Preventing SPA-type Attacks for Hyperelliptic Curve Cryptography

– O. Diao (Freelance – Rennes)

– M. Joye (Technicolor – Rennes)

Journées Codage et Cryptographie 2012

Dinard, October 7-12

Submitted: US Patent-2012, WMC-2012, JSC-2013.

Outline

Outline

Introduction & Motivation

- **D**iscrete **L**ogarithm **P**roblem: let $G := (\langle a \rangle, +)$ be a group and let $b \in G$, how to compute "easily" n such that $b = na = \underbrace{a + \cdots + a}_{n \text{ times}}$

Introduction & Motivation

- **D**iscrete **L**ogarithm **P**roblem: let $G := (\langle a \rangle, +)$ be a group and let $b \in G$, how to compute "easily" n such that $b = na = \underbrace{a + \cdots + a}_{n \text{ times}}$
- [Miller 86] & [Koblitz 87 & 89] conjectured that **DLP** is very hard over rational points of elliptic curves and Jacobian of HEC.
- Security on Jacobian of HEC is based on **DLP**
- Solve HCDLP is done with generic methods (except $g \geq 3$)

Introduction & Motivation

- **D**iscrete **L**ogarithm **P**roblem: let $G := (\langle a \rangle, +)$ be a group and let $b \in G$, how to compute "easily" n such that $b = na = \underbrace{a + \cdots + a}_{n \text{ times}}$
- [Miller 86] & [Koblitz 87 & 89] conjectured that **DLP** is very hard over rational points of elliptic curves and Jacobian of HEC.
- Security on Jacobian of HEC is based on **DLP**
- Solve HCDLP is done with generic methods (except $g \geq 3$)
- Hyperelliptic curve (HEC) is a "good" alternative to RSA
- Why curves? See [Certicom & Nessie'03]

RSA key size	1024	2048	3072	7680	15360
ECC key size	160	224	256	384	512

Introduction & Motivation

- **D**iscrete **L**ogarithm **P**roblem: let $G := (\langle a \rangle, +)$ be a group and let $b \in G$, how to compute "easily" n such that $b = na = \underbrace{a + \cdots + a}_{n \text{ times}}$
- [Miller 86] & [Koblitz 87 & 89] conjectured that **DLP** is very hard over rational points of elliptic curves and Jacobian of HEC.
- Security on Jacobian of HEC is based on **DLP**
- Solve HCDLP is done with generic methods (except $g \geq 3$)
- Hyperelliptic curve (HEC) is a "good" alternative to RSA
- For security, hardness of HCDLP is necessary but not sufficient
- We can have Simple Power Analysis by monitoring execution of scalar mult. algorithm (compute na from n and a – secret is n)

SPA & Countermeasures

- **Simple Power Analysis** is a form of SCA where attacker measure
  - power consumption [Kocher & al. 99 – CRYPTO]
- **Power consumption** of a chip depends on:
  - the manipulated data
  - the executed instruction

SPA & Countermeasures

- **Simple Power Analysis** is a form of SCA where attacker measure
  - power consumption [Kocher & al. 99 – CRYPTO]
- **Power consumption** of a chip depends on:
  - the manipulated data
  - the executed instruction
- **Countermeasures for genus 2 HECC**:
  - Montgomerry ladder [Duq 04, Gaud 07, GaudLub 08, D. 10]
  - atomicity [Lange & Mishra 04]
  - unified addition law [D. 10]
- Theses countermeasures are at first given for elliptic curves:

[Montgomerry 87, Brier & Joye 03, Edwards 07, $\cdots$]

SPA & Countermeasures

- **Simple Power Analysis** is a form of SCA where attacker measure
  - power consumption [Kocher & al. 99 – CRYPTO]
- **Power consumption** of a chip depends on:
  - the manipulated data
  - the executed instruction
- **Countermeasures for genus 2 HECC**:
  - Montgomerry ladder [Duq 04, Gaud 07, GaudLub 08, D. 10]
  - atomicity [Lange & Mishra 04]
  - unified addition law [D. 10 & **this work**]
- This work is an **efficient** unified addition formulas using **geometric description** of group law as [Costello & Lauter 11]

Outline

Hyperelliptic curves

– Let $\mathbb{K}$ be a field of char. $p \geq 0$ and let $g \geq 1$ be an integer

– HEC of genus g is $C := \{(x, y) \in \overline{\mathbb{K}}^2, y^2 + h(x)y = f(x)\} \cup \{\infty\}$,

where $f, h \in \mathbb{K}[x]$ with f monic, $\deg f = 2g + 1, \deg h \leq g$

– C is smooth, i.e. $H = y^2 + hy - f \in \mathbb{K}[x, y]$ is irreducible

Hyperelliptic curves

– Let $\mathbb{K}$ be a field of char. $p \geq 0$ and let $g \geq 1$ be an integer

– HEC of genus g is $C := \{(x, y) \in \overline{\mathbb{K}}^2, y^2 + h(x)y = f(x)\} \cup \{\infty\}$,

where $f, h \in \mathbb{K}[x]$ with f monic, $\deg f = 2g + 1, \deg h \leq g$

– C is smooth, i.e. $H = y^2 + hy - f \in \mathbb{K}[x, y]$ is irreducible

– $\mathbb{K}[C] = \mathbb{K}[x, y]/(H(x, y))$ is the coordinate ring of C

– $\mathbb{K}(C) :=$ Fraction field($\mathbb{K}[C]$) is the Function field of C

elliptic curves := genus 1 hyperelliptic curves

– Rational points $C(\mathbb{K})$ do not form a group law (except $g = 1$)

$\Longrightarrow$ use divisors to have a group.

