Elliptic Curves

Definition

The set of points (x,y), satisfying the equality

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

with

$$4a^3 + 27b^2 \neq 0$$

is called an *elliptic curve*. a, b, and the variables x and y are elements of the same algebraic structure M.

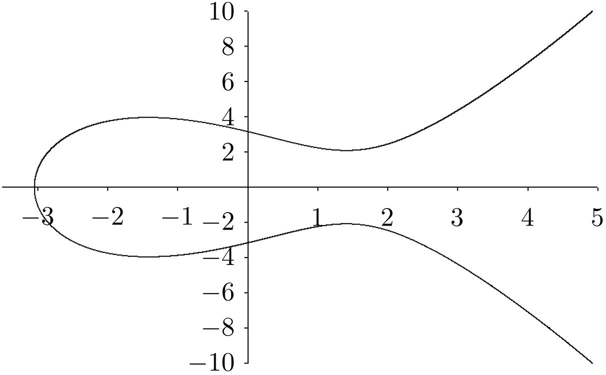
- Some point ∞ is included to form the neutral element.
- a and b are called parameters of the elliptic curve.

Elliptic Curves over the Reals

- Simple graphical representation of the curve
- Graphical representation of addition and doubling of points

Elliptic Curves over the Reals

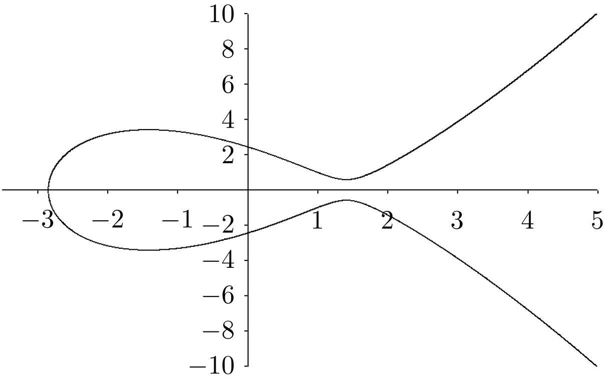
- Simple graphical representation of the curve
- Graphical representation of addition and doubling of points



$$y^2 = x^3 - 6x + 10$$

Elliptic Curves over the Reals

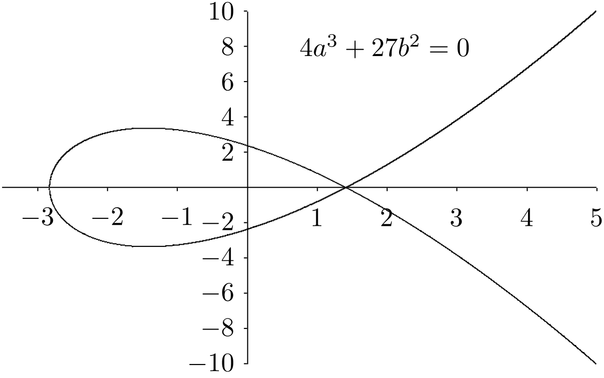
- Simple graphical representation of the curve
- Graphical representation of addition and doubling of points



$$y^2 = x^3 - 6x + 6$$

Elliptic Curves over the Reals

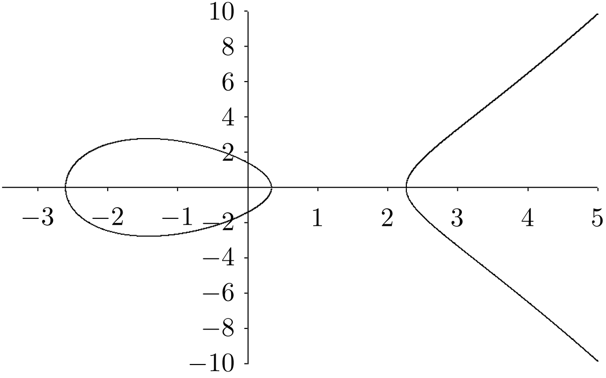
- Simple graphical representation of the curve
- Graphical representation of addition and doubling of points



