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

01.07.2004

Overview

- Groups for DL-systems
- Introduction to side-channel attacks
- Introduction to elliptic curves
- Countermeasures against SPA
- Introduction to hyperelliptic curves
- Countermeasures against DPA

Groups for DL Systems

- Diffie, Hellman (1976): $G = \mathbb{F}_p^*$, i.e.

$$G = \{ 1, 2, \ldots, p-1 \}$$

- $G = \mathbb{F}_q^*$, $q = p^l$
- Koblitz/Miller (1985): $G = E(\mathbb{F}_q)$, group of points on an elliptic curve, i.e.

$$G = \{ (x, y) \in \mathbb{F}_q^2 \, : \, y^2 = x^3 + ax + b \} \cup \{ P_\infty \}$$

- Koblitz (1989): $G = \mathbf{Cl}(C/\mathbb{F}_q)$, divisor (ideal) class group of a hyperelliptic curve C over $\mathbb{F}_q$
- Using explicit group laws elliptic and hyperelliptic curves are extremely interesting for small devices like smart-cards.

Side-Channels

Attacker can measure

- Time to perform operations,
- Power consumption during operations,
- Electro-magnetic radiation during computation,
- Noise produced during computation.

Obviously, addition is cheaper than multiplication
$\Rightarrow$ needs more clock cycles, different characteristics of power trace.

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

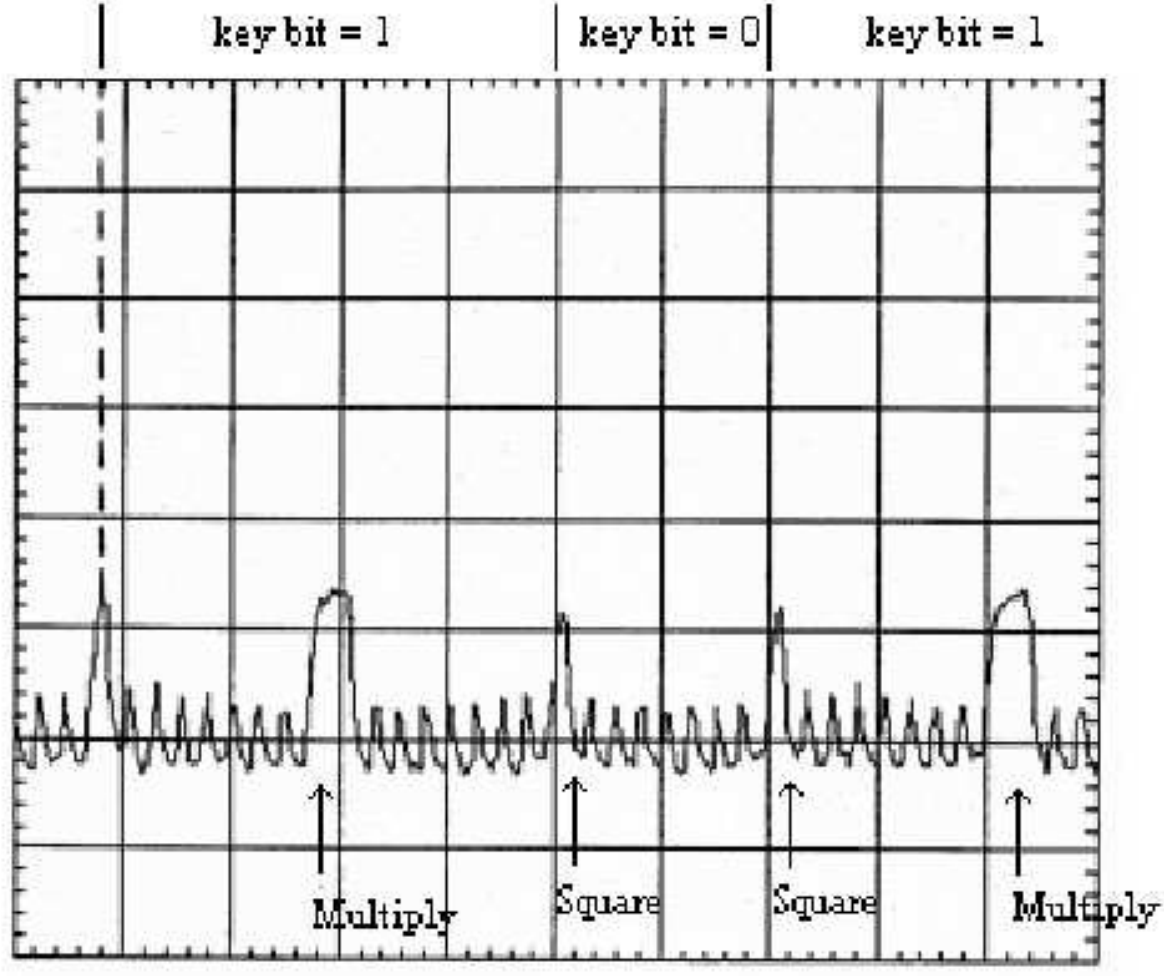
Consequences I

If sequence of operations depends on the secret key and this is directly translated to the observed data, one can reconstruct the key

⇒ Simple Side-Channel Analysis (SSCA)
(often SPA= Simple Power Analysis).

(e. g. in binary square-and-multiply one has

S M S S M ∼
$(1101)_2 = 13$).



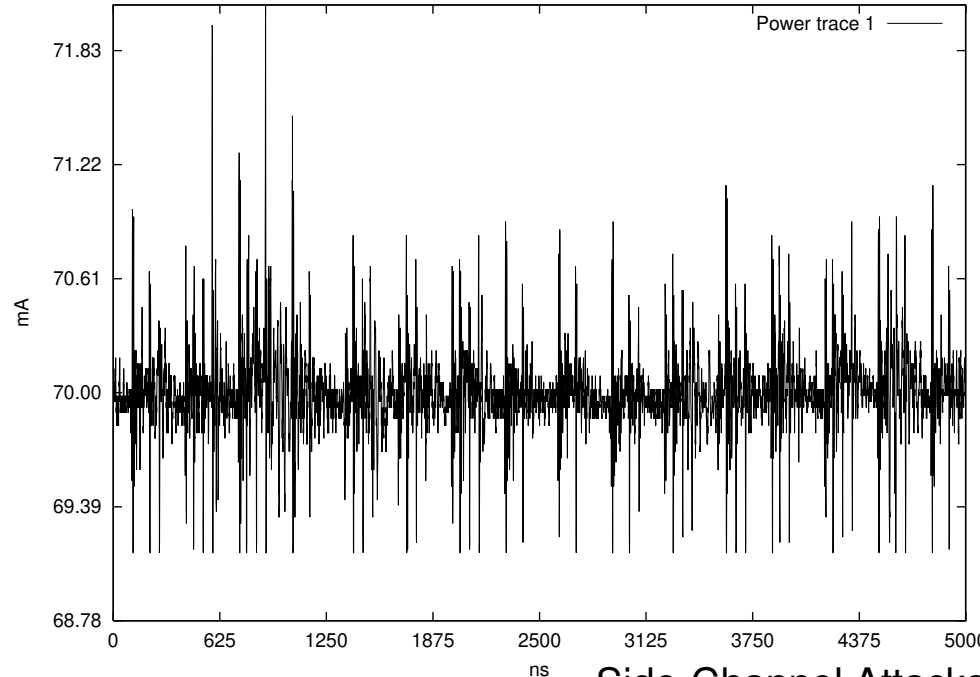
Consequences II

For algorithm shielded against SCA (e. g. by using uniform group operations – topic of these talks) the performance might still depend on the internal representation of the intermediate group elements. Averaging over different inputs reveals intermediate results

$\Rightarrow$ secret key is recovered bit-by-bit from most-significant bit.

