Real Hyperelliptic Curves

Renate Scheidler

rscheidl@math.ucalgary.ca

Centre for Information Security and Cryptography

Joint work with

Mike Jacobson (CISaC, University of Calgary) and **Andreas Stein** (University of Wyoming)

Research supported in part by NSERC of Canada

Hyperelliptic Curves over $\mathbb{F}_q$

Hyperelliptic Curves over $\mathbb{F}_q$

$$\boxed{C \; : \quad y^2 + h(x)y \; = \; f(x)}$$

Hyperelliptic Curves over $\mathbb{F}_q$

$$\boxed{C \; : \quad y^2 + h(x)y \; = \; f(x)}$$

$f, h \in \mathbb{F}_q[x]$; $h = 0$ if q odd;
absolutely irreducible; non-singular; of *genus* g

Hyperelliptic Curves over $\mathbb{F}_q$

$$\boxed{C : \quad y^2 + h(x)y = f(x)}$$

$f, h \in \mathbb{F}_q[x]$; $h = 0$ if q odd;
absolutely irreducible; non-singular; of *genus* g

- **Imaginary Model**
  - f monic and $\deg(f) = 2g + 1$
  - $\deg(h) \leq g$ if q even

Hyperelliptic Curves over $\mathbb{F}_q$

$$\boxed{C \; : \quad y^2 + h(x)y \; = \; f(x)}$$

$f, h \in \mathbb{F}_q[x]$; $h = 0$ if q odd;
absolutely irreducible; non-singular; of *genus* g

- **Imaginary Model**
  - f monic and $\deg(f) = 2g + 1$
  - $\deg(h) \leq g$ if q even
- **Real Model**
  - If q odd: f monic and $\deg(f) = 2g + 2$
  - If q even: h monic, $\deg(h) = g + 1$ and
    - $\deg(f) \leq 2g + 1$ or
    - $\deg(f) = 2g + 2$, $\mathrm{sgn}(f) = e^2 + e$ $(e \in \mathbb{F}_q^*)$

Notation

Notation

- $\mathbb{F}_q[C] = \mathbb{F}_q[x, y]$
  coordinate ring of C

Notation

- $\mathbb{F}_q[C] = \mathbb{F}_q[x, y]$
  coordinate ring of C
- $\mathbb{F}_q(C) = \mathbb{F}_q(x, y) = \text{Quot}(\mathbb{F}_q[C])$
  function field of C

Notation

- $\mathbb{F}_q[C] = \mathbb{F}_q[x, y]$
  coordinate ring of C
- $\mathbb{F}_q(C) = \mathbb{F}_q(x, y) = \mathrm{Quot}(\mathbb{F}_q[C])$
  function field of C
- $\mathrm{Cl}(\mathbb{F}_q[C])$
  ideal class group of $\mathbb{F}_q[C]$ (group of fractional $\mathbb{F}_q[C]$-ideals modulo principal ideal equivalence)

Notation

- $\mathbb{F}_q[C] = \mathbb{F}_q[x,y]$
  coordinate ring of C
- $\mathbb{F}_q(C) = \mathbb{F}_q(x,y) = \text{Quot}(\mathbb{F}_q[C])$
  function field of C
- $\mathrm{Cl}(\mathbb{F}_q[C])$
  ideal class group of $\mathbb{F}_q[C]$ (group of fractional $\mathbb{F}_q[C]$-ideals modulo principal ideal equivalence)
- $\mathrm{Pic}_q^0(C)$
  Degree zero divisor class group of C over $\mathbb{F}_q$ (group of degree zero divisors defined over $\mathbb{F}_q$ modulo principal divisor equivalence)

Properties

Properties

Imaginary Model

Properties

Imaginary Model

- C has one totally ramified point ∞ at infinity

Properties

Imaginary Model

- C has one totally ramified point ∞ at infinity
- The unit group $\mathbb{F}_q[C]^*$ of $\mathbb{F}_q[C]$ is simply $\mathbb{F}_q^*$

Properties

Imaginary Model

- C has one totally ramified point ∞ at infinity
- The unit group $\mathbb{F}_q[C]^*$ of $\mathbb{F}_q[C]$ is simply $\mathbb{F}_q^*$
- $\mathrm{Pic}_q^0(C)$ is isomorphic to $\mathrm{Cl}(\mathbb{F}_q[C])$

Properties

Imaginary Model

- C has one totally ramified point ∞ at infinity
- The unit group $\mathbb{F}_q[C]^*$ of $\mathbb{F}_q[C]$ is simply $\mathbb{F}_q^*$
- $\mathrm{Pic}_q^0(C)$ is isomorphic to $\mathrm{Cl}(\mathbb{F}_q[C])$

Real Model

Properties

Imaginary Model

- C has one totally ramified point ∞ at infinity
- The unit group $\mathbb{F}_q[C]^*$ of $\mathbb{F}_q[C]$ is simply $\mathbb{F}_q^*$
- $\mathrm{Pic}_q^0(C)$ is isomorphic to $\mathrm{Cl}(\mathbb{F}_q[C])$

Real Model

- C has two unramified points ∞_+ and ∞_- at infinity

Properties

Imaginary Model

- C has one totally ramified point ∞ at infinity
- The unit group $\mathbb{F}_q[C]^*$ of $\mathbb{F}_q[C]$ is simply $\mathbb{F}_q^*$
- $\mathrm{Pic}_q^0(C)$ is isomorphic to $\mathrm{Cl}(\mathbb{F}_q[C])$

Real Model

- C has two unramified points ∞_+ and ∞_- at infinity
- The class of the degree zero divisor $\infty_+ - \infty_-$ has order R, the *regulator* of C

Properties

Imaginary Model

- C has one totally ramified point ∞ at infinity
- The unit group $\mathbb{F}_q[C]^*$ of $\mathbb{F}_q[C]$ is simply $\mathbb{F}_q^*$
- $\mathrm{Pic}_q^0(C)$ is isomorphic to $\mathrm{Cl}(\mathbb{F}_q[C])$

Real Model

- C has two unramified points ∞_+ and ∞_- at infinity
- The class of the degree zero divisor $\infty_+ - \infty_-$ has order R, the *regulator* of C
- $\mathbb{F}_q[C]^* = \mathbb{F}_q^* \times \langle \epsilon \rangle, \quad (\epsilon) = R(\infty_+ - \infty_-)$

Properties

Imaginary Model

- C has one totally ramified point ∞ at infinity
- The unit group $\mathbb{F}_q[C]^*$ of $\mathbb{F}_q[C]$ is simply $\mathbb{F}_q^*$
- $\mathrm{Pic}_q^0(C)$ is isomorphic to $\mathrm{Cl}(\mathbb{F}_q[C])$

Real Model

- C has two unramified points ∞_+ and ∞_- at infinity
- The class of the degree zero divisor $\infty_+ - \infty_-$ has order R, the *regulator* of C
- $\mathbb{F}_q[C]^* = \mathbb{F}_q^* \times \langle \epsilon \rangle, \quad (\epsilon) = R(\infty_+ - \infty_-)$
- $|\mathrm{Pic}_q^0(C)| = R \cdot |\mathrm{Cl}(\mathbb{F}_q[C])|$
  generally $\mathrm{Cl}(\mathbb{F}_q[C])$ is small and $R \approx |\mathrm{Pic}_q^0(C)| \sim q^g$

Ideals and Degree 0 Divisors

Ideals and Degree 0 Divisors

Every degree zero divisor has a unique representation

Ideals and Degree 0 Divisors

Every degree zero divisor has a unique representation

Imaginary Model:

$$D = D_x - \deg(D_x)\infty \quad (\infty \nmid D_x)$$

Ideals and Degree 0 Divisors

Every degree zero divisor has a unique representation

Imaginary Model:

$$D \;=\; D_x - \deg(D_x)\infty \quad (\infty \nmid D_x)$$

Real Model:

$$D \;=\; D_x - \deg(D_x)\infty_- + v_{\infty_+}(D)(\infty_+ - \infty_-) \quad (\infty_+, \infty_- \nmid D_x)$$

Ideals and Degree 0 Divisors

Every degree zero divisor has a unique representation

Imaginary Model:

$$D \;=\; D_x - \deg(D_x)\infty \quad (\infty \nmid D_x)$$

Real Model:

$$D \;=\; D_x - \deg(D_x)\infty_- + v_{\infty_+}(D)(\infty_+ - \infty_-) \quad (\infty_+, \infty_- \nmid D_x)$$

Finite divisors D_x	$\leftrightarrow$	Fractional $\mathbb{F}_q[C]$-Ideals
Effective	$\leftrightarrow$	Integral
Semi-Reduced	$\leftrightarrow$	Primitive
Reduced	$\leftrightarrow$	Reduced

