Mathematical Countermeasures Against Side-Channel Attacks on ECC/HECC

Tanja Lange

ITSC - Information-Security and Cryptography

Ruhr-University of Bochum

lange@itsc.ruhr-uni-bochum.de

02.06.2004

Overview

- Introduction to side-channel attacks
- Introduction to elliptic and hyperelliptic curves
- Countermeasures against SPA
- Countermeasures against DPA

Side-Channals

Attacker can measure

- Time to perform operations
- Power consumption during operations
- Electro-magnetic radiation during computation

Obviously, addition is cheaper than multiplication $\Rightarrow$ need more clock cycles, different characteristics.

Attacker might be able to reconstruct sequence of operations (power & EM) or at least learn how many of each kind were performed (timing).

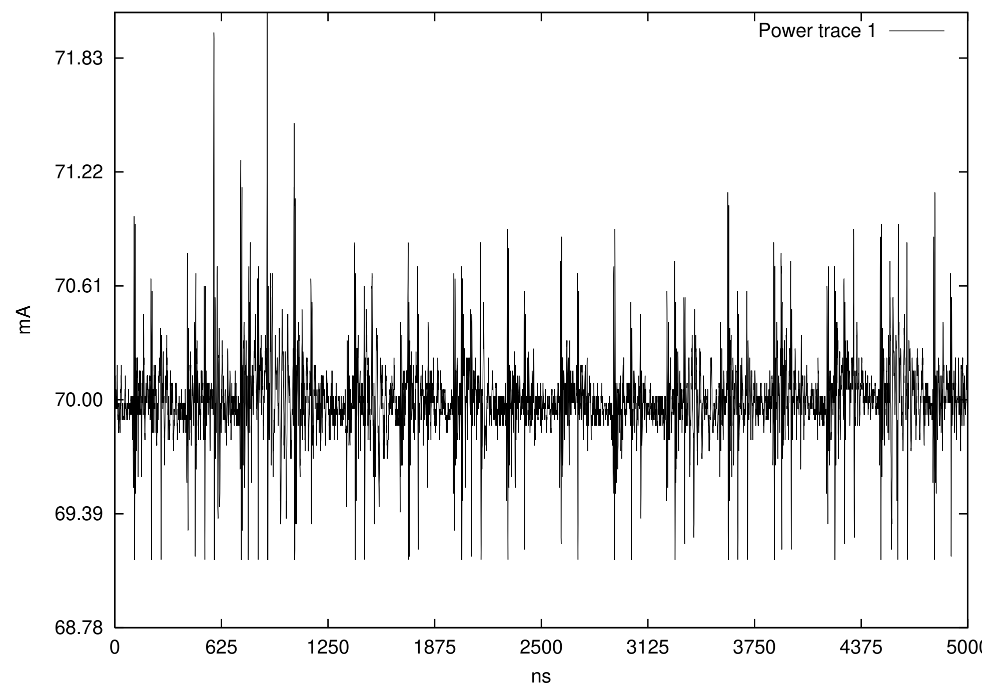
Consequences I

If sequence of operations depends on the secret key (e. g. binary double-and-add) and this is directly translated to the observed data, one can reconstruct the key

$\Rightarrow$ Simple Side-Channel Analysis (SSCA) (often SPA= Simple Power Analysis).