$\Rightarrow$ Differential Side-Channel Analysis (DSCA)

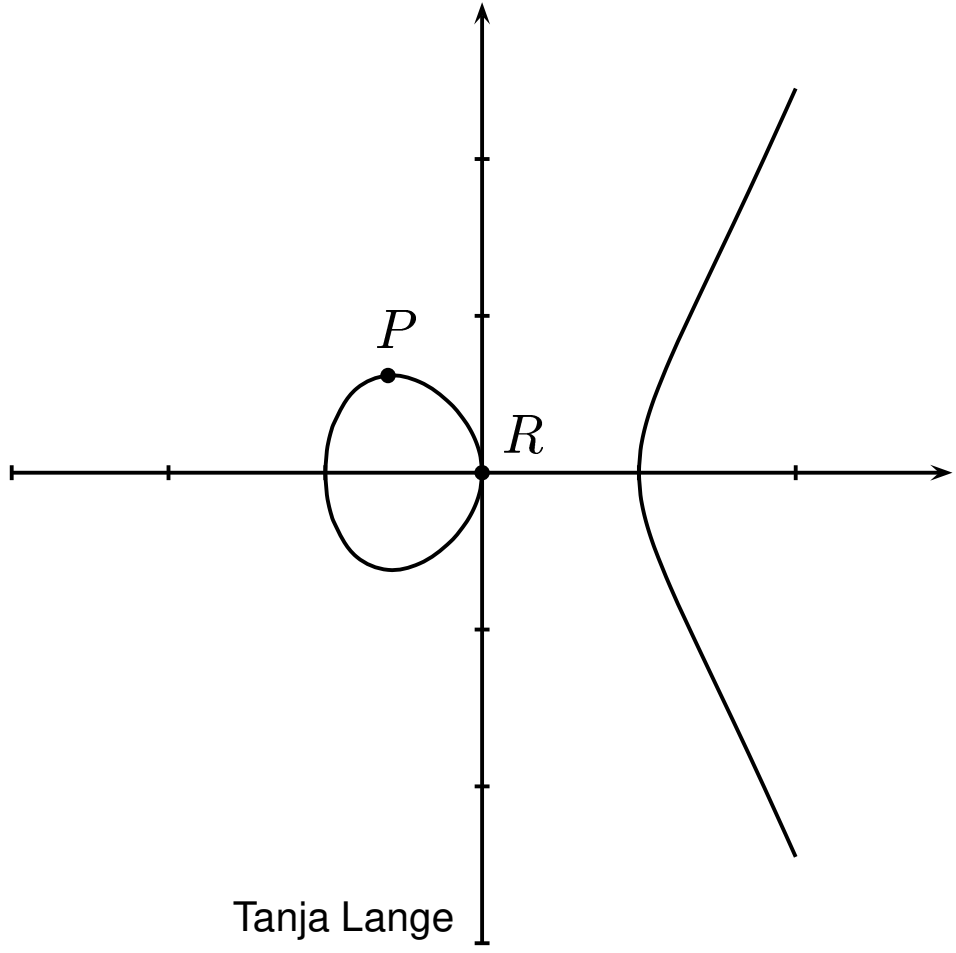
(often DPA= Differential Power Analysis)