$$y^2 = x^3 - 6x + 5.657$$

Elliptic Curves over the Reals

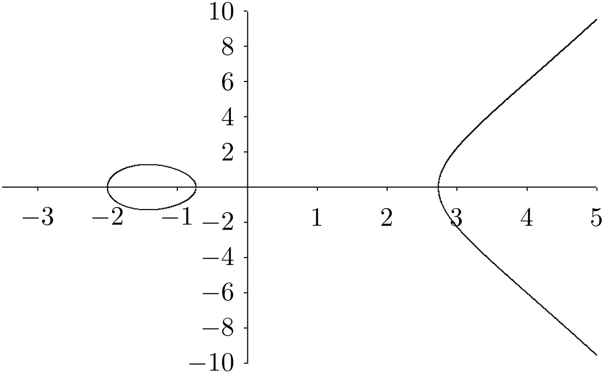
- Simple graphical representation of the curve
- Graphical representation of addition and doubling of points



$$y^2 = x^3 - 6x + 2$$

Elliptic Curves over the Reals

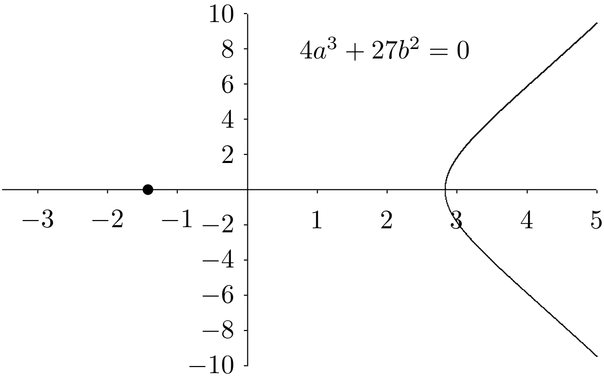
- Simple graphical representation of the curve
- Graphical representation of addition and doubling of points



$$y^2 = x^3 - 6x - 4$$

Elliptic Curves over the Reals

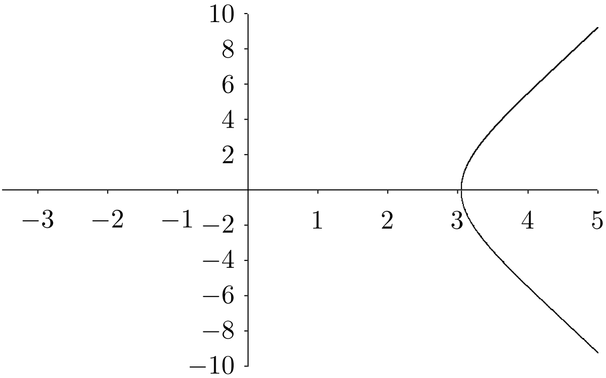
- Simple graphical representation of the curve
- Graphical representation of addition and doubling of points



$$y^2 = x^3 - 6x - 5.657$$

Elliptic Curves over the Reals

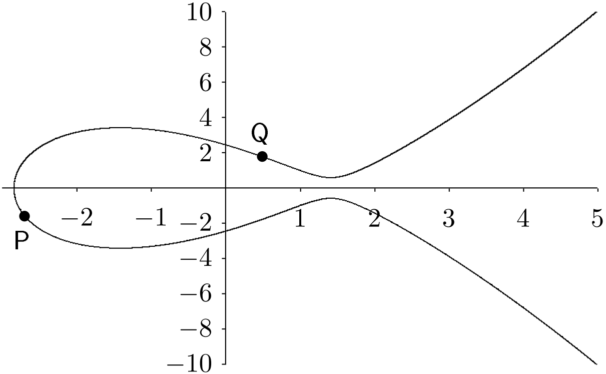
- Simple graphical representation of the curve
- Graphical representation of addition and doubling of points