Consequences II

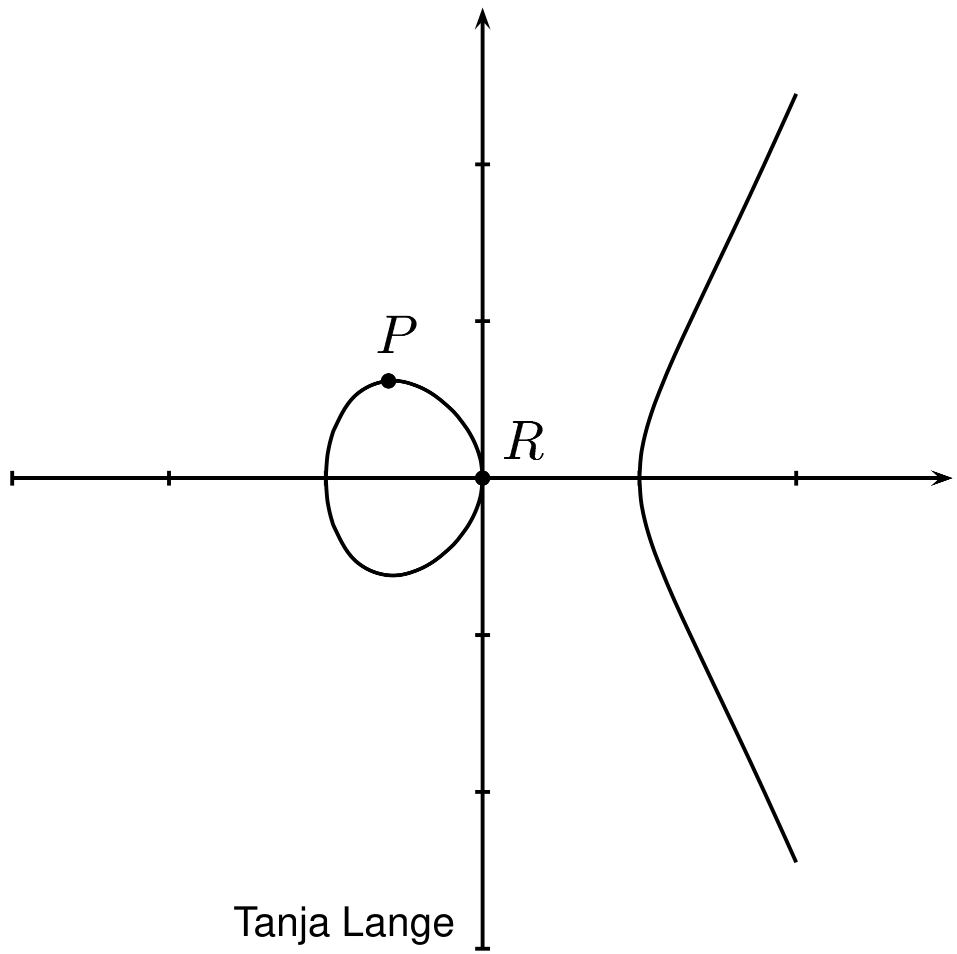
Assume algorithm is shielded against SCA (e. g. using uniform group operations). Still the performance might depend on the internal representation of the intermediate group elements. Averaging over different inputs reveals intermediate results ⇒ secret key is recovered bit-by-bit from most-significant bit.
⇒ Differential Side-Channel Analysis (DSCA) (often DPA= Differential Power Analysis)



Elliptic Curve

$$E : y^2 + \underbrace{(a_1x + a_3)}_{h(x)}\, y = \underbrace{x^3 + a_2x^2 + a_4x + a_6}_{f(x)}, \;\; h, f \in \mathbb{F}_q[x]$$

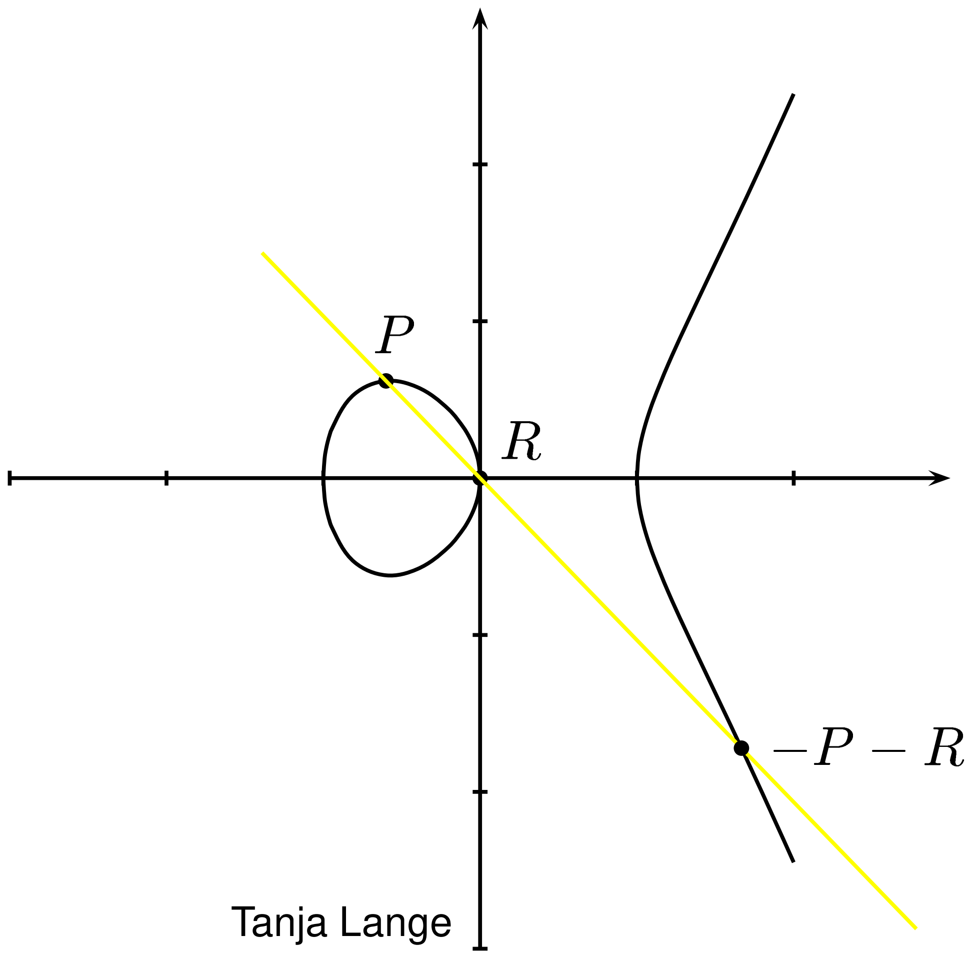
Group: $E(\mathbb{F}_q) = \{\, (x, y) \in \mathbb{F}_q^2 \; : \; y^2 + h(x)y = f(x) \,\} \cup \{\, \infty \,\}$



