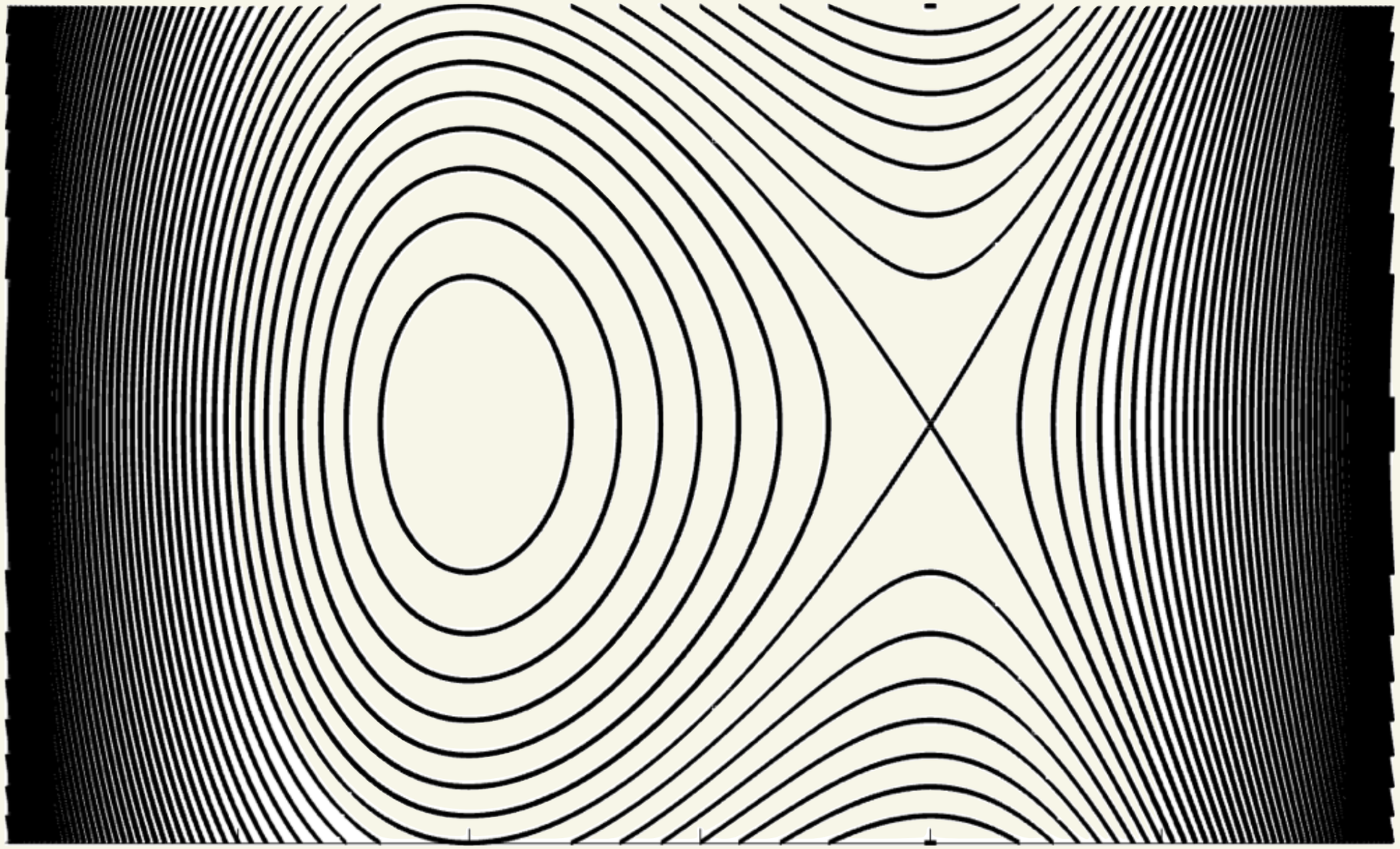
Dynamics through the lens of cryptography