Jacobian of hyperelliptic curves

Divisor: finite formal sum of points $D := \sum_{P \in C(\overline{\mathbb{K}})} n_P(P), \quad n_P \in \mathbb{Z}$

– $\mathrm{Div}(C) = \{\text{set of divisors}\}$ is a group divisors

– degree $\deg D := \sum_{P \in C(\overline{\mathbb{K}})} n_P$

– $\psi \in \mathbb{K}(C) \Rightarrow \mathrm{div}(\psi) := \sum_{P \in C(\overline{\mathbb{K}})} \nu_P(\psi)(P)$ of degree zero

– $\mathrm{Div}^0(C)$: group of divisors of degree zero

– $\mathrm{Princ}(C)$: group of divisors of functions (subset of $\mathrm{Div}^0(C)$)

Jacobian: $J(C) := \mathrm{Div}^0(C)/\mathrm{Princ}(C)$.

Jacobian of hyperelliptic curves

Divisor: finite formal sum of points $D := \sum_{P \in C(\overline{\mathbb{K}})} n_P(P), \quad n_P \in \mathbb{Z}$

– $\mathrm{Div}(C) = \{\text{set of divisors}\}$ is a group divisors

– degree $\deg D := \sum_{P \in C(\overline{\mathbb{K}})} n_P$

– $\psi \in \mathbb{K}(C) \Rightarrow \mathrm{div}(\psi) := \sum_{P \in C(\overline{\mathbb{K}})} \nu_P(\psi)(P)$ of degree zero

– $\mathrm{Div}^0(C)$: group of divisors of degree zero

– $\mathrm{Princ}(C)$: group of divisors of functions (subset of $\mathrm{Div}^0(C)$)

Jacobian: $J(C) := \mathrm{Div}^0(C)/\mathrm{Princ}(C)$.

Elements of $J(C)$ can be uniquely represented as reduced divisor

[Riemann-Roch]:

$$D = \sum_{i=1}^{m} (P_i) - m(\infty), \text{ with } m \leq g$$

Jacobian of hyperelliptic curves

Divisor: finite formal sum of points $D := \sum_{P \in C(\overline{\mathbb{K}})} n_P(P), \quad n_P \in \mathbb{Z}$

– $\mathrm{Div}(C) = \{\text{set of divisors}\}$ is a group divisors

– degree $\deg D := \sum_{P \in C(\mathbb{K})} n_P$

– $\psi \in \mathbb{K}(C) \Rightarrow \mathrm{div}(\psi) := \sum_{P \in C(\overline{\mathbb{K}})} \nu_P(\psi)(P)$ of degree zero

– $\mathrm{Div}^0(C)$: group of divisors of degree zero

– $\mathrm{Princ}(C)$: group of divisors of functions (subset of $\mathrm{Div}^0(C)$)

Jacobian: $J(C) := \mathrm{Div}^0(C)/\mathrm{Princ}(C)$.

– For all $D = \sum_{i=1}^{m}(P_i) - m(\infty) \in J(C)$, $\exists\ !\ u(x), v(x) \in \mathbb{K}[x]$ s.t.

(i) $u(x) = \prod_{i=1}^{m}(x - x_i)$, where $x_i = x(P_i)$

(ii) $v(x)$ is polynomial of degree $< m$ such that $v(x_i) = y_i$

Jacobian of hyperelliptic curves

Divisor: finite formal sum of points $D := \sum_{P \in C(\overline{\mathbb{K}})} n_P(P), \quad n_P \in \mathbb{Z}$

– $\mathrm{Div}(C) = \{\text{set of divisors}\}$ is a group divisors

– degree $\deg D := \sum_{P \in C(\overline{\mathbb{K}})} n_P$

– $\psi \in \mathbb{K}(C) \Rightarrow \mathrm{div}(\psi) := \sum_{P \in C(\overline{\mathbb{K}})} \nu_P(\psi)(P)$ of degree zero

– $\mathrm{Div}^0(C)$: group of divisors of degree zero

– $\mathrm{Princ}(C)$: group of divisors of functions (subset of $\mathrm{Div}^0(C)$)

Jacobian: $J(C) := \mathrm{Div}^0(C)/\mathrm{Princ}(C)$.

– For all $D = \sum_{i=1}^{m}(P_i) - m(\infty) \in J(C)$, $\exists\ !\ u(x), v(x) \in \mathbb{K}[x]$ s.t.

(i) $u(x) = \prod_{i=1}^{m}(x - x_i)$,

(ii) $\iff v^2 + vh - f \equiv 0 \bmod u$

$D := [u, v]$ is the Mumford representation of semi-reduced divisor

Jacobian of hyperelliptic curves

Divisor: finite formal sum of points $D := \sum_{P \in C(\overline{\mathbb{K}})} n_P(P), \quad n_P \in \mathbb{Z}$

– $\mathrm{Div}(C) = \{\text{set of divisors}\}$ is a group divisors

– degree $\deg D := \sum_{P \in C(\overline{\mathbb{K}})} n_P$

– $\psi \in \mathbb{K}(C) \Rightarrow \mathrm{div}(\psi) := \sum_{P \in C(\overline{\mathbb{K}})} \nu_P(\psi)(P)$ of degree zero

– $\mathrm{Div}^0(C)$: group of divisors of degree zero

– $\mathrm{Princ}(C)$: group of divisors of functions (subset of $\mathrm{Div}^0(C)$)

Jacobian: $J(C) := \mathrm{Div}^0(C)/\mathrm{Princ}(C)$.