$$y^2 = x^3 - 6x - 10$$

Elliptic Curves over the Reals

Graphical Representation of Addition

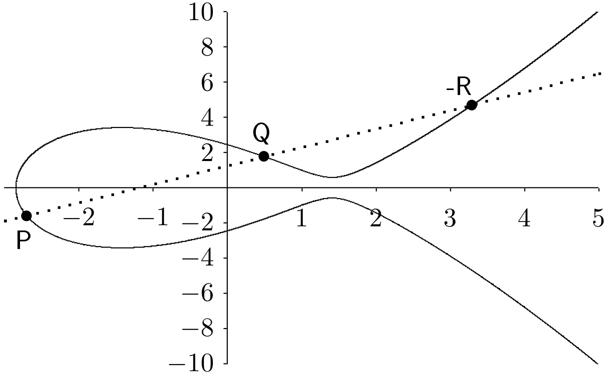


$$y^2 = x^3 - 6x + 6$$

Elliptic Curves over the Reals

Graphical Representation of Addition

- Define a line through P and Q.
- The third intersecting point on the curve is -R.

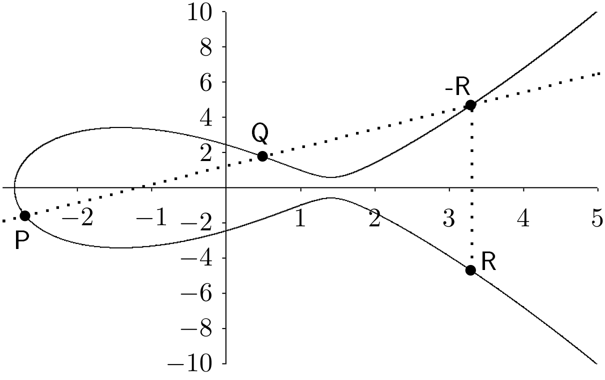


$$y^2 = x^3 - 6x + 6$$

Elliptic Curves over the Reals

Graphical Representation of Addition

- Define a line through P and Q.
- The third intersecting point on the curve is -R.
- Mirror the point $-R$ at the x-axis to obtain R = P + Q.

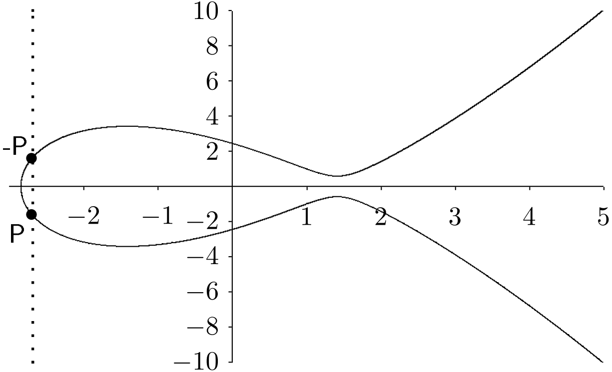


$$y^2 = x^3 - 6x + 6$$

Elliptic Curves over the Reals

Graphical Representation of Addition

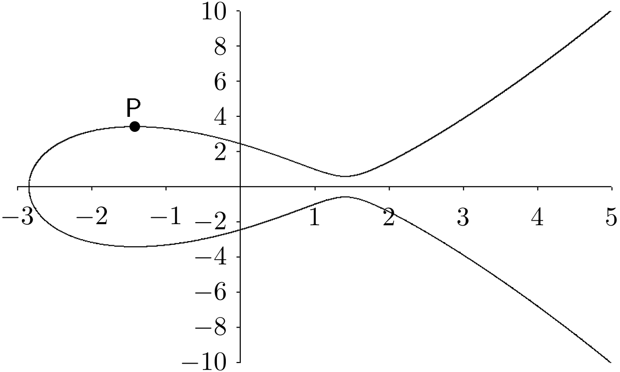
- Special case $P + (-P) = \infty$
- ∞ is the neutral element w.r.t. addition of points.