Elliptic Curve

$$E : y^2 + \underbrace{(a_1 x + a_3)}_{h(x)} y = \underbrace{x^3 + a_2 x^2 + a_4 x + a_6}_{f(x)}, \quad h, f \in \mathbb{F}_q[x]$$

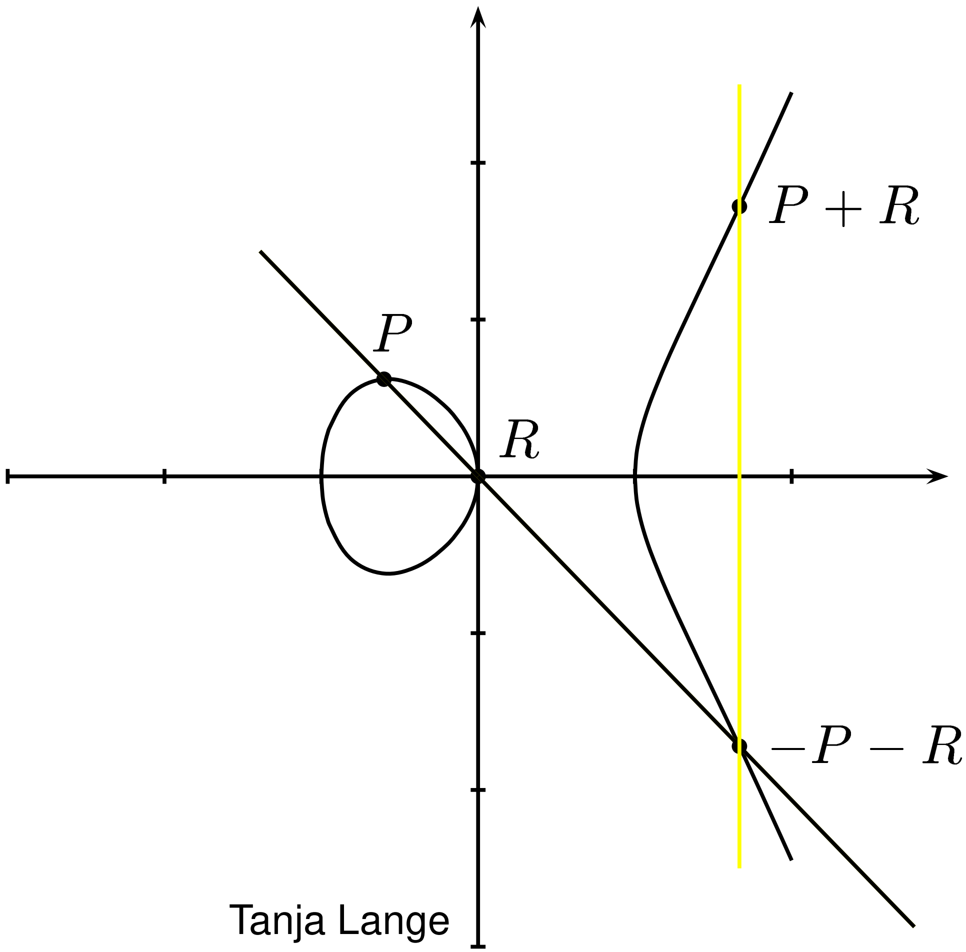
Group: $E(\mathbb{F}_q) = \{ (x, y) \in \mathbb{F}_q^2 \; : \; y^2 + h(x)y = f(x) \} \cup \{ \infty \}$