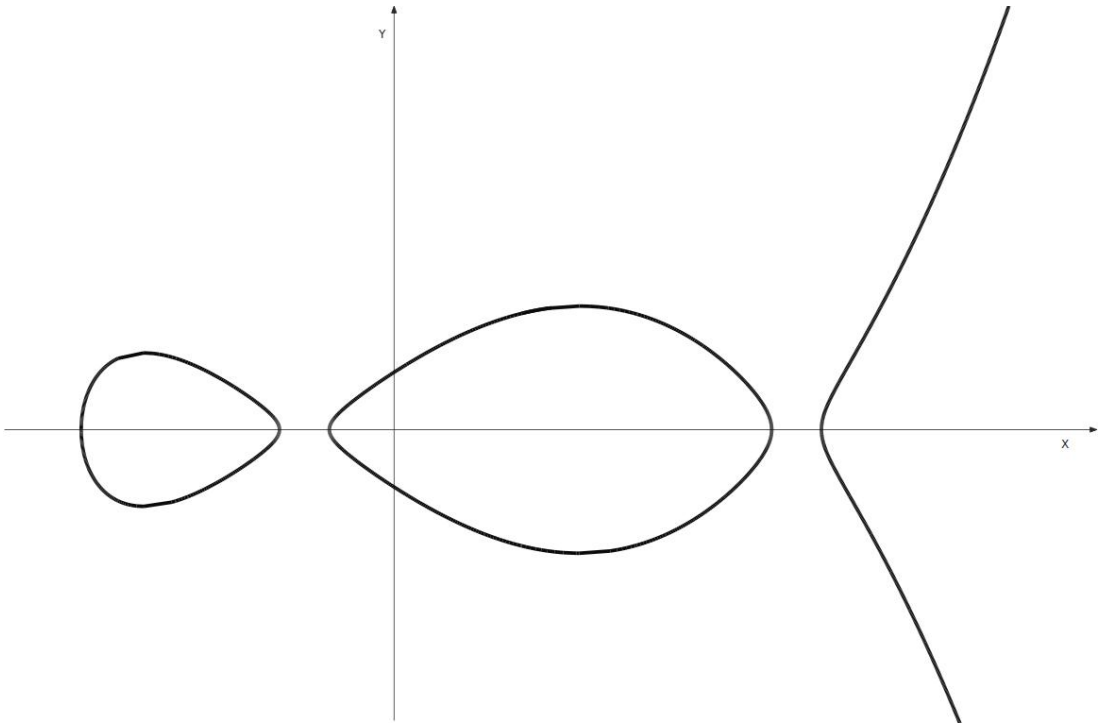
– For all $D = \sum_{i=1}^{m}(P_i) - m(\infty) \in J(C)$, $\exists\ !\ u(x), v(x) \in \mathbb{K}[x]$ s.t.

(i) $u(x) = \prod_{i=1}^{m}(x - x_i)$,

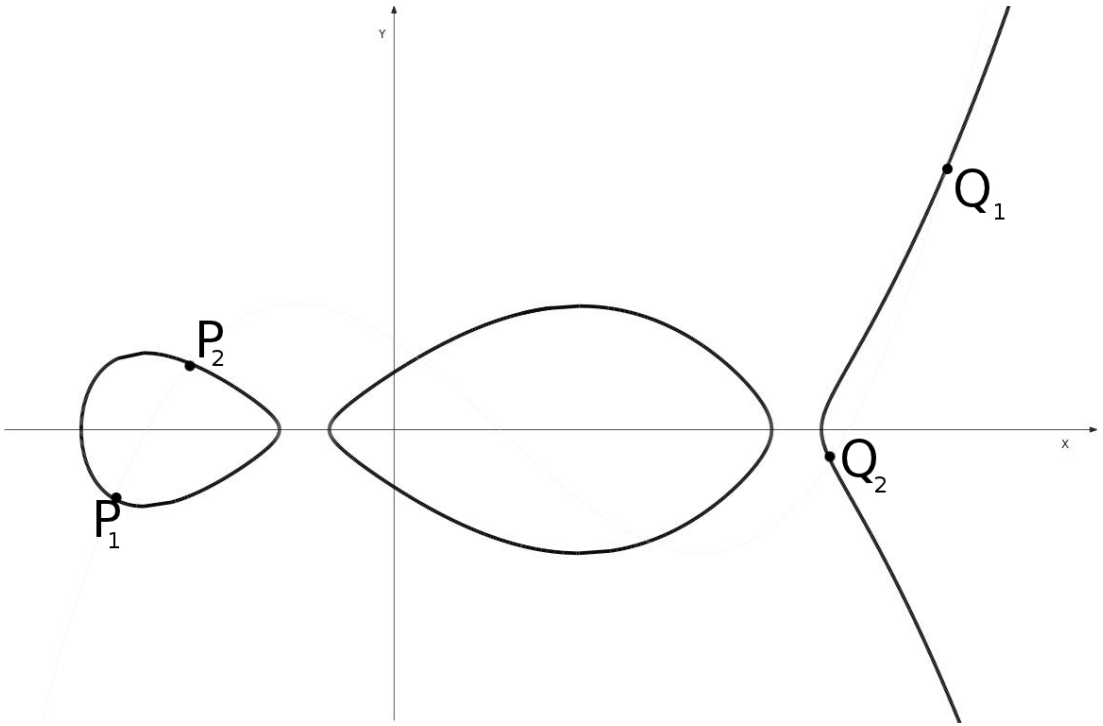
(ii) $\iff v^2 + vh - f \equiv 0 \bmod u$

- [Cantor 87] gives an algorithm for the arithmetic on Jacobian.

