Decomposition Attack for the Jacobian of a Hyperelliptic Curve over an Extension Field

Koh-ichi Nagao (Kanto Gakuin Univ.)

Outline of this talk

1. Summary of Index calculus

1-1 An example of index calc. of $\mathbb{F}_p^*$

1-2 Some notations

1-3 Index cal. of Jacobian over a general finite field

2. Index cal. of Jacobian over an extension field

2-1 Elliptic curve case (Gaudry)

2-2 Improvement by using function field.

$\rightarrow$ hyperelliptic curve case

2-3 example

Index Calculus of $\mathbb{F}_p^*$

DLP: $a, b \in \mathbb{F}_p^* st. a^n = b$ => Find n

Factor base

$B_0 = \{-1, 2, 3, 5, 7..., p_n\}$

Collect more than $|B_0| + 1$ number of $a^i b^j \in< B_0 >$

$\rightarrow$

Solve around $|B_0| \times |B_0|$ lin. alg. mod. $|\mathbb{F}_p^*|$

Example

$p = 179$, $a = 23$, $b = a^{23} = 111$, $B_0 = \{2, 3\}$

Collect relations

$$\begin{cases} a^1 \cdot b^{20} = 96 = 2^5 3^1 \\ a^2 \cdot b^{16} = 12 = 2^2 3^1 \\ a^3 \cdot b^{17} = 27 = 2^0 3^3 \end{cases}$$

Solving lin. alg. mod $p - 1$

$$\left[\begin{array}{cc|cc} 1 & 20 & 5 & 1 \\ 2 & 16 & 2 & 1 \\ 3 & 17 & 0 & 3 \end{array}\right]$$

$$\left[\begin{array}{cc|cc} 3 & 60 & 15 & 3 \\ 6 & 48 & 6 & 3 \\ 3 & 17 & 0 & 3 \end{array}\right]$$

$$\left[\begin{array}{cc|cc} 0 & 43 & 15 & 0 \\ 3 & 31 & 6 & 0 \\ 3 & 17 & 0 & 3 \end{array}\right]$$

$$\left[\begin{array}{cc|cc} 0 & 86 & 30 & 0 \\ 15 & 155 & 30 & 0 \end{array}\right]$$

$$\left[\begin{array}{cc|cc} 15 & 69 & 0 & 0 \end{array}\right] \times -1/69 \bmod 178$$

$$\left[\begin{array}{cc|cc} 23 & -1 & 0 & 0 \end{array}\right]$$

So we have $a^{23} \cdot b^{-1} = 1 \bmod 178$

Large prime variations of $\mathbb{F}_p^*$

Factor base and Large prime

$B = \{-1, 2, 3, 5, 7..., p_N\}$, $B_0 \subset B$

Large primes: $B \backslash B_0$

Collect enough number of $a^i b^j \in < B >$

$\rightarrow$ eliminate the terms of $B \backslash B_0$

$\rightarrow$ Solve around $|B_0| \times |B_0|$ lin. alg. mod. $|\mathbb{F}_p^*|$

Index calc. of group 1

G (Additive) Group, Solve DLP i.e.

$a, b \in G$ s.t. $n \cdot a = b$ $=>$ Find $n \in \mathbb{Z}/|G|\mathbb{Z}$

Factor base $\cup$ Large prime $B(\subset G)$(subset)

Factor base $B_0(\subset B)$ (subset)

Large prime $B \backslash B_0$

Further, we will assume

Assumption of Decomposition

$\exists N$ fix

For $g \in G$

$g = g_1 + g_2 + ... + g_N$ for $g_i \in B$

$O(1)$ probability

$O(1)$ cost (seeking g_i's)

Index calc. of group 2

Normal Index Calc.

The case $B = B_0$

Collect more than $|B| + 1$ number of

$i \cdot a + j \cdot b \in < B >$

$\rightarrow$ Solve around $|B| \times |B|$ lin. alg. mod. $|G|$

Note the cost of lin.alg. is dominant.