Elliptic Curve

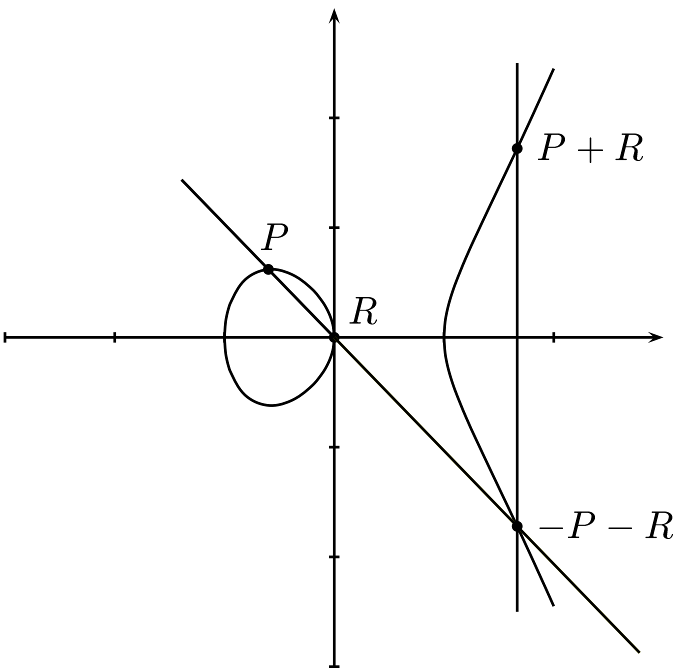
$$E : y^2 + \underbrace{(a_1x + a_3)}_{h(x)}\,y = \underbrace{x^3 + a_2x^2 + a_4x + a_6}_{f(x)},\ \ h, f \in \mathbb{F}_q[x]$$

Group: $E(\mathbb{F}_q) = \{\,(x, y) \in \mathbb{F}_q^2 \ :\ y^2 + h(x)y = f(x)\,\} \cup \{\,\infty\,\}$



Group Law

$$E : y^2 + \underbrace{(a_1x + a_3)}_{h(x)} y = \underbrace{x^3 + a_2x^2 + a_4x + a_6}_{f(x)}, \; h, f \in \mathbb{F}_q[x]$$



Addition law (q odd, $a_1 = a_2 = a_3 = 0$)

$$(x_1, y_1) + (x_2, y_2) = (x_3, y_3) =$$
$$= (\lambda^2 - x_1 - x_2, \lambda(x_1 - x_3) - y_1),$$

where

$$\lambda = \begin{cases} (y_2 - y_1)/(x_2 - x_1) & \text{if } x_1 \neq x_2, \\ (3x_1^2 + a_4)/(2y_1) & \text{else.} \end{cases}$$

$\Rightarrow$ Addition and Doubling differ considerably.

Different coordinate systems $y^2 = x^3 + ax + b$

system	points	correspondence
affine ($\mathcal{A}$)	(x, y)	
projective ($\mathcal{P}$)	(X, Y, Z)	$(X/Z, Y/Z)$
jacobian ($\mathcal{J}$)	(X, Y, Z)	$(X/Z^2, Y/Z^3)$
Chudnovsky jacobian ($\mathcal{J}^C$)	(X, Y, Z, Z^2, Z^3)	$(X/Z^2, Y/Z^3)$
modified jacobian ($\mathcal{J}^m$)	(X, Y, Z, aZ^4)	$(X/Z^2, Y/Z^3)$

system	addition			doubling		
affine ($\mathcal{A}$)	2M	1S	1I	2M	2S	1I
projective ($\mathcal{P}$)	12M	2S	–	7M	5S	–
jacobian ($\mathcal{J}$)	12M	4S	–	4M	6S	–
Chudnovsky jacobian ($\mathcal{J}^C$)	11M	3S	–	5M	6S	–
modified jacobian ($\mathcal{J}^m$)	13M	6S	–	4M	4S	–

Scalar Multiplication – Double-and-Add

$\texttt{IN:}\ P \in E(\mathbb{F}_q),\ n \in \mathbb{Z},\ n = \sum_{i=0}^{l} n_i 2^i$
$\texttt{OUT:}\ Q = nP$

1. $Q = P$
2. $\texttt{for}\ i = l-1\ \texttt{down to}\ 0\ \texttt{do}$
3. $\quad Q = 2Q$
4. $\quad \texttt{if}\ (n_i = 1)\ \texttt{then}\ Q = Q + P$
5. $\texttt{output}\ Q$

If ADD $\neq$ DBL one can easily determine n from the sequence of ADD and DBL:

$$\text{DBL DBL ADD DBL ADD DBL DBL} \Leftrightarrow (101100)_2 = 44$$

Countermeasures against SPA

Double-and-always-Add

IN: $P \in E(\mathbb{F}_q)$, $n \in \mathbb{Z}$, $n = \sum_{i=0}^{l} n_i 2^i$
OUT: $Q = nP$

1. $Q = P$
2. for $i = l - 1$ down to 0 do
3. $\quad Q = 2Q$
4. $\quad$ if $n_i == 1$ then $Q = Q + P$
   $\qquad$ else $R = Q + P$ //dummy operation
5. output Q

If an active adversary is allowed, the dummy operations might be detected (fault attacks)

Montgormery Ladder

Idea: Make used addition per round.