Addition law on genus 2 curve over $\mathbb{R}$

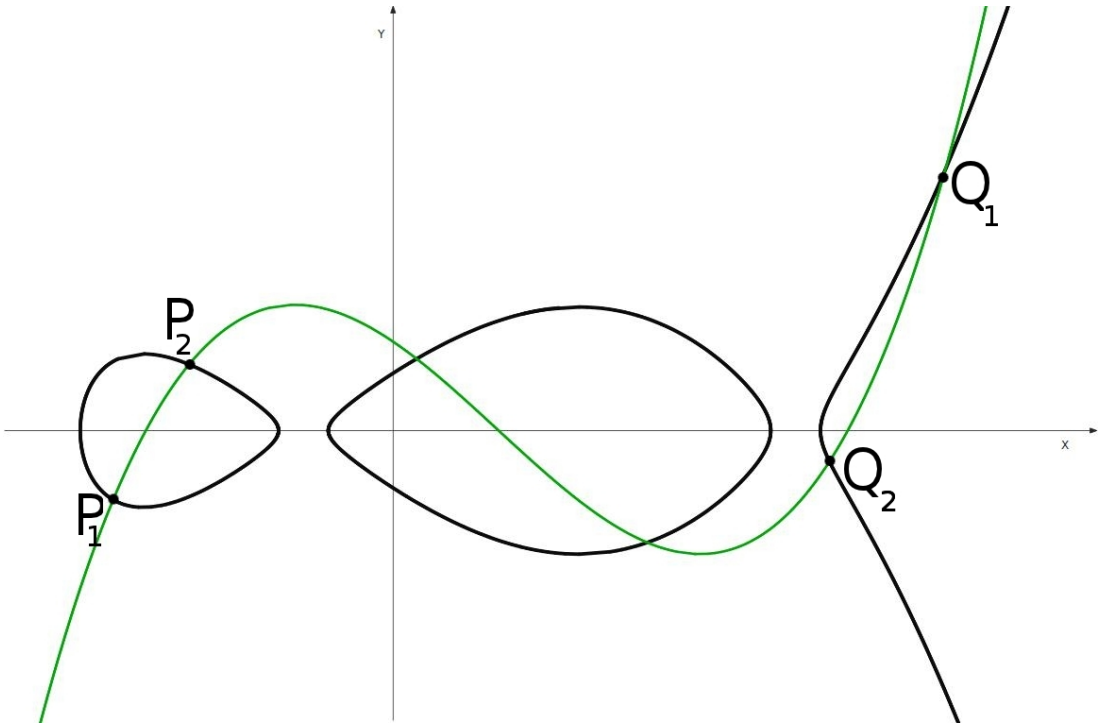


Addition law on genus 2 curve over $\mathbb{R}$



$$D_1 = (P_1) + (P_2) - 2(\infty) = [u_1, v_1] \qquad D_2 = (Q_1) + (Q_2) - 2(\infty) = [u_2, v_2]$$

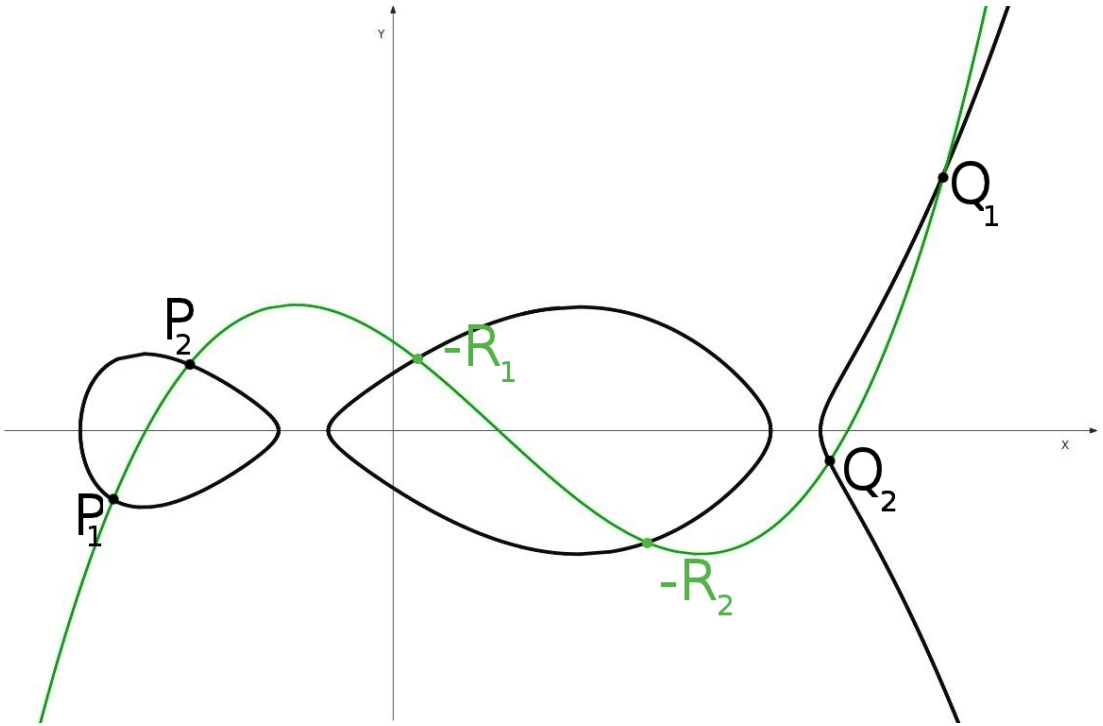
Addition law on genus 2 curve over $\mathbb{R}$



$D_1 = (P_1) + (P_2) - 2(\infty) = [u_1, v_1]$ $\quad$ $D_2 = (Q_1) + (Q_2) - 2(\infty) = [u_2, v_2]$

polynomial $\mathbf{v}$ s.t. $\mathbf{v(x_i) = y_i} \Leftrightarrow \mathbf{v \equiv v_i} \bmod \mathbf{u_i} \Leftrightarrow \mathbf{v^2 + vh - f \equiv 0} \bmod \mathbf{u_1 u_2}$

