Curve-based Cryptography

Diego F. Aranha

Institute of Computing
UNICAMP

Introduction

Elliptic Curve Cryptography (ECC):

- Underlying problem harder than integer factoring (RSA)
- Same security level with smaller parameters
- Efficiency in storage and execution time

Pairing-Based Cryptography (PBC):

- Initially destructive
- Allows innovative protocols
- Flexibilizes curve-based cryptography

Finite fields

A *finite field* is an algebraic structure composed of a finite set $\mathbb{F}$ and two operations $+, \times$, such that $\mathbb{F}$ is an abelian group under each of these operations, and $\times$ distributes over $+$.

Finite fields exist only for $|\mathbb{F}| = p^k$, where p^k is a prime power, $k > 1$. We write $\mathbb{F}_{p^m}$ for a field with p^m elements.

One of the most convenient ways to represent (and operate with) elements in $\mathbb{F}_{p^m}$ uses polynomials with coefficients in $\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$, p prime, modulo a polynomial $f(z)$ of degree m irreducible over $\mathbb{Z}_p$.

Finite fields

That is, $\mathbb{F}_{p_m}$ is the set of all polynomials with coefficients in $\mathbb{Z}_p$ and degree at most $m-1$, and $+, \times$ are the usual operations of polynomial addition and multiplication, provided that the resulting polynomial is taken modulo $f(z)$, and its coefficients are reduced modulo p.

The **binary** field $\mathbb{F}_{2^m}$ is the special case $p = 2$. It is formed by polynomials with binary coefficients.

The **prime** field $\mathbb{F}_p$ is the special case $m = 1$. It consists of the elements from $\mathbb{Z}_p$.

Exercise: Check that $f(z) = x^3 + x + 1$ is irreducible over $\mathbb{Z}_2$ and show the addition and multiplication tables of elements of $\mathbb{F}_{2^3}$ with this $f(z)$.

Elliptic curves

Definition

An *elliptic curve* is the set of solutions $(x, y) \in \mathbb{F}_q \times \mathbb{F}_q$ that satisfy the equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

where $a_i \in \mathbb{F}_q$ with $\Delta \neq 0$, and a **point at infinity** $\mathcal{O}$.

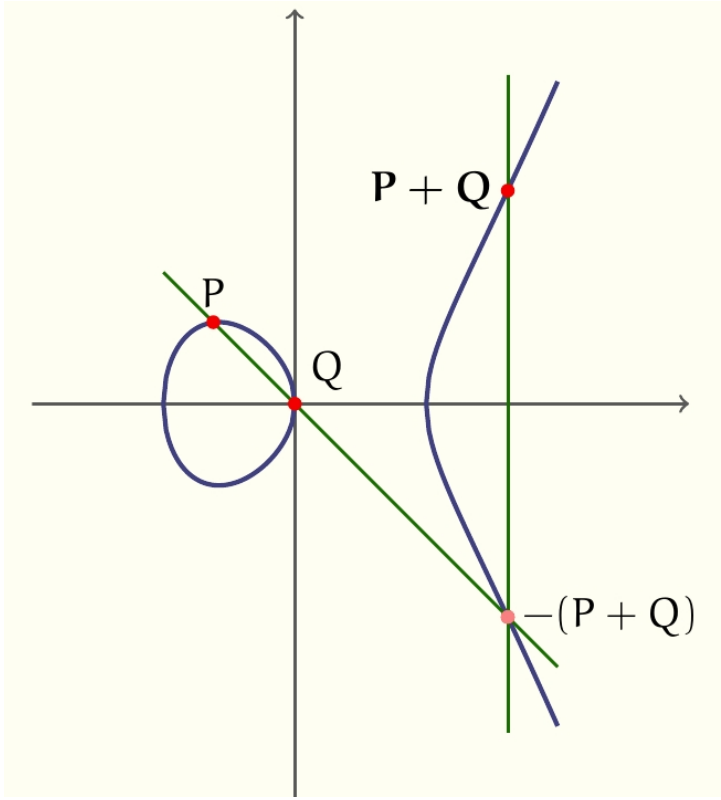
The order n of the curve E is the number of points satisfying its defining equation.

Hasse's condition states that $n = q + 1 - t$, where $|t| \leq 2\sqrt{q}$.

The curve is called **supersingular** when $q|t$.