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

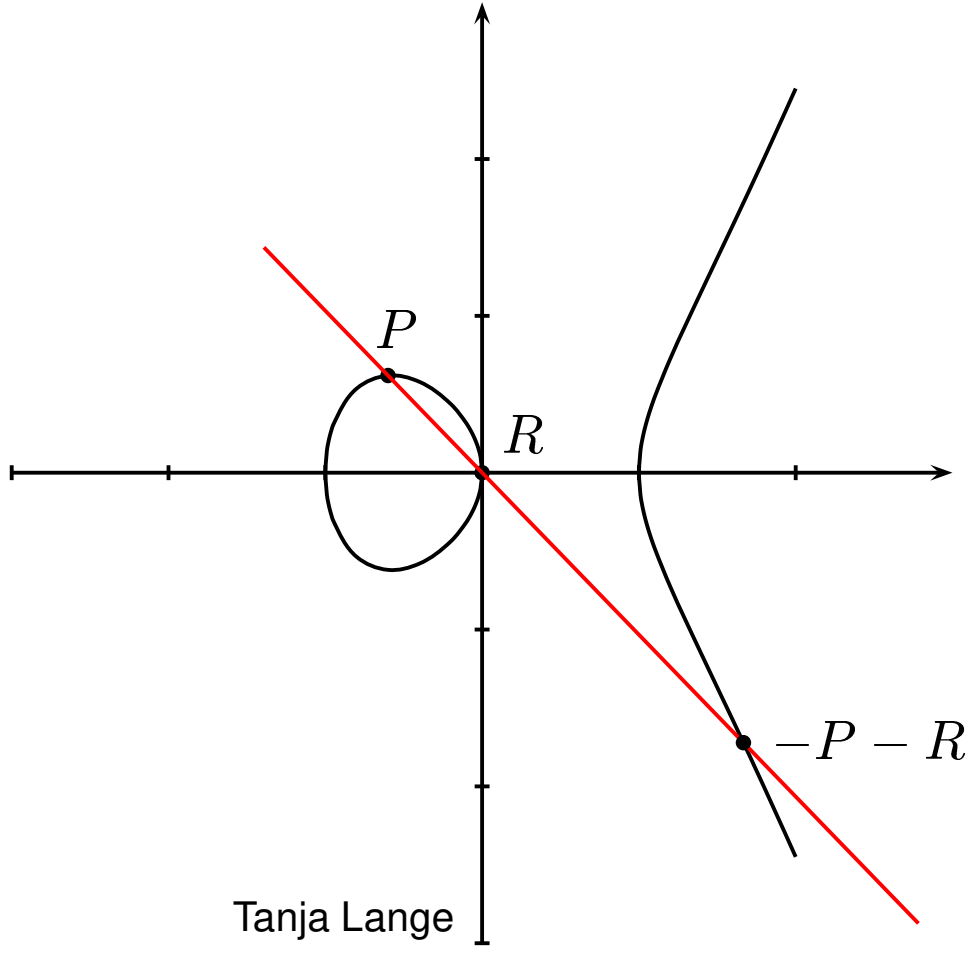


over $\mathbb{R}$

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

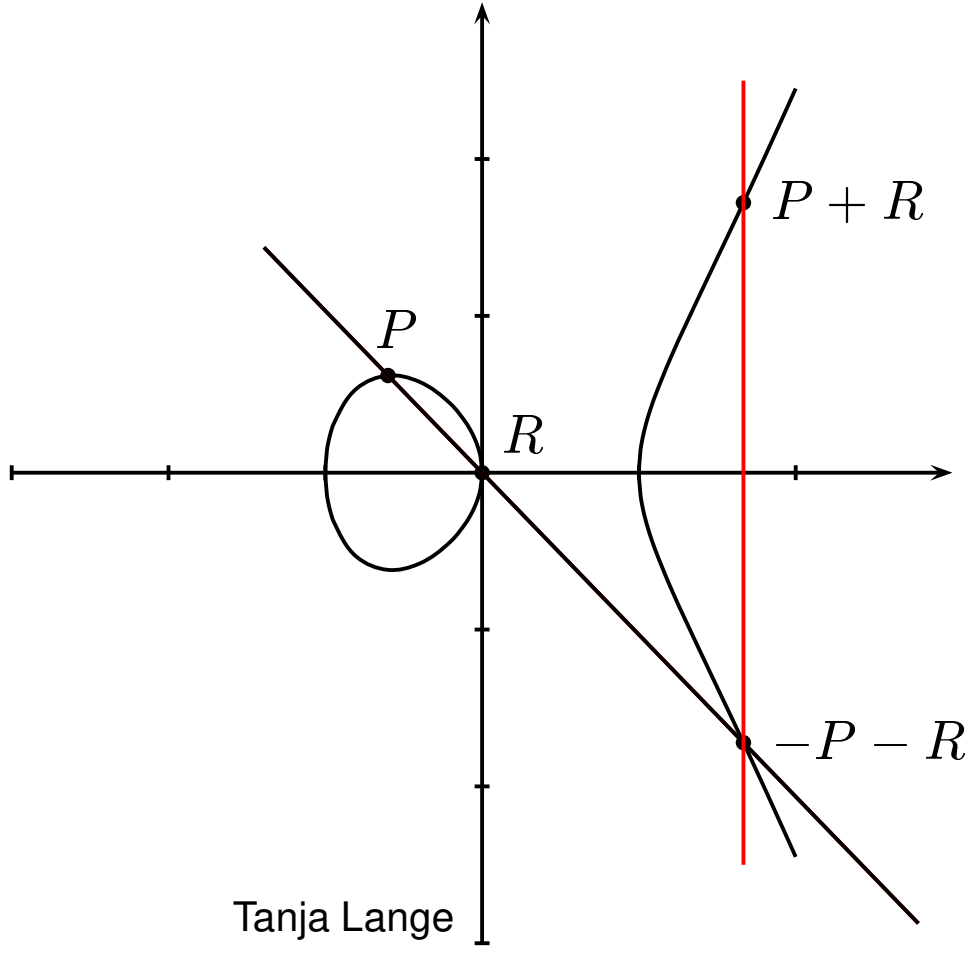


over $\mathbb{R}$

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

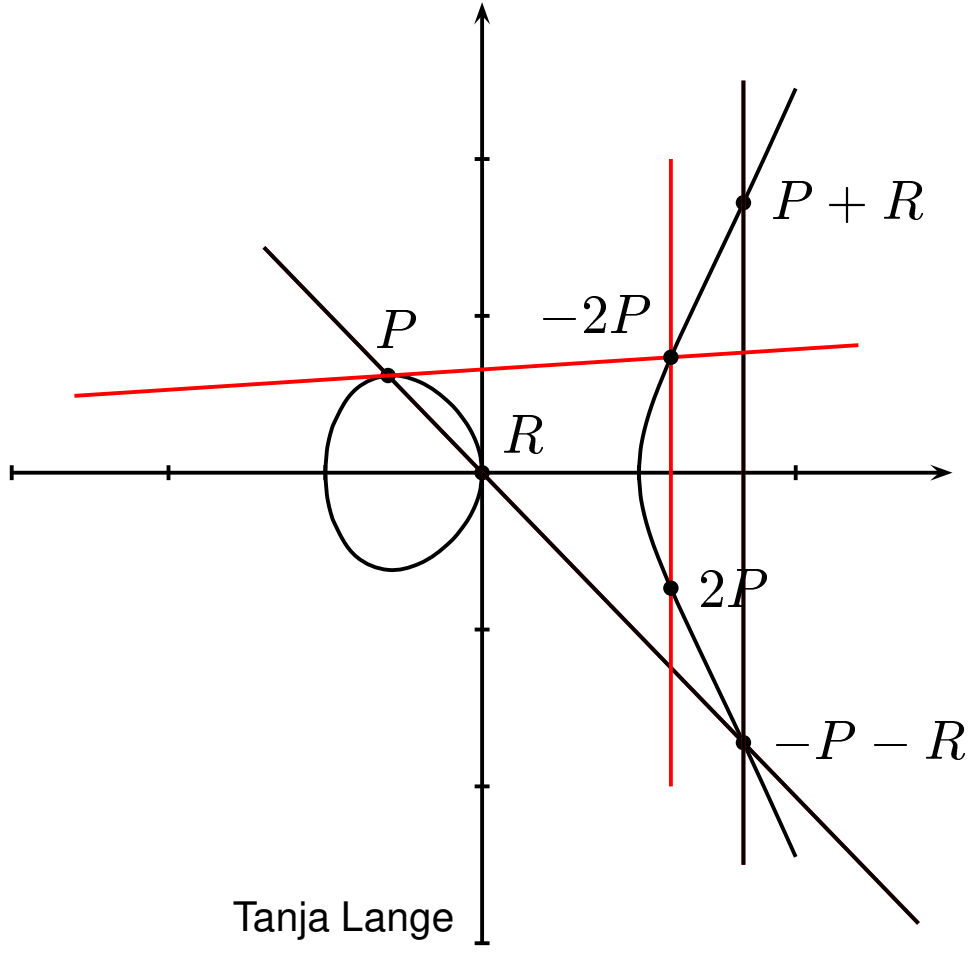


over $\mathbb{R}$

Elliptic Curve

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

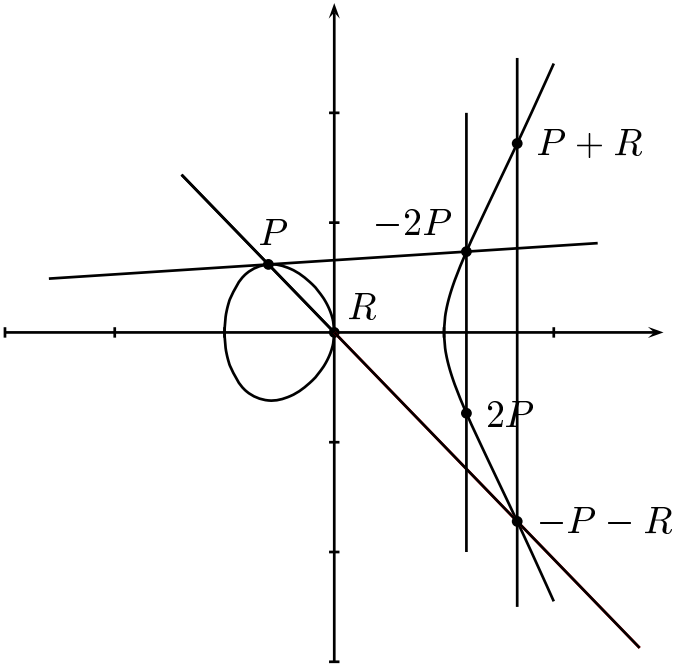
Group: $E(\mathbb{F}_q) = \{\, (x, y) \in \mathbb{F}_q^2 \,:\, y^2 + h(x)y = f(x) \,\} \cup \{\, P_\infty \,\}$



over $\mathbb{R}$

Group Law (q odd)

$$E : y^2 = x^3 + a_4x + a_6, \ a_i \in \mathbb{F}_q$$



for $(x_1, y_1) \neq (x_2, -y_2)$:

$$\begin{aligned}(x_1, y_1) + (x_2, y_2) &= \\ &= (x_3, y_3) = \\ &= (\lambda^2 - x_1 - x_2, \lambda(x_1 - x_3) - y_1),\end{aligned}$$

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.

1 I, 2M, 1S vs. 1 I, 2M, 2S

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

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 $Q = Q + P$
5. 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 $Q = Q + P$
   else $R = Q + P$ //dummy operation
5. output Q

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

Montgomery Ladder (Arbitrary Group)

Idea: Make used addition per round.

Consider the intermediate results (i is decreasing).

$Q_i = \sum_{j=i}^{l} n_j 2^{j-i} P$, 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

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