Large Prime method

Collect enough number of

$i \cdot a + j \cdot b \in < B >$

$\rightarrow$ Eliminate Large primes and

$\rightarrow$ Solve around $|B_0| \times |B_0|$ lin. alg. mod. $|G|$

Index calc. of Jacobian (over general finite field)

$C/\mathbb{F}_q$ curve genus g, $G = Jac_c(\mathbb{F}_q)$, solve DLP

1) Gaudry

$B = B_0 = C(\mathbb{F}_q) = \{P - \infty | P \in C(\mathbb{F}_q)\}$

=> it works well. Cost $O(q^{2+\epsilon})$.

2) Revalance (Gaudry,Harley)

Take $B_0 \subset B$(subset, only size is optimized).

Cost $O(q^{(4g-2)/(2g+1)+\epsilon})$.

3) Using Large prime Elimination (Thériault, Nagao,Gaudry,Thomé, Diem) Cost $O(q^{(2g-2)/g+\epsilon})$.

Index calc. of Jac. over extension field 1

$C/\mathbb{F}_{q^n}$ curve genus g, $G = Jac_C(\mathbb{F}_{q^n})$, solve DLP

1) Gaudry

The case of Elliptic curve($g = 1$)

$E/\mathbb{F}_{q^n}$ elliptic curve, $G = E(\mathbb{F}_{q^n})$,

$B = \{(x, y) \in E(\mathbb{F}_{q^n}) | x \in \mathbb{F}_q\}$

Index calc. works well(using Semaev's formula).

Semaev's formula

Given $(x, y) \in E(\overline{\mathbb{F}}_{p^n})$, $x_1, ..., x_n \in \overline{\mathbb{F}}_{p^n}$

$\exists \phi(X, X_1, .., X_n) \in \mathbb{F}_{p^n}[X, X_1, ..., X_n]$, $\deg \phi = 2^{n-1}$, s.t.

$\phi(x, x_1, ...x_n) = 0 \leftrightarrow$

$(x, y) + (x_1, y_1) + ... + (x_n, y_n) = 0$ for some

$(x_i, y_i) \in E(\overline{\mathbb{F}}_{p^n})$

Index calc. of Jac. over extension field 2

Recall

$G = E(\mathbb{F}_{q^n})$ $B = \{(x, y) \in E(\mathbb{F}_{q^n}) | x \in \mathbb{F}_q\}$

Given $(x, y) \in G$,

Condition $\exists (x_i, y_i) \in B (i = 1, .., n)$

$(x, y) + (x_1, y_1) + .. + (x_n, y_n) = 0$ induces

$\phi(x, X_1, .., X_n) = 0$ has some solutions $(X_1, ..., X_n) = (x_1, ..., x_n) \in \mathbb{A}^n(\mathbb{F}_p)$.

Prob.of (x, y) being written by this form $= 1/n!(= O(1))$.

Index calc.of Jac. over extension field 3

Remark that $x \in \mathbb{F}_{q^n}$ being the x-coor. of a fixed pt. of $E(\mathbb{F}_{q^n})$.

Fix $[\alpha_1, .., \alpha_n]$ base of $\mathbb{F}_{q^n}/\mathbb{F}_q$.

$\phi(x, X_1, .., X_n) \in \mathbb{F}_{q^n}[X_1, ..., X_n]$ is written by

$\phi(x, X_1, .., X_n) = \sum_{i=1}^{n} \alpha_i \phi_i(X_1, ..., X_n)$

for some $\phi_{x,i}(X_1, ..., X_n) \in \mathbb{F}_q[X_1, ..., X_n]$

$\phi(x, X_1, .., X_n) = 0$ has some solutions $(X_1, , , X_n) = (x_1, ..., x_n) \in \mathbb{A}^n(\mathbb{F}_q)$ is equiv. to solving eq.system

$\phi_{x,i}(X_1, ..., X_n) = 0, /\mathbb{F}_q \qquad (i = 1, ..., n)$

Find x_i

$\rightarrow$ Solve degree 2^{n-1}, n variables,n equations equations system over $\mathbb{F}_q$

$n, g = 1$ small, $q \rightarrow \infty$, Cost $O(q^{(2ng-2)/ng+\epsilon})$.

