Reduction Algorithm for Genus 3 non Hyperelliptic Curves

$$C : y^4 = p_3(x, z)$$

Maria Petkova
mpetkova@mathematik.hu-berlin.de
Department of Mathematics
Humboldt University
Berlin, Germany

Cryptographical Background

1. Discret Logarithm Problem
2. Jacobians of algebraic curves as groups suitable for cryptographic purposes

Explicit Representation of the Group Operation Principle

1. Find in each coset of $Jac(C) = Div^0(C)/P(C)$ an unique element: reduced divisor
   Reduction Algorithm

2. Define explicit an addition on the set of all reduced divisors
   Addition Algorithm

Non Hyperelliptic Curves of Genus 3

• The canonical map $\varphi : C \to \mathbb{P}^2$ is an injection
• $\varphi(C) \subset \mathbb{P}^2$ is a quartic
• Is $X \subset \mathbb{P}^2$ a quartic, then $X = \varphi(C)$ is a canonical curve of a non hyperelliptic curve of genus 3

Conjugate Points

$$C: y^4 = x^3 z + a_2 x^2 z^2 + a_1 x z^3 + a_0 z^4$$

$$\sigma : C \to C$$

$$(x : y : z) \mapsto (x : \varrho y : z)$$

ϱ - a primitiv fourth root of unity

$P_1, P_2 \in C(k)$ are conjugate Points, if

$$P_1 = \sigma^k(P_2), k = 1, 2, 3$$

Divisors on C

Reduced Divisor:

For each $D \in Div(C)$, $P_\infty \notin supp(D)$ there exists a *reduced Divisor* D' with

$$D - deg(D)P_\infty \sim D' - deg(D')P_\infty \quad and \quad deg(D') \leq g(C)$$

Reduction Algorithm - Idea

1. Every $D \in Div(C)$ is equivalent to a reduced divisor
2. Coordinate representation for $D \in Div(C)$
3. Geometric construction of the reduced divisor (Bézout theorem)

Coordinate Representation for $D \in Div(C)$

$$D = (u_D(x), q_D(x,y), w_D(y)), \quad with$$

$$u_D(x) := \prod_{P_i \in supp(D)} (x - x_i)$$

$$w_D(y) := \prod_{P_i \in supp(D)} (y - y_i) \quad and$$

$$q_D := a_{02}y^2 + a_{01}y + a_{11}xy + a_{10}x + a_{00},$$

the conic of maximal valuation at P_∞ and monic leading term

Typical Divisors

$$\cup_{\mathbf{i=2}}^{\mathbf{4}} \mathbf{Div}_{\mathbf{0}}^{+,\mathbf{i}}(\mathbf{C}) := \{ D \in Div^{+,i}(C);$$

$$D \in Div^{+,2}, D \neq (x_1, y_1) + (x_2, y_1),$$

$$D \in Div^{+,3}, D \neq (x_1, y_1) + (x_2, y_1) + (x_3, y_3),$$

$$with \quad y_1 \neq y_3$$

$$D \in Div^{+,4}, D \neq P_1 + P_2 + P_3 + P_4 \quad with$$

$$y_{P_1} = y_{P_2} = y_{P_3}, y_{P_1} \neq y_{P_2} \quad or$$

$$y_{P_1} = y_{P_2}, y_{P_3} = y_{P_4}, y_{P_1} \neq y_{P_2} \}$$

Bijection Theorem

Let $C/\bar{\mathbb{F}}_q$, then

$$\Phi : \cup_{i=2}^{4} D_0^{+,i}(C/\bar{\mathbb{F}}_q) \rightarrow \Phi(\cup_{i=2}^{4} D_0^{+,i}(C/\bar{\mathbb{F}}_q))$$

is a bijection.

Lemma: For $D \in \cup_{i=2}^{4} Div_0^{+,i}(C)$ always exists an unique conic q_D.

Reduction Algorithm

Problem: $D \in Div^+(C(k))$
Find: $D' \in Div^+(C(\bar{k}))$ with $D - deg(D)P_\infty \sim D' - deg(D')P_\infty$, $deg(D') \leq 3$

