拡大体上定義された超楕円曲線のヤコビアン群のindex calclusについて

長尾孝一（関東学院大学）

Index Calculus of $\mathbb{F}_p$

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

Smooth elements

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

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

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

Potentially smooth elements

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

Large primes: $B_0 \backslash B$

Collect enough number of $a^i b^j \in < B_0 >$

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

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

Index calc. of group

G Group, Solve DLP i.e.
$a, b \in G$ s.t. $a^n = b$ $=>$ Find n

Potentially Smooth element $B_0 (\subset G)$(subset)
Smooth elements $B (\subset B_0)$ (subset)

Assumption of Decomposition
$\exists N$ fix
For $g \in G$
$g = g_1 g_2 .... g_N$ for $g_i \in B_0$
(or $g = g_1 + g_2 + ... + g_N$ for $g_i \in B_0$ add. gr.case)
$O(1)$ probability
$O(1)$ cost (seeking g_i's)

Normal Index Calc.

The case $B = B_0$

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

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

Note the cost of lin.alg. is dominant.

Revalanced method

The case $B \not\subset B_0$

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

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

Large Prime method

Collect enough number of $a^i b^j p_1 p_2 \in < B >$

$p_1, p_2 \in B_0 \backslash B$

$\rightarrow$ Eliminate Large primes and

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

Index calc. of Jacobian

$C/\mathbb{F}_q$ 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 $B \subset B_0$(subset, 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 Jacobian over extension field

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

1) Gaudry (previous research)

$\exists$ some representation $G = \{(x_1, x_2, ..)|x_i \in \mathbb{F}_{q^n}\}$

$B_0 = \{(x_1, x_2, ..)|x_1, x_2, .., x_g \in \mathbb{F}_q\}$

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

$G = E(\mathbb{F}_{q^n})$ $B_0 = \{(x, y) \in E(\mathbb{F}_{q^n})|x \in \mathbb{F}_q\}$

Given $(X, Y) \in G$

Check $(X, Y) = (x_1, y_1)+...+(x_n, y_n)$ for $(x_i, y_i) \in B_0$

Prob.$= 1/n!(= O(1))$

Eliminate $y_1, y_2, ...y_n$(Semaev's formula)

Find x_i

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

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

Index calc. of Jacobian over extension field

$C/\mathbb{F}_{q^n}$ 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

$B_0 = \{(x,y) - \infty | (x,y) \in C(\mathbb{F}_{q^n}), x \in \mathbb{F}_q\}$ or

$B_0 = \{(x,y) | (x,y) \in C(\mathbb{F}_{q^n}), x \in \mathbb{F}_q\}$

(Note. In Ell. cur. case,the same as Gaudry's)

D_0:Reduced divisor

$D_0 = (\phi_1(x), \phi_2(x))$ mumford rep.

$= Q_1 + Q_2 + ... + Q_g - (g)\infty$

Definition D_0 decomposed $\leftrightarrow$

$D_0 + P_1 + P_2 + ... + P_{ng} - (ng)\infty \sim 0$ for some

$P_i \in B_0$

Pob. of D_0 is decomposed $= 1/(ng)!$

$\{P_i\}$ decomposed factor

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

$$C_{i,j} \in \mathbb{F}_q[V_1, V_2, ..., V_{(n^2-n)g}] \quad (0 \leq i \leq ng-1,\ 0 \leq j \leq n-1)$$

satisfying the following.

The condition that D_0 is potentially B_0-smooth 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 potentially B_0-smooth, the x-coordinates of the decomposed factor are the solution of $G(x) = 0$

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 $O(q^{(2ng-2)/ng+\epsilon})$

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

Explain the construction of Eq. sys. of above case

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

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, $3 \geq \deg \phi_1 \geq \phi_2$,

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

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

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

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 $L(D)$.

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 $h(x, y) := (A_0 + A_1 x)\phi_1(x) + (B_0 + 1)(y - \phi_2(x))$.

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.

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

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

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

Put

$$p(x) := (x+B_0)^2(x^7+...)-((A_0+A_1x)\phi_1(x)-(B_0+1)\phi_2(x))^2.$$

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

Put $g(x) := p(x)/\phi_1(x) = x^6 + C_5x^5 + ... + C_0$.

Then

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

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

D_0 decomposed $\rightarrow \forall x(P_i) \in \mathbb{F}_q \rightarrow g(x) \in \mathbb{F}_q[x]$.

Seeking the condition $g(x) \in \mathbb{F}_q[x]$

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. $g(x) \in \mathbb{F}_q[x]$

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

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

1)The cond. $g(x) \in \mathbb{F}_q[x]$ 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."

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.

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

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

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

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

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

$$+(2731187820537041 03*t+577497766)+(153381525, 983211238*t+517037777)-6\infty$$

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

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

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

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

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

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

- Preprint
  http://eprint.iacr.org/2007/112.pdf