Nalini Joshi
@monsoon0

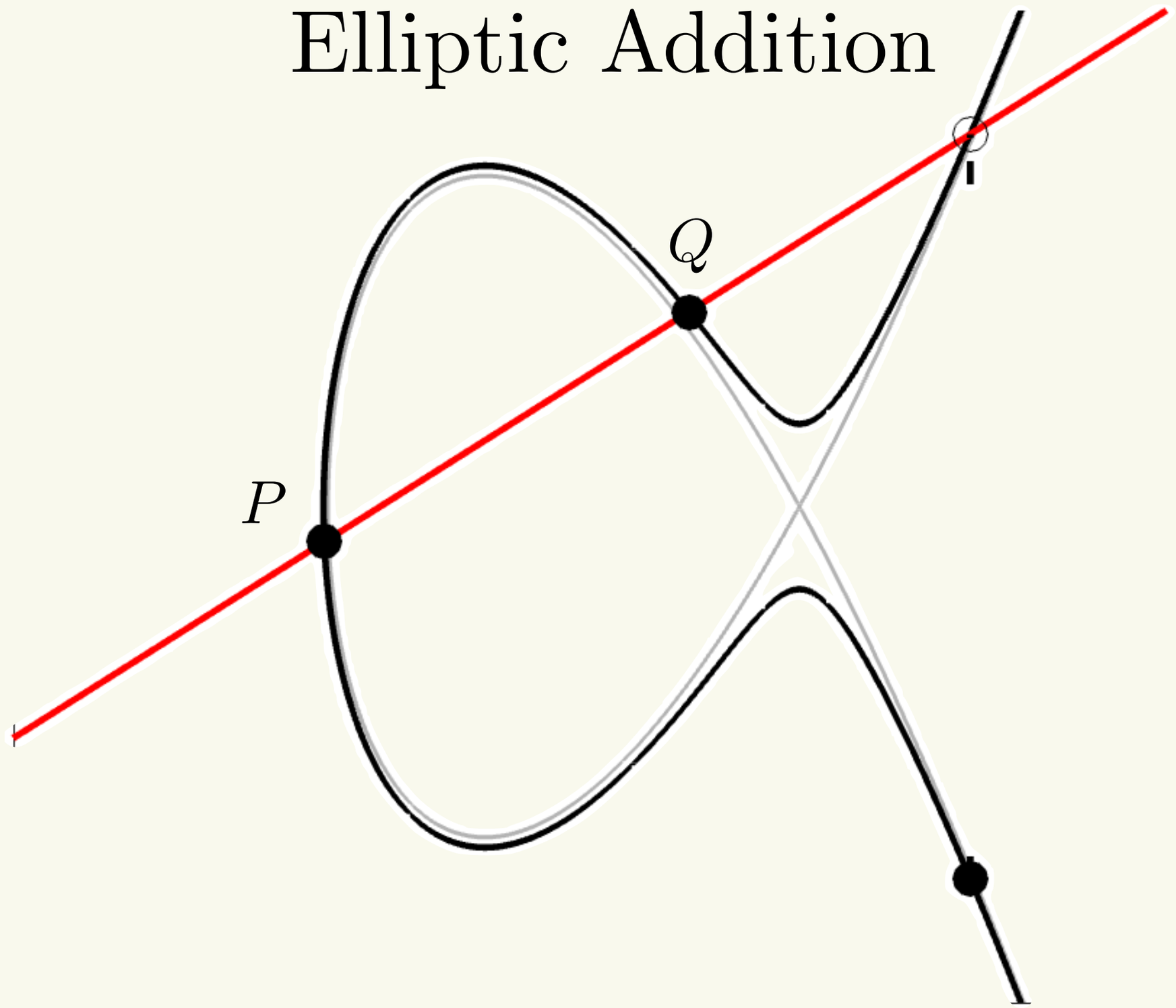
THE UNIVERSITY OF SYDNEY

Elliptic Curves

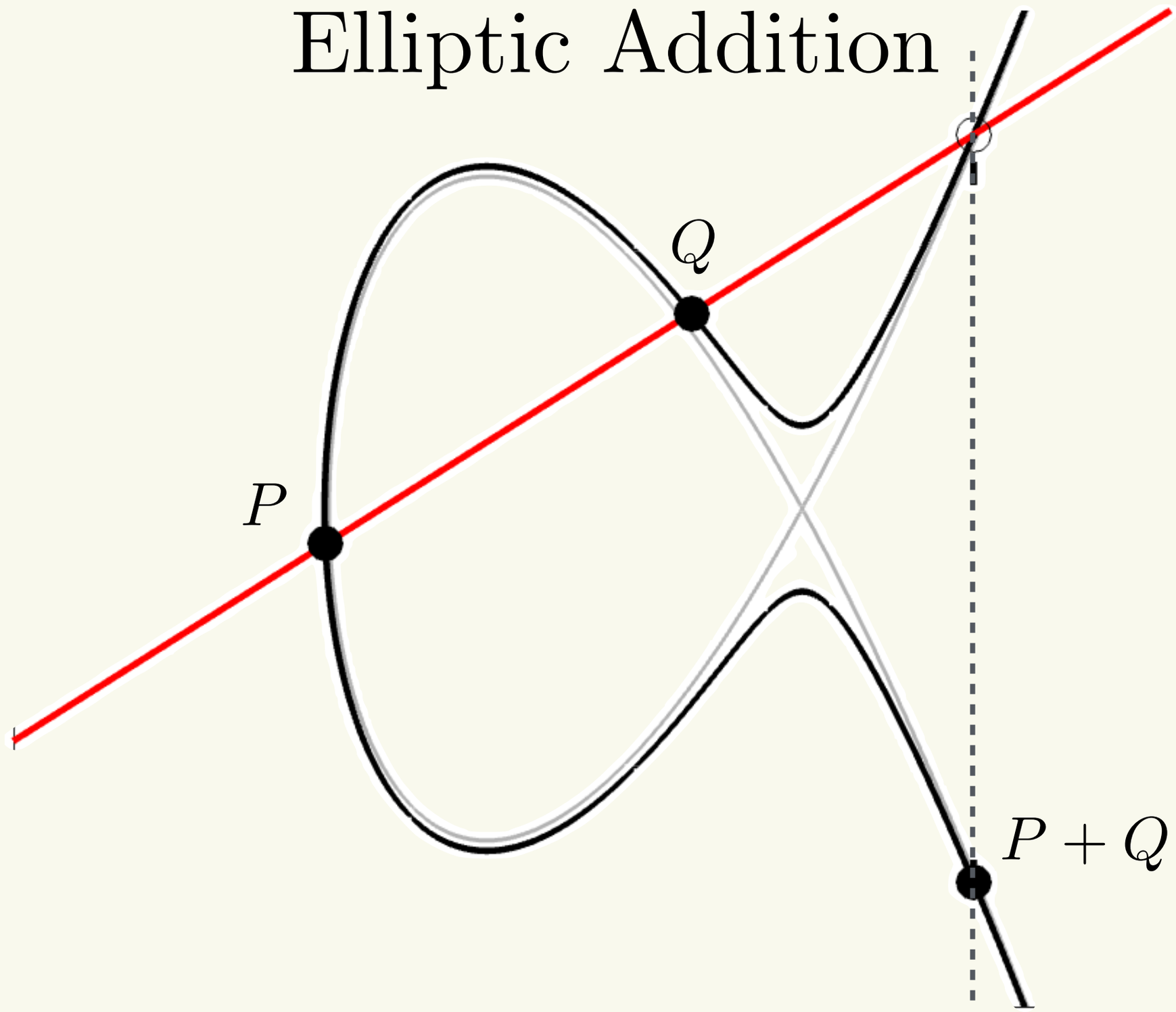