Improvement of the algorithm 1(Notation)
$C/\mathbb{F}_{q^n}$ Hyperelliptic curve genus g(odd degree)
$ch(\mathbb{F}_q) \neq 2$, ∞ unique point at infinfity,
$G = Jac_c(\mathbb{F}_{q^n})$, solve DLP
$B = \{(x, y) - \infty | (x, y) \in C(\mathbb{F}_{q^n}), x \in \mathbb{F}_q\}$ or
$B = \{(x, y) | (x, y) \in C(\mathbb{F}_{q^n}), x \in \mathbb{F}_q\}$
(Note. In Ell. cur. case,the same as Gaudry's)
idea: Semaev's formula $\rightarrow$ function field
it also works well in Hyperell case.

D_0:Fixed reduced divisor
$D_0 = (\phi_1(x), \phi_2(x))$ mumford rep.
$\quad = Q_1 + Q_2 + ... + Q_g - (g)\infty$

Definition D_0 decomposed $\leftrightarrow$
$D_0 + P_1 + P_2 + ... + P_{ng} - (ng)\infty \sim 0$ for some
$P_i \in B$
Pob. of D_0 being decomposed $= 1/(ng)!$
$\{P_i\}$ being called decomposed factor

Improvement of the algorithm 2

The case $g = 3$, $n = 2$ part 1

Explain the construction of Eq. sys. of above case

HEC $C : y^2 = f(x)/\mathbb{F}_{q^2}, \quad f(x) = x^7 + ... + a_0$

Fix reduced divisor $D_0 \in Jac(C/\mathbb{F}_{q^2})$

1)Mumford rep. $D_0 = (\phi_1(x), \phi_2(x))$ s.t.

$\phi_1, \phi_2 \in \mathbb{F}_{q^2}[x], \phi_1$monic, $3 \geq \deg \phi_1 > \phi_2$,

$\phi_2^2 - f(x) \equiv 0 \bmod \phi_1$

2)Representation using points

$\exists Q_1, Q_2, Q_3 \in C(\bar{\mathbb{F}_q})$ s.t.

$D_0 = Q_1 + Q_2 + Q_3 - 3\infty$

D:divisor, $L(D) := \{h \in C(\bar{\mathbb{F}_{q^2}}) | (h) + D \geq 0\}$

Theorem(Riemann Roch)$L(D)$vector space

$\deg D \geq 2g - 1 \to \mathbf{dim} L(D) = \deg D - g + 1$

Improvement of the algorithm 3

The case $g = 3$, $n = 2$ part 2

Here, reduded divisor D_0 is fixed

Put $D = 6\infty - D_0 = 9\infty - (Q_1 + Q_2 + Q_3)$.

Then $\{\phi_1(x), \phi_1(x)x, (y - \phi_2(x)), (y - \phi_2(x))x\}$

is a base of $L(D)$.

When D_0 is decomposed, the points $\{P_i\}$ of the form

$$D_0+P_1+...+P_6-6\infty = Q_1+...+Q_3+P_1+...+P_6-9\infty \sim 0$$

are the zeros of some elements of $L(D)$

Note. $h \in L(D), \mathrm{ord}_\infty h = 9$

$\rightarrow h$ has term of $(y - \phi_2(x))x$

Put $h(x, y) := (A_0+A_1x)\phi_1(x)+(B_0+1)(y-\phi_2(x))$.

where A_0, A_1, B_0 are the parameter moving $\mathbb{F}_{q^2}$.

Seeking cross pts of $h(x, y) = 0$ on C.

Improvement of the algorithm 4

The case $g = 3$, $n = 2$ part 3

Recall $C : y^2 = x^7 + ... + a_0$

$$h(x, y) = 0 \to y = \frac{(A_0 + A_1 x)\phi_1(x) - (B_0 + 1)\phi_2(x)}{B_0 + x}.$$

Put

$$p(x) := (x+B_0)^2(x^7+...)-((A_0+A_1 x)\phi_1(x)-(B_0+1)\phi_2(x))^2.$$

Roots of $p(x) = 0$ are x-cor. of $Q_1, ..., Q_3, P_1, ..., P_6$

Put $g(x) := p(x)/\phi_1(x) = x^6 + C_5 x^5 + ... + C_0$.