Semi-Reduced & Reduced Divisors

Semi-Reduced & Reduced Divisors

D **semi-reduced**: $D_x = (a, b)$ where

- $a, b \in \mathbb{F}_q[x]$, a monic (note: $\deg(a) = \deg(D_x)$)
- a unique, b (mod a) unique
- $a \mid f + hb - b^2$

Semi-Reduced & Reduced Divisors

D **semi-reduced**: $D_x = (a, b)$ where

- $a, b \in \mathbb{F}_q[x]$, a monic (note: $\deg(a) = \deg(D_x)$)
- a unique, b (mod a) unique
- $a \mid f + hb - b^2$

D **reduced** if D is semi-reduced and $\deg(D_x) \leq g$

Semi-Reduced & Reduced Divisors

D **semi-reduced**: $D_x = (a, b)$ where

- $a, b \in \mathbb{F}_q[x]$, a monic (note: $\deg(a) = \deg(D_x)$)
- a unique, b (mod a) unique
- $a \mid f + hb - b^2$

D **reduced** if D is semi-reduced and $\deg(D_x) \leq g$

Imaginary Model:

- Every degree zero divisor class has a unique (and efficiently computable) reduced representative $D = (a, b)$

Semi-Reduced & Reduced Divisors

D **semi-reduced**: $D_x = (a, b)$ where

- $a, b \in \mathbb{F}_q[x]$, a monic (note: $\deg(a) = \deg(D_x)$)
- a unique, b (mod a) unique
- $a \mid f + hb - b^2$

D **reduced** if D is semi-reduced and $\deg(D_x) \leq g$

Imaginary Model:

- Every degree zero divisor class has a unique (and efficiently computable) reduced representative $D = (a, b)$

Real Model:

- Every degree zero divisor class has a unique (but not efficiently computable) reduced representative $D = (a, b)$ with $0 \leq -v_{\infty_+}(D) \leq g - \deg(D_x)$ (Paulus-Rück 1999)

Infrastructures, Real Model, I

Infrastructures, Real Model, I

Fix any *ideal* class **C**

Infrastructures, Real Model, I

Fix any *ideal* class **C**

Every reduced ideal $\mathfrak{a} \in \mathbf{C}$ corresponds to a unique reduced divisor $D(\mathfrak{a})$ with $v_{\infty_+}(D(\mathfrak{a})) = 0$:

$$D(\mathfrak{a}) = D(\mathfrak{a})_x - \deg(D(\mathfrak{a})_x)\infty_- \quad \text{with} \quad D(\mathfrak{a})_x \leftrightarrow \mathfrak{a}$$

Infrastructures, Real Model, I

Fix any *ideal* class **C**

Every reduced ideal $\mathfrak{a} \in \mathbf{C}$ corresponds to a unique reduced divisor $D(\mathfrak{a})$ with $v_{\infty_+}(D(\mathfrak{a})) = 0$:

$$D(\mathfrak{a}) = D(\mathfrak{a})_x - \deg(D(\mathfrak{a})_x)\infty_- \quad \text{with} \quad D(\mathfrak{a})_x \leftrightarrow \mathfrak{a}$$

Infrastructure of **C**: $\boxed{\mathcal{R}_{\mathbf{C}} = \{D(\mathfrak{a}) \mid \mathfrak{a} \in \mathbf{C} \text{ reduced}\}}$

Infrastructures, Real Model, I

Fix any *ideal* class **C**

Every reduced ideal $\mathfrak{a} \in \mathbf{C}$ corresponds to a unique reduced divisor $D(\mathfrak{a})$ with $v_{\infty_+}(D(\mathfrak{a})) = 0$:

$$D(\mathfrak{a}) = D(\mathfrak{a})_x - \deg(D(\mathfrak{a})_x)\infty_- \quad \text{with} \quad D(\mathfrak{a})_x \leftrightarrow \mathfrak{a}$$

Infrastructure of **C**: $\boxed{\mathcal{R}_{\mathbf{C}} = \{D(\mathfrak{a}) \mid \mathfrak{a} \in \mathbf{C} \text{ reduced}\}}$

Properties:

Infrastructures, Real Model, I

Fix any *ideal* class **C**

Every reduced ideal $\mathfrak{a} \in \mathbf{C}$ corresponds to a unique reduced divisor $D(\mathfrak{a})$ with $v_{\infty_+}(D(\mathfrak{a})) = 0$:

$$D(\mathfrak{a}) = D(\mathfrak{a})_x - \deg(D(\mathfrak{a})_x)\infty_- \quad \text{with} \quad D(\mathfrak{a})_x \leftrightarrow \mathfrak{a}$$

Infrastructure of **C**: $\boxed{\mathcal{R}_{\mathbf{C}} = \{D(\mathfrak{a}) \mid \mathfrak{a} \in \mathbf{C} \text{ reduced}\}}$

Properties:

- $\mathcal{R}_{\mathbf{C}}$ is finite; $g^{-1}(R-1) \leq |\mathcal{R}_{\mathbf{C}}| \leq R - g$

Infrastructures, Real Model, I

Fix any *ideal* class **C**

Every reduced ideal $\mathfrak{a} \in \mathbf{C}$ corresponds to a unique reduced divisor $D(\mathfrak{a})$ with $v_{\infty_+}(D(\mathfrak{a})) = 0$:

$$D(\mathfrak{a}) = D(\mathfrak{a})_x - \deg(D(\mathfrak{a})_x)\infty_- \quad \text{with} \quad D(\mathfrak{a})_x \leftrightarrow \mathfrak{a}$$

Infrastructure of **C**: $\boxed{\mathcal{R}_{\mathbf{C}} = \{D(\mathfrak{a}) \mid \mathfrak{a} \in \mathbf{C} \text{ reduced}\}}$

Properties:

- $\mathcal{R}_{\mathbf{C}}$ is finite; $g^{-1}(R-1) \leq |\mathcal{R}_{\mathbf{C}}| \leq R - g$
- The divisors in $\mathcal{R}_{\mathbf{C}}$ are pairwise inequivalent

Infrastructures, Real Model, I

Fix any *ideal* class **C**

Every reduced ideal $\mathfrak{a} \in \mathbf{C}$ corresponds to a unique reduced divisor $D(\mathfrak{a})$ with $v_{\infty_+}(D(\mathfrak{a})) = 0$:

$$D(\mathfrak{a}) = D(\mathfrak{a})_x - \deg(D(\mathfrak{a})_x)\infty_- \quad \text{with} \quad D(\mathfrak{a})_x \leftrightarrow \mathfrak{a}$$

Infrastructure of **C**: $\boxed{\mathcal{R}_{\mathbf{C}} = \{D(\mathfrak{a}) \mid \mathfrak{a} \in \mathbf{C} \text{ reduced}\}}$

Properties:

- $\mathcal{R}_{\mathbf{C}}$ is finite; $g^{-1}(R-1) \leq |\mathcal{R}_{\mathbf{C}}| \leq R - g$
- The divisors in $\mathcal{R}_{\mathbf{C}}$ are pairwise inequivalent
- If $\mathfrak{b} \in \mathcal{R}_{\mathbf{C}}$, say $\mathfrak{b} = (\alpha)\mathfrak{a}$ with $\alpha \in \mathbb{F}_q(C)^*$, then

$$D(\mathfrak{a}) = D(\mathfrak{b}) \quad \Leftrightarrow \quad v_{\infty_+}(\alpha) \equiv 0 \pmod{R}$$

Infrastructures, Real Model, II

Infrastructures, Real Model, II

Fix any reduced ideal $\mathfrak{a}_1 \in \mathbf{C}$

Infrastructures, Real Model, II

Fix any reduced ideal $\mathfrak{a}_1 \in \mathbf{C}$

Write every divisor in $D_i \in \mathcal{R}_{\mathbf{C}}$ as $D_i = D(\mathfrak{a}_i)$ where

$$\mathfrak{a}_i = (\alpha_i)\mathfrak{a}_1, \quad \alpha_i \in \mathbb{F}_q(C)^* \text{ with } -R < v_{\infty_+}(\alpha_i) \leq 0$$

Infrastructures, Real Model, II

Fix any reduced ideal $\mathfrak{a}_1 \in \mathbf{C}$

Write every divisor in $D_i \in \mathcal{R}_{\mathbf{C}}$ as $D_i = D(\mathfrak{a}_i)$ where

$$\mathfrak{a}_i = (\alpha_i)\mathfrak{a}_1, \quad \alpha_i \in \mathbb{F}_q(C)^* \text{ with } -R < v_{\infty_+}(\alpha_i) \leq 0$$

This defines an *ordering* on $\mathcal{R}_{\mathbf{C}}$ via

$$D_j > D_i \quad \Leftrightarrow \quad v_{\infty_+}(\alpha_j) < v_{\infty_+}(\alpha_i)$$