$$f(x, y) = y^2 - 4x^3 + 12x - k = 0$$

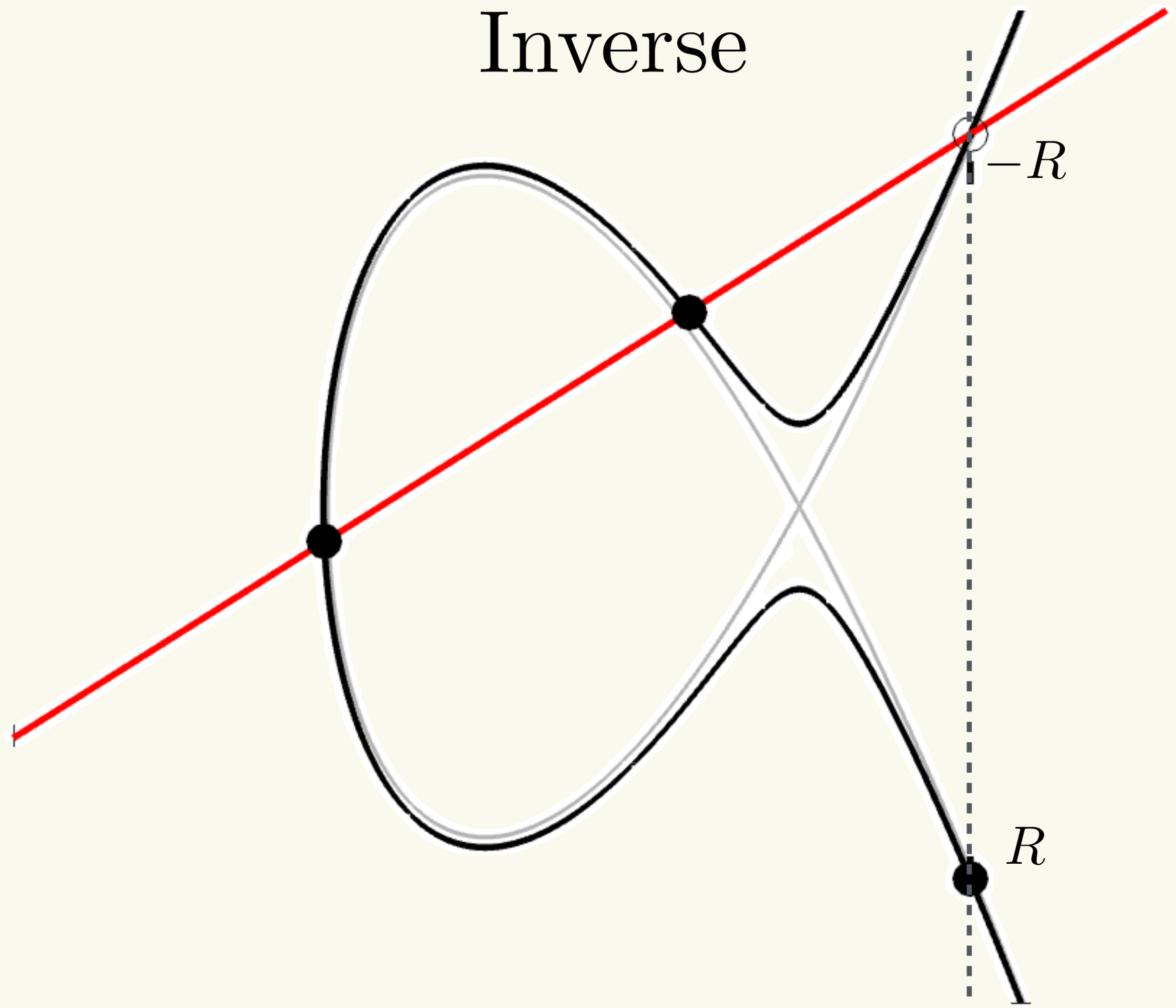
Elliptic Addition



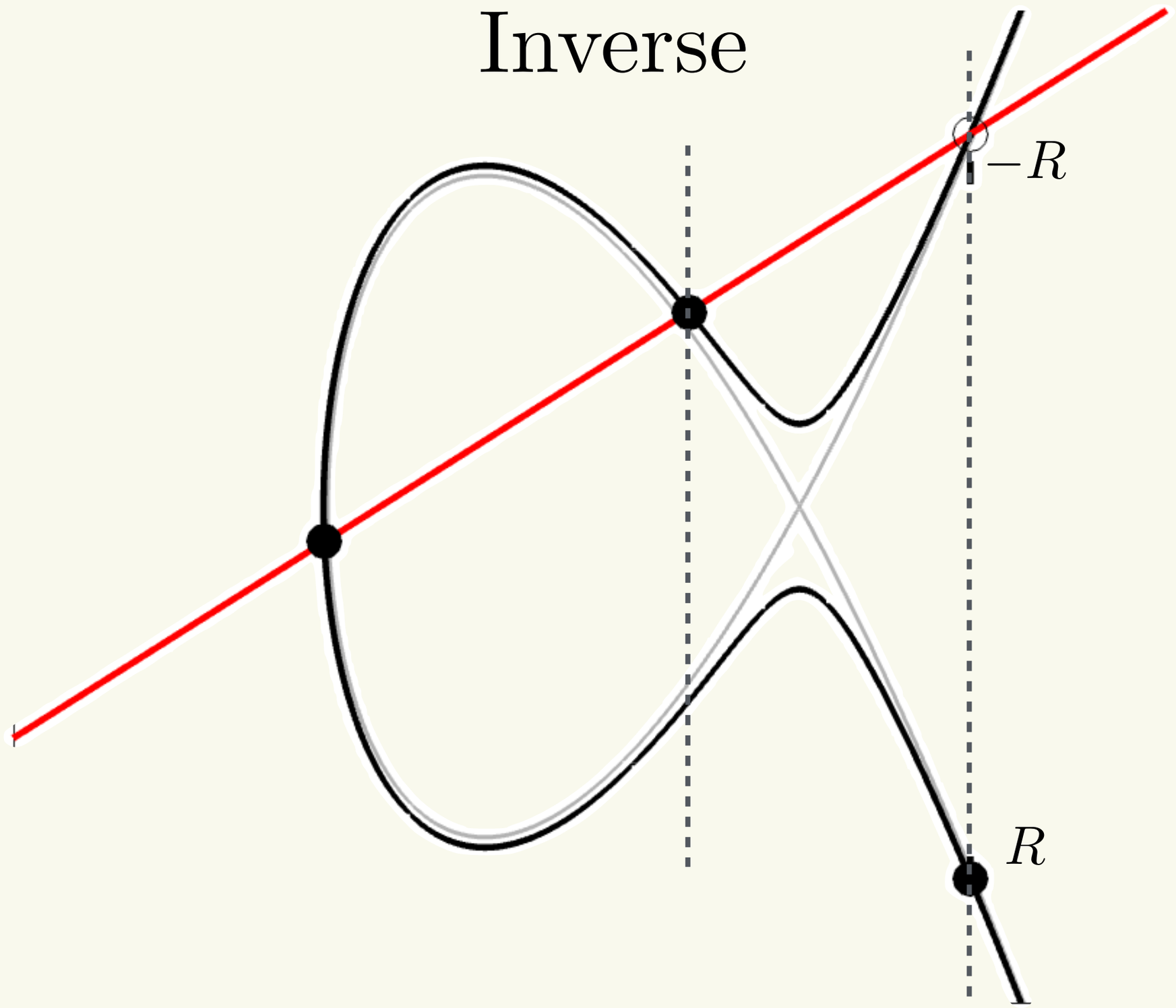
Elliptic Addition



