every positive polynomial $P(\cdot)$ and all sufficiently large k, s.t.

$$\Pr[A(i, B, aB, bB) = abB: i \leftarrow K(1^k); a, b, c \leftarrow Z_q^*; B, aB, bB, cB \leftarrow G_1] \leq 1/P(k)$$ and

$$|\Pr(A(i, B, aB, bB, cB: i \leftarrow K(1^k); a, b, c \leftarrow Z_q^*; B, aB, bB, cB \leftarrow G_1) = 1) - \Pr(A(i, B, aB, bB, abB: i \leftarrow K(1^k); a, b \leftarrow Z_q^*; B, aB, bB, abB \leftarrow G_1) = 1)| \geq 1/P(k).$$

Koblitz's Cryptosystem over EC

- **Notations:**

  d: private key

  Q: public key s.t. $Q = dG$ over E

- **Encryption:**

  Note: M has to be a point on $E(K)$.

  $M = (m_x, m_y)$ over $E(K)$
  $C_1 = wG$ where w is a random number
  $C_2 = M + wQ$
  $\mathrm{E}_Q(M) = (C_1, C_2)$

- **Decryption:**

  $M = (m_x, m_y) = C_2 - dC_1$

The Menezes-Vanston Cryptosystem over EC

- **Notations:**

  d: private key

  Q: public key s.t. $Q = dG$ over E

- **Encryption:**

  Note: M does not necessary to be a point on $E(K)$.

  $M = (m_x, m_y)$

  $R = wG$ where w is a random number

  $(a, b) = wQ$

  $(c_1, c_2) = (a \cdot m_x \bmod p, b \cdot m_y \bmod p)$

  $\mathrm{E}_Q(M) = (R, c_1, c_2)$

- **Decryption:**

  $(a, b) = dR$

  $M = (m_x, m_y) = (c_1 \cdot a^{-1} \bmod p, c_2 \cdot b^{-1} \bmod p)$

Jurisic-Menezes's Signature Scheme over EC

- **Notations:**

  d: private key

  Q: public key s.t. $Q = dG$ over E

- **Signing:**

  $(x_1, y_1) = wG$
  $r = x_1 \bmod q$
  $s = w^{-1}(h(M) + dr) \bmod q$
  $S_d(M) = (r, s)$

- **Verifying:**

  $(x_1, y_1) = (h(M)s^{-1} \bmod q)G + (rs^{-1} \bmod q)Q$
  Accept iff $r = x_1 \bmod q$