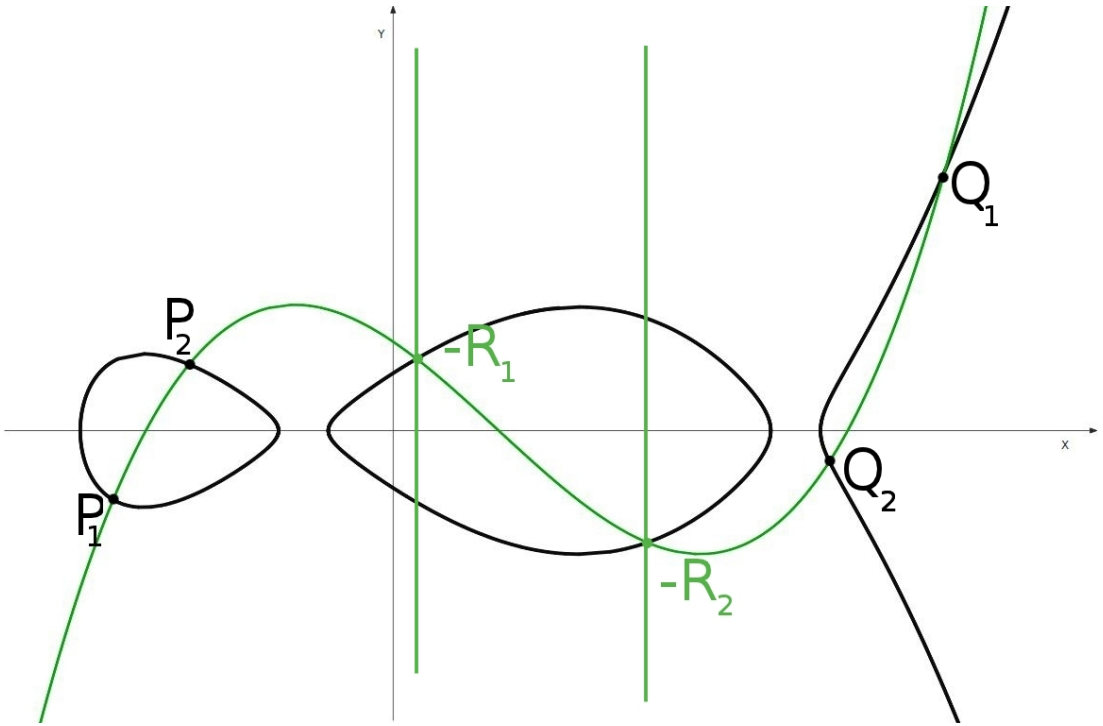
Addition law on genus 2 curve over $\mathbb{R}$



$D_1 = (P_1) + (P_2) - 2(\infty) = [u_1, v_1]$ $\quad$ $D_2 = (Q_1) + (Q_2) - 2(\infty) = [u_2, v_2]$

polynomial $\mathbf{v}$ s.t. $\mathbf{v(x_i) = y_i} \Leftrightarrow \mathbf{v \equiv v_i} \bmod \mathbf{u_i} \Leftrightarrow \mathbf{v^2 + vh - f \equiv 0} \bmod \mathbf{u_1 u_2}$

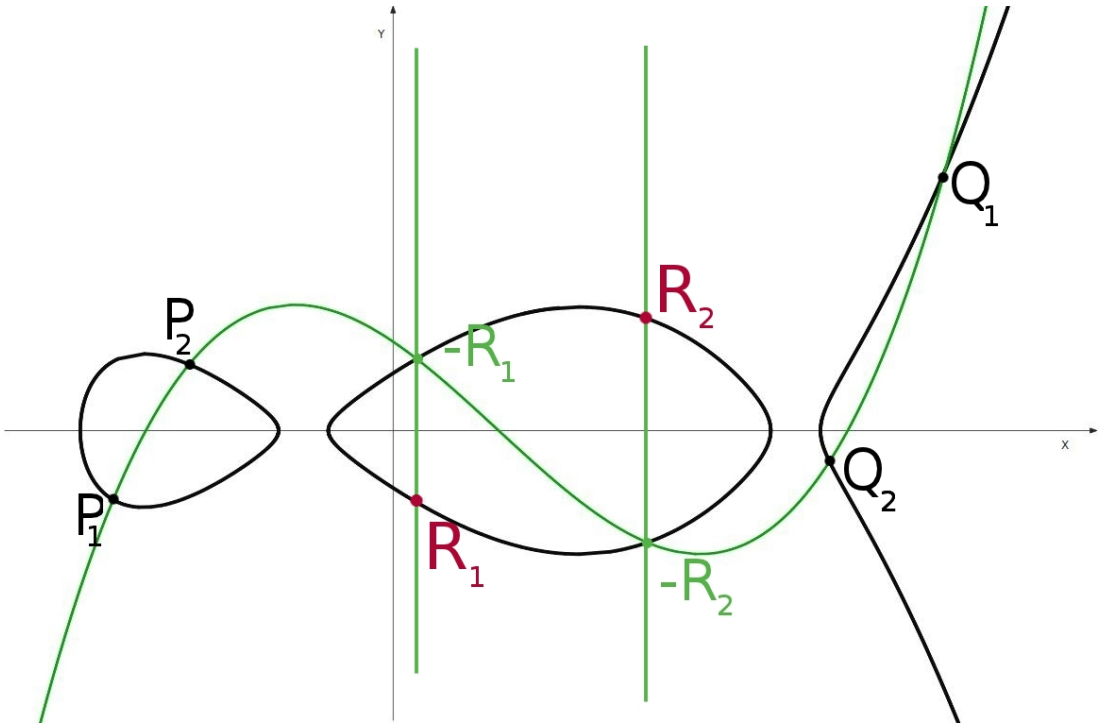
Addition law on genus 2 curve over $\mathbb{R}$