$$y^2 = x^3 - 6x + 6$$

Elliptic Curves over the Reals

Graphically doubling a point, $P + P$

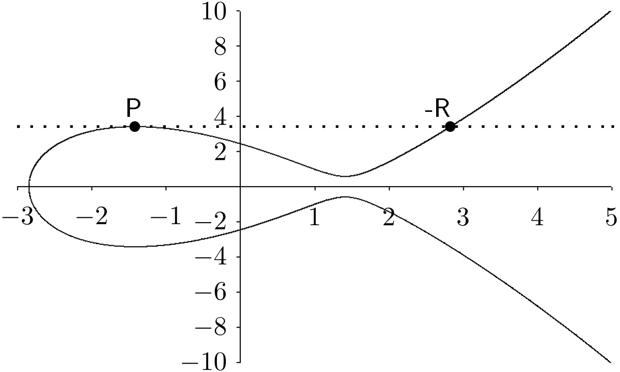


$$y^2 = x^3 - 6x + 6$$

Elliptic Curves over the Reals

Graphically doubling a point, $P + P$

- Draw the tangent line at the elliptic curve in P.
- The second intersecting point of the tangent line defines $-R$.

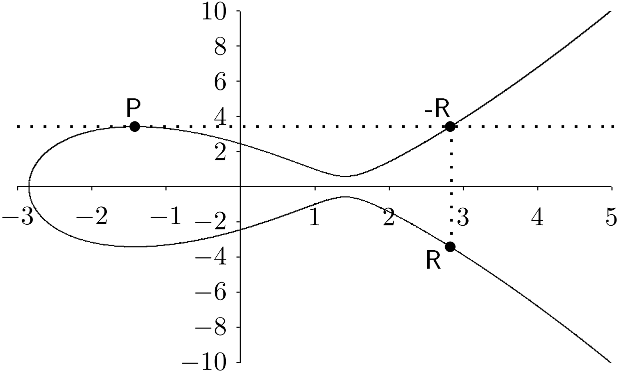


$$y^2 = x^3 - 6x + 6$$

Elliptic Curves over the Reals

Graphically doubling a point, $P + P$

- Draw the tangent line at the elliptic curve in P.
- The second intersecting point of the tangent line defines $-R$.
- Mirror $-R$ at the x-axis to obtain R = 2P.

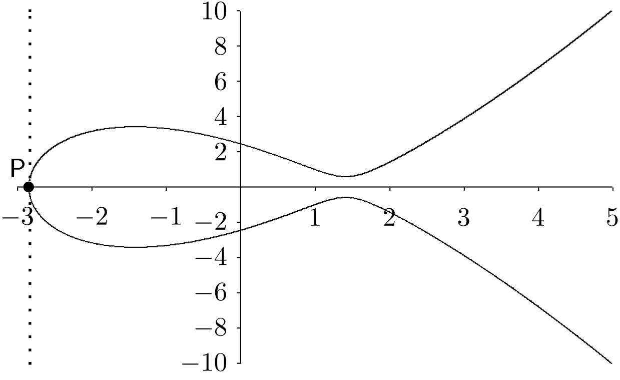


$$y^2 = x^3 - 6x + 6$$

Elliptic Curves over the Reals

Graphically doubling a point, $P + P$

- Special case $2P = \infty$, if $y_P = 0$



$$y^2 = x^3 - 6x + 6$$

Elliptic Curves over the Reals

Algebraic representation of addition

- $R = P + Q$ with $P \neq \pm Q$:

$$
\begin{aligned}
s &= \frac{y_P - y_Q}{x_P - x_Q} \\
x_R &= s^2 - x_P - x_Q \\
y_R &= -y_P + s(x_P - x_R)
\end{aligned}
$$

Elliptic Curves over the Reals
Algebraic representation of addition

- $R = P + Q$ with $P \neq \pm Q$:

$$s = \frac{y_P - y_Q}{x_P - x_Q}$$
$$x_R = s^2 - x_P - x_Q$$
$$y_R = -y_P + s(x_P - x_R)$$