Intermediate result $Q_i = \sum_{j=i}^{l} n_j 2^{j-i} P$, put $R_i = Q_i + P$, then

$$Q_i = 2Q_{i+1} + n_i P = Q_{i+1} + R_{i+1} + n_i P - P = 2R_{i+1} + n_i P - 2P.$$

This implies

$$(Q_i, R_i) = \begin{cases} (2Q_{i+1}, Q_{i+1} + R_{i+1}) & \text{if } n_i = 0 \\ (Q_{i+1} + R_{i+1}, 2R_{i+1}) & \text{if } n_i = 1 \end{cases}$$

Advantages:

- Needs only x coordinate (not y).
- Projective version (no inversion) extremely efficient for special curves (uses x and z) $\Rightarrow$ Montgormery curves
- Shielded against SPA (Brier/Joye for arbitrary curves)

Uniform Group Operations

$$\left.\begin{array}{l}\text{Liardet and Smart CHES 2001}\\ \text{Billet and Joye AAECC 2003}\end{array}\right\} \Rightarrow \text{ Jacobi-Model}$$

Joye and Quisquater $\Rightarrow$ Hessian Curve

Proposed formulae still might involve inversions, can be generalized to projective coordinates.

(Some special cases may occur, but with very low probability.)

Side-Channel Atomicity

Chevallier-Mames, Ciet, and Joye 2003:
Make operations uniform at low level
$\Rightarrow$ build group operation from identical blocks.

Each block consists of:

1 multiplication, 1 addition, 1 negation, 1 addition;

fill with dummy operations
(only addition and negation $\Rightarrow$ cheap!).

ADD $(\mathcal{A} + \mathcal{P})$ needs 11 blocks
DBL $(2\mathcal{P})$ needs 10 blocks
(same as number of multiplications).

Can be used in parallel/pipelining (Mishra 2004)

Hyperelliptic curve

$$C : y^2 + h(x)y = f(x)$$

$h(x), f(x) \in \mathbb{F}_q[x]$, q prime power,
f monic, $\deg f = 2g + 1, \deg h \leq g$
nonsingular, i. e. not both partial derivatives zero for
$(a, b) \in C/\bar{\mathbb{F}}_q$

C hyperelliptic curve of genus g

with at least one $\mathbb{F}_q$-rational Weierstraß point
(elliptic curves are seen here as curves of genus 1)

Group

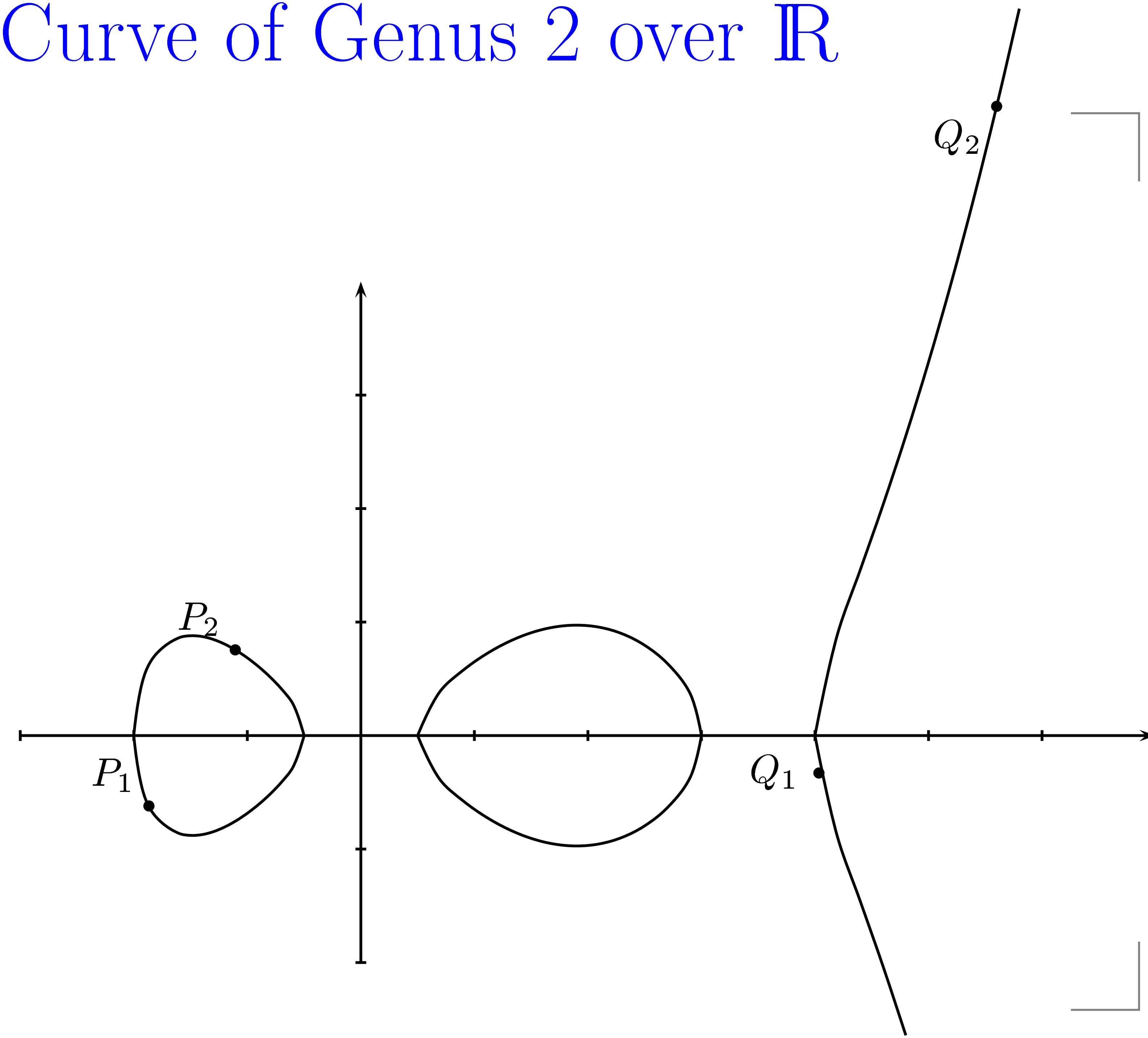
Use divisors, i. e. sums of points, of degree zero and reduce modulo principal divisors
$\Rightarrow$ divisor class group.