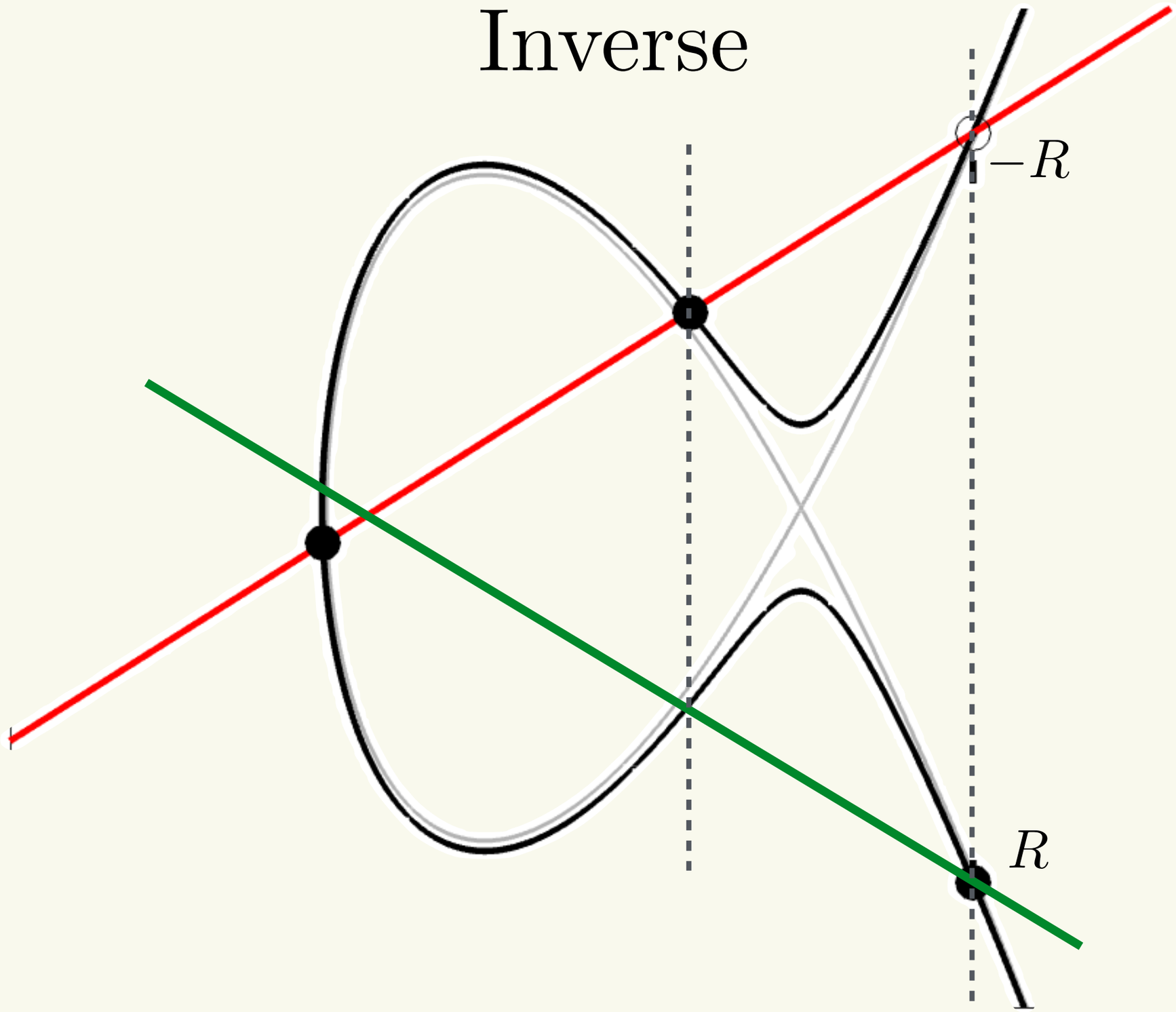
Inverse



Inverse



Inverse



Elliptic Curve Cryptography

THE UNIVERSITY OF SYDNEY

Elliptic Curve Cryptography

- Consider an elliptic curve E over a finite field $\mathbb{F}_q$ ($q = p^n$, p a prime number).

Elliptic Curve Cryptography

- Consider an elliptic curve E over a finite field $\mathbb{F}_q$ ($q = p^n$, p a prime number).
- The discrete logarithm problem: given points P and $\tilde{P}$ on E, find k such that $\tilde{P} = kP$.