$$13 = (1101)_2 \sim \begin{array}{rcl} (Q_3, R_3) & = & (P, 2P) \\ (Q_2, R_2) & = & (3P, 4P) \\ (Q_1, R_1) & = & (6P, 7P) \\ (Q_0, R_0) & = & (13P, 14P) \end{array}$$

Montgomery Arithmetic for EC

Advantages:

- Needs only x coordinate (not y)
  $\Rightarrow$ lower storage requirement compared to full Montgomery ladder.
- Projective version (no inversion) extremely efficient for special curves (uses x and z) $\Rightarrow$ Montgomery curves (curves were proposed for ECM factoring due to fast group operation).
- Shielded against SPA (Brier/Joye for arbritrary curves), slower than for general curves but faster than full doubling and addition and less storage needed.

Uniform Group Operations

Liardet and Smart CHES 2001
Brier and Joye AAECC 2003
Brier, Déchène, and Joye 2004
$\Rightarrow$ Jacobi-Model

Joye and Quisquater $\Rightarrow$ Hessian Curve

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

$$\lambda = \frac{(x_1 + x_2)^2 - x_1 x_2 + a + y_1 - y_2}{y_1 + y_2 + x_1 - x_2}$$

(Some special cases may occur, but with very low probability, e. g. $x_2 = y_1 + y_2 + x_1$.)

Side-Channel Atomicity

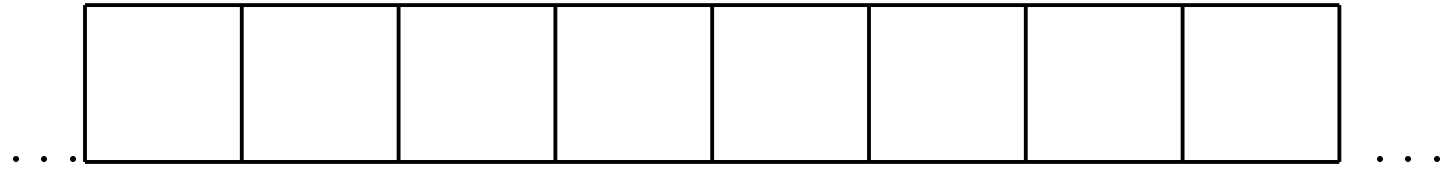
Chevallier-Mames, Ciet, and Joye 2003:
add only cheap dummy operations
⇒ build group operation from identical blocks.

Each block consists of:

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

fill with dummy operations
(only addition and negation ⇒ 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)

Side-Channel Atomicity

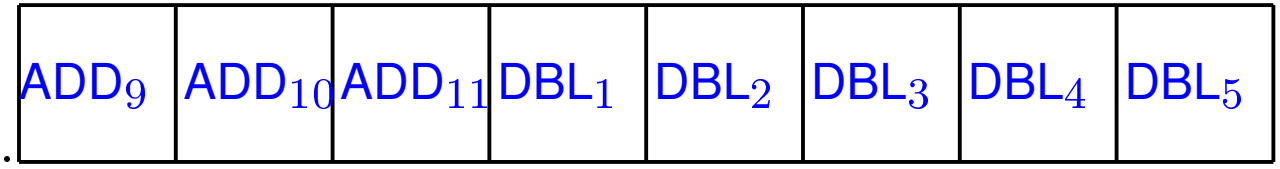
Chevallier-Mames, Ciet, and Joye 2003:
add only cheap dummy operations
$\Rightarrow$ build group operation from identical blocks.