$$\mathrm{Pic}^0(C/\mathbb{F}_q) = Div^0(\mathbb{F}_q)/P(\mathbb{F}_q)$$

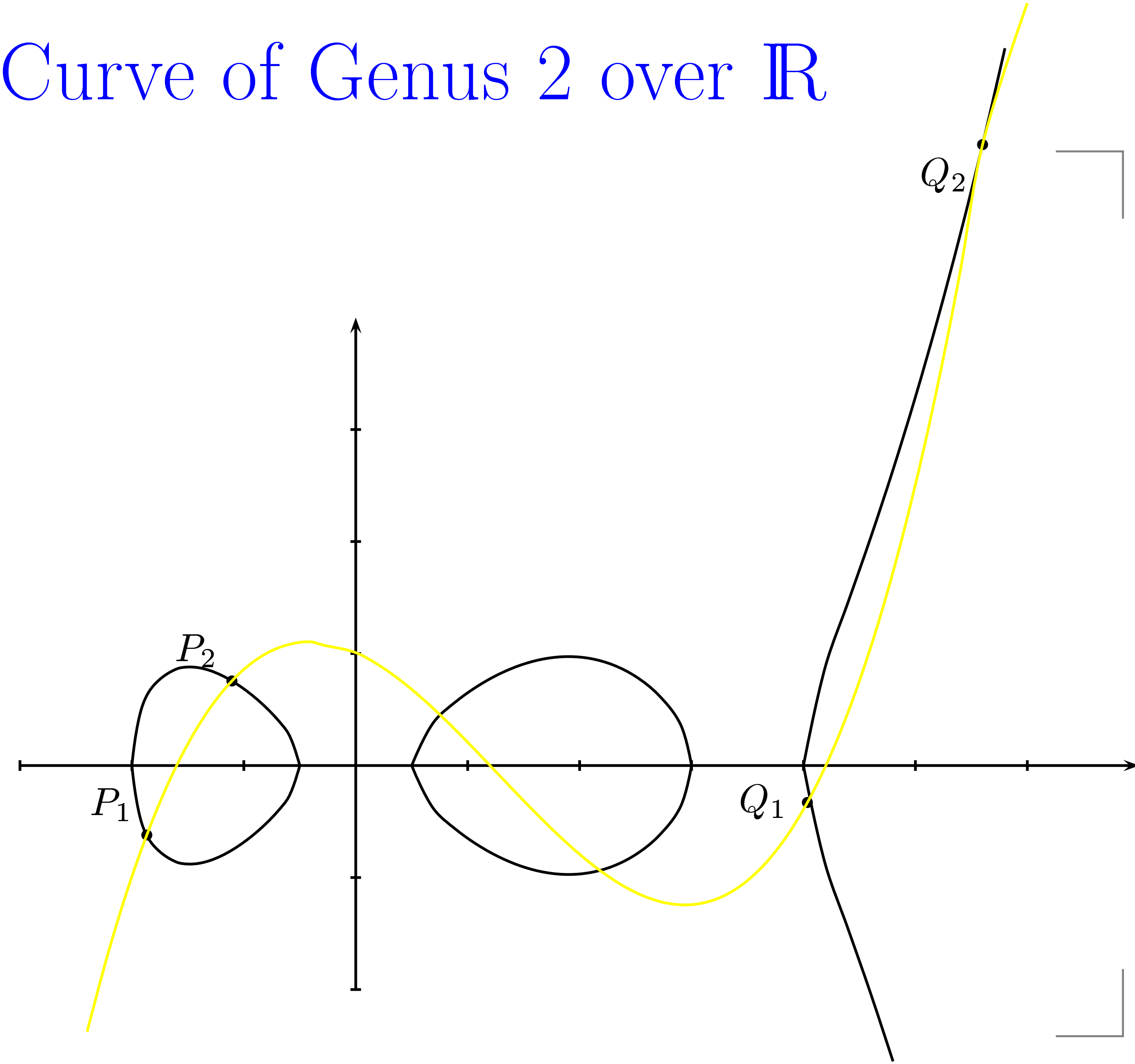
each class represented by degree zero divisor with $m \leq g$