Infrastructures, Real Model, II

Fix any reduced ideal $\mathfrak{a}_1 \in \mathbf{C}$

Write every divisor in $D_i \in \mathcal{R}_{\mathbf{C}}$ as $D_i = D(\mathfrak{a}_i)$ where

$$\mathfrak{a}_i = (\alpha_i)\mathfrak{a}_1, \quad \alpha_i \in \mathbb{F}_q(C)^* \text{ with } -R < v_{\infty_+}(\alpha_i) \leq 0$$

This defines an *ordering* on $\mathcal{R}_{\mathbf{C}}$ via

$$D_j > D_i \quad \Leftrightarrow \quad v_{\infty_+}(\alpha_j) < v_{\infty_+}(\alpha_i)$$

Distance of D_i is $\delta_i = \delta(D_i) = -v_{\infty_+}(\alpha_i)$

$$\mathcal{R}_{\mathbf{C}} = \{D_1, D_2, \ldots, D_{|\mathcal{R}_{\mathbf{C}}|}\}, \qquad 0 = \delta_1 < \delta_2 < \cdots < \delta_{|\mathcal{R}_{\mathbf{C}}|} < R$$

Infrastructures, Real Model, II

Fix any reduced ideal $\mathfrak{a}_1 \in \mathbf{C}$

Write every divisor in $D_i \in \mathcal{R}_{\mathbf{C}}$ as $D_i = D(\mathfrak{a}_i)$ where

$$\mathfrak{a}_i = (\alpha_i)\mathfrak{a}_1, \quad \alpha_i \in \mathbb{F}_q(C)^* \text{ with } -R < v_{\infty_+}(\alpha_i) \leq 0$$

This defines an *ordering* on $\mathcal{R}_{\mathbf{C}}$ via

$$D_j > D_i \quad \Leftrightarrow \quad v_{\infty_+}(\alpha_j) < v_{\infty_+}(\alpha_i)$$

Distance of D_i is $\delta_i = \delta(D_i) = -v_{\infty_+}(\alpha_i)$

$$\mathcal{R}_{\mathbf{C}} = \{D_1, D_2, \ldots, D_{|\mathcal{R}_{\mathbf{C}}|}\}, \qquad 0 = \delta_1 < \delta_2 < \cdots < \delta_{|\mathcal{R}_{\mathbf{C}}|} < R$$

Baby Step in $\mathcal{R}_{\mathbf{C}}$: $\boxed{D_i \rightarrow D_{i+1}}$

Baby Steps, Real Model, I

Baby Steps, Real Model, I

Baby step $D_i = (a_{i-1}, b_{i-1}) \rightarrow D_{i+1} = (a_i, b_i)$:

Baby Steps, Real Model, I

Baby step $D_i = (a_{i-1}, b_{i-1}) \rightarrow D_{i+1} = (a_i, b_i)$:

$$q_{i-1} = \left\lfloor \frac{b_{i-1} + e_{i-1}\lfloor y \rfloor}{a_{i-1}} \right\rfloor \quad \text{where}$$

$$e_{i-1} = \begin{cases} 1 & \text{if } C \text{ is real and } \deg(a_{i-1}) \leq g+1 \\ 0 & \text{otherwise} \end{cases}$$

$$b_i = h + q_{i-1}a_{i-1} - b_{i-1}$$

$$a_i = \frac{f + hb_i - {b_i}^2}{a_{i-1}}$$

($\lfloor y \rfloor$ is the polynomial part of the Laurent series of y in x^{-1})

Baby Steps, Real Model, I

Baby step $D_i = (a_{i-1}, b_{i-1}) \rightarrow D_{i+1} = (a_i, b_i)$:

$$q_{i-1} = \left\lfloor \frac{b_{i-1} + e_{i-1}\lfloor y \rfloor}{a_{i-1}} \right\rfloor \quad \text{where}$$

$$e_{i-1} = \begin{cases} 1 & \text{if } C \text{ is real and } \deg(a_{i-1}) \leq g+1 \\ 0 & \text{otherwise} \end{cases}$$

$$b_i = h + q_{i-1}a_{i-1} - b_{i-1}$$

$$a_i = \frac{f + hb_i - {b_i}^2}{a_{i-1}}$$

($\lfloor y \rfloor$ is the polynomial part of the Laurent series of y in x^{-1})

Complexity of a baby step: $O(g)$ field operations

Baby Steps, Real Model, II

Baby Steps, Real Model, II

- Baby steps preserve ideal equivalence

Baby Steps, Real Model, II

- Baby steps preserve ideal equivalence
- The q_i are the partial quotients of the continued fraction expansion of $(b + y)/a$

Baby Steps, Real Model, II

- Baby steps preserve ideal equivalence
- The q_i are the partial quotients of the continued fraction expansion of $(b + y)/a$
- Baby steps move forward cyclically through $\mathcal{R}_{\mathbf{c}}$ ($D_{|\mathcal{R}_{\mathbf{c}}|+1} = D_1$)

Baby Steps, Real Model, II

- Baby steps preserve ideal equivalence
- The q_i are the partial quotients of the continued fraction expansion of $(b + y)/a$
- Baby steps move forward cyclically through $\mathcal{R}_{\mathbf{C}}$ ($D_{|\mathcal{R}_{\mathbf{C}}|+1} = D_1$)
- $|\mathcal{R}_{\mathbf{C}}|$ baby steps applied to any divisor of $\mathcal{R}_{\mathbf{C}}$ produce all of $\mathcal{R}_{\mathbf{C}}$ (*not recommended!*)

Baby Steps, Real Model, II

- Baby steps preserve ideal equivalence
- The q_i are the partial quotients of the continued fraction expansion of $(b + y)/a$
- Baby steps move forward cyclically through $\mathcal{R}_{\mathbf{C}}$ ($D_{|\mathcal{R}_{\mathbf{C}}|+1} = D_1$)
- $|\mathcal{R}_{\mathbf{C}}|$ baby steps applied to any divisor of $\mathcal{R}_{\mathbf{C}}$ produce all of $\mathcal{R}_{\mathbf{C}}$ (*not recommended!*)
- Can also use backward baby steps to move backward through $\mathcal{R}_{\mathbf{C}}$

Distances, Real Model

Distances, Real Model

Properties of the distance

Distances, Real Model

Properties of the distance

- $\delta_1 = 0, \quad \text{“}\delta_{|\mathcal{R}_{\mathbf{c}}|+1}\text{”} = R$

Distances, Real Model

Properties of the distance

- $\delta_1 = 0, \quad \text{“}\delta_{|\mathcal{R}_{\mathbf{c}}|+1}\text{”} = R$
- $\delta_{i+1} = \delta_i + \deg(q_{i-1})$

Distances, Real Model

Properties of the distance

- $\delta_1 = 0, \quad \text{“}\delta_{|\mathcal{R}_{\mathbf{C}}|+1}\text{”} = R$
- $\delta_{i+1} = \delta_i + \deg(q_{i-1})$
- $\delta_2 = g + 1$ if $D_1 = 0 = (1, 0)$ (**C** the principal class)

Distances, Real Model

Properties of the distance

- $\delta_1 = 0, \quad \text{“}\delta_{|\mathcal{R}_{\mathbf{C}}|+1}\text{”} = R$
- $\delta_{i+1} = \delta_i + \deg(q_{i-1})$
- $\delta_2 = g + 1$ if $D_1 = 0 = (1, 0)$ (**C** the principal class)
- $1 \leq \delta_{i+1} - \delta_i \leq g$ otherwise

Distances, Real Model

Properties of the distance

- $\delta_1 = 0, \quad \text{“}\delta_{|\mathcal{R}_{\mathbf{C}}|+1}\text{”} = R$
- $\delta_{i+1} = \delta_i + \deg(q_{i-1})$
- $\delta_2 = g + 1$ if $D_1 = 0 = (1, 0)$ (**C** the principal class)
- $1 \leq \delta_{i+1} - \delta_i \leq g$ otherwise
- Given $D = (a, b) \in \mathcal{R}_{\mathbf{C}}$, it is computationally infeasible to find $\delta(D)$ (*Principal Ideal Problem*)

Distances, Real Model

Properties of the distance

- $\delta_1 = 0, \quad \text{“}\delta_{|\mathcal{R}_{\mathbf{C}}|+1}\text{”} = R$
- $\delta_{i+1} = \delta_i + \deg(q_{i-1})$
- $\delta_2 = g + 1$ if $D_1 = 0 = (1, 0)$ (**C** the principal class)
- $1 \leq \delta_{i+1} - \delta_i \leq g$ otherwise
- Given $D = (a, b) \in \mathcal{R}_{\mathbf{C}}$, it is computationally infeasible to find $\delta(D)$ (*Principal Ideal Problem*)