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 Curves

Hyperelliptic curve

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

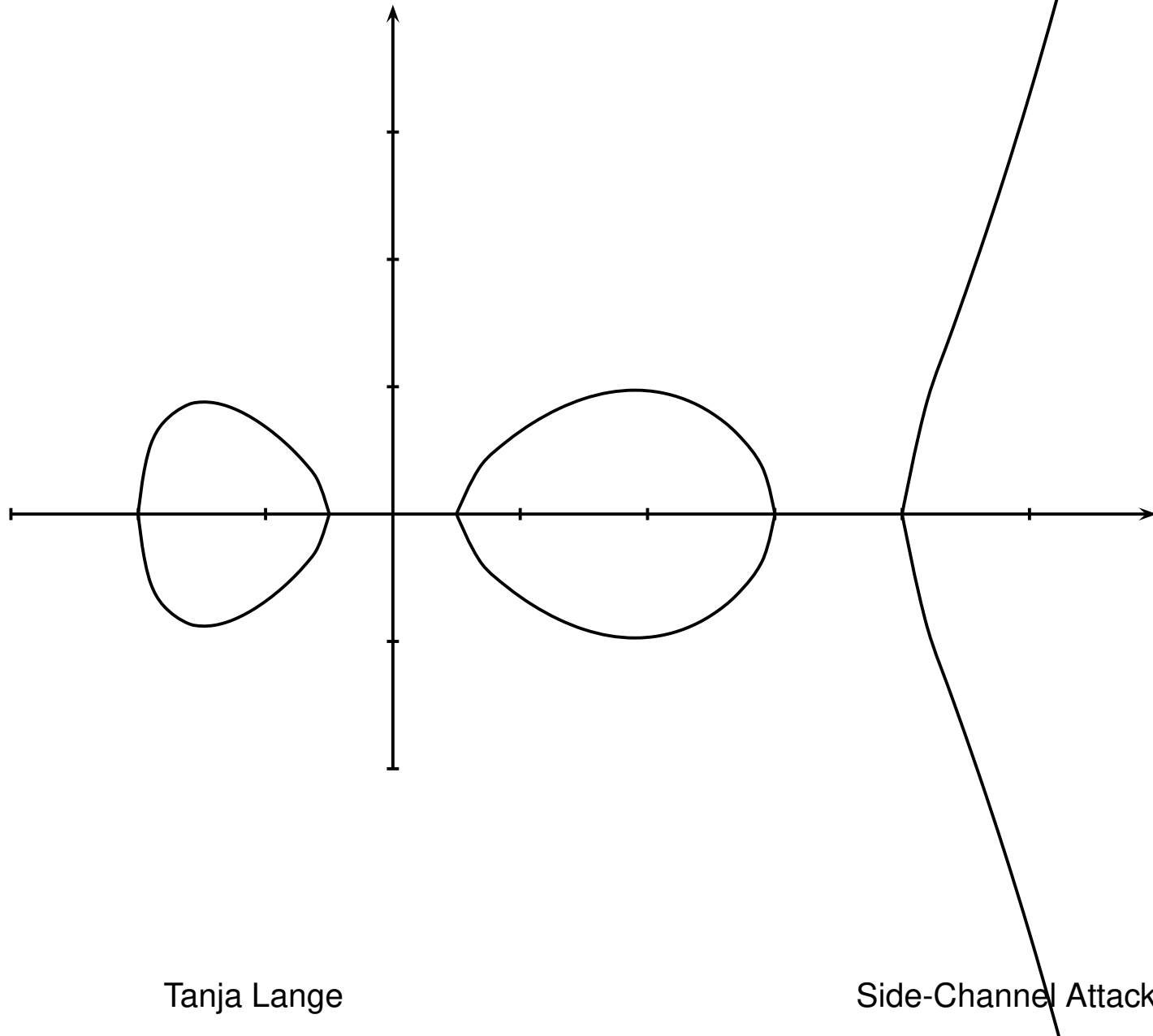
$h(x), f(x) \in \mathbb{F}_q[x]$, q prime power,
f monic, $\deg f = 2g + 1, \deg h \leq g$
nonsingular, i. e. not both partial derivatives zero for
$(a, b) \in C/\bar{\mathbb{F}}_q$

C hyperelliptic curve of genus g

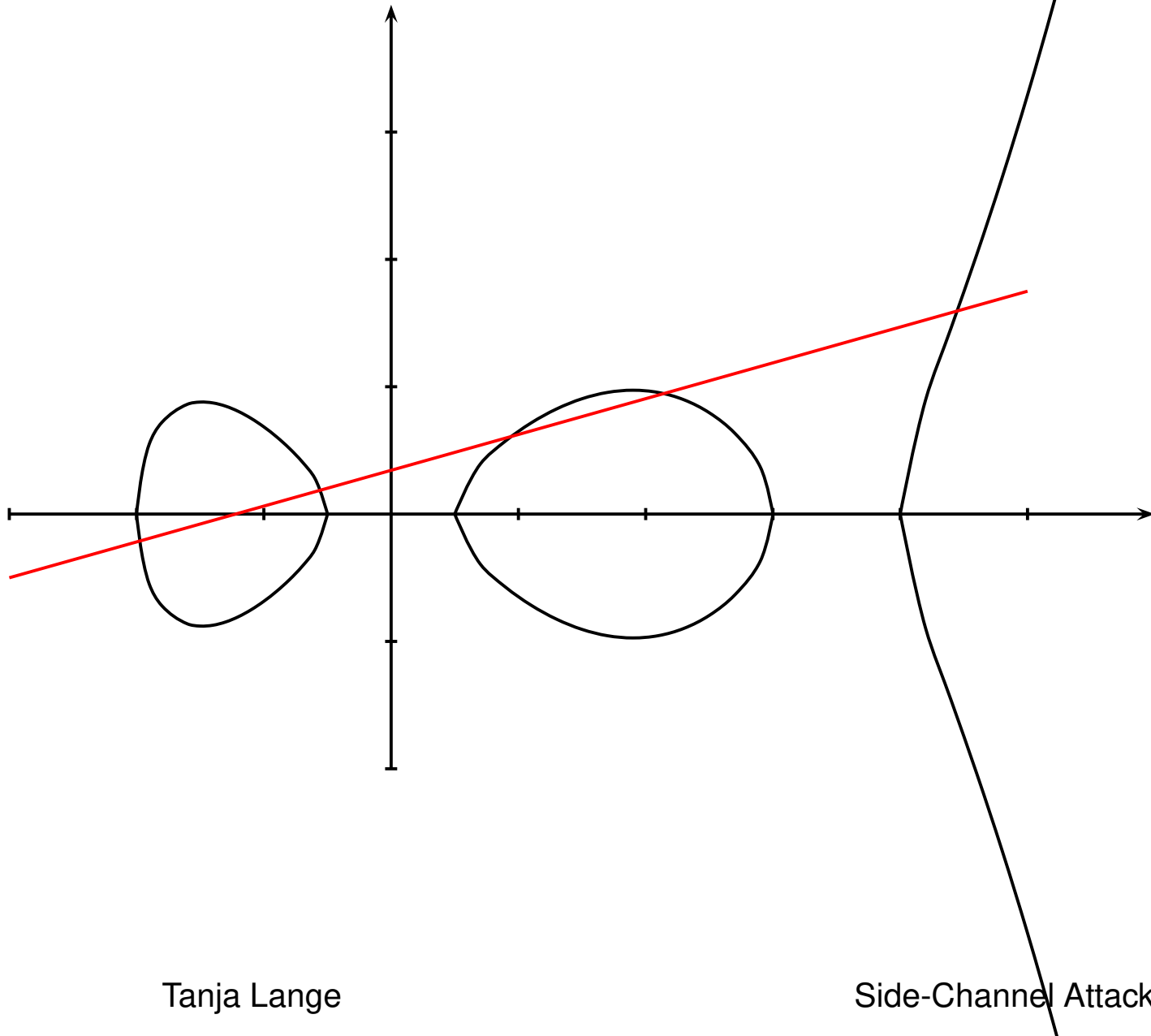
with at least one $\mathbb{F}_q$-rational Weierstraß point
(elliptic curves are seen here as curves of genus 1)
We concentrate on $g = 2$ and odd characteristic > 5