Then

1)Roots of $g(x) = 0$ are x-cor. of $P_1, ..., P_6$

2)Considering parameters as variable,

$C_0, .., C_5 \in \mathbb{F}_{q^2}[A_0, A_1, B_0]$, $\deg C_i = 2$

3)D_0 decomposed $\to \forall x(P_i) \in \mathbb{F}_q$

$\to \exists a_0, a_1, b_0 \in \mathbb{F}_{q^2} s.t. C_i(a_0, a_1, b_0) \in \mathbb{F}_q$.

Further, we seek the condition

$C_i(a_0, a_1, b_0) \in \mathbb{F}_q \, (i = 0, ..., 5)$

Improvement of the algorithm 5

The case $g = 3$, $n = 2$ part 4

Fix $[1, \alpha]$ base of $\mathbb{F}_{q^2}/\mathbb{F}_q$

Put new parameters $A_{0,0}, A_{0,1}, A_{1,0}, A_{1,1}, B_{0,0}, B_{0,1}$ moves in $\mathbb{F}_q$ s.t.

$A_0 = A_{0,0} + A_{0,1}\alpha$

$A_1 = A_{1,0} + A_{1,1}\alpha$

$B_0 = B_{0,0} + B_{0,1}\alpha$

Then C_i are considerd in $\mathbb{F}_{q^2}[A_{0,0}, A_{0,1}, ..., B_{0,1}]$

Put $C_{i,j} \in \mathbb{F}_q[A_{0,0}, A_{0,1}, A_{1,0}, A_{1,1}, B_{0,0}, B_{0,1}]$ by

$C_i = C_{i,0} + C_{i,1}\alpha \ (i = 0, 1, ..., 5, j = 0, 1)$

Then $\deg C_{i,0} = \deg C_{i,1} = 2$

The cond. values $C_i \in \mathbb{F}_q, i = 0, 1, .., 5$

$\rightarrow C_{i,1} = 0$ for $i = 0, 1, .., 5.$

Improvement of the algorithm 6

The case $g = 3$, $n = 2$ part 5

1)The cond. $C_i(a_0, ..) = 0 \in \mathbb{F}_q$ reduces to Eqs. sys. $\{C_{i,1} = 0/\mathbb{F}_q | i = 0, 1, .., 5\}$ (degree 2, 6 vars, 6 eqs)

Let $\vec{v} = (a_{00}, a_{01}, a_{1,0}, a_{11}, b_{00}, b_{11}) \in \mathbb{A}^6(\mathbb{F}_q)$ be a sol. of Eqs. sys..
Put $c_i := C_{i,0}(\vec{v})$ and $g(x)$ is written by $g(x) = x^6 + c_5 x^5 + ... + c_0$

2)Then $x^6 + c_5 x^5 + ... + c_0$ factors completely in $\mathbb{F}_q[x]$ is equiv to $x(P_1), ..., x(P_6) \in \mathbb{F}_q$

Note. Dominant part is 1) and the computation of "Seeking decomposed factos" reduces to "Solving Eqs. Sys."

Improvement of the algorithm 7(general case)
Recall $C/\mathbb{F}_{p^n}$ HyperEll. of genus g, $D_0 \in \mathrm{Jac}_c(\mathbb{F}_{p^n})$fixed
Theorem Let $V_1, V_2, ..., V_{(n^2-n)g}$ be variables and let D_0 be a reduced divisor of $C/\mathbb{F}_{q^n}$. Then there are some degree 2 polynomials
$C_{i,j} \in \mathbb{F}_q[V_1, V_2, ..., V_{(n^2-n)g}]$ $(0 \leq i \leq ng - 1,\ 0 \leq j \leq n-1)$
satisfying the following.