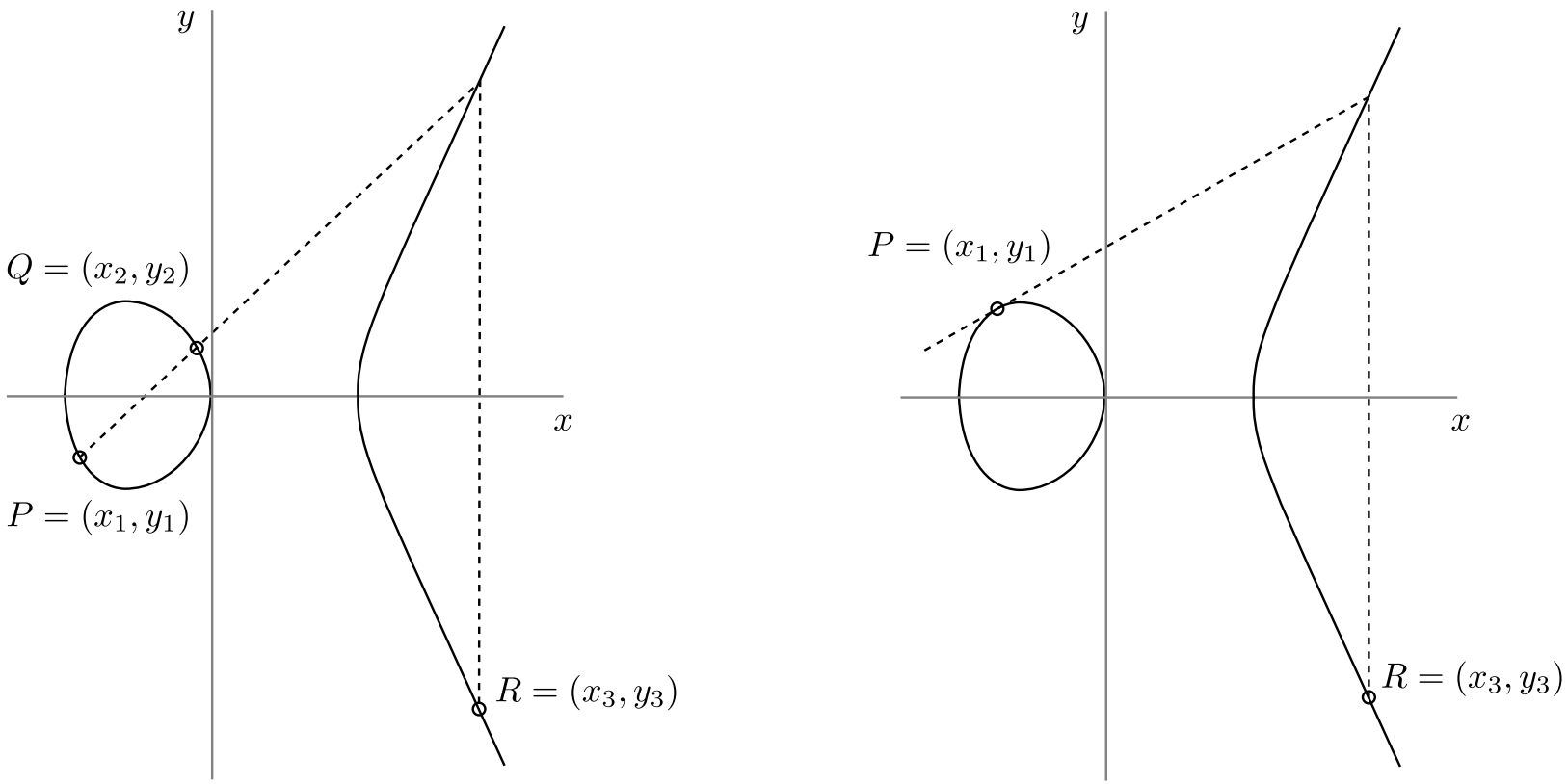
Important: Avoid supersingular curves!

Elliptic curves



$$E(\mathbb{F}_p) : y^2 = x^3 + ax + b, \quad E(\mathbb{F}_{2^m}) : y^2 + xy = x^3 + ax^2 + b$$

Elliptic curves



(a) Point addition $R = P + Q$; (b) Point doubling $R = 2P$;

Figure: Elliptic curve arithmetic.