Elliptic Curve Cryptography

- Consider an elliptic curve E over a finite field $\mathbb{F}_q$ ($q = p^n$, p a prime number).
- The discrete logarithm problem: given points P and $\tilde{P}$ on E, find k such that $\tilde{P} = kP$.
- $\exists$ E and q for which it is extremely difficult to find k.

Elliptic Curve Cryptography

- Consider an elliptic curve E over a finite field $\mathbb{F}_q$ ($q = p^n$, p a prime number).
- The discrete logarithm problem: given points P and $\tilde{P}$ on E, find k such that $\tilde{P} = kP$.
- $\exists$ E and q for which it is extremely difficult to find k.

  "Curve25519": $y^2 = x^3 + 486662\,x^2 + x$, $p = 2^{255} - 19$

Elliptic Curve Cryptography

- Consider an elliptic curve E over a finite field $\mathbb{F}_q$ ($q = p^n$, p a prime number).
- The discrete logarithm problem: given points P and $\tilde{P}$ on E, find k such that $\tilde{P} = kP$.
- $\exists$ E and q for which it is extremely difficult to find k.

  "Curve25519": $y^2 = x^3 + 486662\,x^2 + x$, $p = 2^{255} - 19$ requires more than 2^{128} bit operations.

Elliptic Curve Cryptography

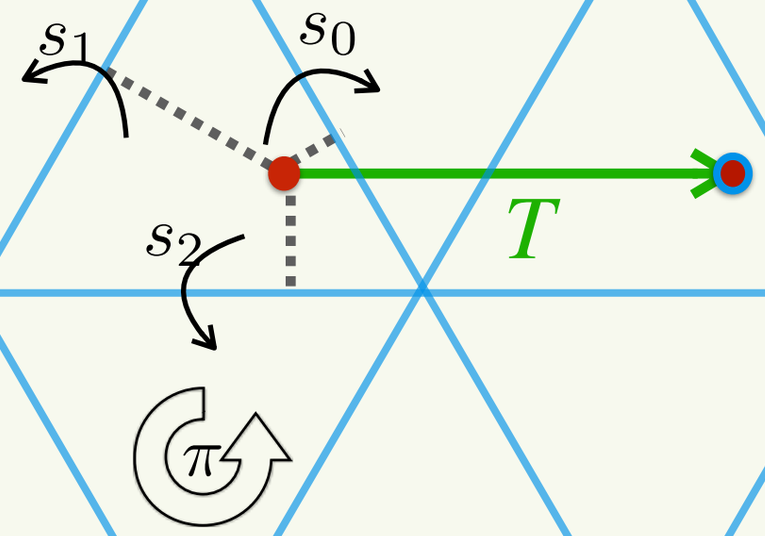
- Consider an elliptic curve E over a finite field $\mathbb{F}_q$ ($q = p^n$, p a prime number).
- The discrete logarithm problem: given points P and $\tilde{P}$ on E, find k such that $\tilde{P} = kP$.
- $\exists$ E and q for which it is extremely difficult to find k. "Curve25519": $y^2 = x^3 + 486662\,x^2 + x$, $p = 2^{255} - 19$ requires more than 2^{128} bit operations.
- The equivalent RSA version needs a key size of 3072 bits.

Shor's Algorithm

- Shor's algorithm is a quantum algorithm for finding the prime factors of an integer.
- 1600 qubits would be enough to break *Curve25519*.
- 6147 qubits are needed to break *RSA-3072*.
- But Shor's algorithm makes assumptions.
- One assumption is that the group operation stays fixed throughout the algorithm.

Changing Elliptic Curves

- Families of elliptic curves have symmetries, which preserve the family but change individual curves.
- These are well known for integrable dynamical systems.