$$C : y^2 = x^5 + f_3x^3 + f_2x^2 + f_1x + f_0.$$

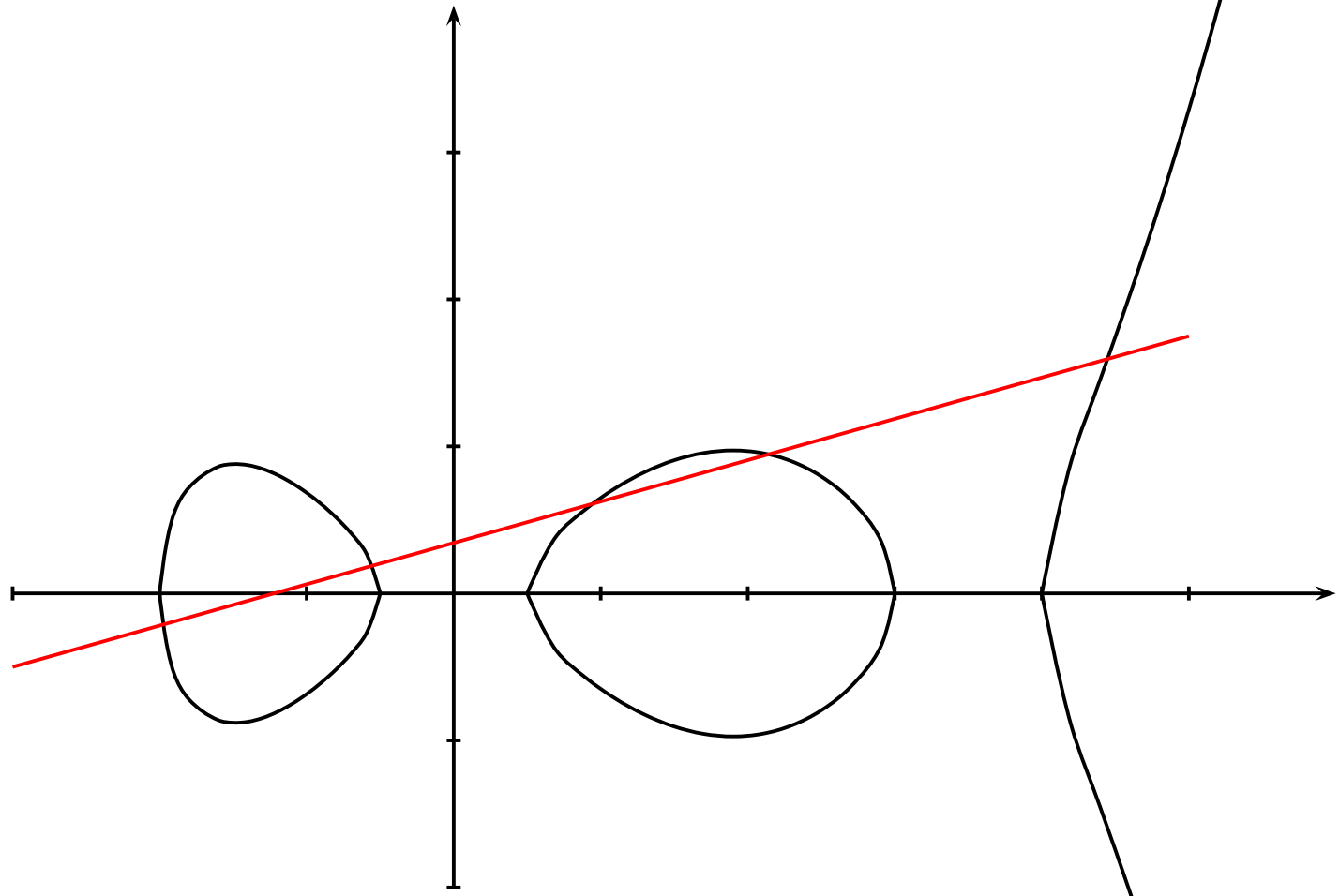
Curve of Genus 2 over $\mathbb{R}$



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



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



Points do not form a group

Group

Use divisors, i. e. sums of points, of degree zero and reduce modulo principal divisors (divisors belonging to functions)

$\Rightarrow$ divisor class group

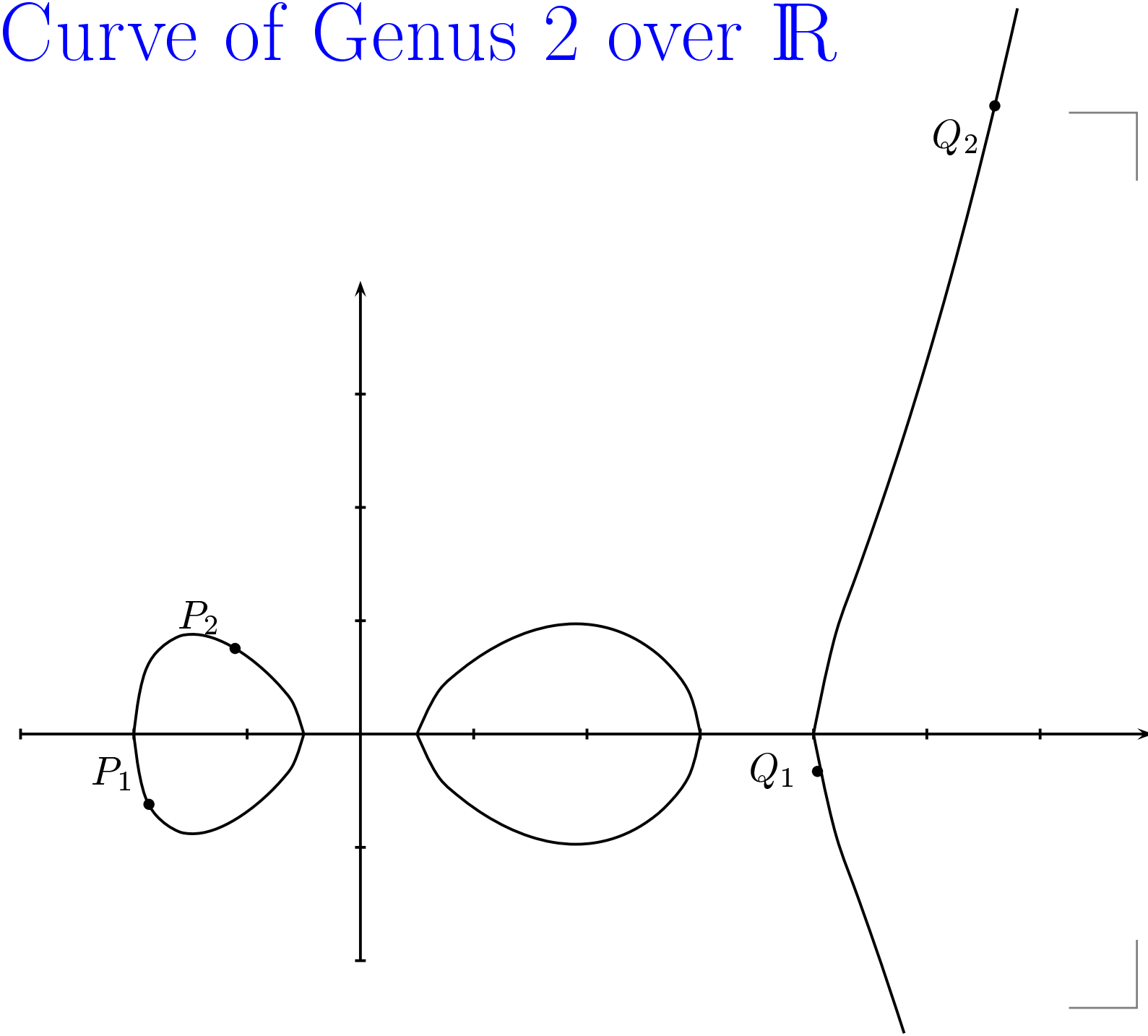
$$\mathrm{Pic}^0(C/\mathbb{F}_q) = Div^0(C/\mathbb{F}_q)/P(C/\mathbb{F}_q).$$