Divisors of Fixed Distance

Distances, Real Model

Properties of the distance

- $\delta_1 = 0, \quad \text{“}\delta_{|\mathcal{R}_{\mathbf{C}}|+1}\text{”} = R$
- $\delta_{i+1} = \delta_i + \deg(q_{i-1})$
- $\delta_2 = g + 1$ if $D_1 = 0 = (1, 0)$ (**C** the principal class)
- $1 \leq \delta_{i+1} - \delta_i \leq g$ otherwise
- Given $D = (a, b) \in \mathcal{R}_{\mathbf{C}}$, it is computationally infeasible to find $\delta(D)$ (*Principal Ideal Problem*)

Divisors of Fixed Distance

For $r \in [0, R)$, the divisor $D_i \in R_{\mathbf{C}}$ *below* r is defined via

$$\delta_i \leq r < \delta_{i+1}$$

Baby Steps, Both Models

Baby Steps, Both Models

Baby Steps = Reduction Steps, Imaginary Model

$$b_{i+1} \equiv h - b_i \pmod{a_i}, \qquad a_{i+1} = \frac{f + hb_{i+1} - b_{i+1}^2}{a_i}$$

Baby Steps, Both Models

Baby Steps = Reduction Steps, Imaginary Model

$$b_{i+1} \equiv h - b_i \pmod{a_i}, \qquad a_{i+1} = \frac{f + hb_{i+1} - b_{i+1}^2}{a_i}$$

Real & Imaginary Model:

Baby Steps, Both Models

Baby Steps = Reduction Steps, Imaginary Model

$$b_{i+1} \equiv h - b_i \pmod{a_i}, \qquad a_{i+1} = \frac{f + hb_{i+1} - b_{i+1}^2}{a_i}$$

Real & Imaginary Model:

- Applying at most $\lceil (\deg(a) - g)/2 \rceil$ baby steps to a semi-reduced divisor $D = (a, b)$ produces a reduced divisor

Baby Steps, Both Models

Baby Steps = Reduction Steps, Imaginary Model

$$b_{i+1} \equiv h - b_i \pmod{a_i}, \qquad a_{i+1} = \frac{f + hb_{i+1} - b_{i+1}^2}{a_i}$$

Real & Imaginary Model:

- Applying at most $\lceil (\deg(a) - g)/2 \rceil$ baby steps to a semi-reduced divisor $D = (a, b)$ produces a reduced divisor
- If D is the sum of two reduced divisors, this requires at most $\lceil g/2 \rceil$ baby steps

Divisor Addition

Divisor Addition

Cantor's Algorithm:

Divisor Addition

Cantor's Algorithm:

If $D' = (a', b')$ and $D'' = (a'', b'')$, then

$D' + D'' = s(a, b)$ where

$$
\begin{aligned}
s &= \gcd(a', a'', b' + b'') \\
&= Va' + Wa'' + X(b' + b'') \\
U &\equiv W(b' - b'') + X\,\frac{f - (b'')^2}{a''} \quad \left(\text{mod } \frac{a'}{s}\right) \\
a &= \frac{a'a''}{s^2} \\
b &= b'' + Ua''/s
\end{aligned}
$$

Giant Steps

Giant Steps

Giant Step $(D', D'') \rightarrow D' \oplus D''$

Giant Steps

Giant Step $(D', D'') \rightarrow D' \oplus D''$

Definition:

Giant Steps

Giant Step $(D', D'') \rightarrow D' \oplus D''$

Definition:

- *Imaginary Model*: If D', D'' are reduced divisors, then $D' \oplus D''$ is the reduced divisor in the class of $D' + D''$

Giant Steps

Giant Step $(D', D'') \rightarrow D' \oplus D''$

Definition:

- *Imaginary Model*: If D', D'' are reduced divisors, then $D' \oplus D''$ is the reduced divisor in the class of $D' + D''$
- *Real Model*: Apply the same arithmetic as for the imaginary model to define $D' \oplus D''$

Giant Steps

Giant Step $(D', D'') \rightarrow D' \oplus D''$

Definition:

- *Imaginary Model*: If D', D'' are reduced divisors, then $D' \oplus D''$ is the reduced divisor in the class of $D' + D''$
- *Real Model*: Apply the same arithmetic as for the imaginary model to define $D' \oplus D''$

Algorithms:

Giant Steps

Giant Step $(D', D'') \rightarrow D' \oplus D''$

Definition:

- *Imaginary Model*: If D', D'' are reduced divisors, then $D' \oplus D''$ is the reduced divisor in the class of $D' + D''$
- *Real Model*: Apply the same arithmetic as for the imaginary model to define $D' \oplus D''$

Algorithms:

- Cantor's algorithm (1987) with subsequent baby steps

Giant Steps

Giant Step $(D', D'') \rightarrow D' \oplus D''$

Definition:

- *Imaginary Model*: If D', D'' are reduced divisors, then $D' \oplus D''$ is the reduced divisor in the class of $D' + D''$
- *Real Model*: Apply the same arithmetic as for the imaginary model to define $D' \oplus D''$

Algorithms:

- Cantor's algorithm (1987) with subsequent baby steps
- NUCOMP (Shanks 1989; Atkin, early 1990's)

Giant Steps

Giant Step $(D', D'') \rightarrow D' \oplus D''$

Definition:

- *Imaginary Model*: If D', D'' are reduced divisors, then $D' \oplus D''$ is the reduced divisor in the class of $D' + D''$
- *Real Model*: Apply the same arithmetic as for the imaginary model to define $D' \oplus D''$

Algorithms:

- Cantor's algorithm (1987) with subsequent baby steps
- NUCOMP (Shanks 1989; Atkin, early 1990's)
- Explicit Formulas – imaginary model, low genus (Lange 2005; Wollinger-Pelzl-Paar 2003 & 2005)

Giant Steps

Giant Step $(D', D'') \rightarrow D' \oplus D''$

Definition:

- *Imaginary Model*: If D', D'' are reduced divisors, then $D' \oplus D''$ is the reduced divisor in the class of $D' + D''$
- *Real Model*: Apply the same arithmetic as for the imaginary model to define $D' \oplus D''$

Algorithms:

- Cantor's algorithm (1987) with subsequent baby steps
- NUCOMP (Shanks 1989; Atkin, early 1990's)
- Explicit Formulas – imaginary model, low genus (Lange 2005; Wollinger-Pelzl-Paar 2003 & 2005)

Complexity: $O(g^2)$ field operations

Giant Steps à la Cantor

Giant Steps à la Cantor

To obtain $D' \oplus D''$:

Giant Steps à la Cantor

To obtain $D' \oplus D''$:

1. Compute $D' + D'' = s(a, b)$ using Cantor's algorithm

Giant Steps à la Cantor

To obtain $D' \oplus D''$:

1. Compute $D' + D'' = s(a, b)$ using Cantor's algorithm
2. Apply at most $\lceil g/2 \rceil$ baby steps to $D' + D''$ to obtain the $\left\{ \begin{array}{c} \text{first} \\ \text{unique} \end{array} \right\}$ divisor $D' \oplus D''$ in the $\left\{ \begin{array}{c} \text{real} \\ \text{imaginary} \end{array} \right\}$ case

Giant Steps à la Cantor

To obtain $D' \oplus D''$:

1. Compute $D' + D'' = s(a, b)$ using Cantor's algorithm
2. Apply at most $\lceil g/2 \rceil$ baby steps to $D' + D''$ to obtain the $\left\{ \begin{array}{c} \text{first} \\ \text{unique} \end{array} \right\}$ divisor $D' \oplus D''$ in the $\left\{ \begin{array}{c} \text{real} \\ \text{imaginary} \end{array} \right\}$ case

Step 2 amounts to computing part of the continued fraction expansion of $(b + ey)/a$
($e = 1$, real model; $e = 0$, imaginary model)

Giant Steps à la Cantor

To obtain $D' \oplus D''$:

1. Compute $D' + D'' = s(a, b)$ using Cantor's algorithm
2. Apply at most $\lceil g/2 \rceil$ baby steps to $D' + D''$ to obtain the $\left\{ \begin{array}{c} \text{first} \\ \text{unique} \end{array} \right\}$ divisor $D' \oplus D''$ in the $\left\{ \begin{array}{c} \text{real} \\ \text{imaginary} \end{array} \right\}$ case

Step 2 amounts to computing part of the continued fraction expansion of $(b + ey)/a$
($e = 1$, real model; $e = 0$, imaginary model)

Operand Sizes:

Divisor addition:	$g \ \rightarrow 2g$
Reduction (baby steps):	$2g,\ 2g-2,\ 2g-4,\ \ldots,\ g$