Affine Weyl group

$$\widetilde{W} = \langle s_0, s_1, s_2, \pi \rangle$$

Integrable System

$$f(x,y) = y^2 - x^4 - 4a\,x^3 - 4bx^2 + 4kx - c^2$$

- When $a = t$, k is the Hamiltonian for an associated dynamical system: the fourth Painlevé equation $\mathrm{P_{IV}}$

$$\mathrm{P_{IV}}(\alpha,\beta):\ \ w'' = \frac{1}{2w}(w')^2 + \frac{3w^3}{2} + 4tw^2 + 2(t^2-\alpha)w + \frac{\beta}{w}$$

$$\begin{cases} f_0' &= f_0(f_1 - f_2) + \alpha_0, \\ f_1' &= f_1(f_2 - f_0) + \alpha_1, \\ f_2' &= f_2(f_0 - f_1) + \alpha_2, \end{cases}$$

$$\begin{aligned} f_0' + f_1' + f_2' &= \alpha_0 + \alpha_1 + \alpha_2, \\ &= 1, \ \text{w.l.o.g.} \end{aligned}$$

Discrete Dynamics

Using

$$T_1(a_0) = a_0 + 1, T_1(a_1) = a_1 - 1, T_1(a_2) = a_2$$

Define

$$u_n = T_1^n(f_1), v_n = T_1^n(f_0)$$

$$w_{n+1} = -w_n - w_{n-1} - 2t + \frac{c_0 n + c_1 + c_2(-1)^n}{w_n}$$

First discrete Painlevé equation (string equation).

Discrete Dynamics

Using

$$T_1(a_0) = a_0 + 1, T_1(a_1) = a_1 - 1, T_1(a_2) = a_2$$

Define

$$u_n = T_1^n(f_1), v_n = T_1^n(f_0)$$

$$\Rightarrow \qquad \begin{cases} u_n + u_{n+1} & = t - v_n - \frac{a_0+n}{v_n} \\ v_n + v_{n-1} & = t - u_n + \frac{a_1-n}{u_n} \end{cases}$$

$$w_{n+1} = -w_n - w_{n-1} - 2t + \frac{c_0 n + c_1 + c_2(-1)^n}{w_n}$$

First discrete Painlevé equation (string equation).

Discrete Dynamics

Using

$$T_1(a_0) = a_0 + 1, T_1(a_1) = a_1 - 1, T_1(a_2) = a_2$$

Define

$$u_n = T_1^n(f_1), v_n = T_1^n(f_0)$$

$$\Rightarrow \qquad \begin{cases} u_n + u_{n+1} & = t - v_n - \frac{a_0+n}{v_n} \\ v_n + v_{n-1} & = t - u_n + \frac{a_1-n}{u_n} \end{cases}$$

$$\Rightarrow$$

$$w_{n+1} = -w_n - w_{n-1} - 2t + \frac{c_0 n + c_1 + c_2(-1)^n}{w_n}$$

First discrete Painlevé equation (string equation).

Key exchange protocol

Assume $\quad c_0 = 0$

- Alice and Bob agree on $\mathbb{F}_p, w_0, w_1, c_1, c_2$.
- Alice $\Rightarrow$ Bob: w_{n-1}, w_n and parity of n
- Bob $\Rightarrow$ Alice: w_{m-1}, w_m and parity of m

- Alice iterates $w_m, n-$times
- Bob iterates $w_n, m-$times

$\Big\} \Rightarrow w_{m+n}$

Key exchange protocol

Assume $c_0 = 0$

- Alice and Bob agree on $\mathbb{F}_p, w_0, w_1, c_1, c_2$.
- Alice $\Rightarrow$ Bob: w_{n-1}, w_n and parity of n
- Bob $\Rightarrow$ Alice: w_{m-1}, w_m and parity of m

- Alice iterates $w_m, n-$times
- Bob iterates $w_n, m-$times

$\Big\}$ $\Rightarrow$ w_{m+n}

Shared key

Exponentially hard to decode...

Diffie-Hellman, 1976

Implications

- Shor's algorithm assumes that the group generator g is constant.
- In our case, g is changing from curve to curve.
- A quantum-proof algorithm arises from dPI, but it is $\mathcal{O}(n)$, which is not as efficient as ECC.

Questions:

1. Can Shor's algorithm be extended to such cases?
2. Can the complexity of the discrete logarithm problem in initial-value space be reduced?