- $P + (-P) = \infty$

Elliptic Curves over the Reals
Algebraic representation of addition

- $R = P + Q$ with $P \neq \pm Q$:

$$s = \frac{y_P - y_Q}{x_P - x_Q}$$
$$x_R = s^2 - x_P - x_Q$$
$$y_R = -y_P + s(x_P - x_R)$$

- $P + (-P) = \infty$
- $P + P \Rightarrow$ Doubling of points

Elliptic Curves over the Reals
Algebraic doubling of points

- $R = 2P$ with $y_P \neq 0$:

$$s = \frac{3x_P^2 + a}{2y_P}$$
$$x_R = s^2 - 2x_P$$
$$y_R = -y_P + s(x_P - x_R)$$

Elliptic Curves over the Reals
Algebraic doubling of points

- $R = 2P$ with $y_P \neq 0$:

$$s = \frac{3x_P^2 + a}{2y_P}$$
$$x_R = s^2 - 2x_P$$
$$y_R = -y_P + s(x_P - x_R)$$

- $2P = \infty$, if $y_P = 0$

Elliptic Curves over Finite Fields

Finite field $\mathbb{F}_p$

In cryptography elliptic curves over finite fields are used.

- Avoid floating point arithmetic.
- No rounding errors, essential for deciphering messages.

Elliptic Curves over Finite Fields

Finite field $\mathbb{F}_p$

In cryptography elliptic curves over finite fields are used.

- Avoid floating point arithmetic.
- No rounding errors, essential for deciphering messages.

Elliptic curves over $\mathbb{F}_p$

$y^2 = x^3 + ax + b \pmod{p}$ with a, b, x, y integers $\in \{0, 1, \ldots, p-1\}$

Elliptic Curves over Finite Fields

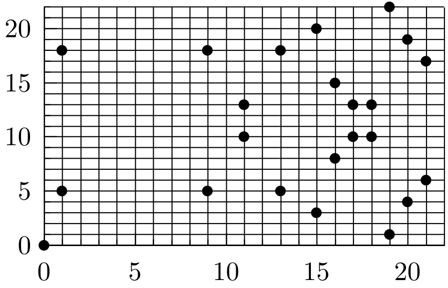
Finite field $\mathbb{F}_p$

In cryptography elliptic curves over finite fields are used.

- Avoid floating point arithmetic.
- No rounding errors, essential for deciphering messages.

Elliptic curves over $\mathbb{F}_p$

$y^2 = x^3 + ax + b \pmod{p}$ with a, b, x, y integers $\in \{0, 1, \ldots, p-1\}$



$y^2 = x^3 + x$ in $\mathbb{F}_{23}$

Elliptic Curves over Finite Fields

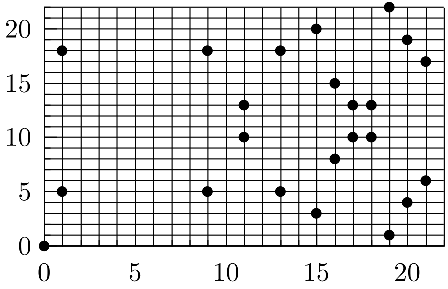
Finite field $\mathbb{F}_p$

In cryptography elliptic curves over finite fields are used.

- Avoid floating point arithmetic.
- No rounding errors, essential for deciphering messages.

Elliptic curves over $\mathbb{F}_p$

$y^2 = x^3 + ax + b \pmod{p}$ with a, b, x, y integers $\in \{0, 1, \ldots, p-1\}$



$y^2 = x^3 + x$ in $\mathbb{F}_{23}$

Algebraic Formulae as above with reduction modulo p

Elliptic Curves over Finite Fields

Finite field $\mathbb{F}_{p^k}$

Each $a \in \mathbb{F}_{p^k}$ is represented as coefficients $(a_{k-1}, \ldots, a_0) \in \{0, \ldots, p-1\}^k$ of a polynomial of order $k-1$:

$$f(x) = \sum_{i=0}^{k-1} a_i x^i = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \ldots + a_1 x + a_0$$