The condition that D_0 is decomposed is equivalent to the following 1) and 2).
1) The equations system $S = \{C_{i,j} = 0 \,|\, 0 \leq i \leq ng-1, 1 \leq j \leq n-1\}$ has some solution $\vec{v} = (v_1, .., v_{(n^2-n)g}) \in \mathbb{A}^{(n^2-n)g}(\mathbb{F}_q)$.
2) Put $c_i = C_{i,0}(v_1, .., v_{(n^2-n)g})$ for $0 \leq i \leq ng-1$. Then $G(x) = x^{ng} + c_{ng-1}x^{ng-1} + ... + c_0 \in \mathbb{F}_q[x]$ factors completely.
Moreover, if D_0 is decomposed, the x-coordinates of the decomposed factor are the solution of $G(x) = 0$

Improvement of the algorithm 7(conclusion)
Seeking decompsed factor
$\rightarrow$ Solving degree2, $(n^2 - n)g$ vars, eqs, equations system over $\mathbb{F}_q$ (we assume the cost is in $O(1)$,since n, g are small and fixed.)

Note. In Ell. cur. case, the cost of computing decomposed factor is as same as Gaudry's method

Note. Total cost of solving DLP is $O(q^{(2ng-2)/ng+\epsilon})$

Example We can compute the decomposed factor in three cases
1) $(g,n)=(1,3)$, 2) $(g,n)=(2,2)$, 3) $(g,n)=(3,2)$

Show an example of the case of $(g,n)=(3,2)$

Let $q=1073741789$(prime number),
$\mathbb{F}_{q^2} := \mathbb{F}_q[t]/(t^2+746495860*t+206240189)$,

$C/\mathbb{F}_{q^2} : y^2 = x^7+(111912375*t+1046743132)*x+6*t+9$

and

$D_0 := (x^2+1073741787*t*x+327245929*t+867501600,$

$(473621736*t+256126568)*x+145989647*t+687383736) \in Jac(C)$

(Mumford representation).
We investigate whether $nD_0 : n=1,2,..3000$ are decomposed and find the following 6 decompositions.

$$414D_0 \sim (1001437837, 752632260{*}t{+}700158497){+}(747112084, 656073918{*}t{+}400137619)$$

$$+(620249588, 127943213{*}t{+}635474623){+}(614180498, 206297635{*}t{+}445250468)$$

$$+(515769009, 607297126{*}t{+}554290493){+}(488549466, 627952783{*}t{+}854182612){-}6\infty$$

$$657D_0 \sim (939617127, 695261735{*}t{+}239531611){+}(933351280, 935312661{*}t{+}961494096)$$

$$+(799612924, 341923983{*}t{+}677495100){+}(294787599, 279723229{*}t{+}760003067)$$

$$+(273118782053704103{*}t{+}577497766){+}(153381525, 983211238{*}t{+}517037777){-}6\infty$$

$$921D_0 \sim (1034634787, 400751409{*}t{+}829801342){+}(763888873, 757155774{*}t{+}829936954)$$

$$+(619620874, 800641683{*}t{+}200272230){+}(603032615, 115219564{*}t{+}655011145)$$

$$+(436423191, 285214454{*}t{+}450812747){+}(125198811, 884750621{*}t{+}123305741){-}6\infty$$

$$1026D_0 \sim (1024020017, 267457905{*}t{+}41452942){+}(794174628, 615676821{*}t{+}723336407)$$

$$+(738567269, 433647609{*}t{+}128304659){+}(629287731, 465842490{*}t{+}789390318)$$

$$+(435082408, 878213106{*}t{+}603353206){+}(79621979, 479459622{*}t{+}672937516){-}6\infty$$

Conclusion

We have proposed an algorithm which checks whether a reduced divisor is decomposed or not, and we have computed the decomposed factors, if it is decomposed. From this algorithm, concrete computations of decomposed factors are done by computer experiments when the pairs of the genus of the hyperelliptic curve and the degree of extension field are $(1,3), (2,2)$, and $(3,2)$.

Acknowledgment

The author would like to thank the program committee that gives me a chance to talk and anonymous reviewers who pointed out many mistakes and suggested a revisal plan.