$D_1 = (P_1) + (P_2) - 2(\infty) = [u_1, v_1]$ $\quad$ $D_2 = (Q_1) + (Q_2) - 2(\infty) = [u_2, v_2]$

polynomial $\mathbf{v}$ s.t. $\mathbf{v(x_i) = y_i} \Leftrightarrow \mathbf{v \equiv v_i} \bmod \mathbf{u_i} \Leftrightarrow \mathbf{v^2 + vh - f \equiv 0} \bmod \mathbf{u_1 u_2}$

Addition law on genus 2 curve over $\mathbb{R}$



$D_1 = (P_1) + (P_2) - 2(\infty) = [u_1, v_1]$ $\quad$ $D_2 = (Q_1) + (Q_2) - 2(\infty) = [u_2, v_2]$

polynomial $\mathbf{v}$ s.t. $\mathbf{v(x_i) = y_i} \Leftrightarrow \mathbf{v \equiv v_i} \bmod \mathbf{u_i} \Leftrightarrow \mathbf{v^2 + vh - f \equiv 0} \bmod \mathbf{u_1 u_2}$

$\mathbf{D_1 + D_2 = (R_1) + (R_2) - 2(\infty)}$

Outline

Unified addition formulas

Proposition

Let $D_1 = [u_1, v_1]$ *and* $D_2 = [u_2, v_2] \in J(C) \Rightarrow D_1 + D_2 \sim [u, v]$ *where*

$$u = u_1 u_2 \quad \text{and} \quad v(h + v_1 + v_2) \equiv f + v_1 v_2 \pmod{u} \ . \tag{1}$$

Goal: compute efficiently the polynomial v.

Proof: we have $v^2 + vh - f \equiv 0 \bmod u$

Unified addition formulas

Proposition

Let $D_1 = [u_1, v_1]$ *and* $D_2 = [u_2, v_2] \in J(C) \Rightarrow D_1 + D_2 \sim [u, v]$ *where*

$$u = u_1 u_2 \quad \text{and} \quad v(h + v_1 + v_2) \equiv f + v_1 v_2 \pmod{u} \ . \tag{1}$$

Goal: compute efficiently the polynomial v.

Proof: we have $v(v + h) \equiv f \bmod u$

Unified addition formulas

Proposition

Let $D_1 = [u_1, v_1]$ *and* $D_2 = [u_2, v_2] \in J(C) \Rightarrow D_1 + D_2 \sim [u, v]$ *where*

$$u = u_1 u_2 \quad \text{and} \quad v(h + v_1 + v_2) \equiv f + v_1 v_2 \pmod{u} \ . \tag{1}$$

Goal: compute efficiently the polynomial v.

Proof: we have

$$v(v + h) \equiv f \bmod u$$

$$v(v_1 + s_1 u_1 + h) \equiv f \bmod u$$

because $v \equiv v_i \bmod u_i$ for $i = 1, 2, \implies v = v_1 + s_1 u_1$.

Unified addition formulas

Proposition

Let $D_1 = [u_1, v_1]$ *and* $D_2 = [u_2, v_2] \in J(C) \Rightarrow D_1 + D_2 \sim [u, v]$ *where*

$$u = u_1 u_2 \quad \text{and} \quad v(h + v_1 + v_2) \equiv f + v_1 v_2 \pmod{u} \ . \tag{1}$$

Goal: compute efficiently the polynomial v.

Proof: we have

$$v(v + h) \equiv f \bmod u$$

$$v(v_1 + s_1 u_1 + h) + v_1 v_2 \equiv f + v_1 v_2 \bmod u$$

Unified addition formulas

Proposition

Let $D_1 = [u_1, v_1]$ *and* $D_2 = [u_2, v_2] \in J(C) \Rightarrow D_1 + D_2 \sim [u, v]$ *where*

$$u = u_1 u_2 \quad \text{and} \quad v(h + v_1 + v_2) \equiv f + v_1 v_2 \pmod{u} \ . \tag{1}$$

Goal: compute efficiently the polynomial v.

Proof: we have

$$v(v + h) \equiv f \bmod u$$

$$v(v_1 + s_1 u_1 + h) + v_2 v_1 \equiv f + v_1 v_2 \bmod u$$

$$v(v_1 + s_1 u_1 + h) + v_2(v - s_1 u_1) \equiv f + v_1 v_2 \bmod u$$

remenber $v = v_1 + s_1 u_1 \implies v_1 = v - s_1 u_1$.

Unified addition formulas

Proposition

Let $D_1 = [u_1, v_1]$ *and* $D_2 = [u_2, v_2] \in J(C) \Rightarrow D_1 + D_2 \sim [u, v]$ *where*

$$u = u_1 u_2 \quad \text{and} \quad v(h + v_1 + v_2) \equiv f + v_1 v_2 \pmod{u} \ . \tag{1}$$

Goal: compute efficiently the polynomial v.

Proof: we have

$$\begin{aligned} v(v + h) &\equiv f \bmod u \\ v(v_1 + s_1 u_1 + h) + v_2 v_1 &\equiv f + v_1 v_2 \bmod u \\ v(v_1 + s_1 u_1 + h) + v_2 v - s_1 u_1 v_2 &\equiv f + v_1 v_2 \bmod u \end{aligned}$$

Unified addition formulas

Proposition

Let $D_1 = [u_1, v_1]$ *and* $D_2 = [u_2, v_2] \in J(C) \Rightarrow D_1 + D_2 \sim [u, v]$ *where*

$$u = u_1 u_2 \quad \text{and} \quad v(h + v_1 + v_2) \equiv f + v_1 v_2 \pmod{u} \ . \tag{1}$$

Goal: compute efficiently the polynomial v.