[Picture: Hankerson *et al.* 2003]

Elliptic curves

The group of points under the operation $+$ (chord and tangent forms an additive froup. The *scalar multiplication* is defined by the recurrence relation:

$$kP = \begin{cases} \mathcal{O}, & \text{se } k = 0. \\ (-k)(-P) & \text{se } k \leq -1. \\ (k-1)P + P & \text{se } k \geq 1. \end{cases}$$

The order of P is the smallest integer r such that $rP = \mathcal{O}$. We have $r|n$.

Elliptic Curve Discrete Logarithm Problem (ECDLP)

Let E an elliptic curve of order n. Given $P \in E(\mathbb{F}_q)$ and a multiple Q of P, find an integer $0 \leq k \leq n-1$ such that $Q = kP$.

Bilinear pairings

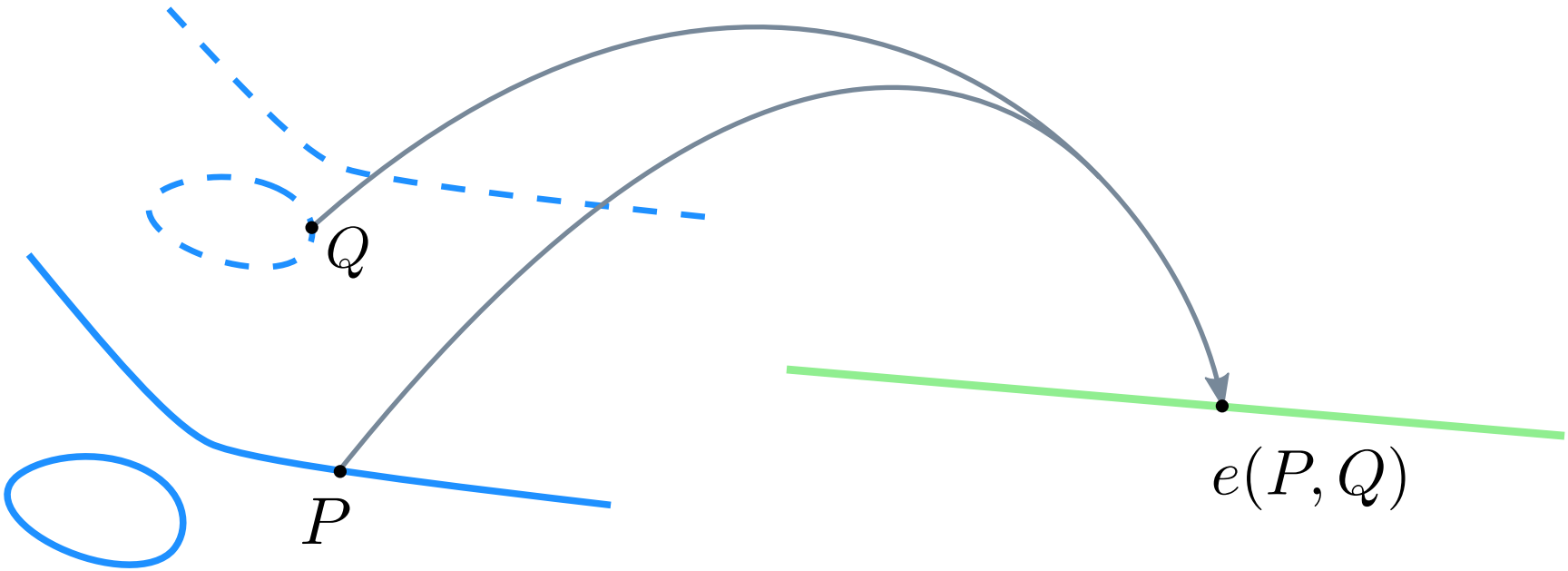
Let $\mathbb{G}_1 = \langle P \rangle$ and $\mathbb{G}_2 = \langle Q \rangle$ be additive groups and $\mathbb{G}_T$ be a multiplicative group such that $|\mathbb{G}_1| = |\mathbb{G}_2| = |\mathbb{G}_T| =$ prime n.

An efficiently-computable map $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ is an **admissible bilinear map** if the following properties are satisfied:

1. *Bilinearity:* given $(V,\ W) \in \mathbb{G}_1 \times \mathbb{G}_2$ and $(a,\ b) \in \mathbb{Z}_q^*$: $e(aV, bW) = e(V, W)^{ab} = e(abV, W) = e(V, abW)$.