Giant Steps with NUCOMP

Giant Steps with NUCOMP

- *Idea*: Replace the partial quotients in $(b+ey)/a$ by those in the rational function $U/(a'/s)$:

$$\frac{b+ey}{a} = \frac{U}{a'/s} + \frac{b''+ey}{a} = \frac{U}{a'/s} + O(x^{1-g})$$

Giant Steps with NUCOMP

- *Idea*: Replace the partial quotients in $(b + ey)/a$ by those in the rational function $U/(a'/s)$:

$$\frac{b + ey}{a} = \frac{U}{a'/s} + \frac{b'' + ey}{a} = \frac{U}{a'/s} + O(x^{1-g})$$

- Produces the same sequence of partial quotients as Cantor giant steps, but uses only the Euclidean Algorithm (no costly a_i, b_i)

Giant Steps with NUCOMP

- *Idea*: Replace the partial quotients in $(b+ey)/a$ by those in the rational function $U/(a'/s)$:

$$\frac{b+ey}{a} = \frac{U}{a'/s} + \frac{b''+ey}{a} = \frac{U}{a'/s} + O(x^{1-g})$$

- Produces the same sequence of partial quotients as Cantor giant steps, but uses only the Euclidean Algorithm (no costly a_i, b_i)
- There are formulas for recovering the coefficients of $D' \oplus D''$ at the end (Shanks 1989, van der Poorten 2003, Jacobson-Scheidler-Williams 2006)

Giant Steps with NUCOMP

- *Idea*: Replace the partial quotients in $(b+ey)/a$ by those in the rational function $U/(a'/s)$:

$$\frac{b+ey}{a} = \frac{U}{a'/s} + \frac{b''+ey}{a} = \frac{U}{a'/s} + O(x^{1-g})$$

- Produces the same sequence of partial quotients as Cantor giant steps, but uses only the Euclidean Algorithm (no costly a_i, b_i)
- There are formulas for recovering the coefficients of $D' \oplus D''$ at the end (Shanks 1989, van der Poorten 2003, Jacobson-Scheidler-Williams 2006)
- Still $O(g^2)$ field operations, but we only work with operands of degree $\leq g$ (and a few of degree $3g/2$)

Principal Infrastructure

Principal Infrastructure

Set $\mathfrak{a}_1 = (1) = \mathbb{F}_q[C]$, $\quad D_1 = 0 = (1, 0)$

Principal Infrastructure

Set $\mathfrak{a}_1 = (1) = \mathbb{F}_q[C], \quad D_1 = 0 = (1, 0)$

Principal Infrastructure $\mathcal{R} = \{D_1, D_2, \ldots, D_{|\mathcal{R}|}\}$

Principal Infrastructure

Set $\mathfrak{a}_1 = (1) = \mathbb{F}_q[C], \quad D_1 = 0 = (1, 0)$

Principal Infrastructure $\mathcal{R} = \{D_1, D_2, \ldots, D_{|\mathcal{R}|}\}$

$\delta_i = -\nu_{\infty_+}(\alpha_i)$ where $\mathfrak{a}_i = (\alpha_i)$

Principal Infrastructure

Set $\mathfrak{a}_1 = (1) = \mathbb{F}_q[C], \quad D_1 = 0 = (1,0)$

Principal Infrastructure $\mathcal{R} = \{D_1, D_2, \ldots, D_{|\mathcal{R}|}\}$

$\delta_i = -\nu_{\infty_+}(\alpha_i)$ where $\mathfrak{a}_i = (\alpha_i)$

$\delta_1 = 0, \quad \delta_2 = g+1, \quad 1 \leq \delta_{i+1} - \delta_i \leq g$ for $2 \leq i \leq |\mathcal{R}| - 1$

Principal Infrastructure

Set $\mathfrak{a}_1 = (1) = \mathbb{F}_q[C], \quad D_1 = 0 = (1, 0)$

Principal Infrastructure $\mathcal{R} = \{D_1, D_2, \ldots, D_{|\mathcal{R}|}\}$

$\delta_i = -\nu_{\infty_+}(\alpha_i)$ where $\mathfrak{a}_i = (\alpha_i)$

$\delta_1 = 0, \quad \delta_2 = g + 1, \quad 1 \leq \delta_{i+1} - \delta_i \leq g$ for $2 \leq i \leq |\mathcal{R}| - 1$

$\mathcal{R}$ is closed under

Principal Infrastructure

Set $\mathfrak{a}_1 = (1) = \mathbb{F}_q[C], \quad D_1 = 0 = (1,0)$

Principal Infrastructure $\mathcal{R} = \{D_1, D_2, \ldots, D_{|\mathcal{R}|}\}$

$\delta_i = -\nu_{\infty_+}(\alpha_i)$ where $\mathfrak{a}_i = (\alpha_i)$

$\delta_1 = 0, \quad \delta_2 = g+1, \quad 1 \leq \delta_{i+1} - \delta_i \leq g$ for $2 \leq i \leq |\mathcal{R}| - 1$

$\mathcal{R}$ is closed under

- conjugation: $D(\mathfrak{a}) = (a,b) \in \mathcal{R} \quad \Rightarrow \quad D(\overline{\mathfrak{a}}) = (a, -b-h) \in \mathcal{R}$

$$\delta(D(\overline{\mathfrak{a}})) \;=\; R + \deg(a) - \delta(D(\mathfrak{a}))$$

Principal Infrastructure

Set $\mathfrak{a}_1 = (1) = \mathbb{F}_q[C], \quad D_1 = 0 = (1,0)$

Principal Infrastructure $\mathcal{R} = \{D_1, D_2, \ldots, D_{|\mathcal{R}|}\}$

$\delta_i = -\nu_{\infty_+}(\alpha_i)$ where $\mathfrak{a}_i = (\alpha_i)$

$\delta_1 = 0, \quad \delta_2 = g+1, \quad 1 \leq \delta_{i+1} - \delta_i \leq g$ for $2 \leq i \leq |\mathcal{R}| - 1$

$\mathcal{R}$ is closed under

- conjugation: $D(\mathfrak{a}) = (a,b) \in \mathcal{R} \quad \Rightarrow \quad D(\overline{\mathfrak{a}}) = (a, -b-h) \in \mathcal{R}$

  $\delta(D(\overline{\mathfrak{a}})) \;=\; R + \deg(a) - \delta(D(\mathfrak{a}))$
- giant steps: $D', D'' \in \mathcal{R} \quad \Rightarrow \quad D' \oplus D'' \in \mathcal{R}$

  $\delta(D' \oplus D'') \;=\; \delta(D') + \delta(D'') - d$ with $0 \leq d \leq 2g$

Principal Infrastructure

Set $\mathfrak{a}_1 = (1) = \mathbb{F}_q[C], \quad D_1 = 0 = (1,0)$

Principal Infrastructure $\mathcal{R} = \{D_1, D_2, \ldots, D_{|\mathcal{R}|}\}$

$\delta_i = -\nu_{\infty_+}(\alpha_i)$ where $\mathfrak{a}_i = (\alpha_i)$

$\delta_1 = 0, \quad \delta_2 = g+1, \quad 1 \leq \delta_{i+1} - \delta_i \leq g$ for $2 \leq i \leq |\mathcal{R}| - 1$

$\mathcal{R}$ is closed under

- conjugation: $D(\mathfrak{a}) = (a,b) \in \mathcal{R} \quad \Rightarrow \quad D(\overline{\mathfrak{a}}) = (a, -b-h) \in \mathcal{R}$

  $\delta(D(\overline{\mathfrak{a}})) = R + \deg(a) - \delta(D(\mathfrak{a}))$
- giant steps: $D', D'' \in \mathcal{R} \quad \Rightarrow \quad D' \oplus D'' \in \mathcal{R}$

  $\delta(D' \oplus D'') = \delta(D') + \delta(D'') - d$ with $0 \leq d \leq 2g$

$\mathcal{R}$ is NOT a group under $\oplus$ since it is not associative

Scalar Multiplication in $\mathrm{Pic}_q^0(C)$

Scalar Multiplication in $\mathrm{Pic}_q^0(C)$

Input: a divisor D and a scalar $n = \sum_{i=0}^{l} b_i 2^{l-i}$ in NAF

Scalar Multiplication in $\mathrm{Pic}_q^0(C)$

Input: a divisor D and a scalar $n = \sum_{i=0}^{l} b_i 2^{l-i}$ in NAF

Output: the reduced divisor $D \oplus D \oplus \cdots \oplus D$ (n times) in the divisor class of nD

Scalar Multiplication in $\mathrm{Pic}_q^0(C)$

Input: a divisor D and a scalar $n = \sum_{i=0}^{l} b_i 2^{l-i}$ in NAF

Output: the reduced divisor $D \oplus D \oplus \cdots \oplus D$ (n times) in the divisor class of nD