Proof: we have

$$\begin{aligned} v(v + h) &\equiv f \bmod u \\ v(v_1 + s_1 u_1 + h) + v_2 v_1 &\equiv f + v_1 v_2 \bmod u \\ v(v_1 + s_1 u_1 + h) + v_2 v - s_1 u_1 v_2 &\equiv f + v_1 v_2 \bmod u \end{aligned}$$

Unified addition formulas

Proposition

Let $D_1 = [u_1, v_1]$ *and* $D_2 = [u_2, v_2] \in J(C) \Rightarrow D_1 + D_2 \sim [u, v]$ *where*

$$u = u_1 u_2 \quad \text{and} \quad v(h + v_1 + v_2) \equiv f + v_1 v_2 \pmod{u} \ . \tag{1}$$

Goal: compute efficiently the polynomial v.

Proof: we have

$$\begin{aligned} v(v + h) &\equiv f \bmod u \\ v(v_1 + s_1 u_1 + h) + v_2 v_1 &\equiv f + v_1 v_2 \bmod u \\ v(v_1 + s_1 u_1 + h) + v_2 v - s_1 u_1 v_2 &\equiv f + v_1 v_2 \bmod u \\ v(v_1 + v_2 + h) + s_1 u_1 (v - v_2) &\equiv f + v_1 v_2 \bmod u \end{aligned}$$

Unified addition formulas

Proposition

Let $D_1 = [u_1, v_1]$ *and* $D_2 = [u_2, v_2] \in J(C) \Rightarrow D_1 + D_2 \sim [u, v]$ *where*

$$u = u_1 u_2 \quad \text{and} \quad v(h + v_1 + v_2) \equiv f + v_1 v_2 \pmod{u} \ . \tag{1}$$

Goal: compute efficiently the polynomial v.

Proof: we have

$$\begin{aligned} v(v + h) &\equiv f \bmod u \\ v(v_1 + s_1 u_1 + h) + v_2 v_1 &\equiv f + v_1 v_2 \bmod u \\ v(v_1 + s_1 u_1 + h) + v_2 v - s_1 u_1 v_2 &\equiv f + v_1 v_2 \bmod u \\ v(v_1 + v_2 + h) + \underbrace{s_1 u_1 (v - v_2)}_{= 0 \bmod u} &\equiv f + v_1 v_2 \bmod u \end{aligned}$$

because $v = v_2 + s_2 u_2 \implies s_1 u_1 (v - v_2) = s_1 s_2 u_1 u_2 = 0 \bmod u$. □

Explicit formulas for genus 2

Let $D_i := [\underbrace{x^2 + u_{i,1}x + u_{i,0}}_{u_i}, \underbrace{v_{i,1}x + v_{i,0}}_{v_i}]$, where $u_{i,j}, v_{i,j} \in \mathbb{K}, i = 1, 2$

Goal 1: compute efficiently u, v, s.t. $D_1 + D_2 \sim [u, v]$.

We have $u = u_1 u_2$ and $v = \ell_3 x^3 + \ell_2 x^2 + \ell_1 x + \ell_0$.

Explicit formulas for genus 2

Let $D_i := [\underbrace{x^2 + u_{i,1}x + u_{i,0}}_{u_i}, \underbrace{v_{i,1}x + v_{i,0}}_{v_i}]$, where $u_{i,j}, v_{i,j} \in \mathbb{K}, i = 1, 2$

Goal 1: compute efficiently u, v, s.t. $D_1 + D_2 \sim [u, v]$.

We have $u = u_1 u_2$ and $v = \ell_3 x^3 + \ell_2 x^2 + \ell_1 x + \ell_0$.

$$v \equiv v_1 \bmod u_1 \Longrightarrow \begin{cases} (u_{1,1}^2 - u_{1,0})\ell_3 - u_{1,1}\ell_2 + \ell_1 = v_{1,1} \\ u_{1,1}u_{1,0}\ell_3 - u_{1,0}\ell_2 + \ell_0 = v_{1,0} \end{cases},$$

Equation $v(h + v_1 + v_2) \equiv f + v_1 v_2 \pmod{u}$ of above proposition gives 4 equations with unknown ℓ_i follow powers of x (x^0, x, x^2 and x^3).

Explicit formulas for genus 2

Let $D_i := [\underbrace{x^2 + u_{i,1}x + u_{i,0}}_{u_i}, \underbrace{v_{i,1}x + v_{i,0}}_{v_i}]$, where $u_{i,j}, v_{i,j} \in \mathbb{K}, i = 1, 2$

Goal 1: compute efficiently u, v, s.t. $D_1 + D_2 \sim [u, v]$.

$$\begin{pmatrix} u_{1,1}^2 - u_{1,0} & -u_{1,1} & 1 & 0 \\ u_{1,1}u_{1,0} & -u_{1,0} & 0 & 1 \\ H_0 - (u_{1,1} + u_{2,1})H_1 & H_1 & 0 & 0 \\ -H_1(u_{1,0} + u_{2,0} + u_{1,1}u_{2,1}) & H_0 & H_1 & 0 \\ -H_1(u_{1,1}u_{2,0} + u_{1,0}u_{2,1}) & 0 & H_0 & H_1 \\ -H_1 u_{1,0}u_{2,0} & 0 & 0 & H_0 \end{pmatrix} \cdot \begin{pmatrix} \ell_3 \\ \ell_2 \\ \ell_1 \\ \ell_0 \end{pmatrix} = \begin{pmatrix} v_{1,1} \\ v_{1,0} \\ F_3 \\ F_2 \\ F_1 \\ F_0 \end{pmatrix}.$$