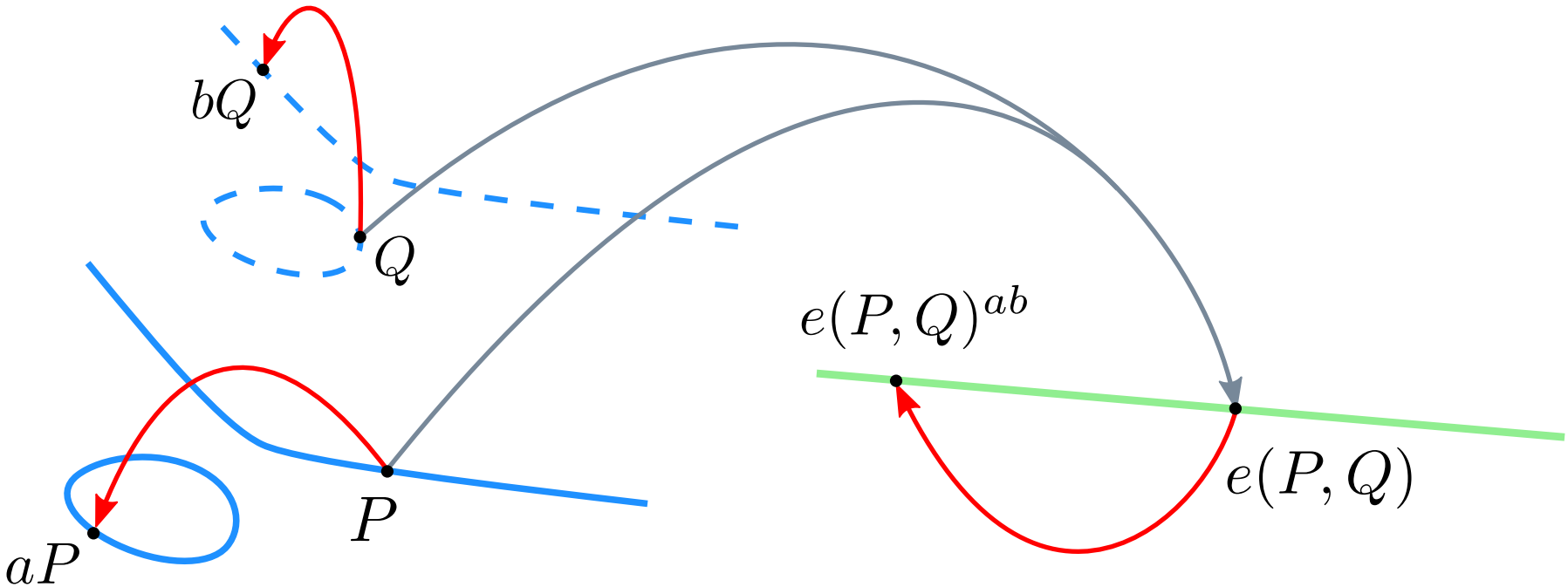
2. *Non-degeneracy:* $e(P, Q) \neq 1_{\mathbb{G}_T}$, where $1_{\mathbb{G}_T}$ is the identity of the group $\mathbb{G}_T$.

Bilinear pairings



[Picture: Avanzi, Cesena 2009]

Bilinear pairings



If $\mathbb{G}_1 = \mathbb{G}_2$, the pairing is **symmetric**.

Example of protocol

Joux's tripartite Diffie-Hellman:

1. Define an elliptic curve E with generator G and order n
2. Parties A, B, C generate short-lived secrets a, b, c from $\mathbb{Z}_n^*$ respectively
3. Parties A, B, C broadcast aG, bG, cG to the other parties, respectively
4. A computes $K_A = e(bG, cG)^a$
5. B computes $K_B = e(aG, cG)^b$
6. C computes $K_C = e(bG, cG)^c$
7. Shared key is $K = K_A = K_B = K_C = e(G, G)^{abc}$.

Example of protocol

Joux's tripartite Diffie-Hellman:

1. Define an elliptic curve E with generator G and order n
2. Parties A, B, C generate short-lived secrets a, b, c from $\mathbb{Z}_n^*$ respectively
3. Parties A, B, C broadcast aG, bG, cG to the other parties, respectively
4. A computes $K_A = e(bG, cG)^a$
5. B computes $K_B = e(aG, cG)^b$
6. C computes $K_C = e(bG, cG)^c$
7. Shared key is $K = K_A = K_B = K_C = e(G, G)^{abc}$.

Bilinear Diffie Hellman Problem (BDHP)

Compute $e(P, Q)^{abc}$ from $\langle P, aP, bP, cP, Q, aQ, bQ, cQ \rangle$.