1. Set $E = D$
2. For $i = 1$ to l do

   // Double Replace E by $E \oplus E$

   // Add If $b_i = 1$, replace E by $E \oplus D$

   If $b_i = -1$, replace E by $E \oplus \overline{D}$
3. Output E

Scalar Multiplication in $\mathrm{Pic}_q^0(C)$

Input: a divisor D and a scalar $n = \sum_{i=0}^{l} b_i 2^{l-i}$ in NAF

Output: the reduced divisor $D \oplus D \oplus \cdots \oplus D$ (n times) in the divisor class of nD

1. Set $E = D$
2. For $i = 1$ to l do

   // Double Replace E by $E \oplus E$

   // Add If $b_i = 1$, replace E by $E \oplus D$

   If $b_i = -1$, replace E by $E \oplus \overline{D}$
3. Output E

Expected number of operations: l doubles, $l/3$ adds

Variable Base, Real Model

Variable Base, Real Model

Input: a divisor $D(\mathfrak{a}) \in \mathcal{R}$ and a "scalar" $n = \sum b_i 2^{l-i}$ in NAF

Variable Base, Real Model

Input: a divisor $D(\mathfrak{a}) \in \mathcal{R}$ and a "scalar" $n = \sum b_i 2^{l-i}$ in NAF
Output: The divisor $E \in \mathcal{R}$ below $n\delta(D(\mathfrak{a}))$

Variable Base, Real Model

Input: a divisor $D(\mathfrak{a}) \in \mathcal{R}$ and a "scalar" $n = \sum b_i 2^{l-i}$ in NAF
Output: The divisor $E \in \mathcal{R}$ below $n\delta(D(\mathfrak{a}))$

1. Set $E = D(\mathfrak{a})$
2. For $i = 1$ to l do
   // Double Replace E by $E \oplus E$
   // Adjust Apply at most $2g$ baby steps to reach the divisor below $2\delta(E)$
   If $b_i \neq 0$ then
      If $b_i = 1$, set $D' = D(\mathfrak{a})$; if $b_i = -1$, set $D_i = D(\overline{\mathfrak{a}})$
      // Add replace E by $E \oplus D'$
      // Adjust Apply at most $2g$ baby steps to reach the divisor below $\delta(E) + \delta(D')$
3. Output E

Variable Base, Real Model

Input: a divisor $D(\mathfrak{a}) \in \mathcal{R}$ and a "scalar" $n = \sum b_i 2^{l-i}$ in NAF
Output: The divisor $E \in \mathcal{R}$ below $n\delta(D(\mathfrak{a}))$

1. Set $E = D(\mathfrak{a})$
2. For $i = 1$ to l do
   // Double Replace E by $E \oplus E$
   // Adjust Apply at most $2g$ baby steps to reach the divisor below $2\delta(E)$
   If $b_i \neq 0$ then
      If $b_i = 1$, set $D' = D(\mathfrak{a})$; if $b_i = -1$, set $D_i = D(\overline{\mathfrak{a}})$
      // Add replace E by $E \oplus D'$
      // Adjust Apply at most $2g$ baby steps to reach the divisor below $\delta(E) + \delta(D')$
3. Output E

Exp. no. of ops: l doubles, $l/3$ adds, $cg \cdot 4l/3$ baby steps

Fixed Base, Real Model

Fixed Base, Real Model

Input: $n \in \mathbb{N}$, $s = \lfloor n/(g+1) \rfloor$ in NAF

Fixed Base, Real Model

Input: $n \in \mathbb{N}$, $s = \lfloor n/(g+1) \rfloor$ in NAF

Output: The divisor $E \in \mathcal{R}$ below n

Fixed Base, Real Model

Input: $n \in \mathbb{N}$, $s = \lfloor n/(g+1) \rfloor$ in NAF

Output: The divisor $E \in \mathcal{R}$ below n

1. Compute the divisor E' below $s(g+1)$ by calling the previous algorithm on inputs s and D_2
2. Apply at most $n - s(g+1)$ baby steps to E' to compute the divisor E below n
3. Output E

Fixed Base, Real Model

Input: $n \in \mathbb{N}$, $s = \lfloor n/(g+1) \rfloor$ in NAF

Output: The divisor $E \in \mathcal{R}$ below n

1. Compute the divisor E' below $s(g+1)$ by calling the previous algorithm on inputs s and D_2
2. Apply at most $n - s(g+1)$ baby steps to E' to compute the divisor E below n
3. Output E

Expected no. of ops:

- one integer division with remainder
- all the operations from previous algorithm
- at most g baby steps

Heuristics, Real Model

Heuristics, Real Model

Notation: Baby step forward: $D \to D_+$
Baby step backwards: $D \to D_-$

Heuristics, Real Model

Notation: Baby step forward: $D \to D_+$
Baby step backwards: $D \to D_-$

Heuristics: with probability $1 - O(q^{-1})$, we have

Heuristics, Real Model

Notation: Baby step forward: $D \to D_+$
Baby step backwards: $D \to D_-$

Heuristics: with probability $1 - O(q^{-1})$, we have

- $\delta_{i+1} - \delta_i = 1$ for $2 \leq i \leq |\mathcal{R}|$

Heuristics, Real Model

Notation: Baby step forward: $D \to D_+$
Baby step backwards: $D \to D_-$

Heuristics: with probability $1 - O(q^{-1})$, we have

- $\delta_{i+1} - \delta_i = 1$ for $2 \leq i \leq |\mathcal{R}|$
- $\delta(D' \oplus D'') = \delta(D') + \delta(D'') - d$ where $d = \lceil g/2 \rceil$

Heuristics, Real Model

Notation: Baby step forward: $D \to D_+$
Baby step backwards: $D \to D_-$

Heuristics: with probability $1 - O(q^{-1})$, we have

- $\delta_{i+1} - \delta_i = 1$ for $2 \leq i \leq |\mathcal{R}|$
- $\delta(D' \oplus D'') = \delta(D') + \delta(D'') - d$ where $d = \lceil g/2 \rceil$

Consequences:

Heuristics, Real Model

Notation: Baby step forward: $D \to D_+$
Baby step backwards: $D \to D_-$

Heuristics: with probability $1 - O(q^{-1})$, we have

- $\delta_{i+1} - \delta_i = 1$ for $2 \leq i \leq |\mathcal{R}|$
- $\delta(D' \oplus D'') = \delta(D') + \delta(D'') - d$ where $d = \lceil g/2 \rceil$

Consequences:

- $\delta_i = g - 1 + i$ for $2 \leq i \leq |\mathcal{R}|$

Heuristics, Real Model

Notation: Baby step forward: $D \to D_+$
Baby step backwards: $D \to D_-$

Heuristics: with probability $1 - O(q^{-1})$, we have

- $\delta_{i+1} - \delta_i = 1$ for $2 \le i \le |\mathcal{R}|$
- $\delta(D' \oplus D'') = \delta(D') + \delta(D'') - d$ where $d = \lceil g/2 \rceil$

Consequences:

- $\delta_i = g - 1 + i$ for $2 \le i \le |\mathcal{R}|$
- $|\mathcal{R}| = R - g$

Heuristics, Real Model

Notation: Baby step forward: $D \to D_+$
Baby step backwards: $D \to D_-$

Heuristics: with probability $1 - O(q^{-1})$, we have

- $\delta_{i+1} - \delta_i = 1$ for $2 \leq i \leq |\mathcal{R}|$
- $\delta(D' \oplus D'') = \delta(D') + \delta(D'') - d$ where $d = \lceil g/2 \rceil$

Consequences:

- $\delta_i = g - 1 + i$ for $2 \leq i \leq |\mathcal{R}|$
- $|\mathcal{R}| = R - g$
- If $D_i = (a_{i-1}, b_{i-1})$, then $\deg(a_{i-1}) = g$ for $2 \leq i \leq |\mathcal{R}|$

Heuristics, Real Model

Notation: Baby step forward: $D \to D_+$
Baby step backwards: $D \to D_-$

Heuristics: with probability $1 - O(q^{-1})$, we have

- $\delta_{i+1} - \delta_i = 1$ for $2 \leq i \leq |\mathcal{R}|$
- $\delta(D' \oplus D'') = \delta(D') + \delta(D'') - d$ where $d = \lceil g/2 \rceil$

Consequences:

- $\delta_i = g - 1 + i$ for $2 \leq i \leq |\mathcal{R}|$
- $|\mathcal{R}| = R - g$
- If $D_i = (a_{i-1}, b_{i-1})$, then $\deg(a_{i-1}) = g$ for $2 \leq i \leq |\mathcal{R}|$
- Relative distances known (computation no longer necessary)

Improvements, Real Model

Improvements, Real Model

Variable Base Scenario:

Improvements, Real Model

Variable Base Scenario:

- Eliminate all adjustment steps, at the expense of d baby steps at the beginning (independent of l)

Improvements, Real Model

Variable Base Scenario:

- Eliminate all adjustment steps, at the expense of d baby steps at the beginning (independent of l)

Fixed Base Scenario:

Improvements, Real Model

Variable Base Scenario:

- Eliminate all adjustment steps, at the expense of d baby steps at the beginning (independent of l)

Fixed Base Scenario:

- Replace all adds by baby steps

Improvements, Real Model

Variable Base Scenario:

- Eliminate all adjustment steps, at the expense of d baby steps at the beginning (independent of l)

Fixed Base Scenario:

- Replace all adds by baby steps
- Eliminate all adjustment steps, at the expense of the following pre-computation:

Improvements, Real Model

Variable Base Scenario:

- Eliminate all adjustment steps, at the expense of d baby steps at the beginning (independent of l)

Fixed Base Scenario:

- Replace all adds by baby steps
- Eliminate all adjustment steps, at the expense of the following pre-computation:
  - D_{d+3} with $\delta_{d+3} = d + g + 2 : d + 2$ baby steps

Improvements, Real Model

Variable Base Scenario:

- Eliminate all adjustment steps, at the expense of d baby steps at the beginning (independent of l)

Fixed Base Scenario:

- Replace all adds by baby steps
- Eliminate all adjustment steps, at the expense of the following pre-computation:
  - D_{d+3} with $\delta_{d+3} = d + g + 2$: $d + 2$ baby steps
  - D^* with $\delta(D^*) = 2^l(g + 1) + g$
    - l doubles with subsequent d adjustment baby steps, starting with D_2 : gets to distance $2^l(g + 1)$
    - g baby steps

Improvements, Variable Base

Improvements, Variable Base

Input: $D(\mathfrak{a}) \in \mathcal{R}$, $n = \sum b_i 2^{l-i}$ in NAF

Improvements, Variable Base

Input: $D(\mathfrak{a}) \in \mathcal{R}$, $n = \sum b_i 2^{l-i}$ in NAF

Output: The divisor $E \in \mathcal{R}$ of distance $n\delta(D(\mathfrak{a})) + d$

Improvements, Variable Base

Input: $D(\mathfrak{a}) \in \mathcal{R}$, $n = \sum b_i 2^{l-i}$ in NAF

Output: The divisor $E \in \mathcal{R}$ of distance $n\delta(D(\mathfrak{a})) + d$

1. For $i = 1$ to $d - 1$ do

   Replace D by D_+
2. Set $D' = D(\mathfrak{a}), \quad D'' = D(\mathfrak{a})_+, \quad E = D(\mathfrak{a})_+$
3. For $i = 1$ to l do

   // Double Replace E by $E \oplus E$;

   // Add If $b_i = 1$, replace E by $E \oplus D''$;

   If $b_i = -1$ and g is even. replace E by $E \oplus \overline{D''}$;

   If $b_i = -1$ and g is odd, replace E by $E \oplus \overline{D'}$;
4. Output E.

Improvements, Variable Base

Input: $D(\mathfrak{a}) \in \mathcal{R}$, $n = \sum b_i 2^{l-i}$ in NAF

Output: The divisor $E \in \mathcal{R}$ of distance $n\delta(D(\mathfrak{a})) + d$

1. For $i = 1$ to $d - 1$ do

   Replace D by D_+
2. Set $D' = D(\mathfrak{a}), \quad D'' = D(\mathfrak{a})_+, \quad E = D(\mathfrak{a})_+$
3. For $i = 1$ to l do

   // Double Replace E by $E \oplus E$;

   // Add If $b_i = 1$, replace E by $E \oplus D''$;

   If $b_i = -1$ and g is even. replace E by $E \oplus \overline{D''}$;

   If $b_i = -1$ and g is odd, replace E by $E \oplus \overline{D'}$;
4. Output E.

Expected no. of ops: l doubles, $l/3$ adds, d baby steps

Improvements, Fixed Base

Improvements, Fixed Base

Precomputation: D_{d+3}, D^*

Improvements, Fixed Base

Precomputation: D_{d+3}, D^*

Input: $n = \sum b_i 2^{l-i}$ in NAF

Improvements, Fixed Base

Precomputation: D_{d+3}, D^*

Input: $n = \sum b_i 2^{l-i}$ in NAF

Output: The divisor $E \in \mathcal{R}$ of distance n

Improvements, Fixed Base

Precomputation: D_{d+3}, D^*

Input: $n = \sum b_i 2^{l-i}$ in NAF

Output: The divisor $E \in \mathcal{R}$ of distance n

1. Set $E = D_{d+3}$;
2. For $i = 1$ to l do

   // Double Replace E by $E \oplus E$;

   // Baby Step If $b_i = 1$ then replace E by E_+;

   If $b_i = -1$ then replace E by E_-;

   // Now at distance $2^{l+1} + n + d$
3. Compute $D = E \oplus \overline{D^*}$;
4. Output D.

Improvements, Fixed Base

Precomputation: D_{d+3}, D^*

Input: $n = \sum b_i 2^{l-i}$ in NAF

Output: The divisor $E \in \mathcal{R}$ of distance n

1. Set $E = D_{d+3}$;
2. For $i = 1$ to l do

   // Double Replace E by $E \oplus E$;

   // Baby Step If $b_i = 1$ then replace E by E_+;

   If $b_i = -1$ then replace E by E_-;

   // Now at distance $2^{l+1} + n + d$
3. Compute $D = E \oplus \overline{D^*}$;
4. Output D.

Expected no. of ops: l doubles, one add, $l/3$ baby steps

Operation Count

Operation Count

Random base divisor:

Operation Count

Random base divisor:

	Doubles	Adds	Baby Steps
Imaginary	l	$l/3$	-
Real, Variable Base	l	$l/3$	d
Real, Fixed Base	l	1	$l/3$

Operation Count

Random base divisor:

	Doubles	Adds	Baby Steps
Imaginary	l	$l/3$	-
Real, Variable Base	l	$l/3$	d
Real, Fixed Base	l	1	$l/3$

Degenerate base divisor (point):

(Katagi, Kitamura, Akishita, Takagi 2005)

Operation Count

Random base divisor:

	Doubles	Adds	Baby Steps
Imaginary	l	$l/3$	-
Real, Variable Base	l	$l/3$	d
Real, Fixed Base	l	1	$l/3$

Degenerate base divisor (point):

(Katagi, Kitamura, Akishita, Takagi 2005)

	Doubles	Adds	Other
Imag, Fixed Base	l	-	$l/3$ point adds
Real, Fixed Base	l	1	$l/3$ baby steps

Naive Analysis

Naive Analysis

Simplifying Assumptions:

Naive Analysis

Simplifying Assumptions:

- Cost of baby steps is negligible compared to giant steps

Naive Analysis

Simplifying Assumptions:

- Cost of baby steps is negligible compared to giant steps
- Cost of giant steps is the same for both models

Naive Analysis

Simplifying Assumptions:

- Cost of baby steps is negligible compared to giant steps
- Cost of giant steps is the same for both models
- Random fixed base divisor, imaginary model

Naive Analysis

Simplifying Assumptions:

- Cost of baby steps is negligible compared to giant steps
- Cost of giant steps is the same for both models
- Random fixed base divisor, imaginary model

Analysis Under These Assumptions:

Naive Analysis

Simplifying Assumptions:

- Cost of baby steps is negligible compared to giant steps
- Cost of giant steps is the same for both models
- Random fixed base divisor, imaginary model

Analysis Under These Assumptions:

- Real model variable base scenario has the same speed as imaginary model

Naive Analysis

Simplifying Assumptions:

- Cost of baby steps is negligible compared to giant steps
- Cost of giant steps is the same for both models
- Random fixed base divisor, imaginary model

Analysis Under These Assumptions:

- Real model variable base scenario has the same speed as imaginary model
- Real model fixed base scenario is 25 percent faster than imaginary model (factor 3/4)

Naive Analysis

Simplifying Assumptions:

- Cost of baby steps is negligible compared to giant steps
- Cost of giant steps is the same for both models
- Random fixed base divisor, imaginary model

Analysis Under These Assumptions:

- Real model variable base scenario has the same speed as imaginary model
- Real model fixed base scenario is 25 percent faster than imaginary model (factor 3/4)
  - For example, Diffie-Hellman is 12.5 percent faster for the real model (factor 7/8)

Naive Analysis

Simplifying Assumptions:

- Cost of baby steps is negligible compared to giant steps
- Cost of giant steps is the same for both models
- Random fixed base divisor, imaginary model

Analysis Under These Assumptions:

- Real model variable base scenario has the same speed as imaginary model
- Real model fixed base scenario is 25 percent faster than imaginary model (factor 3/4)
  - For example, Diffie-Hellman is 12.5 percent faster for the real model (factor 7/8)
  - DSA signature generation is 25 percent faster for the real model (factor 3/4)

Naive Analysis

Simplifying Assumptions:

- Cost of baby steps is negligible compared to giant steps
- Cost of giant steps is the same for both models
- Random fixed base divisor, imaginary model

Analysis Under These Assumptions:

- Real model variable base scenario has the same speed as imaginary model
- Real model fixed base scenario is 25 percent faster than imaginary model (factor 3/4)
  - For example, Diffie-Hellman is 12.5 percent faster for the real model (factor 7/8)
  - DSA signature generation is 25 percent faster for the real model (factor 3/4)
  - IES decryption the same for both models

Numerical Data

Numerical Data

Implementation

- Pentium IV, 2.53 GHz, Linux, GNU C++, NTL

Numerical Data

Implementation

- Pentium IV, 2.53 GHz, Linux, GNU C++, NTL

Parameter Sizes

- $2 \leq g \leq 6$
- $q^{g/2}$ has 80, 112, 128, 192, 256 bits

Numerical Data

Implementation

- Pentium IV, 2.53 GHz, Linux, GNU C++, NTL

Parameter Sizes

- $2 \leq g \leq 6$
- $q^{g/2}$ has 80, 112, 128, 192, 256 bits

Arithmetic: Cantor's algorithm

Numerical Data

Implementation

- Pentium IV, 2.53 GHz, Linux, GNU C++, NTL

Parameter Sizes

- $2 \leq g \leq 6$
- $q^{g/2}$ has 80, 112, 128, 192, 256 bits

Arithmetic: Cantor's algorithm

Timings (Random Base Divisor)

	Real Var/Imag	*Real Fixed/Imag*
q prime	1.01 - 1.10	0.83 - 0.89
$q = 2^n$	1.01 - 1.22	0.78 - 0.84

Numerical Data

Implementation

- Pentium IV, 2.53 GHz, Linux, GNU C++, NTL

Parameter Sizes

- $2 \leq g \leq 6$
- $q^{g/2}$ has 80, 112, 128, 192, 256 bits

Arithmetic: Cantor's algorithm

Timings (Random Base Divisor)

	Real Var/Imag	*Real Fixed/Imag*
q prime	1.01 - 1.10	0.83 - 0.89
$q = 2^n$	1.01 - 1.22	0.78 - 0.84

Ratios more favourable toward real model for higher genus and higher security levels

Discrete Logarithm Problem

Discrete Logarithm Problem

Imaginary Model – Degree 0 Divisor Class Group DLP

Discrete Logarithm Problem

Imaginary Model – Degree 0 Divisor Class Group DLP

- Given a reduced divisor D and the reduced divisor in the divisor class of nD, find n

Discrete Logarithm Problem

Imaginary Model – Degree 0 Divisor Class Group DLP

- Given a reduced divisor D and the reduced divisor in the divisor class of nD, find n

Real Model – Infrastructure DLP

Discrete Logarithm Problem

Imaginary Model – Degree 0 Divisor Class Group DLP

- Given a reduced divisor D and the reduced divisor in the divisor class of nD, find n

Real Model – Infrastructure DLP

- Given a divisor $D \in \mathcal{R}$ and the divisor $E \in \mathcal{R}$ below $n\delta(D)$, find n

Discrete Logarithm Problem

Imaginary Model – Degree 0 Divisor Class Group DLP

- Given a reduced divisor D and the reduced divisor in the divisor class of nD, find n

Real Model – Infrastructure DLP

- Given a divisor $D \in \mathcal{R}$ and the divisor $E \in \mathcal{R}$ below $n\delta(D)$, find n
- Given n, find the divisor $E \in \mathcal{R}$ below n

Discrete Logarithm Problem

Imaginary Model – Degree 0 Divisor Class Group DLP

- Given a reduced divisor D and the reduced divisor in the divisor class of nD, find n

Real Model – Infrastructure DLP

- Given a divisor $D \in \mathcal{R}$ and the divisor $E \in \mathcal{R}$ below $n\delta(D)$, find n
- Given n, find the divisor $E \in \mathcal{R}$ below n
- Given a divisor $E \in \mathcal{R}$, find $\delta(E)$

Discrete Logarithm Problem

Imaginary Model – Degree 0 Divisor Class Group DLP

- Given a reduced divisor D and the reduced divisor in the divisor class of nD, find n

Real Model – Infrastructure DLP

- Given a divisor $D \in \mathcal{R}$ and the divisor $E \in \mathcal{R}$ below $n\delta(D)$, find n
- Given n, find the divisor $E \in \mathcal{R}$ below n
- Given a divisor $E \in \mathcal{R}$, find $\delta(E)$
- Given a reduced principal $\mathbb{F}_q[C]$-ideal $\mathfrak{a}$, find a generator of $\mathfrak{a}$ (*Principal Ideal Problem*)

Discrete Logarithm Problem

Imaginary Model – Degree 0 Divisor Class Group DLP

- Given a reduced divisor D and the reduced divisor in the divisor class of nD, find n

Real Model – Infrastructure DLP

- Given a divisor $D \in \mathcal{R}$ and the divisor $E \in \mathcal{R}$ below $n\delta(D)$, find n
- Given n, find the divisor $E \in \mathcal{R}$ below n
- Given a divisor $E \in \mathcal{R}$, find $\delta(E)$
- Given a reduced principal $\mathbb{F}_q[C]$-ideal $\mathfrak{a}$, find a generator of $\mathfrak{a}$ (*Principal Ideal Problem*)

Security of both scenarios seems to be the same

Present & Future Work

Present & Future Work

Idea: Exploit baby step operation (faster than giant steps)

Present & Future Work

Idea: Exploit baby step operation (faster than giant steps)

Work in Progress

Present & Future Work

Idea: Exploit baby step operation (faster than giant steps)

Work in Progress

- Exact operation count for NUCOMP, comparison with Cantor giant steps

Present & Future Work

Idea: Exploit baby step operation (faster than giant steps)

Work in Progress

- Exact operation count for NUCOMP, comparison with Cantor giant steps
- Explicit formulas for low genus giant steps, real model

Present & Future Work

Idea: Exploit baby step operation (faster than giant steps)

Work in Progress

- Exact operation count for NUCOMP, comparison with Cantor giant steps
- Explicit formulas for low genus giant steps, real model

Some Questions

Present & Future Work

Idea: Exploit baby step operation (faster than giant steps)

Work in Progress

- Exact operation count for NUCOMP, comparison with Cantor giant steps
- Explicit formulas for low genus giant steps, real model

Some Questions

- Can we use the baby step giant step framework to speed up infrastructure DLP? Or point counting?

Present & Future Work

Idea: Exploit baby step operation (faster than giant steps)

Work in Progress

- Exact operation count for NUCOMP, comparison with Cantor giant steps
- Explicit formulas for low genus giant steps, real model

Some Questions

- Can we use the baby step giant step framework to speed up infrastructure DLP? Or point counting? (Polynomial factor speed-up if any)

Present & Future Work

Idea: Exploit baby step operation (faster than giant steps)

Work in Progress

- Exact operation count for NUCOMP, comparison with Cantor giant steps
- Explicit formulas for low genus giant steps, real model

Some Questions

- Can we use the baby step giant step framework to speed up infrastructure DLP? Or point counting? (Polynomial factor speed-up if any)
- Can we convert the degree zero divisor class group DLP to the infrastructure DLP and vice versa?

Present & Future Work

Idea: Exploit baby step operation (faster than giant steps)

Work in Progress

- Exact operation count for NUCOMP, comparison with Cantor giant steps
- Explicit formulas for low genus giant steps, real model

Some Questions

- Can we use the baby step giant step framework to speed up infrastructure DLP? Or point counting? (Polynomial factor speed-up if any)
- Can we convert the degree zero divisor class group DLP to the infrastructure DLP and vice versa?
  - Easy to convert imaginary to real model over $\mathbb{F}_q$ and (if C has an $\mathbb{F}_q$-rational Weierstraß point) vice versa

Present & Future Work

Idea: Exploit baby step operation (faster than giant steps)

Work in Progress

- Exact operation count for NUCOMP, comparison with Cantor giant steps
- Explicit formulas for low genus giant steps, real model

Some Questions

- Can we use the baby step giant step framework to speed up infrastructure DLP? Or point counting? (Polynomial factor speed-up if any)
- Can we convert the degree zero divisor class group DLP to the infrastructure DLP and vice versa?
  - Easy to convert imaginary to real model over $\mathbb{F}_q$ and (if C has an $\mathbb{F}_q$-rational Weierstraß point) vice versa
  - Also convert divisor arithmetic (Paulus-Rück 1999)

* * * **The End !** * * *