Each class is uniquely represented by degree zero divisor with $m \leq g$

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

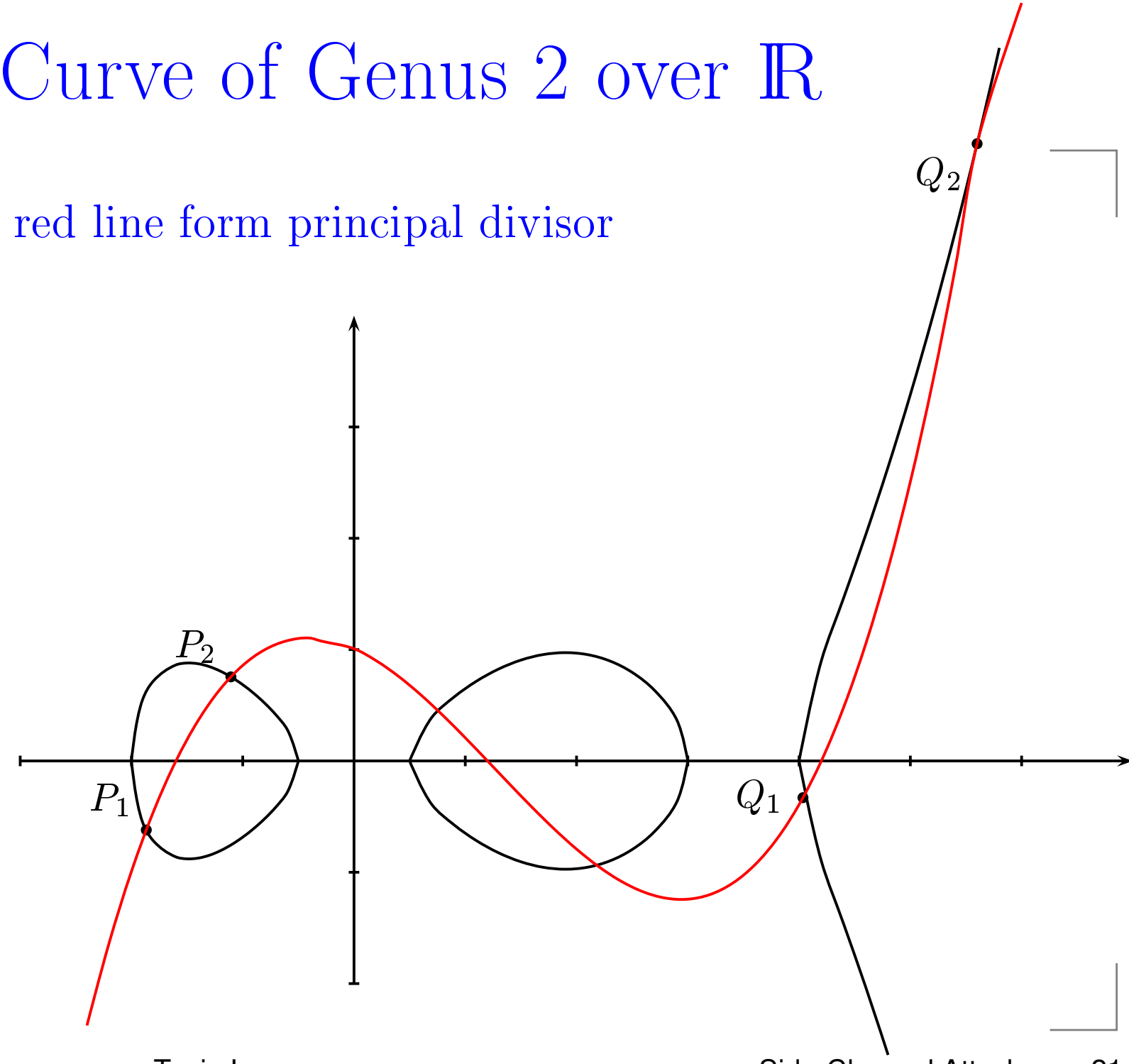
and $P_i \neq -P_j$ for $i \neq j$.