Elliptic Curves over Finite Fields

Finite field $\mathbb{F}_{p^k}$

Each $a \in \mathbb{F}_{p^k}$ is represented as coefficients $(a_{k-1}, \ldots, a_0) \in \{0, \ldots, p-1\}^k$ of a polynomial of order $k-1$:

$$f(x) = \sum_{i=0}^{k-1} a_i x^i = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \ldots + a_1 x + a_0$$

Definition

A polynomial $f_{irr}(x)$ is called irreducible over the field $\mathbb{F}_{p^k}$, if

- deg $f_{irr}(x) > 0$
- There is <u>no</u> factorization $f_{irr}(x) = g(x) \cdot h(x)$ with deg $g(x) > 0$ and deg $h(x) > 0$.

Elliptic Curves over Finite Fields

Finite field $\mathbb{F}_{p^k}$

Each $a \in \mathbb{F}_{p^k}$ is represented as coefficients $(a_{k-1}, \ldots, a_0) \in \{0, \ldots, p-1\}^k$ of a polynomial of order $k-1$:

$$f(x) = \sum_{i=0}^{k-1} a_i x^i = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \ldots + a_1 x + a_0$$

Definition

A polynomial $f_{irr}(x)$ is called irreducible over the field $\mathbb{F}_{p^k}$, if

- deg $f_{irr}(x) > 0$
- There is no factorization $f_{irr}(x) = g(x) \cdot h(x)$ with deg $g(x) > 0$ and deg $h(x) > 0$.

Elliptic curve over $\mathbb{F}_{p^k}$

$y^2 = x^3 + ax + b \pmod{f_{irr}}$ with a, b, x, y polynomials

Elliptic Curves over Finite Fields

Finite field $\mathbb{F}_{p^k}$

Each $a \in \mathbb{F}_{p^k}$ is represented as coefficients $(a_{k-1}, \ldots, a_0) \in \{0, \ldots, p-1\}^k$ of a polynomial of order $k-1$:

$$f(x) = \sum_{i=0}^{k-1} a_i x^i = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \ldots + a_1 x + a_0$$

Definition

A polynomial $f_{irr}(x)$ is called irreducible over the field $\mathbb{F}_{p^k}$, if

- deg $f_{irr}(x) > 0$
- There is no factorization $f_{irr}(x) = g(x) \cdot h(x)$ with deg $g(x) > 0$ and deg $h(x) > 0$.

Elliptic curve over $\mathbb{F}_{p^k}$

$y^2 = x^3 + ax + b \pmod{f_{irr}}$ with a, b, x, y polynomials

Algebraic formulae as above with reduction modulo f_{irr}

Diffie-Hellman Key Exchange

Cryptographic Framework

- Elliptic curve over the finite field $\mathbb{F}_{p^k}$
- Generator G of some cyclic subgroup of order n

User A   User B

Diffie-Hellman Key Exchange

Cryptographic Framework

- Elliptic curve over the finite field $\mathbb{F}_{p^k}$
- Generator G of some cyclic subgroup of order n

User A

User B

- selects an integer
  $k_A \in \{2, \ldots, n-1\}$ at random.

Diffie-Hellman Key Exchange

Cryptographic Framework

- Elliptic curve over the finite field $\mathbb{F}_{p^k}$
- Generator G of some cyclic subgroup of order n

User A

- selects an integer $k_A \in \{2, \ldots, n-1\}$ at random.
- $Q = k_A G$

User B

Diffie-Hellman Key Exchange

Cryptographic Framework

- Elliptic curve over the finite field $\mathbb{F}_{p^k}$
- Generator G of some cyclic subgroup of order n

User A

- selects an integer $k_A \in \{2, \ldots, n-1\}$ at random.
- $Q = k_A G$

User B

- selects an integer $k_B \in \{2, \ldots, n-1\}$ at random.