$$\sum_{\substack{i=1 \\ P_i \in C \setminus \{\infty\}}}^{m} P_i - m\infty$$

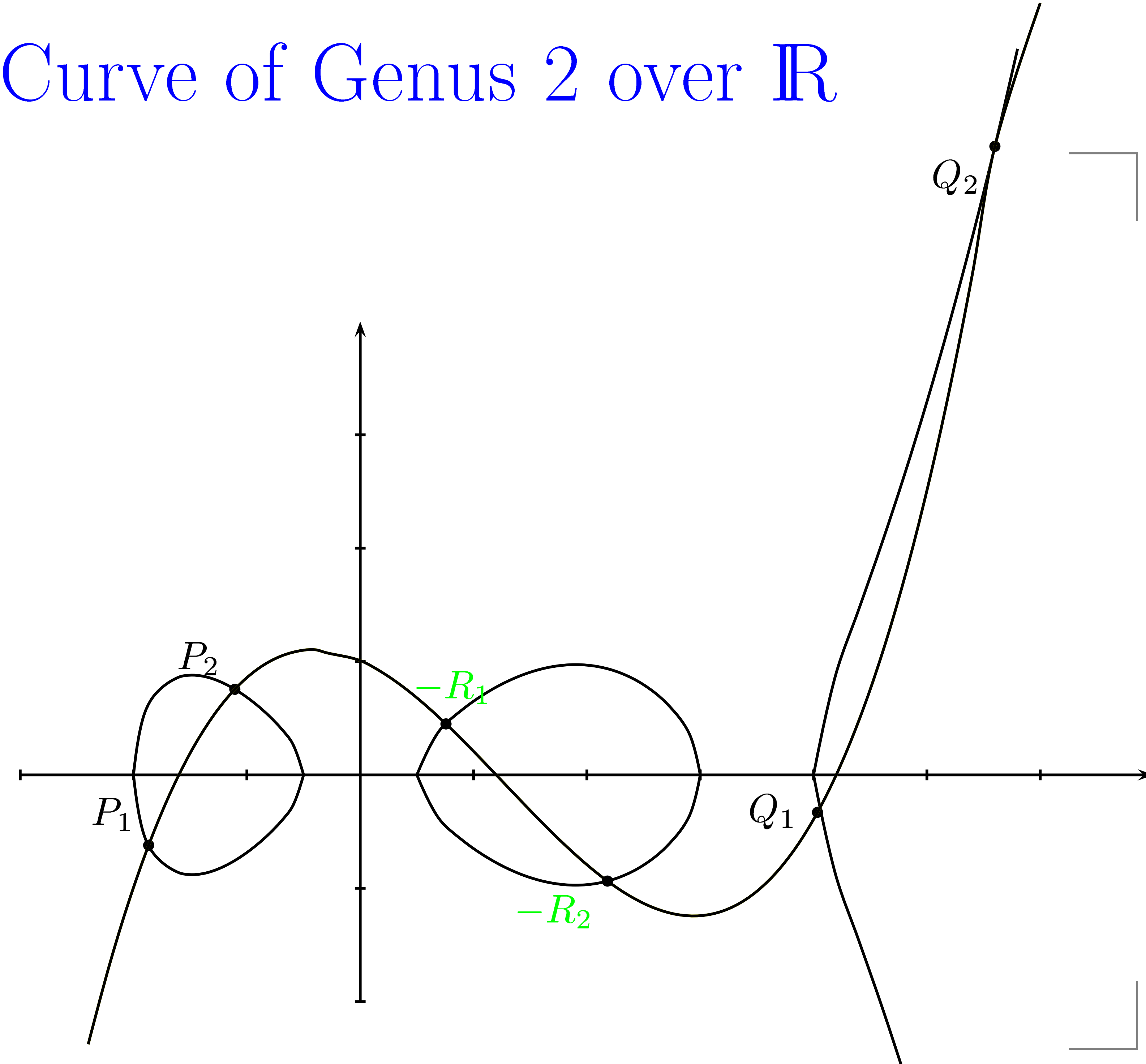
Curve of Genus 2 over $\mathbb{R}$



Curve of Genus 2 over $\mathbb{R}$

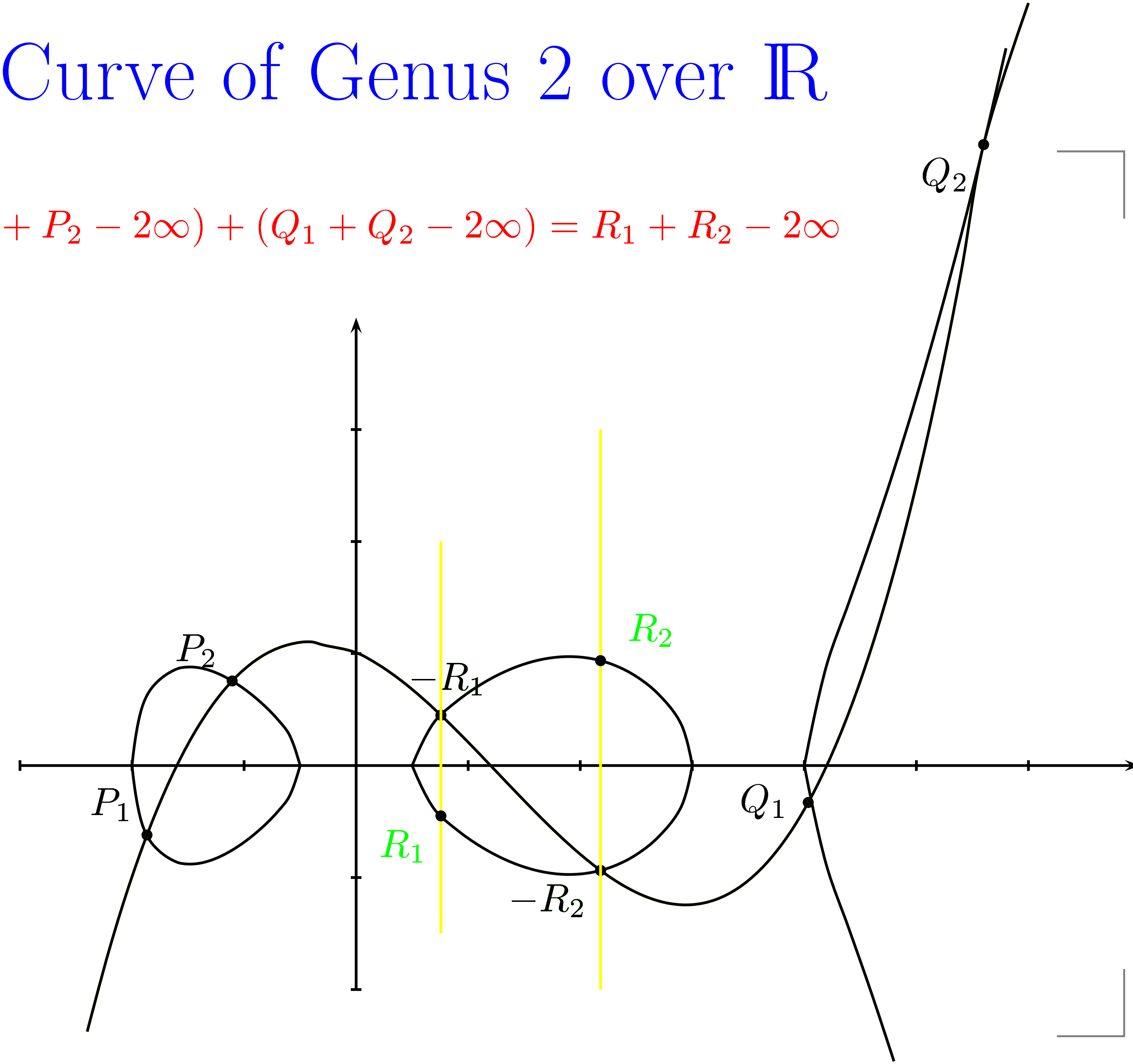


Curve of Genus 2 over $\mathbb{R}$



Curve of Genus 2 over $\mathbb{R}$

$$(P_1 + P_2 - 2\infty) + (Q_1 + Q_2 - 2\infty) = R_1 + R_2 - 2\infty$$



Countermeasures

- Double-and-Always-Add (folklore)
- Montgomery arithmetic: L., Duquesne (both ANTS 2004)
- Unified group law: still open
- Atomicity: L. and Mishra 2004

Countermeasures against DPA

Main Idea

Differential methods need to simulate group operations on known input. Guess bits one by one and test for correlation between groupings depending on internal representation.
$\Rightarrow$ introduce randomness!

- Choose differnt n' in equivalence class of n, e. g. use $n' = n + k\ell$, for group order ℓ.
- Modify group representation, e. g. use isomorphic curve.
- Modify element representation.

ECC: many papers during last ~ 10 years.
Generalization to HECC: Avanzi at CHES 2003
Koblitz curves allow more efficient shielding, (L. 2001)

The End

The END

Thanks!