Explicit formulas for genus 2

Let $D_i := [\underbrace{x^2 + u_{i,1}x + u_{i,0}}_{u_i}, \underbrace{v_{i,1}x + v_{i,0}}_{v_i}]$, where $u_{i,j}, v_{i,j} \in \mathbb{K}, i = 1, 2$

Goal 1: compute efficiently u, v, s.t. $D_1 + D_2 \sim [u, v]$.

$$\begin{pmatrix} u_{1,1}^2 - u_{1,0} & -u_{1,1} & 1 & 0 \\ u_{1,1}u_{1,0} & -u_{1,0} & 0 & 1 \\ H_0 - (u_{1,1} + u_{2,1})H_1 & H_1 & 0 & 0 \\ -H_1(u_{1,0} + u_{2,0} + u_{1,1}u_{2,1}) & H_0 & H_1 & 0 \\ -H_1(u_{1,1}u_{2,0} + u_{1,0}u_{2,1}) & 0 & H_0 & H_1 \\ -H_1 u_{1,0}u_{2,0} & 0 & 0 & H_0 \end{pmatrix} \cdot \begin{pmatrix} \ell_3 \\ \ell_2 \\ \ell_1 \\ \ell_0 \end{pmatrix} = \begin{pmatrix} v_{1,1} \\ v_{1,0} \\ F_3 \\ F_2 \\ F_1 \\ F_0 \end{pmatrix}.$$

Goal 2: compute the reduced divisor $[u', v']$ s.t. $D_1 + D_2 := [u', v']$

Explicit formulas for genus 2

Let $D_i := [\underbrace{x^2 + u_{i,1}x + u_{i,0}}_{u_i}, \underbrace{v_{i,1}x + v_{i,0}}_{v_i}]$, where $u_{i,j}, v_{i,j} \in \mathbb{K}, i = 1, 2$

Goal 1: compute efficiently u, v, s.t. $D_1 + D_2 \sim [u, v]$.

$$\begin{pmatrix} u_{1,1}^2 - u_{1,0} & -u_{1,1} & 1 & 0 \\ u_{1,1}u_{1,0} & -u_{1,0} & 0 & 1 \\ H_0 - (u_{1,1} + u_{2,1})H_1 & H_1 & 0 & 0 \\ -H_1(u_{1,0} + u_{2,0} + u_{1,1}u_{2,1}) & H_0 & H_1 & 0 \\ -H_1(u_{1,1}u_{2,0} + u_{1,0}u_{2,1}) & 0 & H_0 & H_1 \\ -H_1 u_{1,0}u_{2,0} & 0 & 0 & H_0 \end{pmatrix} \cdot \begin{pmatrix} \ell_3 \\ \ell_2 \\ \ell_1 \\ \ell_0 \end{pmatrix} = \begin{pmatrix} v_{1,1} \\ v_{1,0} \\ F_3 \\ F_2 \\ F_1 \\ F_0 \end{pmatrix}.$$

Goal 2: compute the reduced divisor $[u', v']$ s.t. $D_1 + D_2 := [u', v']$

[CosLau 11]: addition $1\mathrm{I} + 17\mathrm{M} + 4\mathrm{S}$ and doubling $1\mathrm{I} + 19\mathrm{M} + 6\mathrm{S}$

Explicit formulas for genus 2

Let $D_i := [\underbrace{x^2 + u_{i,1}x + u_{i,0}}_{u_i}, \underbrace{v_{i,1}x + v_{i,0}}_{v_i}]$, where $u_{i,j}, v_{i,j} \in \mathbb{K}, i = 1, 2$

Goal 1: compute efficiently u, v, s.t. $D_1 + D_2 \sim [u, v]$.

$$\begin{pmatrix} u_{1,1}^2 - u_{1,0} & -u_{1,1} & 1 & 0 \\ u_{1,1}u_{1,0} & -u_{1,0} & 0 & 1 \\ H_0 - (u_{1,1} + u_{2,1})H_1 & H_1 & 0 & 0 \\ -H_1(u_{1,0} + u_{2,0} + u_{1,1}u_{2,1}) & H_0 & H_1 & 0 \\ -H_1(u_{1,1}u_{2,0} + u_{1,0}u_{2,1}) & 0 & H_0 & H_1 \\ -H_1 u_{1,0}u_{2,0} & 0 & 0 & H_0 \end{pmatrix} \cdot \begin{pmatrix} \ell_3 \\ \ell_2 \\ \ell_1 \\ \ell_0 \end{pmatrix} = \begin{pmatrix} v_{1,1} \\ v_{1,0} \\ F_3 \\ F_2 \\ F_1 \\ F_0 \end{pmatrix}.$$

Goal 2: compute the reduced divisor $[u', v']$ s.t. $D_1 + D_2 := [u', v']$

Our unified addition formulas cost $1\mathrm{I} + 21\mathrm{M} + 6\mathrm{S}$ in odd char.

Outline

Conclusion

We presented:

- Unified addition formulas valid for any genus and any field
- For $g = 2$ HECC, explicit efficient unified addition formulas

Method	Atomicity [LM04]	[D. thesis 10]	Our formulas
Complexity	$1\mathrm{I} + 23\mathrm{M} + 5\mathrm{S}$	$1\mathrm{I} + 25\mathrm{M} + 6\mathrm{S}$	$1\mathrm{I} + 21\mathrm{M} + 6\mathrm{S}$

Table: comparison some countermeasures of SPA in odd characteristic

Future work:

- Complete addition formulas for genus 2 hyperelliptic curves.

Thank you!

Merci!

Any questions?