Extended Cantor's Algorithm for Non-Singular Hyperelliptic curves to Singular Hyperelliptic curves

Haythem Ghani Ahmed

Software engineering Dept. Baghdad College of Economic Science University

Abstract

There are many applications for elliptic curves in cryptography.Cantor's algorithm relies on the Mumford representation of the points in jacobians. This compact representation of points in jacobians and Cantor's algorithm make non-singular hyperelliptic curves suitable for many applications in cryptography. This paper show the extension of cantor's representation for singular hyperelliptic curves.

Key words: Hyperelliptic curves, Jacobian, cantor's algorithm, Mumford representation

الخلاصة

يوجد استخدام واسع لموضوع المنحنيات البيضوية في التشفير. خوارزمية كانتور تعتمد على تمثيل ممفرود للنقاط في الجاكوبيان. هذا الترابط الشديد للنقاط يعمل على جعل المنحنيات البيضوية غير الاحادية مناسبة الاستخدام في كثير من التطبيقات لموضوع التشفير. في هذا البحث سوف نستعرض خوارزمية جديدة لتوسيع هذا الاستخدام ليشمل المنحنيات البيضوية الأحادية.

Introduction

Cantor's Algorithm gives an efficient way for computing in the Jacobian of a nonsingular hyperelliptic curve[3]. This algorithm relies on the Mumford Representation of points in Jacobian and Cantor's Algorithm make non-singular hyperelliptic curves suitable for many applications in cryptography. This paper show the extension of the Cantor's Algorithm for singular hyperelliptic curves. The algorithm that we present in section 3 mainly depends on this extension.

The use of non-singular hyperelliptic curves, especially lower genus ones, mainly depends on the hardness of the Discrete Logarithm Problem (DLP) on their Jacobians in a finite field [4]. The DLP in the Jacobian of a singular hyperelliptic curve is at most hard as the DLP in the multiplicative group of the finite field.

Background

Hyperelliptic curves:

Definition: A curve over a field k is a reduced Noetherian connected scheme of dimension, a complete irreducible curve x is called hyperelliptic if there is a morphisim

h: x → P_1 of degree 2 **[5] .**

Jacobian

Definition: Jac(x), of a hyperelliptic curve x is isomorphic to the identity component, the group Pic(x) which is the free abelian group of divisor classes of x modulo principle divisor **[1]** .

Cantor's algorithm[2]

This algorithm takes two divisor classes $D_1 = [u_1(x), v_1(x)]$ and $D_2 = [u_2(x), v_2(x)]$ on X and outputs the unique reduced divisor D such that $D = D_1 + D_2$. The algorithm can be clarified as shown below :-

1. **D=gcd(u_1,u_2,v_1+v_2)** With ***polynomials h_1,h_2,h_3*** such that $d = h_1 u_1 + h_2 u_2 + h_3(v_1 + v_2)$
2. $u = \frac{u_1 u_2}{d^2}$ *and* $v \equiv \frac{h_1 u_1 v_2 + h_2 u_2 v_1 + h_3(v_1 v_2 + f)}{d} \, mod(u)$
3. Repeat:
4. $\tilde{u} = \frac{v^2 - f}{u}$ $\quad and\ \tilde{v} \equiv v(mod\ \tilde{u})$
5. $u = \tilde{u}\ \ and\ v = \tilde{v}$

U*ntil* deg $(u) \leq g$

6. Multiply u by a constant to make u manic.

Mumford representation[5]

Let $P_i = (x_i, y_i)$ be a point on X. the map $w: X \rightarrow X, w(x_i, y_i) = (x_i, -y_i)$ is called the hyperelliptic involution. Let D be a divisor class in Jac (X). Then D can be written as $\sum_i n_i(P_i - \infty)$.

Let $D = \sum_i n_i(P_i - \infty)$ with $P_i = (x_i, y_i)$ be a divisor class in Jac (X). D is called a reduced divisor if it satisfies the following:

1. $n_i \geq 0 \ for\ all\ i$
2. If y_i=0 then n_i=0 or1
3. If P_i with $y_i \neq 0$ Occurs in the sum, then $[w(P_i)]$ does not occurs.
4. $\sum_i n_i \leq g$.

There is a unique reduced divisor D for each divisor class in Jac (X). The representation $\sum_i n_i(P_i - \infty)$ a divisor class is not concrete enough to perform group operations efficiently in Jac (X).

The Developed Algorithm

We show in this section that the above methods for non-singular hyperelliptic curves can be extended to singular hyperelliptic curves. The curve $X: \ y^2 = f(x)$ is singular if $f(x)$ has a multiple root ($\deg f(x) is\ still\ 2g + 1$). The curve $\acute{X}$ is is normalization of X. The singular points of X are of the form (a, 0) where (a) is a root of $f(x)$ with multiplicity greater than 1. Any divisor class D in Jac (X) has a unique representative $(u(x), v(x))$ satisfying the following:

1. $u(x)$ is a monic polynomial in $k[x]$
2. $\deg(v(x)) < \deg(u(x)) \ \leq g$

3. $v(x)^2 - f(x)$ is divisible by $u(x)$.
4. If $u(x)$ and $v(x)$ are multiples of $(x-a)$ for a singular point (a,0) then $\frac{f(x)-v(x)^2}{u(x)}$ is not a multiple of $(x-a)$.

Conclusion

This paper show that Cantor's Algorithm works for singular Hyperelliptic curves as the same way in the non-singular case.

References

1. A.Basiri, A. Enge, J-H. Faugere, N. Gurel," the Arithmetic of Jacobian groups of superelliptic curves", math. Comp, (74)2004 .
2. D.G.Cantor," computing in the Jacobian of a hyperelliptic curve", Math. Comp. 48 (1987).
3. D. Mumford," Tata Lectures on theta II, Birkhauser", 1982.
4. D. R. Kohel, "constructive and destructive facets of torus-based cryptography", preprint, available at http://echidna.maths.usyd.edu.au/kohel/index.html.
5. L. C. Washington," Elliptic curves: number theory and cryptography", 2nd edition, Chapman & Hall/ CRC 2008.