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



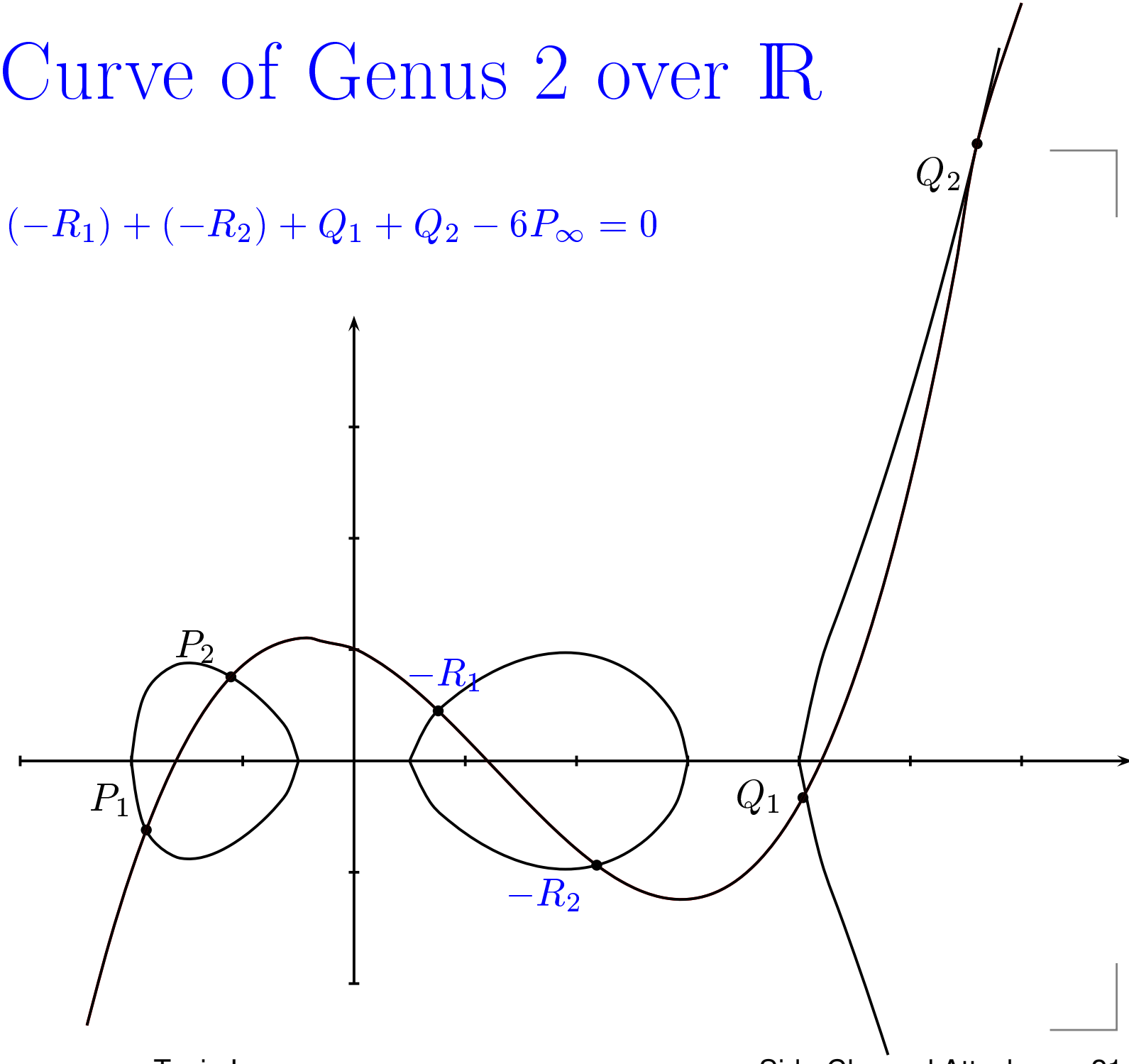
Curve of Genus 2 over $\mathbb{R}$

points on red line form principal divisor



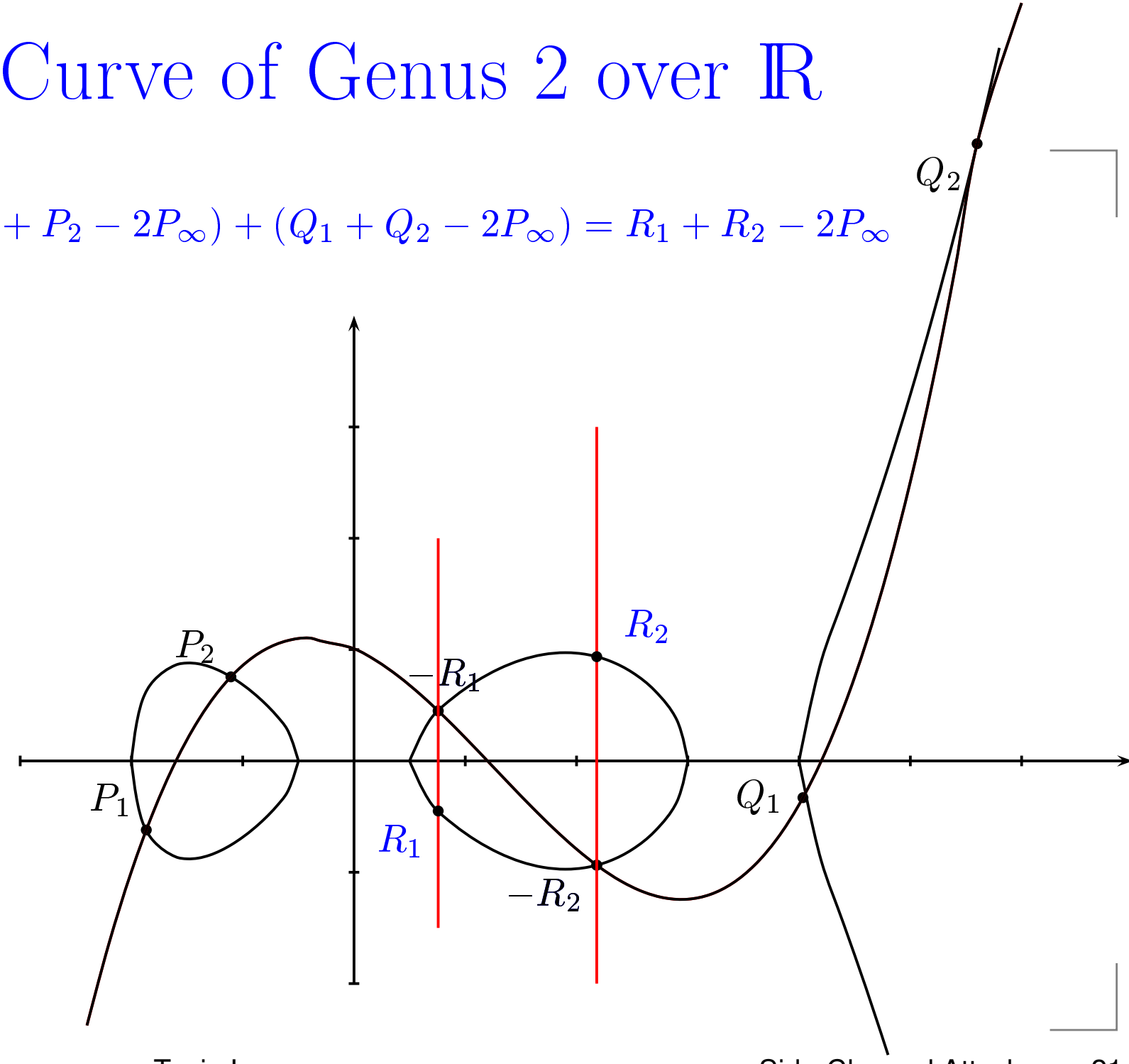
Curve of Genus 2 over $\mathbb{R}$

$$P_1 + P_2 + (-R_1) + (-R_2) + Q_1 + Q_2 - 6P_\infty = 0$$



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

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



Countermeasures for HECC (SPA)

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

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 different 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 $\sim$ 10 years.
Generalization to HECC: Avanzi at CHES 2003
Koblitz curves allow more efficient shielding, (L. 2001)

The End

The END

Thanks!