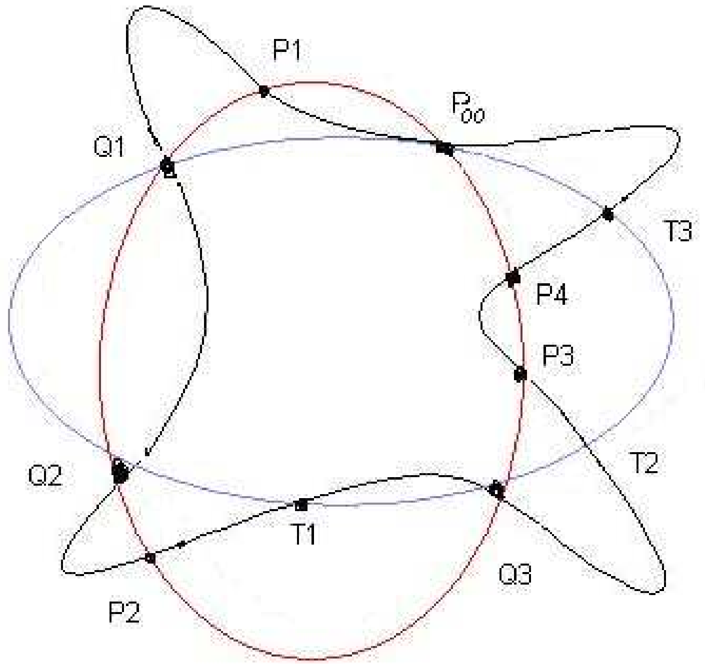

Figure 1: $D = P_1 + P_2 + P_3 + P_4, D_1 = Q_1 + Q_2 + Q_3, D_2 = T_1 + T_2 + T_3$

Reduction Algorithm

$$D = P_1 + P_2 + P_3 + P_4$$

1. D lies on a line $\Rightarrow D' - 4P_\infty \sim 0$
2. $\bullet$Determine the interpolating conic q_D of $D - 4P_\infty$
   Bézout theorem $\Rightarrow$ there exist at most 3 more points in $q_D \cap D$
   $(q_D) = P_1 + P_2 + P_3 + P_4 + Q_1 + Q_2 + Q_3 - 7P_\infty$
   $(q_D) = (D - 4P_\infty) + (D_1 - 3P_\infty)$
   $D_1 = Q_1 + Q_2 + Q_3$
   $D - 4P_\infty \sim -(D_1 - 3P_\infty)$
   $\bullet$ Determine the interpolating conic q_{D_1} of $D_1 + 2P_\infty$
   Construction of the inverse of $D_1 - 3P_\infty$
   $(q_{D_1}) = Q_1 + Q_2 + Q_3 + T_1 + T_2 + T_3 - 6P_\infty$
   $(q_{D_1}) = (D_1 - 3P_\infty) + (D_2 - 3P_\infty)$
   $D_1 - 3P_\infty \sim -(D_2 - 3P_\infty)$
   $D - 4P_\infty \sim D_2 - 3P_\infty$ - Reduction of D

Reduction Algorithm

$$D = D_0 + E_0 + E_1 + ... + E_{N-1}, deg(D) > 4$$

1. Reduce $D_0, deg(D_0) = 4$

   $D \sim D_2 + E_0 + E_1 + ... + E_{N-1}$

2. Constructe a sequence

   $D_0, D_1, D_2, ..., D_{3j}, D_{3j+1}, D_{3j+2}, ..., D_{3N}, D_{3N+1}, D_{3N+2}$

   • Each three $(D_{3j}, D_{3j+1}, D_{3j+2})$ correspond to a reduction step

   • $d_{3j} := D_{3(j-1)+2} + E_{(j-1)}, j = 1, ..., N$

   $D_{3j} - 4P_\infty \sim -(D_{3j+1} - deg(D_{3j-1})P_\infty) \sim$

   $D_{3j+2} - 3deg(D_{3j+2})P_\infty$

   $0 \leq deg(D_{3j+1}), deg(D_{3j+2}) \leq 3$

   $deg(D_{3j}) = 4, deg(E_{(j-1)}) = 4 - deg(D_{3j+2})$

   • $D - deg(D)P_\infty \sim D_{3N+2} - deg(D_{3N+2})P_\infty$ - reduction of D

   • $\bar{D}$ - coordinates of D

Theorem 1

Given $\bar{D}_{3j+1}$, then we can compute $\bar{D}_{3j+2}$:

$$
\begin{aligned}
q_{3j+2} &= q_{3j+1} \\
u_{3j+2} &= \left(\frac{R_y(q_{3j+1}, C)}{u_{3j+1}} \right)^* \\
w_{3j+2} &= \left(\frac{R_x(q_{3j+1}, C)}{w_{3j+1}} \right)^* .
\end{aligned}
$$

Theorem 2

Let $D \in Div^{+,4}$, then we can explicitely calculate the coordinates:

1. $\bar{D}_{3j}$, if $D \in Div_0^{+,4}$
   or
2. $\bar{D}_{3j+1}, \bar{D}_{3j+2}$, if $D \notin Div_0^{+,4}$.

Theorem 3

From the coordinates $\bar{D}_{3j} = (u_{3j}, q_{3j}, w_{3j})$, for $D_{3j} \in Div_0^{+,4}$ we can determine:

1. The coordinates $\bar{D}_{3j+1}, \bar{D}_{3j+2}$

   or

2. D_{3j+2}.

Theorem 4

Given $\bar{D}_{3j+1}, \bar{D}_{3j+2}$. First we compute E_j and then one of the following situations:

1. $D_{3(j+1)}$
   or
2. $\bar{D}_{3(j+1)}$.