Diffie-Hellman Key Exchange

Cryptographic Framework

- Elliptic curve over the finite field $\mathbb{F}_{p^k}$
- Generator G of some cyclic subgroup of order n

User A

- selects an integer $k_A \in \{2, \ldots, n-1\}$ at random.
- $Q = k_A G$

User B

- selects an integer $k_B \in \{2, \ldots, n-1\}$ at random.
- $R = k_B G$

Diffie-Hellman Key Exchange

Cryptographic Framework

- Elliptic curve over the finite field $\mathbb{F}_{p^k}$
- Generator G of some cyclic subgroup of order n

User A

- selects an integer $k_A \in \{2, \ldots, n-1\}$ at random.
- $Q = k_A G$
- transmits point Q to user B.

User B

- selects an integer $k_B \in \{2, \ldots, n-1\}$ at random.
- $R = k_B G$
- transmits point R to user A.

Diffie-Hellman Key Exchange

Cryptographic Framework

- Elliptic curve over the finite field $\mathbb{F}_{p^k}$
- Generator G of some cyclic subgroup of order n

User A

- selects an integer $k_A \in \{2, \ldots, n-1\}$ at random.
- $Q = k_A G$
- transmits point Q to user B.
- $K = k_A R = k_A k_B G$

User B

- selects an integer $k_B \in \{2, \ldots, n-1\}$ at random.
- $R = k_B G$
- transmits point R to user A.

Diffie-Hellman Key Exchange

Cryptographic Framework

- Elliptic curve over the finite field $\mathbb{F}_{p^k}$
- Generator G of some cyclic subgroup of order n

User A

- selects an integer $k_A \in \{2, \dots, n-1\}$ at random.
- $Q = k_A G$
- transmits point Q to user B.
- $K = k_A R = k_A k_B G$

User B

- selects an integer $k_B \in \{2, \dots, n-1\}$ at random.
- $R = k_B G$
- transmits point R to user A.
- $K = k_B Q = k_A k_B G$

ElGamal Encryption over Elliptic Curves

Cryptographic Framework

- Elliptic curve over the finite field $\mathbb{F}_{p^k}$
- Generator G of some cyclic subgroup of order n

Private and public key of each user

Sender

Receiver

ElGamal Encryption over Elliptic Curves

Cryptographic Framework

- Elliptic curve over the finite field $\mathbb{F}_{p^k}$
- Generator G of some cyclic subgroup of order n

Private and public key of each user

- Each user selects an integer private key $d \in \{2, \dots, n-1\}$ at random.
- $Q = dG$ is the public key.

Sender | Receiver

ElGamal Encryption over Elliptic Curves

Cryptographic Framework

- Elliptic curve over the finite field $\mathbb{F}_{p^k}$
- Generator G of some cyclic subgroup of order n

Private and public key of each user

- Each user selects an integer private key $d \in \{2, \dots, n-1\}$ at random.
- $Q = dG$ is the public key.

Sender

- selects a random integer $k \in \{2, \dots, n-1\}$.

Receiver

RWTHAACHEN

ElGamal Encryption over Elliptic Curves

Cryptographic Framework

- Elliptic curve over the finite field $\mathbb{F}_{p^k}$
- Generator G of some cyclic subgroup of order n

Private and public key of each user

- Each user selects an integer private key $d \in \{2, \ldots, n-1\}$ at random.
- $Q = dG$ is the public key.

Sender	Receiver
selects a random integer $k \in \{2, \ldots, n-1\}$.	
$C_1 = kG$	
$C_2 = M + kQ$	

ElGamal Encryption over Elliptic Curves

Cryptographic Framework

- Elliptic curve over the finite field $\mathbb{F}_{p^k}$
- Generator G of some cyclic subgroup of order n

Private and public key of each user

- Each user selects an integer private key $d \in \{2, \dots, n-1\}$ at random.
- $Q = dG$ is the public key.

Sender

- selects a random integer $k \in \{2, \dots, n-1\}$.
- $C_1 = kG$
- $C_2 = M + kQ$

Receiver

- $M = C_2 - dC_1$